(Online) ISSN 2744-1741
Original Research

Defense and Security Studies
Vol. 6, No. 1, 2025, pp.91-102
https://doi.org/10.37868/dss.v6.id285

The evolution of warfare from conventional to a digital battlefield: an analysis of cyber technology and artificial intelligence in the Lebanese-Israel conflicts

Sereina Khalifeh[1*]
[1] Political Science and International Relations, Lebanese American University, Lebanon

*Corresponding author E-mail: Sereinakhalifeh@outlook.com

Received: May 8, 2025
Revised: Jun. 1, 2025
Accepted: Jun. 7, 2025
Online: Jun. 9, 2025

Abstract

This study will evaluate the transition from conventional combat methods to a technology-driven battlefield. In particular, the Lebanon-Israel conflict serves a crucial case study to analyze how digital tools and AI reshape battlefield strategies, operational efficiency, and psychological warfare, triggering a broader evolution in modern military doctrine. This study will tackle a longitudinal comparison of digital strategy evolution in a single dyadic conflict zone. It adds to fields of security studies, cyberwarfare strategy, and AI-driven conflict analysis by analyzing how asymmetric technological adoption constructs long-term power dynamics. Through a theoretical lens of realism and a complementary military geopolitical framework, this research will analyze the impact of cyber warfare, AI-driven decision-making, intelligence, and precision missile systems on military strategies, political decision-making, and regional security.

Keywords: cyber-warfare, artificial intelligence, Lebanon-Israel conflicts, military strategy, technology warfare, hybrid warfare, Middle East security

1. Introduction

The warfare has gone through a significant transition, shifting from conventional combat methods to a technology-driven battlefield. Historically, wars have been fought through direct confrontation, depending on infantry, armored vehicles, and aerial bombardments. However, with the development of military technology, modern warfare has incorporated cyber operations, AI, and precision-guided weapons. This advancement has altered military strategies and significantly impacted war outcomes, reconstructing battlefield dynamics, decision-making processes, and geopolitical power structures.

The Middle East, a central region for persistent conflicts and shifting military strategies, presents an important case for analyzing such shifts. In particular, the Lebanon-Israel conflict serves as a crucial case study to analyze the transition from conventional to technology-advanced warfare. Through the evaluation of the role of cyber technology and artificial intelligence (AI) in the Lebanon-Israel conflict of 2006 and 2023-2024. Through a theoretical lens of realism and a complementary military geopolitical framework, this research will analyze the impact of cyber warfare, AI driven decision-making, intelligence, precision missile systems on military

strategies, political decision-making, and regional security. This research study will evaluate how technological advancements have redefined the nature of modern military engagements and changed the outcomes of wars within the Middle East. Thus, this research seeks to answer the question of how AI and cyber warfare affected the strategic calculus and balance of power between Israel and Hezbollah from 2006 to 2024.

2. Literature Review

The transition from conventional combat to a technology-driven battlefield has redefined military strategies and reconstructed geopolitical dynamics. The introduction of AI-driven military technologies and cyber warfare has altered military engagements in the Middle East. According to Kallenborn [6] and the Marine Corps Association [9], AI has altered decision-making intelligence into modern military strategies and facilitated the dependence on cyber operations and precision-guided weapons. To illustrate, AI has become a centralized tool in target acquisition, predictive analytics, battlefield surveillance, and military operations. According to Daily Sabah [3], both state and non-state actors tend to leverage technology to manipulate adversaries and gain a strategic advantage. For instance, cyber warfare has become an essential element within military operations, where it has a crucial impact on communication networks and intelligence gathering.

As this paper delves into a case study of the 2023-2024 Lebanon-Israel conflict, it shows a rapid evolution of warfare where cyber abilities and AI-driven military systems played a central role within the war. Unlike the 2006 war where Hezbollah employed an asymmetric war and employed a guerrilla tactic.[2] In the 2023-2024 war, it was evident that a transition to cyberwarfare had been launched. To illustrate, AI-guided missile systems and AI- AI-assisted command and control have been utilized to disable communication networks, disrupt enemy defenses, and conduct psychological operations [21]. The digital warfare tactics employed by Israel had a severe impact on Lebanese civilians as beyond the immediate danger of exploding communication devices, these strategies weakened Hezbollah as a party and created fear within the country (Khalifeh 2024).

The psychological impact of such a tactic disrupted everyday life and contributed to a greater terror since anyone can be the victim of such explosions, whether they are affiliated or not. Furthermore, Israel has taken an innovative approach to AI in its conflict with Hezbollah, where it diverted from traditional targeting methods [2]. For example, Israel combined human decision-making alongside AI capabilities to maximize operational efficiency. According to Barazy [1], the conflict between Lebanon and Israel extended beyond modern military confrontation and extended into the digital realm, where platforms such as WhatsApp and Instagram were used to spread false information and share military strategies, such as locations that will be bombed in a specified time.

To further explain, both parties have engaged in cyberattacks, account hacking, and misinformation AI campaigns to destabilize each other's digital infrastructure and manipulate the international opinion [1]. This literature review underscores the importance of understanding the intersection of technology and warfare, especially within the Middle East. The integration of such technology can maneuver outcomes and create challenges for weaker parties, redefining global security.

