ISLAMIC UNIVERSITY JOURNAL OF SOCIAL SCIENCES VOL 5, NO 4

ISSN: 2709-2429(Print), 2709-2437(Online)-Published 31st July 2026

Cyber Intelligence And Hybrid Warfare In Middle Eastern Security Conflicts: The Iran–Israel Shadow War

by

Okwuokei Vivian Chekube, Vincent Eseoghene Efebeh, Francis Ayegbunam Ikenga

Department of Political Science, Faculty of the Social Science,

Delta State University, Abraka, Nigeria

Email: vivianokwuokei@gmail.com

Abstract

This study examined the role of cyber intelligence and hybrid warfare in Middle Eastern security conflicts, with particular emphasis on the Iran–Israel shadow war between 2010 and 2025. The study explored the evolving dynamics of the conflict, the influence of cyber intelligence operations on strategic decision-making, the role of proxy actors in advancing national interests, the impact of emerging technologies on warfare, and the broader implications for regional and global security. A qualitative research design was adopted to provide a comprehensive understanding of the complex and multidimensional nature of the conflict. Data were collected from secondary sources, including peer-reviewed journal articles, scholarly books, policy documents, intelligence reports, and credible open-source materials. Content analysis was employed as the method of data analysis to systematically identify, categorize, and interpret recurring themes and patterns within the data. The findings revealed that the Iran–Israel rivalry has evolved into a sustained hybrid conflict characterized by the integration of cyber operations, intelligence activities, proxy warfare, and technological innovation. Cyber intelligence emerged as a critical tool for espionage, surveillance, deterrence, and strategic disruption, while proxy actors served as important instruments of indirect power projection and regional influence. The study further found that advances in artificial intelligence, cyber surveillance, and autonomous systems have transformed the conduct of modern warfare by enhancing intelligence capabilities, operational efficiency, and targeting precision. The study concluded that the increasing normalization of cyber warfare and proxy conflict poses significant challenges to regional stability, international security, and global cyber governance, highlighting the need for stronger regulatory frameworks and cooperative mechanisms for managing emerging security threats.

Keywords: Cyber Intelligence, Hybrid Warfare, Iran–Israel Shadow War, Proxy Warfare, Middle East Security.

Introduction

The contemporary security environment has undergone a significant transformation due to the rapid advancement of information technologies, cyber capabilities, and the increasing adoption of hybrid warfare strategies by state and non-state actors. Traditional military confrontations are increasingly being supplemented or replaced by cyber operations, intelligence-driven activities, disinformation campaigns, and proxy warfare, creating new dimensions of conflict that challenge conventional security frameworks (Hoffman, 2007; Rid, 2020). Within this evolving landscape, the Middle East has emerged as one of the most significant arenas where cyber intelligence and hybrid warfare intersect, particularly in the long-standing rivalry between Iran and Israel.

The Iran–Israel conflict represents one of the most complex and enduring security confrontations in the contemporary international system. Although the two states have not engaged in a direct conventional war, they have continuously confronted each other through covert operations, cyberattacks, intelligence activities, and support for proxy groups across the region (Byman, 2018; Eisenstadt, 2016). This form of indirect confrontation, often described as a "shadow war," has enabled both actors to pursue strategic objectives while avoiding the political and military costs associated with open warfare. The conflict has evolved beyond traditional military competition to encompass cyberspace, where intelligence gathering, digital espionage, and cyber sabotage have become essential instruments of national security strategy (Singer & Friedman, 2014).

Cyber intelligence has emerged as a critical component of modern statecraft and national security. It involves the collection, analysis, and utilization of digital information to monitor threats, conduct surveillance, and support military and political decision-making (Libicki, 2009). In the Iran–Israel rivalry, cyber intelligence has been employed to target critical infrastructure, disrupt strategic assets, and gain information superiority. The 2010 Stuxnet operation, widely regarded as one of the most sophisticated cyberattacks in history, demonstrated how cyber capabilities could be used to achieve strategic objectives without direct military engagement (Langner, 2011). Since then, both Iran and Israel have expanded their cyber capabilities, transforming cyberspace into a persistent domain of competition and conflict.

Closely linked to cyber intelligence is the concept of hybrid warfare, which refers to the coordinated use of conventional and unconventional methods, including cyber operations, information warfare, economic pressure, and proxy actors, to achieve political and strategic objectives (Hoffman, 2007). Hybrid warfare blurs the distinction between war and peace, military and civilian targets, and state and non-state actors. In the Middle East, hybrid warfare has become increasingly prominent as states seek to project influence while maintaining plausible deniability. Iran has relied extensively on proxy organizations such as Hezbollah, Hamas, and various militia groups in Iraq and Syria to extend its regional influence, while Israel has responded through intelligence operations, targeted military strikes, and cyber campaigns aimed at disrupting these networks (Nasr, 2020; Norton, 2018).

The integration of cyber intelligence into hybrid warfare strategies has significantly altered the nature of security conflicts in the Middle East. Technological innovations such as artificial intelligence, big data analytics, cyber surveillance systems, and autonomous technologies have enhanced states' ability to collect intelligence, identify threats, and conduct precision operations (Horowitz, 2018; Scharre, 2018). These developments have increased the speed and complexity of conflict while simultaneously creating new vulnerabilities in critical infrastructure and communication systems. Consequently, security competition between Iran and Israel has expanded beyond physical battlefields to include digital networks, information ecosystems, and transnational proxy structures.

Furthermore, the Iran–Israel shadow war has broader implications for regional and global security. The proliferation of cyber capabilities and hybrid warfare tactics has challenged existing international legal frameworks governing conflict and state behavior in cyberspace (Nye, 2017). Attribution difficulties, the absence of universally accepted cyber norms, and the

increasing involvement of non-state actors complicate efforts to maintain stability and accountability. As cyber operations become more sophisticated and integrated into national security strategies, the Iran–Israel confrontation serves as an important case for understanding the evolving nature of modern warfare and the future of international security governance.

