ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

THE WAR OF DIGITAL ERA: ROLE OF AI IN IRAN-ISRAEL CONFRONTATION

Muhammad Rizwan Majeed[1]*, Muhammad Imran Majeed[2], Dr. Imran Ali[3]
[1,3]Department of Pakistan Studies, The Islamia University of Bahawalpur, Pakistan.
[2]Department of History, The Islamia University of Bahawalpur, Pakistan.
Corresponding Author: Email: mrizwanmajeed78@gmail.com

Abstract
The use of artificial intelligence has transformed military strategy and national interest preservation due to its rapid integration and improvement into valuable supplies. A key aspect of recent developments is the growing reliance on Artificial Intelligence (AI) and integrated algorithms in shaping modern military strategy. This study used the descriptive research method to explore the Iran-Israel war and the uses of AI technology. Israel employs Artificial intelligence and its integrated algorithms in its military as a military strategy to predict aerial targeting and utilize drone systems. Israel has a technological edge in the military systems applied in artificial intelligence, while having technological edge of military combat systems. Iran, despite economic constraints, has developed strong asymmetric capabilities through cyber warfare, UAVs, and AI-enabled proxy networks. This evolution has turned their longstanding conflict into a technologically advanced confrontation defined by speed, automation, and increasing unpredictability.
Keywords: *Israel, Iran, Warfare, Security, Technological Advancements, Cyber security, Artificial Intelligence*

Introduction of AI in Current Era

Artificial Intelligence has gone through three main phases during the past 70 years. Initially, it consisted of rudimentary systems, developed as expert systems, which incorporated decision trees, Boolean logic and fuzzy logic. In the second period, systems went through a statistical shift which fuelled functions as Machine Learning, enabling the devices to be incorporated into the operational framework of spam filters and search engines. In the contemporary scene, the focus has shifted to a more sophisticated level aimed at emulating the human learning system, which utilizes neural networks and deep learning, thus enabling the systems to achieve advanced sensing and perception. Existing systems are expected to be even more advanced and to include technologies such as neuromorphic computing which emulates the human brain and adversarial material which seeks sensitive data embedded in AI systems. Through the years, considerable attention to the advanced technologies has been necessary to ensure the systems are high functioning in the fields of defense and strategy. (Science & Technology Organization, 2020)

AI as Autonomously Guard

AI has expanded the capabilities of machines so that, rather than simply carrying out instructed tasks, they can perform autonomously and make their own critical (and sometimes, unilateral) decisions. Self-operating machines have assumed roles and made decisions within Intelligence Gathering, Surveillance, Reconnaissance, and Cyber-Security (Roberts, 2022).

AI and ML both dual use technologies, but they are particularly effective when used for offensive operations. Major military powers are integrating intelligent systems into their operations for enhanced situational awareness. Nations are streamlining data to devise strategies through cyberspace, and the collected information is being used to optimize the processes involved in making decisions (Dayal, Garg & Shrivastava, 2014).

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

As long as leading technologically advanced states continue to incorporate various new technological innovations into their military practices and attempt to gain new adaptive advantages associated with their control over worldwide military dominance, a change, or new shift, of a military strategy will be apparent and inevitable. The integration of Artificial Intelligence and Machine Learning into new defense systems technology, in particular, new advanced technological military defense systems, is intended to help mitigate the defense technology systems risks associated with new adversaries and military defense systems, in particular, new technologically adversaries who, in contrast, possess a lower technological defense military systems capability. Increased attention within defense and military systems strategies has focused upon the autonomous systems as well as self-operating systems and military command & control such that the systems can avoid unintended harm (collateral damage) while maximizing independence and autonomy within the Observe Orient Decide Act (OODA) loops for defensive and offensive military engagements, and provides for greater operational freedom and latitude and flexibility in the execution of warfare and combat actions.

As a result of this, other military and defense systems of other great leaders and powers have manually accelerated and increased their own military and defense systems strategies in a manner designed to outdistance and outpace their most significant and primary adversaries. One significant common aspect of their military doctrines is the concept of the incorporation of self and autonomous systems and military command & control systems with advanced algorithmic strategy to provide the front lines of battle combat formations and units with advanced military systems that incorporate military tactics and technologies of high energy kinetic and directed energy (HEWD) weapons systems (Cummings, 2017).