3. Methodology

This study will employ a mixed-methods approach, combining both qualitative and quantitative research methodologies. Through integrating diverse data sources and analytical frameworks, the research seeks to provide a comprehensive examination of the transition from conventional warfare to technology-driven battlefield while focusing on the impact of technology on the outcome of the Lebanon-Israel conflicts of 2006 and 2023-2024.

The study will incorporate both Primary sources, such as military reports, government statements, and expert interviews, where it will gather first-hand data on military strategies and technological applications. As well as secondary sources such as academic articles, media coverage, and policy analyses, which will provide contextual and historical insight into the evolution of modern warfare. Additionally, this study will employ a strategic approach to analyze the transition from conventional warfare to a technology-driven battlefield, specifically exploring the impact of technology on war outcomes.

Realism: the primary theoretical lens of the research will analyze the evolution of military strategies, technological integration, and information warfare, emphasizing state behavior, power dynamics, and security competition. Furthermore, a case study methodology will be applied to evaluate the impact of AI and

Technological advancements in the Lebanon-Israel wars in 2006 and 2023-2024. By focusing on this case study, the study will highlight patterns, strategic shifts, and the role of emerging military technologies in determining outcomes of wars.

The study justifies its methodology by integrating both primary and secondary accounts, ensuring a balanced assessment of the evolution of modern warfare. By systematically examining available tools, data, and research frameworks, the study aligns its objectives to provide a detailed analysis of shifting warfare trends and the way technological advancements have shaped military successes or failures. Moreover, the research is highly feasible since it tackles a modern time conflict that destabilizes the Mena region and the central case study is manageable since it is within two specific time frames July 12, 2006, till August 14, 2006) and (October 8, 2023, till November 17, 2024) [26], and it relies on well documented events and assessable scholarly sources.

The focus is on the existing conflicts, and it ensures that data availability will not pose a barrier. Moreover, by leveraging existing analytical frameworks in conflict studies, the study can provide meaningful insight within a structured timeline. Given the volatile nature of cyberwarfare reporting, this study will tackle the triangulation methods. An open-source intelligence is cross-verified with credible think tanks and defense institutes such as NATO, CSIS, Cyber Readiness Reports, and IISS strategic briefing assures data reliability. Misinformation risk can be monitored through proper dependency on verified military communiques, academic sources, and media triangulation.

The study is grounded on the basis of a realist theoretical lens, especially Neorealism (Waltz 1979), which highlights the anarchic structure of international systems and the ways AI and cyber warfare have redefined power competition. Hybrid Warfare [16] will be integrated to showcase a mix of conventional, psychological tactics. To illustrate, the Cyber deterrence theory [22] will be emphasized to examine the escalation dynamics and retaliatory calculations surrounding cyber operations. These frameworks will collectively provide insight into how technological advancement has transitioned not only the battlefield but also has affected structural dynamics of power competition within the region.

According to neorealism (Waltz 1979), the international system is anarchic, and it is driven by a sense of survival through the accumulation of relative power. Within this context, Israel has invested in AI and cyber warfare capabilities to showcase a strategic response in the evolving nature of threats, especially those posed by non-state actors such as Hezbollah. Technological dominance has become a form of structural power within the anarchic system, where military superiority ensures deterrence and regional influence. Neorealism facilitates Israel's proactive cyber strategy to balance regional power and deter Iran-backed asymmetric threats.

Hybrid warfare theory [16] is important to highlight Hezbollah's military adaptation. Hybrid warfare is the blending of conventional warfare, irregular tactics, cyber operations, and psychological campaigns. Hezbollah as. Anon state actor has combined guerrilla warfare, social media misinformation, cyber destruction, and encrypted communication to counter Israel's technological advantages. This approach showcases the stretch of the battlefield beyond physical terrains into digital and psychological domains, maximizing the effectiveness of limited sources.

Whereas the Cyber deterrence theory [22] provides a different layer of interpretation, where the logic of escalation and retaliation in digital warfare is considered. During the 2023-2024 conflict, the cyberattacks were utilized to disable infrastructure, disrupt financial systems, and demoralize enemy forces without engaging in full-scale kinetic warfare. The theory tends to underscore the strategic ambiguity and asymmetric potential of cyber warfare where attribution is challenging, and retaliation can be calibrated it avoid traditional escalation.

This model tends to suit both state actors, such as Israel, who aim for precise strikes with minimal fallout, and non-state actors such as Israel who aim towards precise and minimal fallout, and non-actors such as "Hezbollah" that aim towards benefiting from anonymity and unpredictability within the cyber domain.

Combined, all these theoretical perspectives tend to offer a multi-layered understanding of Lebanon-Israel conflicts. Realism and Neorealism target the broader strategic motivation of different state actors, where hybrid warfare theory illuminates the developing tactics of asymmetric military groups such a Hezbollah, and cyber deterrence theory contextualizes the operational logic behind the non-kinetic forms of engagement. This showcases that rage technology is not a tool but a determinant of contemporary military strategy and geopolitical behavior.

4. Comparative analytical framework

To evaluate the shift between the Lebanon-Israel conflict of 2006 and 2023-2024, a comparative matrix was developed alongside four critical dimensions (Table 1).