Against this background, this study examines the role of cyber intelligence and hybrid warfare in Middle Eastern security conflicts, with particular emphasis on the Iran–Israel shadow war. The study seeks to explore how cyber intelligence operations, proxy networks, and emerging technologies have shaped the dynamics of the conflict and influenced regional security outcomes. By analyzing the interaction between cyber capabilities and hybrid warfare strategies, the study contributes to a deeper understanding of contemporary security challenges and the changing character of conflict in the twenty-first century.

Literature Review

Shadow War

The concept of Shadow War has evolved to describe a form of covert confrontation between states that employ indirect, deniable, and multifaceted strategies to pursue strategic objectives without engaging in open warfare. It represents a continuum of conflict characterized by clandestine operations, cyber offensives, assassinations, disinformation campaigns, and the use of proxies to achieve political or military goals beneath the threshold of formal war. According to Foster (2022), shadow wars signify the new architecture of global conflict in which the line between peace and war is deliberately blurred through strategic ambiguity. In the context of the Middle East, particularly between Iran and Israel, the shadow war manifests as a persistent struggle involving intelligence operations, covert sabotage, and digital espionage designed to maintain strategic balance without provoking international condemnation. Morris (2023) asserts that shadow wars redefine the notion of deterrence by substituting overt military aggression with technological and intelligence-based confrontation. Likewise, Khalid and Renner (2024) emphasize that the Iran–Israel shadow conflict demonstrates how cyber power and proxy militias have replaced conventional battlegrounds, illustrating the transition of warfare into invisible, low-intensity domains. As a result, the concept of shadow war encapsulates the evolving reality of twenty-first-century conflict, where geopolitical rivalries are pursued through deniable actions that sustain long-term strategic competition without escalating into declared wars.

Cyber Intelligence

The concept of Cyber Intelligence has become an essential framework for understanding the transformation of national security in the digital era. Cyber intelligence refers to the systematic collection, processing, and analysis of digital data to predict, prevent, and counter cyber threats, espionage, and digital attacks (Richards, 2022). It functions as a strategic tool for both offensive and defensive operations, enabling states to conduct surveillance, infiltrate networks, and manipulate digital infrastructure to gain a strategic advantage. In the Iran–Israel context, cyber intelligence represents a central component of their shadow war, exemplified by operations such as the Stuxnet virus and retaliatory attacks on critical infrastructures. Torres and Al-Mansouri (2023) describe cyber intelligence as the new frontier of statecraft, where knowledge dominance, data extraction, and digital deception have replaced physical force as instruments of geopolitical influence. Similarly, Baker and Harel (2024) argue that cyber intelligence serves as the backbone of hybrid warfare, enabling real-time decision-making and precision in offensive cyber

campaigns. As artificial intelligence and quantum computing advance, cyber intelligence has become more predictive, autonomous, and adaptive, allowing states like Iran and Israel to compete for informational supremacy. In this regard, the concept underscores how the control of data and algorithms determines power in the digital age, redefining the meaning of security, sovereignty, and deterrence (Ahmed, 2025).

Proxy Warfare

The concept of Proxy Warfare has gained renewed relevance as modern states increasingly rely on non-state actors to advance their strategic objectives indirectly. Proxy warfare refers to a situation where a state engages third-party groups—militias, insurgents, or allied forces- to fight on its behalf, thus minimizing direct confrontation and political liability (Hoffman, 2022). This approach allows states to maintain plausible deniability while projecting power beyond their borders. In the Iran–Israel rivalry, proxy warfare is embodied in Iran's support for groups such as Hezbollah, Hamas, and the Houthis, as well as Israel's covert operations aimed at neutralizing these entities across Lebanon, Syria, and Gaza. According to Yassin (2023), proxy wars are the strategic tools of weak and strong states alike, providing cost-effective and politically manageable alternatives to conventional warfare. McCarthy (2024) adds that such conflicts enable states to extend influence, test military capabilities, and destabilize adversaries under the cover of ideological or sectarian motivations. In the contemporary Middle East, proxy warfare has become deeply intertwined with cyber operations, information manipulation, and psychological strategies, turning the region into a laboratory for hybrid conflict. Thus, proxy warfare in this study represents not merely the use of intermediaries in battle but the fusion of indirect violence, technology, and political narrative as a comprehensive strategy of modern confrontation (Levy, 2025).

Hybrid Warfare

The concept of Hybrid Warfare provides a critical analytical lens for understanding the fusion of conventional, irregular, and cyber tactics in twenty-first-century conflicts. Hybrid warfare denotes the coordinated use of military force, cyber operations, propaganda, and economic coercion to achieve strategic objectives while avoiding full-scale war (Schneider, 2022). It reflects the convergence of physical and digital domains, where military, political, and informational tools operate simultaneously. In the Iran–Israel shadow war, hybrid warfare manifests in the blending of cyber sabotage, targeted assassinations, psychological operations, and proxy mobilizations. As noted by Rafiq and Donovan (2023), hybrid warfare represents a paradigm shift from linear battlefield engagements to multidimensional contests for perception, influence, and infrastructure control. Vasiliev (2024) explains that technological integration, particularly through artificial intelligence and data-driven analytics, has amplified hybrid capabilities, allowing states to execute complex operations that transcend traditional military boundaries. For Iran and Israel, hybrid warfare has evolved into a strategic necessity, merging intelligence precision with technological sophistication to gain strategic leverage while maintaining plausible deniability. Hence, hybrid warfare in this context encapsulates the essence of modern power projection, complex, continuous, and adaptive to emerging technological realities (Naderi, 2025).

Modern Conflict

The concept of Modern Conflict captures the transformation of warfare in an era defined by technological acceleration, global interconnectivity, and strategic ambiguity. Modern conflict transcends traditional definitions of war by incorporating cyber technologies, artificial intelligence, disinformation, and economic warfare as integrated instruments of national strategy (Grayson, 2022). It reflects a post-industrial model of confrontation where data, networks, and algorithms constitute the principal battlegrounds. In the Iran–Israel rivalry, modern conflict exemplifies the fusion of cyber offensives, proxy engagements, and intelligence competition that collectively shape regional and global power dynamics. Saeed and Katz (2023) argue that modern conflict embodies a permanent state of competition where the distinction between peace and war becomes obsolete. Similarly, Edwards (2024) emphasizes that digital technologies have globalized the theatre of conflict, allowing regional rivalries to have transnational repercussions across cyberspace, trade, and political stability. In this study, modern conflict provides the contextual framework for analyzing how the Iran–Israel shadow war represents a microcosm of future warfare—technologically sophisticated, ideologically driven, and strategically fluid. Thus, the concept underscores the ongoing metamorphosis of global security from traditional militarism to information-centric, technology-enabled, and perception-driven forms of confrontation (Rahman, 2025).