AI in Modern Warfare

Advancements in strategy, technology, and methods of operation have transformed the scope of warfare. Artificial Intelligence (AI) is one of the most recent and most profound changes in the way the technology of the military is viewed. The introduction and incorporation of AI in military technology is not merely a step forward technologically but a profound change in the way military organizations function, make operational decisions, and fight wars. This change, and especially the introduction of previously unheard-of technologies, improves the operational efficiency, speed, and the quality of decision-making made in warfare. AI is the most recent of the technologies to have a profound and disruptive impact on military strategy and the conduct of warfare (Scharre, 2018).

An essential attribute of AI is its ability to handle large volumes of information, recognize trends, and provide actionable predictions. This ability assists military institutions in threat forecasting and threat mitigation. One of the most impactful outcomes of AI is the development of autonomous weaponry, or as is commonly termed, ‘killer robots.’ Such weaponry can, either fully or partially, make operational decisions that determine the use of resources to quantify targets and open fire. Drones and similar technology can autonomously determine if and when to attack and remove the necessity for human oversight (Binns, 2018).

Although the potential to increase operational efficiencies and grant protections to human combatants wins the support of the military, the developments provoke ethical and legal disputes of an alarming magnitude. The legal consequences of an attack by autonomous weaponry are of immediate and extreme consequence. Who, if anyone, is culpable: the military officer in command, the programmer, or the weapon itself? These disputes adjust the boundaries of legal frameworks and the core assumptions underlying the law of armed conflict (Cummings, 2017).

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

The implementation of AI technologies is modifying the manner in which the military functions. Analysts in the military report that there is an increase in the use of AI technologies by military leaders for the purposes of planning and analyzing the military situation. Predictive AI technologies use data sets comprised of communication patterns, data exchanges, and information to provide military leaders with guidance regarding. A military AI system provides data and predictions to defensive military systems so that the military implements proactive rather than reactive defensive strategies. Military AI systems are developed to reduce the mental strain and military cognitive effort of analyzing therefore, strategizing, and planning by automating processes. Military AI systems classify and conduct primary data analysis to provide synthesized data for military strategists to develop strategies at higher mental prioritized tasks (Kott and Linkov, 2021).

Nevertheless, a time sensitive critical environment demonstrates how these systems form multiple of these layers into a structure that can accomplish significantly complex tasks which can save a vast amount of time. Nonetheless, these systems are complex. Autonomous systems can classify and analyze data to provide an automated military analysis. Military predictive analysis can provide a military with a broad analysis of a conflict and offer guidance on how the military can use offensive or defensive maneuvers. Unfortunately, there is a broad range of military analysis systems and military prediction systems, so it can be difficult for a military to classify what type of system is which. Predictive military analysis systems can provide or offer military guidance without the use of offensive weapon systems. Predictive military analysis systems can provide or offer guidance on how to use offensive military weapon systems in ways that can increase the prediction of military guidance. Predictive military analysis systems can provide or offer guidance to a military on how to increase the expected outcomes of a conflict (Sparrow, 2007).

Considering these gaps, it is important to find a sweet spot between efficiency and moral duty in military organizations. Deontological and consequentialist approaches need to be integrated more rigorously in the design and use of self-functioning military systems. This would involve the delineation of autonomy, the imposition of substantive control, and the promotion of AI explain ability. These systems need to be integrated in ways that align with the principles of international humanitarian law (IHL) and the prudent use of military self-functioning systems (Sparrow, 2007). This is where the AI contestable systems become pertinent to IHL, and especially to the humanitarian principles of necessity and proportionality.

On the other hand, the AI systems being developed and deployed have no geographical, political, or national boundaries. Autonomous military systems pose threats that no single State can solve on its own. IHL gives States the ability to negotiate and collaborate on military engagements, and that is what is needed here. Robust defenses on military self-functioning systems are needed on a multilateral basis. Dialogue between States, International Organizations, Civil Society, and Experts is valuable, perhaps even pivotal, in setting and maintaining lower standards of acceptable IHL. These collective efforts, as Scharre reminds us, are paramount to dealing with the proliferation of autonomous systems thoughtfully and effectively (Scharre, 2018).