Table 1. Comparative matrix with four critical dimensions

Dimension	2006 War	2023-2024 War
Weapons Systems	Conventional artillery, airstrikes, and guerrilla tactics	AI-guided missile systems, autonomous drones, cyberattacks
Communication Strategies	Radio transmissions, satellite phones, centralized media	Encrypted messaging apps, cyber-infiltration, and decentralized misinformation
Psychological Operations	Traditional media propaganda (TV, newspapers)	AI-generated misinformation, deepfake videos, and real-time digital manipulation
Civilian Impacts	Physical destruction (infrastructure bombing)	Digital infrastructure targeting (banking systems, health networks), psychological destabilization via social media

4.1. The evolution of military technology and strategic doctrine

The advancement of military technology has transformed the warfare arena, transitioning from traditional methods that rely on conventional weapons and large-scale troop deployments to a technology-driven battlefield dominated by cyber warfare and AI [2]. Throughout history, technological advancements have served as a central trigger for military superiority, enabling states to exert their power and maintain security in an increasingly competitive international system (Chin 2019). The development of military technology showcases that a state seeks relative gains in power to maintain dominance and counterbalance rivals (Waltz 1979). The evolution of military technology can be classified into different stages.

Early warfare relied on direct combat strategies, with heavy use of infantry, cavalry, and siege warfare. The industrialized revolution had evolved mechanized warfare, such as tanks, aircraft, and long-range artillery, which altered battlefield dynamics. With modernization and globalization, military operations have expanded to include cyberattacks, AI-assisted reconnaissance, and precision-guided weaponry, demonstrating a shift from physical confrontation to strategic technological dominance [3]. Moreover, Cyber warfare has emerged as a dominant asset within modern conflict as it has reconstructed traditional military engagement. It became an essential element for state actors providing the capability to disrupt the enemy infrastructure, shape geopolitical strategies without any direct military confrontation, and win intelligence advantages (Khalifeh 2024). Unlike conventional warfare, cyber warfare allows states to exert power asymmetrically through digital systems to weaken adversaries without threatening any conventional military engagement (Marine Corps Association 2023).

The reliance on cyber capabilities showcases the transition from traditional kinetic warfare to a more network centric warfare where success is often measured by a sense of ability to control and defend information systems [6] Cyber warfare tactics include electronic espionage, sabotage of critical infrastructure, and digital propaganda reflecting its impact on military operations [4]. Digital information warfare has evolved into a strategic tool to influence conflicts. States tend to manipulate information to have a sense of control over narratives and weaken the image of their adversary within the public discourse [5]. Platforms such as WhatsApp and Instagram have been weaponized to spread false information and create psychological fear within the public [15].

The evolution of psychological operations showcases the reality of power dynamics where controlling information flow is as important as controlling physical territories. This has extended to the extent where the government and military forces are using AI to influence campaigns and international responses, mobilize public support, and delegitimize enemy morale [7]. As a result, information dominance is interconnected with military strength in modern conflicts [18]. Additionally, hybrid warfare integrates cyber, conventional, and information warfare into a single strategic framework that works on state power and reduces vulnerabilities [21].

This integration is crucial for evolution as it maximizes a state's security while minimizing any military cost and casualties (Waltz 1979). The effectiveness of hybrid warfare is dictated by its ability to blur lines between state and non-state actors through utilizing cyber capabilities, misinformation, and unconventional tactics to undermine opponents [2]. States tend to deploy AI-driven drones, automated warfare technologies, and cyber

infiltration tactics that enhance strategic advantages [3]. This evolution reflects the priority of adapting military doctrine to maintain the relative power in the evolving international system. Digital warfare has extended beyond just a battlefield but integrated itself into global politics, where technological evolution in warfare has become a significant influence in regional balances, alliances, and international conflict resolutions. Technological dominance has become an asset for securing military and economic power in an anarchic international system (Mearsheimer 2001).

States must adapt to emerging technologies as a need to maintain their relative power and deter any threats. In this context, digital warfare has redefined the balance of power, it shifted geopolitical strategies, and influenced diplomatic relations [3]. States tend to invest their resources in cybersecurity, AI-driven defense systems, and automated military capabilities, reinforcing their strategic importance within modern warfare [6]. To delve into this notion deeper, as automation in warfare increases, concerns about reduction in human oversight, unintended escalations, and algorithmic errors present new security and ethical dilemmas [4].

To illustrate, as states begin to develop advanced cyber capabilities to enhance their security, adversaries perceive this as a threat, which drives them to increase their own AI warfare investment, and it becomes a competition within the international arena. This creates an escalatory cycle like the nuclear deterrence that took place within the Middle East in 2003, yet now it's manifested within cyber arms races and AI-driven military strategies [11]. Therefore, the increased reliance on digital warfare as a tool of power projection can become an asset for security and strategic advantage in an anarchic world. As digital warfare remains shaping global power structures, alliances, and conflict dynamics, states need to balance strategic advantage with ethical responsibility, ensuring technological superiority does not cause destabilization or any unintended escalation within future conflicts.