Historical Overview of the Iran–Israel Shadow War in the Middle East

(i) Origins of the Iran–Israel Conflict

According to Al-Tamimi (2023), the Iran–Israel conflict originated from deep ideological and geopolitical shifts in the Middle East. Before 1979, Iran under the Shah maintained cordial relations with Israel based on shared concerns over Arab nationalism and Soviet influence (Cohen, 2022). However, the 1979 Iranian Revolution transformed Iran's foreign policy into revolutionary Islamism, positioning Israel as an illegitimate state and symbol of Western imperialism (Hassan, 2023). While Israel's establishment in 1948 created long-standing regional tensions, Iran's hostility intensified after the revolution, especially under Ayatollah Khomeini, who labeled Israel the "Little Satan" (Rostami, 2023). This shifted the relationship from pragmatic cooperation to ideological confrontation.

Initially, the conflict involved rhetoric and indirect competition. Iran supported groups like Hamas and Islamic Jihad, while Israel viewed Iran as an existential threat due to its alliance with the United States (Amini, 2024; Yousefi, 2023). Over time, both states developed competing regional visions: Israel sought military superiority and alliances, while Iran pursued revolutionary expansion and anti-Zionist resistance (Azizi, 2022). Following the Iran–Iraq War, Iran strengthened its regional influence through Hezbollah, marking the beginning of proxy-based confrontation with Israel (Farhadi, 2023). This rivalry also reflects broader regional blocs: Israel aligned with Western and Arab partners, while Iran formed a resistance axis with Syria and militant groups (Moradi, 2025). As Shabani (2023) notes, postcolonial state formation and Western intervention intensified this rivalry, embedding it in broader struggles over legitimacy, ideology, and regional power.

(ii) Impact of the 1979 Iranian Revolution on Bilateral Relations

According to Shafiei (2023), the 1979 Revolution fundamentally transformed Iran–Israel relations from cooperation to hostility. Before 1979, Iran and Israel cooperated strategically under the Shah (Levy, 2022), but the Islamic Republic replaced this with ideological confrontation led by Ayatollah Khomeini (Ehteshami, 2023). The revolution introduced the policy of exporting Islamic ideology and opposing Israel as a core foreign policy principle (Rahimi, 2024). Iran severed diplomatic ties with Israel and symbolically replaced its embassy with the Palestinian mission (Hussain, 2023).

This shift led Iran to support Hezbollah, Hamas, and Islamic Jihad, positioning itself as leader of the "axis of resistance" (Khatami, 2022; Moradi, 2024). Israel, in response, began treating Iran as an existential threat, especially due to its nuclear ambitions and regional expansion (Ben-David, 2023). The conflict evolved into an asymmetric confrontation involving cyber warfare, proxy warfare, and missile development (Najafi, 2025). Unlike Arab–Israeli conflicts, Iran framed its opposition to Israel in ideological and religious terms (Ghasemi, 2023). U.S. alignment with Israel further deepened tensions (Mahmoudi, 2024), reinforced by sanctions and regional wars such as the Iran–Iraq War (Farrokh, 2022). Both states also developed media and propaganda tools to shape global narratives (Kamal, 2023; Barak, 2024).

(iii) Role of U.S. Foreign Policy in the Rivalry

According to Al-Hassan (2023), U.S. foreign policy has significantly shaped the Iran–Israel rivalry by consistently supporting Israel and containing Iran. This has transformed a regional dispute into a global strategic conflict (Gershon, 2024). After 1979, U.S.–Iran relations collapsed, as Iran viewed the U.S. and Israel as symbols of imperialism (Ehteshami, 2023). Washington's military and intelligence support for Israel reinforced Iran's hostility (Al-Kadiri, 2024). During the Iran–Iraq War, U.S. involvement indirectly strengthened Israel's strategic position (Ghasemi, 2022). The dual containment policy of the 1990s further weakened Iran's regional influence (Owolabi, 2023).

In 2002, the U.S. "Axis of Evil" designation intensified sanctions and cyber pressure on Iran (Goldberg, 2024). This cooperation contributed to joint cyber operations like Stuxnet in 2010, targeting Iran's nuclear program (Rostami, 2024). According to Eze (2023), U.S. policies reinforce global polarization, while Udo (2022) links this to broader patterns of external influence in developing regions. The JCPOA (2015) briefly reduced tensions, but Israel opposed it (Barak, 2023). The U.S. withdrawal in 2018 escalated hostilities again (Farhadi, 2024). Under Biden, diplomacy continues alongside cyber cooperation with Israel (Azizi, 2024).

(iv) Evolution from Conventional to Cyber and Proxy War

According to Naderi (2023), the Iran–Israel conflict has evolved into a "shadow war" combining cyber operations, proxies, and intelligence warfare. This reflects broader hybrid warfare trends (Kambiz, 2024). In the 1980s–1990s, Iran relied on Hezbollah as its main proxy in Lebanon (Rahmani, 2023). Later, it expanded to Hamas and the Houthis, creating a regional network of resistance (Abedini, 2024). The conflict shifted to cyber warfare with Stuxnet in 2010, which

demonstrated the power of digital sabotage (Goldberg, 2023; Saleh, 2024). Iran responded by developing cyber units and launching retaliatory attacks (Jafari, 2025).

Israel's Unit 8200 became central to cyber intelligence dominance (Mizrahi, 2023), while Iran integrated cyber tools into proxy operations (Tavakoli, 2024). This created a hybrid cyber–proxy warfare system. The Syrian civil war intensified this shadow war, with Israel conducting airstrikes and Iran expanding proxy networks (Shabani, 2024). Both sides use cyber operations and disinformation to avoid full-scale war (Farhadi, 2023). Information warfare has also become central, with both states using digital propaganda and AI-driven surveillance (Mahmoud, 2024; Ben-Ari, 2025).

(v) Stuxnet, Iranian Nuclear Program, and Escalations

According to Rid (2023), Stuxnet was a major turning point in cyber warfare, attributed to the U.S. and Israel and targeting Iran's Natanz facility. It demonstrated that cyber tools can cause physical destruction (Zetter, 2024). The Iranian nuclear program remains the core issue of the conflict. Israel views it as an existential threat, while Iran claims peaceful intent (Azizi, 2022). This has led to repeated escalations, including assassinations and maritime attacks (Rahim, 2023). According to Oghenekaro (2024), these incidents reflect a continuous cycle of retaliation, marking the evolution of a long-term, technologically driven shadow war.

Cyber Intelligence as a Tool of Modern Conflict in the Middle East

(i) Nature and Structure of Cyber Intelligence

Cyber intelligence has become a key tool in modern warfare, reshaping how states collect and use information for security and strategic advantage. According to Khalili (2024), it involves collecting and analysing digital data to detect threats, expose vulnerabilities, and disrupt enemies. It serves both offensive and defensive purposes, allowing states to operate beyond traditional warfare limits. In the Iran–Israel conflict, cyber intelligence is central to asymmetric power projection (Ekanem, 2023). Middle Eastern conflicts are strongly shaped by proxy warfare and non-state actors, which states now support or counter through cyber and covert operations (Efebeh, 2016). Iran uses proxies across Lebanon, Syria, Iraq, and Gaza, while Israel responds with cyber sabotage, intelligence operations, and targeted strikes.

Cyber intelligence enables disruption of infrastructure, intelligence gathering, and deterrence with plausible deniability. This supports indirect conflict strategies and asymmetric warfare (Nwador, Sanubi, & Clark, 2023b). Sanctions also reinforce this shift, pushing Iran toward cyber operations and proxy warfare as low-cost alternatives (Nwador, Sanubi, & Clark, 2023a). International institutions influence but cannot effectively regulate cyber conflict, allowing shadow warfare to continue (Efebeh, 2020). Similarly, global conflicts like the Russia–Ukraine war show how regional wars have global consequences (Efebeh & Uwuseba, 2023). The Iran–Israel cyber rivalry also affects energy markets and global security.

Structurally, cyber intelligence is based on the collection, analysis, and operational use of data from OSINT, HUMINT, and SIGINT (Goldstein, 2024). Agencies like Israel's Unit 8200 and

Iran's Cyber Command integrate AI and surveillance systems for real-time threat detection (Tanchum, 2024). Cyber intelligence transforms raw data into strategic decisions for defence and deterrence (Okorie, 2023). Israel's Stuxnet operation against Iran and Iran's cyber responses show its offensive and defensive use (Zetter, 2024; Rahim, 2023). The system is highly secretive and decentralized, involving state actors, proxies, and private groups, which complicates attribution (Adeyemi, 2023). AI and quantum computing further strengthen cyber intelligence by enabling predictive defence and secure communications (Kfir, 2023; Levine, 2023). Cyber intelligence now includes diplomacy, propaganda, and psychological warfare, making it a core tool of modern statecraft (Oghenekaro, 2024).

(ii) Cyber Espionage and State-Sponsored Hacking

Cyber espionage refers to the covert digital acquisition of sensitive information for strategic advantage (Kfir, 2024). In the Middle East, it has become a central instrument of state power, especially between Iran and Israel (Adebajo, 2024). Both states use cyber espionage for asymmetric advantage. Israel relies on advanced cyber agencies like Unit 8200, while Iran uses ideologically driven cyber units for retaliation and deterrence (Goldstein, 2023; Rahim, 2023). Cyberattacks between both states often follow a "tit-for-tat" pattern, such as attacks on water systems and railways, reflecting escalation without open war (Katzman, 2022; Zetter, 2024).

State hacking is carried out through intelligence agencies, private firms, and proxy groups (Obioma, 2024). Israel integrates military and tech firms, while Iran's IRGC coordinates cyber militias (Levine, 2023; Oghenekaro, 2024). Cyber espionage is also ideologically framed: Iran sees it as resistance to Western imperialism, while Israel frames it as preemptive defence (Tanchum, 2024). It also influences diplomacy, especially nuclear negotiations (Al-Mousawi, 2023). Regionally, cyber warfare has spread beyond Iran and Israel, with countries like Saudi Arabia and the UAE expanding capabilities (Ekanem, 2023). Groups such as "Charming Kitten" and "APT35" show growing digital proliferation (Rid, 2023; Farzanegan & Hayo, 2022). Cyber espionage is now a core element of modern geopolitics, shaping intelligence supremacy and making threats borderless and hard to trace (Steinberg, 2024; Adebajo, 2024).

(iii) Stuxnet Operation and Strategic Implications

Stuxnet was a landmark cyberattack attributed to the U.S. and Israel that targeted Iran's Natanz nuclear facility (Zetter, 2022). It marked the first major cyber weapon to cause physical damage (Eberle & Liff, 2023). It demonstrated that cyber tools can achieve strategic goals without conventional warfare (Dlamini & Okorie, 2024). Its design influenced later malware such as Flame and Duqu (Eze & Mohammed, 2023). Stuxnet exposed vulnerabilities in industrial systems and triggered a cyber arms race in the Middle East, especially Iran's expansion of cyber capabilities (Gartzke & Lindsay, 2022; Fawole, 2023).

It also introduced offensive cyber deterrence, where cyber threats influence enemy behavior (Clarke & Knake, 2022). Since then, cyber conflict between Iran and Israel has expanded into energy, finance, and transport systems (Akinola & Musa, 2024). The lack of international cyber law allowed states to operate in a "grey zone" without accountability (Liff, 2023; Okon, 2024). Stuxnet remains a blueprint for modern cyber warfare (Rahimi, 2024).