4.2. Technological transformation of armed conflict: Lebanon- Israel (2006-2024)

War is an inevitable consequence of power struggles, national interest, and the anarchic nature of international systems (Waltz 1979). The Lebanon-Israel conflicts of 2006 and 2023-2024 exemplify military strength, geopolitical competition, and technological superiority that shape war outcomes. These conflicts were rooted in history and shaped through regional power struggles, driven by security dilemmas. Each side of the conflict had sought to deter future threats through escalating military capabilities [16]. These wars have highlighted the changing nature of warfare, where in 2006 war relied mainly on conventional tactics such as the guerrilla tactic used by Hezbollah against Israel, while in 2023-2024 war introduced cyber warfare, AI, and precision military operations, which altered battlefield strategies [6].

The 2006 war was triggered by a Hezbollah cross-border raid on July 12, 2006, during which two Israeli soldiers were captured [2]. In response, Israel launched a full-scale military operation on Lebanon targeting Hezbollah positions, Lebanese Infrastructure, and key military sites in the south. The war lasted around 34 days, causing extreme destruction in Lebanon and significant losses. The conflict ended with a United Nations-brokered ceasefire (1701 resolution), which called upon the withdrawal of Israeli forces and the deployment of Lebanese and UN peacekeepers along the border [22]. While the 2006 war was fought mainly using conventional combat strategies, the 2023-2024 War between Lebanon and Israel can be understood as the continuation of a power competition where military strength and technological superiority dictate outcomes. Both wars highlighted a sense of a security dilemma where Israel and Hezbollah (supported by Iran) engaged in military escalation to deter future threats. The Lebanon-Israel conflicts of 2023-2024 were shaped by deep-rooted geopolitical tension, historical animosities, and shifting regional power dynamics [3].

The war in 2023-2024 marked a technological and strategic evolution from previous wars. Unlike 2006, this war was infested with cyber warfare, artificial intelligence, and precision military operations. The introduction of AI-assisted battlefield strategies allowed faster response times, predictive analytics for military operations, and enhanced target acquisition [9] The shift from conventional war to technology driven warfare in 2023-2024 war it demonstrates a future conflict that will not be dealt with through physical battlefield but also in cyberspace and digital information domains, making technology superiority a critical factor within military dominance. The integration of AI within military operations has revolutionized modern warfare, where it has enhanced battlefield decision-making, surveillance capabilities, and precision targeting [6]. The Lebanon-Israel conflict of 2006 and 2023-2024 is a case study of how technological advancements have shifted military strategies. In 2006, the guerrilla warfare and decentralized command provided Hezbollah with a strategic edge. For instance, Israel dependency on the conventional doctrine and airpower demonstrated key limitations. In 2023 -2024, Israel

employed AI-powered missile guidance, cyber operations, and drone warfare to disable Hezbollah's communication and logistics. Hezbollah has adapted by employing encrypted messaging, cyber defenses, and AI-assisted drone swarms, which shows the growing sophistication of non-state actors

4.3. The weaponization of information and infrastructure: the strategic transition in digital warfare

AI had minimal to no presence in the Lebanese-Israeli War. Military operations conducted on Human intelligence, traditional surveillance, and manual decision making were utilized. Conventional artillery and piloted airstrikes were employed with no automation or predictive analysis. For instance, the lack of automated systems translated into slower military decision-making, causing it to be slow and heavily reliant on human interpretation of battlefield conditions [13]. While Israel airstrikes targeted Hezbollah's positions and Hezbollah eventually launched missile barrages into Israeli cities with no evident data processing or AI-driven threat analysis to enhance the target precision [11].

In 2024, AI became a main element used in warfare. AI drones, surveillance systems, and predictive algorithms enhanced the battlefield and shifted the outcomes of the war. It allowed a faster automated response to threats. AI-driven missile guidance, drone swarm coordination, and battlefield simulations replaced many traditional command operations, which made warfare efficient and more precise [9]. This allowed a faster, more precise military response, which allowed less human error in decision making [14]. A key advancement in the 2023-2024 war was the usage of AI-driven missile guidance systems that were automated and self-correcting missile trajectories powered by AI algorithms [6].

This transformation from human-led to AI-assisted warfare in the Lebanon-Israel war is a fundamental shift within military dynamics, where machine learning and automated defense systems have replaced traditional command operations. In 2006, cyber warfare played no significant role in military engagements where both parties fought with missiles, airstrikes, and ground invasions, and their communications relied mainly on radio signals and satellite phones. In 2023-2024, cyber warfare revolutionized the battlefield. Cyberattacks targeted infrastructures, soldiers, military command centers, and financial networks, weakening Hezbollah. Physiological warfare leveraged social media and AI-generated misinformation to delegitimize Hezbollah and control the public perception. In 2006, the military communication was state-controlled and centralized, it relied mainly on traditional media outlets, newspapers, and television to shape both war narratives. Both countries used official press statements to communicate and exert their political legitimacy to ensure the information was contained within a state-controlled framework.

However, in 2023-2024, information warfare shifted from state-controlled narratives to decentralized, real-time digital manipulation. Social platforms such as Twitter and WhatsApp emerged as tools for propaganda. Both states and non-state actors weaponized digital platforms to exert their dominance over the public. The revised information transformed the information sphere into an extension of the battlefield. The evolution of cyber warfare showed its significance within the Lebanon-Israel war in 2023-2024, where digital operations have taken control and cyber-attacks played a decisive role, delegitimizing enemy capabilities and shaping global narratives [6]. This marked a radical departure from the 2006 conflict and expanded to a cyberwarfare that was virtually non-existent, and combat relied mainly on solely on conventional military strategies such as air raids, missile strikes, and ground incursions [2].

Communications in 2006 were mainly dependent on radio transmissions, satellite phones, and even basic encryption techniques, with minimal to no reliance on digital warfare as a military tool. As a result, strategic decision-making was slower. By 2023-2024, cyber warfare had been altered it enabling states to destroy enemy infrastructure, intercept military communication, and manipulate financial systems remotely [3]. AI-powered tools were used for cybersecurity attacks. State-backed cyber operations targeted Hezbollah command centers, logistical networks, and secure communications systems, which caused a disruption in battlefield coordination, leading to leakage in the database, intercepted strategic plans, and altered operational directives, which led to tactical disarray among its forces. One of the major cybersecurity attacks within the 2023-2024 conflict between Hezbollah and Lebanon was the explosion of thousands of pagers within the same second, weakening Hezbollah's members, members, and leaders [19].

Beyond military operations, cyber warfare in 2023-2024 had played a crucial role in psychological warfare and information manipulation. AI-generated misinformation, deepfake videos, and automated propaganda campaigns flooded social media to destabilize Hezbollah's leadership, lower troop morale, and influence regional public opinion [11]. Social media platforms such as Twitter and WhatsApp have become the primary

tools for digital propaganda where fabricated war reports, manipulated images, and bot-driven narratives spread, creating fear and threat within the public discourse [18]. Cyber warfare had extended beyond military and psychological dimensions and impacted financial networks, banking systems, and Hezbollah funding channels, which weakened its ability to finance military operations [4]. Israel was able to freeze financial assets, block international transactions, and disrupt logistical supply chains vital to Hezbollah's war efforts [4].

This Transformation from conventional to cyber warfare has highlighted an increased significance of digital battlespaces in shaping military outcomes. Cyber warfare is no longer a secondary tool that complements military strategies but a primary means of military engagement, allowing states to gain a strategic advantage without deploying thousands of troops [6]. This ability to mobilize and manipulate enemies' military infrastructure and attack financial networks remotely can make cyber warfare one of the most powerful and unpredictable aspects of modern military conflict.

4.3.1. Rise of electronic warfare in the Lebanon-Israel conflict

The evolution of electronic warfare and countermeasure technologies has contributed to shaping the modern military conflict, especially within Lebanon and Israel 2006 and 2023-2024 wars. The contrast between these two conflicts highlights the shift from the conventional era to an electronic-dominated battlefield that determines the outcomes of the war. In 2006, there was minimal usage of electronic warfare, and countering technologies were employed, where limited radio frequency jamming, anti-craft countermeasures, and radar-based surveillance were employed. The warfare remained largely mechanical and human-operated [2]. The absence of sophisticated electronic warfare systems meant the dependency on human intelligence, satellite reconnaissance, and conventional command structures to execute military operations (Norton 2007). However, in 2024, electronic warfare expanded to include GPS spoofing and radar interference. This allowed the forces to deceive enemy targeting systems and disrupt precision-guided weaponry [14]. Israel deployed an advanced cyber-offensive capability, launching a cybersecurity attack on Hezbollah military networks, disabling the communication infrastructure. To illustrate, the cybersecurity attack that was carried by Israel against thousands of Hezbollah soldiers and members began as a sign of the war in Lebanon weakening thousands of Hezbollah martyrs.

This demonstrates how electronic warfare can both serve as a strategic weapon and force multiplier on the battlefield (The Intercept 2024). The war also witnessed a significant advancement in anti-jamming and cybersecurity defenses, which prevented intelligence leaks and secured military communications [4]. The assassination of the spokesperson, Hasan Nasrallah, through a precision-guided airstrike demonstrated how real-time technology and cyber-enabled target tracking can be integrated into decisive military strategies. This assassination shocked Hezbollah and destabilized its internal structures, but also showcased the terror of electronic warfare [9]. Ultimately, the shift from conventional to electronic warfare in 2023-2024 illustrates the increasing role of cyber capabilities, AI-driven intelligence, and digital battlefield operations, which determine war outcomes. This transformation will signal future conflicts that are most likely going to rely on cyber-electronic warfare and autonomous combat systems, which reshape modern military strategies and global security. Strategically, the cyber arms race in the Middle East mirrors the Cold War-era deterrence models. In Iran and Israel, they engage in covert cyber campaigns, where Gulf states invest in AI-driven defense systems. Turkey utilizes the AI-powered drones in Syria, Libya, and Azerbaijan. The following dynamics underscore a shifting regional order increasingly shaped by digital capabilities.