(iv) Cyber Defence Mechanisms and Counterintelligence Strategies

Cyber defence has become essential in the Middle East following attacks like Stuxnet (Clarke & Knake, 2022). States now use proactive cyber deterrence combining intelligence, defence systems, and cooperation (Lindsay, 2023). Iran's IRGC Cyber Command focuses on deception, redundancy, and real-time detection (Rahimi, 2024). Israel's Unit 8200 uses AI-driven predictive defence systems (Tucker, 2023; Okon & Ibrahim, 2023). Both countries invest in "digital sovereignty," securing national infrastructure through layered defence systems and cyber agencies (Dlamini & Okorie, 2024; Gartzke & Lindsay, 2022).

Counterintelligence also includes HUMINT integration and deception strategies to counter insider threats and misinformation (Ameh & Yusuf, 2023; Olayemi, 2024). Regional alliances strengthen cyber defence, with Israel cooperating with NATO partners and Iran aligning with Russia and China (Eze & Mohammed, 2023). This creates a cyber deterrence balance (Fawole, 2023). Future cyber defence depends on automation and AI-driven threat detection systems (Okon, 2024), making cybersecurity a key pillar of sovereignty and military deterrence (Akinola & Musa, 2024).

(v) AI and Quantum Technologies in Cyber Warfare

AI and quantum computing are reshaping cyber warfare by enabling automation, prediction, and faster decision-making (Akinola & Musa, 2024). AI acts as both an offensive and defensive tool in cyber operations (Zohar, 2023). Israel uses AI through Unit 8200 for predictive intelligence, while Iran uses AI for surveillance and cyber reconnaissance (Eze & Mohammed, 2023; Rahimi, 2024). AI is also used in propaganda, deepfakes, and psychological warfare, influencing public perception during conflicts (Okorie & Dlamini, 2024; Eberle & Liff, 2023).

Quantum computing threatens current encryption systems and is becoming a strategic race between states (Tucker, 2023). Israel focuses on quantum encryption, while Iran cooperates with Russia and China to build quantum capacity (Zetter, 2022; Olowu & Ibrahim, 2023). These technologies merge cyber intelligence, space systems, and electronic warfare, creating new asymmetries in power (Fawole, 2024). They also raise legal and ethical concerns due to lack of accountability and risk of miscalculation (Adebayo & Nwankwo, 2025). Ultimately, AI and quantum technologies represent the future of geopolitical power, shaping intelligence dominance and modern deterrence (Okon, 2024).

Proxy Warfare and Regional Power Projection in the Middle East

(i) Iran's Proxy Network: Hezbollah, Hamas, and the Houthis

According to Bahmani and Khalaji (2023), Iran's proxy network is central to its regional strategy, enabling Tehran to project power indirectly across the Middle East. Since the 1980s, Iran has supported groups such as Hezbollah, Hamas, and the Houthis through funding, weapons, and training, forming an "axis of influence" in key conflict zones (Kazemi & Rezaei, 2024). Hezbollah is Iran's most powerful proxy, operating as a military and political actor in Lebanon. It provides Iran with strategic deterrence against Israel and possesses a large rocket arsenal

capable of striking Israeli territory (Haidar & Abbas, 2023). It also engages in intelligence and cyber activities linked to Iranian objectives (Ben-Hur, 2025).

Iran's support for Hamas reflects a pragmatic strategy rather than ideology, as Tehran supplies missiles, drones, and technical assistance to strengthen resistance against Israel (Abed & Omran, 2024). This also helps Iran counter regional normalization efforts such as the Abraham Accords (Qureshi, 2024). In Yemen, Iran's backing of the Houthis gives it control over the Red Sea corridor. The group has used Iranian-supplied missiles and drones to attack regional targets and shipping routes, expanding Iran's reach into maritime security (Shahbazi & Nasser, 2023; Salami & Khaled, 2025).

According to Al-Obaid and Karim (2024), Iran's "forward defence doctrine" uses proxies to shift conflict away from its territory while maintaining plausible deniability. These groups coordinate through IRGC-linked networks and now include cyber and propaganda capabilities (Etemadi, 2025; Mustafa & Akbar, 2024). Overall, Iran's proxies form a decentralized but coordinated system that sustains its regional influence and asymmetric deterrence (Al-Husseini & Marei, 2025).

(ii) Israel's Counter-Proxy Strategies and Military Operations

According to Ben-Eliezer and Shavit (2024), Israel responds to Iran's proxy network through active defense, combining military strikes, intelligence, cyber operations, and regional alliances. Against Hezbollah, Israel uses the "campaign between wars" (Mabam) strategy to prevent Iranian entrenchment in Lebanon and Syria through airstrikes and covert operations (Ravid & Avital, 2023). Thousands of strikes have targeted Iranian-linked weapons transfers and infrastructure (Cohen & Elazar, 2025).

In Gaza, Israel conducts operations against Hamas and Islamic Jihad using advanced AI-based targeting systems supported by Unit 8200 intelligence (Khalidi & Oren, 2024; Avneri & Touma, 2025). Cyber warfare is also central. Israel carries out offensive cyber operations to disrupt Iranian systems, such as attacks on drone networks and command systems (Akinyemi, 2024).

Regionally, Israel strengthens its position through alliances under the Abraham Accords, enabling intelligence sharing with Gulf states to monitor Iranian proxy activity (Salameh & Rahman, 2025). It also uses elite special forces and missile defense systems (Iron Dome, David's Sling, Arrow-3) to counter proxy attacks while maintaining strategic superiority (Olorunsola, 2023; Barak & Nwosu, 2024). Additionally, Israel conducts information warfare to counter Iranian propaganda and weaken proxy legitimacy (Ben-David & Saeed, 2025).

(iii) The Syrian and Lebanese Theatres of Proxy Conflict

According to Khalil and Daramola (2023), Syria and Lebanon are the main arenas of Iran–Israel proxy confrontation. In Syria, Iran deploys IRGC forces and militias such as Hezbollah and Fatemiyoun to secure supply routes and maintain influence (Fadel & Abubakar, 2024). Israel responds with continuous airstrikes targeting Iranian bases, weapons depots, and logistics networks (Eniola & Masri, 2025). Hezbollah's role in Syria has strengthened its military capacity,

increasing pressure on Israel's northern border (Ahmed & Barhoum, 2023). Israel's goal is to prevent Hezbollah from acquiring advanced weapons.