4.4. Quantitative analysis of the rising cost of cyber warfare

Globally, the cost of cyber warfare increases frequently. According to the Center for Strategic and International Studies state state-sponsored cyberattacks have caused an estimated 10.5 billion in global damages in 2023, let alone with more than 60% of these attacks targeting critical infrastructure within conflicted zones such as Syria, Ukraine, and the Middle East [12]. In 2006, the Lebanon-Israel war in Lebanon caused an estimated 3.5 billion dollars in physical infrastructure destruction, primarily from digital infrastructure targeted [8]. In contrast, in 2023-2024 conflict saw Israel employ a comprehensive cyber strategy, which resulted in 1.8 to 2.2 billion in damages to Lebanon both digitally and physically, such as banking systems, mobile communications, and power grids [4]. This financial damage has underscored the increasing economic weight of non- kinetic warfare where the costs where not through the destruction of buildings but through the crippled digital networks, information paralysis, and inaccessible financial assets.

Beyond the financial implications, Cyber and AI warfare have shaped operational dynamics. During the 2024-224 war, Israel's cyber units had disabled 40% of Hezbollah's encrypted logistical communication within 72 hours [21]. This showcases how digital disruption can substitute kinetic occupation. This reflects trends observed within the Russia-Ukraine conflict, where Ukrainians had military analysts who estimated that 70% of early-stage battlefield intelligence was derived from AI-enabled drone and satellite imagery, which reduces the reliance on traditional reconnaissance ([21]). Likewise, the Department of Defense estimates that 80% of recent military decision cycles are included in predictive algorithms and real-time battlefield reinsuring the trend towards algorithmic control of combat operations (DoD 2023).

In parallel, the informational domain has founded a critical warfighting environment. In the Lebanon-Israel conflict, psychological operations conducted through Twitter, Telegram, and WhatsApp had spread misinformation, fake airstrike alerts, and deepfake videos, which are utilized by both parties to influence civilian sentiment and international perception. Moreover, certain tactics tend to affect those employed in Syria, where AI-generated content was deployed to shift blame for chemical attacks and destabilize public trust in real time [24]. While casualty figures are lower within modern conflict, the intensity and complexity of damage in both digital and psychological aspects have increased as adversaries target populations, perceptions, and infrastructures rather than only enemy combatants. According to the NATO 2024 Cyber Readiness report, the member states have increased their cyber defense budgets by an average of 17% between 2020 and 2024. This shows that cyber dominance is equivalent now to the air, land, and sea superiority [25]. This transition requires scholars and policy makers to reevaluate the traditional metrics of military success and consider the ethical, legal. And the strategic implications of technological warfare.

4.5. Strategic and humanitarian implications of cyber and AI warfare: empirical data from the 2023-2024 Lebanon-Israel conflict

The evolution of warfare within the digital world has underexamined consequences for civilian populations, specifically within asymmetrically affected regions in Lebanon. The 2023-2024 conflict between Israel and Hezbollah introduced a new dimension of harm, which is not physical destruction, but widespread systemic disruption. Civilian infrastructure such as schools, hospitals, electricity grids, and banking systems was compromised throughout cyberattacks and resulting in medical equipment failures, halted salary payments, and a loss of access to emergency services [4]. The Lebanese central bank had reported temporary shutdowns of interbank transfers while mobile networks were in a 48-hour blackout within the southern district, cutting off vital information and emergency response (Al Jazeera 2024). The psychological toll of digital misinformation, especially deepfake videos of falsified airstrikes and fake evacuation alerts, had triggered mass panic, displacements, and anxiety among the vulnerable and exposed population [1].

The deployment of autonomous weapons and AI-powered targeting systems has raised the critical questions of accountability and legal oversight. The absence of human intervention has caused certain Israeli drones to strike and cause targeting errors, which led to the bombing of several houses mistaken for Hezbollah safe houses [21]. Human Rights Watch [7] and other advocacy organizations have repeatedly warned that the usage of autonomous weapons violates the Martens Clause, which protects the civilian dignity in situations not clearly covered by existing law [19]. The United Nations also urges the monitoring and regulation of lethal autonomous systems and ensuring the need to legally bind frameworks to ensure meaningful human control over AI-driven weaponry [20]. Within the context of Lebanon, this country is fighting against a long-term developmental setback. The intersectionality of warfare, law, and ethics demands an urgent international dialogue to precisely the weaker states and civilian populations become more vulnerable to non-kinetic yet deeply destabilizing military strategies

4.6. Limitation and counterarguments: the risk of overreliance on AI and cyber dominance

The Study provides an overlay of transformative roles artificial intelligence and cyber warfare has reshaped Lebanon-Israel conflicts, it is important to explore the inherited limitations and ethical concerns that are related

to technologies. Technological superiority is not only a guarantee of strategic success, but rather it is immune to unintended consequences. AI-driven military systems are susceptible to algorithmic biases and systemic errors, which may cause civilian casualties or misguided strikes. The precision system promised by AI often shows the reality that machines are still trying to operate based on incomplete or flawed data, especially in a complex urban environment such as southern Lebanon. Moreover, there is a growing concern where the growing erosion of human oversight in lethal decision making. Moreover, AI handles critical battlefield functions and targets acquisition. The risk of strategic miscalculation increases. The systems might cause the conflict to escalate autonomously, especially in environments that lack clear rules of engagement for automated warfare.