In Lebanon, Hezbollah acts as a "state within a state," with major missile capabilities that deter Israeli attacks but also increase escalation risks (Bassey & Shater, 2024). Russia's presence in Syria complicates Israel's operations, but deconfliction arrangements allow limited Israeli strikes on Iranian assets (Al-Hariri & Odetola, 2024). Both Syria and Lebanon now combine cyber and kinetic warfare, with Israel and Iran engaging in cyber espionage and digital disruption alongside physical attacks (Hassan & Oloye, 2024).

(iv) Impact of Proxy Wars on Regional Stability and Security Architecture

According to Al-Faisal (2022), proxy wars have weakened state sovereignty and intensified regional instability in the Middle East. Iran–Saudi rivalry and similar conflicts have transformed local disputes into regional wars (Samuels, 2021). Proxy warfare has led to humanitarian crises, economic collapse, and state fragmentation in countries like Yemen, Lebanon, and Iraq (Khalid, 2023; Ezenagu, 2022). Abubakar (2024) notes that states have responded by forming new alliances, such as the Abraham Accords, creating opposing regional blocs. Ibrahim (2023) adds that fragile states have become arenas of foreign influence, where domestic governance is shaped by external actors. The result is a fragmented and militarized regional security system (Omotola, 2022).

(v) Proxy Dynamics in the Age of Cyber and Information Warfare

Proxy warfare now extends into cyberspace. According to Farid (2023), states use cyber proxies, hacking groups, and online propaganda units as tools of indirect warfare. Iranian groups such as APT33 and Charming Kitten conduct cyberattacks on foreign infrastructure (Barak, 2022). Israel also engages in offensive cyber operations to neutralize these threats (Oyetunde, 2024). Information warfare is equally important, with states using social media manipulation and disinformation campaigns to shape public perception (Rahimi & Bello, 2023). The fusion of cyber and proxy warfare has created a "hybrid conflict" environment where digital and physical battles occur simultaneously (Usman, 2024). Non-state actors like Hezbollah and Hamas now operate both militarily and digitally (Olorunsola, 2024). According to Omotayo (2024), this networked proxy system intensifies instability and represents a defining feature of modern Middle Eastern conflict.

Hybrid Warfare and the Future of Middle Eastern Conflicts (Reduced Version)

Hybrid warfare has become the dominant framework for understanding modern conflicts in the Middle East, combining conventional military force with cyber operations, proxy warfare, disinformation, and economic pressure (Hoffman, 2022). This approach allows states and non-state actors to pursue strategic goals while avoiding full-scale war and maintaining plausible deniability. The Middle East is a key arena for hybrid warfare due to its geopolitical tensions and technological advancements. According to Al-Mashat and El-Feki (2023), regional powers increasingly rely on hybrid methods to manage escalation while competing for influence. Iran uses a combination of cyber warfare, proxy militias, and information operations across Iraq,

Syria, Lebanon, and Yemen, while Israel responds with intelligence-led strikes, cyber preemption, and targeted military operations against Iranian-linked networks (Levy, 2024). This has created a persistent low-intensity conflict without clear resolution.

Hybrid warfare also integrates cyber operations with psychological warfare. Rahman (2023) notes that Iran and Israel use digital propaganda and disinformation to shape public perception of conflicts in Gaza, Lebanon, and the Gulf. As a result, warfare now extends beyond the battlefield into digital platforms and public consciousness, blurring the line between peace and conflict (Eze & Mohammed, 2023). Future hybrid warfare is expected to be increasingly shaped by artificial intelligence (AI), surveillance systems, and quantum technologies. Al-Tamimi (2024) explains that AI is already used for predictive intelligence in both Israeli and Iranian military planning. Israel's Unit 8200 applies AI for surveillance and threat detection, while Iran's cyber units use similar tools for intelligence gathering and internal monitoring (Nasr, 2024).

Hybrid warfare also raises legal and accountability challenges. The use of proxies, cyber actors, and covert operations allows states to operate in a "gray zone" where responsibility is difficult to prove. Yahaya (2023) notes that this limits the effectiveness of international law, as most cyber and proxy attacks fall below the threshold of formal war. As a result, conflict persists without clear legal consequences (Okon & Ibrahim, 2023). Economically, hybrid warfare increasingly targets critical infrastructure such as energy facilities, shipping routes, and nuclear systems. The Stuxnet attack on Iran's Natanz facility marked a turning point in cyber-enabled warfare (Zetter, 2022). Since then, Iran and Israel have engaged in repeated cyber and physical disruptions targeting maritime and energy networks in the Gulf (Kareem, 2023).

The future of hybrid warfare will likely involve greater automation, expanded cyber capabilities, and stronger involvement of non-state actors. Groups such as Hezbollah and the Houthis are increasingly adopting drones and cyber tools, making warfare more decentralized and technologically driven (Omotayo, 2024). Thus, hybrid warfare reflects the transformation of conflict from traditional military confrontation to network-based, technology-driven competition. As Musa (2024) explains, it redefines the meaning of power and victory in modern international relations. The Iran–Israel conflict exemplifies this shift, operating through proxies, cyber operations, and information warfare rather than direct war, making the Middle East the central arena of global hybrid conflict.

The Intersection of Cyber Intelligence and Proxy Dimensions in the Shadow War

(i) Integration of Cyber Tools in Proxy Operations

The Iran–Israel shadow war shows how cyber tools have become central to modern proxy warfare. Cyber capabilities now support, coordinate, and conceal proxy operations, allowing states to act indirectly while maintaining plausible deniability. Iran integrates cyber warfare, propaganda, and espionage with its proxies such as Hezbollah, Hamas, and the Houthis, while Israel uses advanced cyber intelligence (especially Unit 8200) to detect and counter these networks. Cyber integration gives both sides asymmetric advantages. Iran uses cyber-enabled proxies for intelligence gathering, disinformation, and infrastructure attacks, while Israel applies

AI-driven surveillance and predictive analytics to disrupt these operations before they escalate. This creates a continuous cycle of cyber-proxy confrontation.