Unlike human intelligence, machine adapts to the cultural and contextual dimension, machine learning tends to lack the capacity for moral reasoning or situational empathy, where both are essential in minimizing collateral damage. Moreover, the alternative explanation for Israel's strategic advantage cannot be overshadowed. Israel had its success in the 2023-2024 conflict, which not only contributed to AI and cyber capabilities. Its robust intelligence and sharing network with Western allies gave its position a push forward within the arena. Hezbollah has challenge in countering Israel's dominance also originates from deep regional isolation, where limited financial infrastructure and asymmetric resource constraints interfere, not only technological inferiority. The shaping of cyber warfare as a golden bullet diminishes the multifaceted realities of military power, which encompasses diplomatic capital, alliances, economic resilience, and ideological mobilization. Therefore, while AI and cyber technologies remain essential for the battlefield yet their integration. It must be understood as a part of a broader matrix of power, and battlefields still rely on human agency, economic capacity, and geopolitical alliances.

5. Discussion

The comparative analysis between the 2006 and 2023-2024 Lebanon-Israel war demonstrates the profound strategic shift that occurred within modern warfare. The 2006 conflict has been constructed by traditional combat and limited technological integration, while the 2023-2024 war illustrates the dominance of artificial intelligence, cyber operations, and digital information warfare. This transformation is structural and constructs how states tend to conceive and execute military engagements. Through a realist perspective, the transition to a technology-driven battlefield had mirrored the continuous quest for relative power in an anarchic international system.

Technology superiority and dominance have become a determinant of battlefield success, allowing rapid decision-making, psychological manipulation, and infrastructural damage. The incorporation of AI-powered surveillance, missile guidance systems, and cyber-espionage during the 2023-2024 conflict provided Israel with crucial strategic depth and flexibility, especially in targeting Hezbollah's command networks and financial systems. Whereas Hezbollah's shift to encrypted communications and AI-assisted drone swarms portrays how non-state actors can adapt to a new warfare paradigm.

An important pillar is that cyberwarfare is no longer an auxiliary to military strategy; instead, it is central. Information dominance now parallels territorial control. The weaponization of social media platforms such as Twitter and WhatsApp shows the real-time psychological warfare and misinformation campaigns demonstrate how the battlespace has expanded to the civilian digital arena. The following areas blurred the lines between Military and non-military targets, raising ethical and legal concerns under international humanitarian law. The transition into a broader sense of cyber arms race within the Middle East, where states such as Iran, Turkey, and Israel challenge each other towards Technological dominance and hegemony within the area.

As AI-driven systems tend to replace traditional military hierarchies, there is a growing sense of concern over algorithmic escalation, unintended consequences, and the decrease of human oversight in lethal decision-making. The developments echo Cold War deterrence models but also work within a less regulated cyber domain, increasing the risk of miscalculation and unchecked escalation. This discussion illustrates that future

conflicts will be categorized by invisible, instantaneous engagements not labeled by frontlines through data streams, algorithmic commands, and cyber vulnerabilities. The Lebanon-Israel case study is an example for analyzing how technological evolution redefines military doctrine, international law, and regional stability, calling for new regulatory frameworks and strategic foresight in global security planning

6. Conclusions

This study has tackled the transition from conventional warfare to a technology-driven battlefield through a comparative analysis of the Lebanon-Israel wars in 2006 and 2024. Through incorporating a realist perspective, the research highlighted how state and non-state actors continuously adapt their military strategies in response to technological advancements to maximize their power and dominance within the international arena. The finding reveals the nature of warfare within the Middle East, particularly Lebanon and Israel, transitioned from traditional military engagement involving guerrilla tactics, ground incursions, and airstrikes to a high-tech confrontation featuring artificial intelligence, cyberwarfare, and electronic countermeasures. This shift showcases the increasing militarization of cyberspace and automation, where digital capabilities are becoming as important as physical forces.

The 2023-2024 Lebanon-Israel war is the most evident example of how cyber warfare and AI-powered military applications have reshaped battlefield decision-making, targeting precision, and real-time intelligence processing. Unlike in 2006 where human intelligence and conventional tactics were dominant. The study reinforces the notion that future conflicts will not rely on physical force only, but will begin determining their outcomes using digital and cyber technology to enforce their power and dominance. The role of technology in military strategy is now inseparable from geopolitical power struggles as states begin to leverage cyber-attacks and AI-driven battlefield management to gain advantage, as it allows them to deter threats and maintain relative power within the anarchic international system. The warfare in 21 century has been determined through AI, cybersecurity, and digital misinformation: creating more challenges for global military and blurring the boundaries between conventional and cyberwarfare. This has positioned technology as an asset to every factor in military dominance. Policy recommendations tend to arise from analysis that incorporates the need to regulate AI in warfare under international law and instigates cyber norms to prevent escalation when cyberattacks include acts of war.

This study fills in a crucial research gap by offering a rare longitudinal comparison of conventional versus digital battlefield dynamics within a dyadic conflict zone (Lebanon- Israel). It illuminates the evolving nexus of cyberwarfare, regional security, AI, and provides a valuable empirical foundation for future work within security studies, hybrid warfare strategy, and Ai conflict modeling. Through technological escalation increasingly analyzes asymmetric conflicts, this paper aims for a greater integration of AI and cyber dimension into strategic stability theory and the security planning framework. The deployment of autonomous lethal systems tends to raise concerns about miscalculation risk. Future research must explore the role of AI through post-conflict reconstruction, through predictive conflict modeling, and its impact in other asymmetric conflicts such as Syria, Yemen, and Libya. As autonomous systems develop, they both tend to reduce casualties and increase the risks of strategic miscalculation. Therefore, Modern Battlefield is transitioning into a more powerful and technology-driven warfare, influencing and changing the trajectory of several wars in the upcoming years..