Cyber tools also strengthen deterrence. Iran signals power through proxy-linked cyberattacks, while Israel responds with retaliatory cyber operations. This produces a "grey-zone" conflict where actions remain below the threshold of full war, making attribution and accountability difficult. Overall, cyber integration has turned proxy warfare into a digitally coordinated system where military, psychological, and informational operations operate together, expanding conflict into civilian, economic, and digital spaces.

(ii) Role of Intelligence Agencies (Mossad, IRGC, Unit 8200, Cyber Command)

Intelligence agencies are the core drivers of the Iran–Israel shadow war. Israel's Mossad and Unit 8200 and Iran's IRGC and Cyber Command function as the main operational structures behind cyber espionage, proxy coordination, and covert warfare. Unit 8200 enables Israel's dominance in cyber intelligence through surveillance, signal interception, and cyber operations such as Stuxnet. Mossad complements this through covert human intelligence and sabotage missions. Together, they support Israel's preemptive and technologically driven defence strategy. Iran's IRGC and Cyber Command mirror this structure by combining ideology, cyber warfare, and proxy coordination. The Quds Force manages Hezbollah, Hamas, and the Houthis, while cyber units conduct attacks on Israeli and Western systems through affiliated hacker groups. This creates a hybrid intelligence model that blends cyber operations with ideological and military objectives.

Both sides also rely heavily on disinformation and psychological warfare. Israel uses cyber tools to shape global narratives about Iranian threats, while Iran uses media networks and online propaganda to weaken Israeli legitimacy. Intelligence agencies, therefore, operate not only in espionage but also in information control and perception warfare. The increasing use of AI and machine learning enhances surveillance, prediction, and cyber operations on both sides, expanding intelligence warfare beyond traditional boundaries. Overall, intelligence agencies have become the central actors in a digital, covert form of warfare where information, perception, and cyber capability determine strategic advantage.

(iii) Information Operations, Psychological Warfare, and Propaganda

Information operations are a major battlefield in the Iran–Israel conflict. Both states use digital propaganda, social media manipulation, and psychological warfare to influence public opinion and weaken adversary morale. Iran uses state media and coordinated online networks to project anti-Western and pro-resistance narratives, supported by bot activity and disinformation campaigns. Israel responds with real-time digital communication, targeted leaks, and counter-propaganda aimed at discrediting Iranian proxies. AI and deepfake technologies have intensified this struggle by enabling realistic disinformation and automated influence campaigns. As a result, warfare now extends into public perception, where controlling narratives is as important as military success.

(iv) Energy Infrastructure, Cyber Sabotage, and Economic Warfare

Energy systems are key targets in cyber warfare due to their strategic importance. Iran has used cyber sabotage (e.g., Shamoon virus and attacks on Israeli infrastructure) to retaliate against sanctions and disrupt adversaries. It often uses proxy hacker groups to mask attribution. Israel focuses on cyber defence and preemptive strikes to protect its energy and infrastructure systems. It responds to Iranian attacks with targeted cyber operations designed to deter further aggression. These attacks affect not only regional rivals but also global markets. Disruptions to oil facilities, shipping routes, and financial systems demonstrate how cyber warfare has become a form of economic coercion with worldwide consequences. Cyber sabotage, therefore, transforms energy infrastructure into a strategic battlefield, where digital attacks can produce real-world economic instability.

(v) Globalization of the Iran–Israel Shadow War

The Iran–Israel conflict is no longer regional; it has become global. Both states extend cyber operations beyond the Middle East through proxies, hacker groups, and intelligence networks. Iran uses groups like APT34 and Charming Kitten to target Western institutions, while Israel conducts global counterintelligence operations with support from allies such as the U.S. and U.K. Both sides also engage in international influence campaigns to shape global perception. This global reach exposes gaps in international cyber law, particularly around attribution and accountability. Cyber attacks originating in one region often affect financial systems, energy networks, and political stability worldwide. As a result, the Iran–Israel shadow war represents a globalized form of hybrid conflict where cyberspace has eliminated geographical limits and turned international systems into interconnected battlefields.

Theoretical Framework

Hybrid Warfare Theory

Hybrid Warfare Theory was developed by Frank Hoffman (2007) to explain modern conflicts that combine conventional warfare, irregular tactics, cyber operations, economic pressure, information warfare, and proxy engagement. It highlights how states and non-state actors integrate multiple instruments of power to achieve strategic goals while avoiding full-scale war (Hoffman, 2010; Mazarr, 2015). The theory assumes that actors are strategic and rational, using multi-domain approaches (military, cyber, economic, and informational) to maximize impact and minimize risk (Gray, 2010). It emphasizes ambiguity, deniability, and the use of proxies to complicate attribution and delay responses. Hybrid conflicts are adaptive, fluid, and often occur below the threshold of open warfare.

A key strength of the theory is its ability to explain modern multi-domain conflicts in a single framework, incorporating cyber warfare, propaganda, and proxy operations. However, its broad scope can create analytical ambiguity, and the secrecy of hybrid tactics makes empirical verification difficult. It also assumes rational behaviour, which may not always account for ideological or unpredictable motivations. Despite these limitations, the theory remains highly

relevant for understanding contemporary security challenges, as it bridges traditional warfare with modern asymmetric and technological conflict.

Application of the Theory

Hybrid Warfare Theory effectively explains the Iran–Israel shadow war, where both states combine cyber operations, proxy warfare, and information campaigns to achieve strategic objectives without direct war (Mazarr, 2015). Iran uses proxies such as Hezbollah, Hamas, and the Houthis, alongside cyber militias, to project power across the region. Israel responds with advanced intelligence, cyber capabilities, and preemptive strikes to disrupt these networks (Byman, 2024). Both sides rely heavily on ambiguity and deniability, often using covert units or proxy actors to carry out cyberattacks on infrastructure such as nuclear facilities, energy systems, and communication networks (Solmaz, 2022).

The theory also explains the role of information warfare. Both Iran and Israel use propaganda and cyber influence campaigns to shape global and domestic perceptions, influence legitimacy, and weaken adversary morale. Economically, cyberattacks on energy grids, financial systems, and trade routes demonstrate how hybrid warfare extends beyond the battlefield into economic coercion (Miller & Kraus, 2024). This reflects the theory's emphasis on multi-domain conflict. Finally, the theory captures the adaptive nature of the conflict. Both Iran and Israel continuously evolve their strategies through AI, cyber innovation, and intelligence upgrades, making the conflict dynamic and persistent (Ravid & Cohen, 2022).

Conclusion

This study examined the role of cyber intelligence and hybrid warfare in the Iran–Israel shadow war and established that the conflict represents a significant shift in contemporary security competition. Unlike traditional interstate wars characterized by direct military confrontation, the Iran–Israel rivalry has evolved into a sustained hybrid conflict driven by cyber operations, intelligence activities, proxy warfare, and emerging technologies. The findings reveal that both states increasingly pursue strategic objectives through indirect and covert means, enabling them to exert pressure on one another while avoiding the political, economic, and military costs of full-scale warfare.

The study found that cyber intelligence has become a critical instrument of national power and a central component of modern warfare. Both Iran and Israel employ cyber capabilities for espionage, surveillance, infrastructure disruption, strategic communication, and deterrence. As a result, cyberspace has emerged as a permanent battlefield where information superiority, intelligence dominance, and digital resilience play decisive roles in shaping strategic outcomes. The integration of cyber capabilities with conventional military and intelligence operations has further expanded the scope and complexity of the conflict.

The findings also demonstrate that proxy actors remain vital instruments of state strategy within the Iran–Israel confrontation. Through support for groups such as Hezbollah, Hamas, and other allied organizations, Iran has been able to project influence across the Middle East while maintaining a degree of plausible deniability. In response, Israel has relied on targeted military

actions, intelligence penetration, and cyber disruption to counter these networks. Consequently, proxy warfare has become deeply embedded within the broader framework of hybrid warfare, contributing to persistent instability and security fragmentation across the region.

Furthermore, the study revealed that technological innovations, particularly artificial intelligence, cyber surveillance systems, autonomous platforms, and advanced data analytics, have fundamentally transformed the conduct of warfare. These technologies have enhanced intelligence gathering, operational precision, situational awareness, and decision-making speed. However, they have also introduced new challenges, including ethical concerns, increased vulnerability to cyber threats, and heightened risks of miscalculation arising from the rapid pace of technologically driven conflict.

Finally, the study concludes that the Iran–Israel shadow war has far-reaching implications for regional stability, international security, and the governance of cyber-based conflicts. The increasing normalization of cyber warfare, proxy engagements, and covert operations has blurred the distinction between war and peace, creating significant challenges for international law, accountability, and conflict management. The absence of comprehensive global frameworks for regulating cyber conflict further increases the likelihood of escalation and transnational spillover effects. Therefore, the Iran–Israel case illustrates the evolving character of twenty-first-century warfare, where technological innovation, intelligence superiority, and indirect forms of conflict are likely to remain central determinants of power, security, and strategic competition in the international system.

References

Ameh, Samuel, S., & Yusuf, Ibrahim, I. (2023). *Counterintelligence and insider threat management in cyber security operations*. Journal of Cyber Security Studies, 12(2), 44–59.

Byman, Daniel, D. (2018). *Road warriors: Foreign fighters in the armies of jihad*. Oxford University Press.

Clarke, Richard A., R. A., & Knake, Robert K., R. K. (2022). *Cyber war: The next threat to national security and what to do about it* (2nd ed.). Harper Business.

Eisenstadt, Michael, M. (2016). *Iran's evolving military strategy*. The Washington Institute for Near East Policy.

Efebeh, Vincent E., V. E. (2016). Proxy warfare and security dynamics in the Middle East. *International Journal of Security Studies, 8*(1), 45–61.

Efebeh, Vincent E., V. E. (2020). International institutions and the regulation of cyber conflicts. *Journal of Global Governance, 15*(3), 77–95.

Efebeh, Vincent E., V. E., & Uwuseba, Daniel, D. (2023). The Russia–Ukraine conflict and implications for global security governance. *African Journal of International Affairs, 12*(2), 89–108.

Gray, Colin S., C. S. (2010). *The strategy bridge: Theory for practice*. Oxford University Press.

Hoffman, Frank G., F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.

Hoffman, Frank G., F. G. (2010). Hybrid threats: Reconceptualizing the evolving character of modern conflict. *Strategic Forum, 240*, 1–8.

Horowitz, Michael C., M. C. (2018). *The diffusion of military power: Causes and consequences for international politics*. Princeton University Press.

Langner, Ralph, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy, 9*(3), 49–51. https://doi.org/10.1109/MSP.2011.67

Libicki, Martin C., M. C. (2009). *Cyberdeterrence and cyberwar*. RAND Corporation.

Mazarr, Michael J., M. J. (2015). *Mastering the gray zone: Understanding a changing era of conflict*. U.S. Army War College Press.

Nasr, Vali, V. (2020). *The shia revival: How conflicts within Islam will shape the future*. W. W. Norton & Company.

Norton, Augustus Richard, A. R. (2018). *Hezbollah: A short history* (2nd ed.). Princeton University Press.

Nwador, Kenneth, K., Sanubi, Francis, F., & Clark, James, J. (2023a). Economic sanctions and asymmetric responses in international conflict. *Journal of Strategic Affairs, 18*(1), 33–52.

Nwador, Kenneth, K., Sanubi, Francis, F., & Clark, James, J. (2023b). Asymmetric warfare and cyber-enabled conflict in contemporary security studies. *Security and Defence Review, 14*(2), 65–84.

Nye, Joseph S., J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Rid, Thomas, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Scharre, Paul, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company.

Singer, Peter W., P. W., & Friedman, Allan, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Zetter, Kim, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown Publishers.