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

References

[1] M. Barazy, "The role of 'Online' in the Israel-Lebanon Conflict: A study of accounts and cyber warfare," NowLebanon, Oct. 15, 2024. [Online]. Available: https://nowlebanon.com/the-role-of-online-in-the-israel-lebanon-conflict-a-study-of- accounts-and-cyber-warfare/

[2] S. Biddle and J. A. Friedman, "The 2006 Lebanon campaign and the future of warfare," U.S. Army War College Press, 2008. [Online]. Available: https://press.armywarcollege.edu/monographs/641/

[3] Daily Sabah, "Middle East: Battleground of high-tech war," 2024. [Online]. Available: https://www.dailysabah.com

[4] Financial Times, "The Future of AI in Military Conflict and Cyber Warfare," 2024. [Online]. Available: https://www.ft.com

[5] Institute for the Study of War, "Israel's victory in Lebanon," [Online]. Available: https://www.understandingwar.org/backgrounder/israels-victory-lebanon

[6] Z. Kallenborn, "Artificial intelligence and arms races in the Middle East," Taylor & Francis, 2024. [Online]. Available: https://www.tandfonline.com

[7] Human Rights Watch, "Stopping Killer Robots: Protecting Civilians from Autonomous Weapons," 2023. [Online]. Available: https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and

[8] E. Kotia, "The Lebanon-Israel war of 2006: Global effects and its aftermath," 2014. [Online]. Available: https://works.bepress.com/emmanuel_kotia

[9] Marine Corps Association, "Technology and the nature of war," 2023. [Online]. Available: https://www.mca-marines.org

[10] J. Masters, "Lebanon: How Israel, Hezbollah, and regional powers are shaping its future," Council on Foreign Relations, Jan. 27, 2025. [Online]. Available: https://www.cfr.org/backgrounder/lebanon-how-israel-hezbollah-and-regional-powers-are-shaping-its-future

[11] M. M. Matthews, "We were caught unprepared: The 2006 Hezbollah-Israeli war," U.S. Army Combined Arms Center, 2008. [Online]. Available: https://www.armyupress.army.mil

[12] K. and K. Mnejja, "Israel's digital assault on Lebanon," The Tahrir Institute for Middle East Policy, Dec. 4, 2024. [Online]. Available: https://timep.org/2024/12/04/israels-digital-assault-on-lebanon/

[13] A. R. Norton, "The Israel-Lebanon war and its implications for regional security," JSTOR, 2007. [Online]. Available: https://www.jstor.org

[14] A. J. Staff, "How did Hezbollah's pagers explode in Lebanon?" Al Jazeera, Sep. 18, 2024. [Online]. Available: https://www.aljazeera.com/news/2024/9/17/how-did-hezbollahs-pagers-explode-in-lebanon

[15] The Intercept, "Disinformation, Cyber Attacks, and Electronic Warfare in Middle Eastern Conflicts," 2024. [Online]. Available: https://theintercept.com

[16] U.S. Army War College Press, [Online]. Available: https://press.armywarcollege.edu

[17] United Nations Office for Disarmament Affairs (UNODA), "Regulating Lethal Autonomous Weapons Systems," 2024. [Online]. Available: https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on-laws- in-the-ccw/

[18] Center for Strategic and International Studies (CSIS), "Global Cyber Threat Report," 2024. [Online]. Available: https://www.csis.org/topics/cybersecurity

[19] E. Kotia, "The Lebanon–Israel War of 2006: Global Effects and Its Aftermath," 2014. [Online]. Available: https://www.academia.edu/52683096/The_Lebanon_Israel_War_of_2006_Global_Effects_and_its_Aftermath

[20] Financial Times, "The Future of AI in Military Conflict and Cyber Warfare," 2024. [Online]. Available: https://www.ft.com/content/fe136479-9504-4588-869f-900f2b3452c4

[21] K. and K. Mnejja, "Israel's Digital Assault on Lebanon," Tahrir Institute, 2024. [Online]. Available: https://timep.org/2024/12/04/israels-digital-assault-on-lebanon/

[22] Ukrainian Ministry of Defense, "Battlefield Intelligence Report," 2023. [Online]. Available: https://mod.gov.ua/en

[23] U.S. Department of Defense, "AI Integration in Military Decision-Making," 2023. [Online]. Available: https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/

[24] Brookings Institution,"Weaponized Misinformationin Modern Warfare," 2024. [Online]. Available: https://www.brookings.edu/articles/how-do-artificial-intelligence-and-disinformation-impact-elections/

[25] NATO, "Cyber Readiness Report: Strategic Investments in Digital Defense," 2024. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_78170.htm

[26] Global Conflict Tracker, "Conflict with Hezbollah in Lebanon," [Online]. https://www.cfr.org/global-conflict-tracker/conflict/political-instability-lebanon