Perhaps the most significant change in the history of warfare comes from the AI integration into warfare. While operational and strategic improvements are of great importance to a military, the legal, ethical, and security implications of AI in warfare are also of great importance. Militaries are going to have to continue to take a balanced and responsible approach to AI if they are going

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

to continue to protect the principles of humanity and the norms of the international community in a developing global security environment.

AI as Intelligence Tool

AI assists in informed decision-making through comprehensive data evaluation and forecasting outcomes. Algorithms can recognize and learn from various datasets and utilize different structures of neural networks. Text data is processed using Natural Language Processing which is crucial in visioning and prophesizing Analytics. These Functions of Analytics empower institutions to determine consequences predetermining the necessary actions. AI has the capability to examine and draw conclusions from mammoth amounts of data and has an impact on the revolution of industries and intelligent strategically progress (Davenport & Ronanki, 2018).

Precision of AI

Because of the data-driven approach as opposed to working off of instinct or intuition, AI has the ability to improve the accuracy of decision making. In an example from the manufacturing industry, AI-powered quality control systems are able to find defects more reliably than manual quality control inspections would do, therefore, decreasing the amount of defects produced and, in turn, decreasing waste (Adams, 2020).

AI has the ability to improve the accuracy and speed of decision making as a result of being able to automate the analysis of data and provide analysis in real-time. As an example from the logistics industry, AI has the ability to optimize supply chains to provide more efficient and faster processes within the industry. This is done through demand forecasting, inventory management, and efficient route planning (Silver et al, 2017).

There is no doubt that AI has a number of advantages, the primary of which include road and departure automation on a number of supply chain and freight transport functions. There are primary ethical concerns with the use of AI in industry, the primary being fairness and bias concerns. AI systems are able to soften inequitable conditions in society, to sustain or amplify inequitable outcomes, and to give outcomes that are inequitable, with little evidence or socio-historical context to sustain such inequitable outcomes.

The Iran–Israel Conflict: A Historical Analysis

From Cooperation to Confrontation

The ties between Iran and Israel have not always been the same. Iran and Israel have not always had the same view of Israel either. In 2002, Fallahnejad started by explaining that the state of Israel was opposed by Iran. The United Nations, Israel, and other countries around the world proposed the creation of Israel. In 1947 and 1949 the United Nations proposed and voted for resolution 181 and 303. Israel was created, and the other countries around the world and in the Middle East approached Israel with condemnation.

In the history of Israel and Iran relations, there have been many changes. In 2002, Fallahnejad documents Iran's first opposition. In the United States, Israel and Iran have had to create a strategic partnership. Keeping in line with the strategy mentioned, the two countries have been pretty effective in hindering the foreigners like USSR. In the 70's an arms deal estimated to be 500 million was made, and Israel and Iran reached and oil deal. In the 60's to the 70's Iran was Israel's top supplier of oil, and Israel was to Iran military arms. It was top secret to avoid opposition within the countries.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

Iran-Israel since Revolution 1979

The 1979 Islamic Revolution caused the first Iran-Israel conflicts. Ayatollah Khomeini's first Iran-Israel confrontation focused on Iran's new positioning in the Islamic world. He characterized Iran's new ideological stand as the protector of all Muslims and oppressed people. He referenced the Palestinians as primary (Saniabad, 2012). With the Revolution came officially anti-Israel policies, which dominated the Iran Pahlavi era's foreign policies, which focused on diplomacy and maintaining national interests.

Role of AI in the Iran–Israel Hostility

The Stuxtent Operation: Operation Stuxnet, a joint undertaking by Israel and the United States in 2010, stands as the first of its kind in the realm of cyber warfare by targeting and successfully neutralizing a key element of Iran's nuclear program. The attack intricately employed a combination of a trojan and ransomware designed to achieve cyber fragmentation, espionage, and degradation, and was focused on the Natanz Nuclear Facility (Kamiński, 2020).

In the beginning, Iran was simply dismissive of the attack and rationalized the disruptions as the result of human or technical faults, which, without the risk of traditional military engagement, cyber-attacks gain most if not all of their success through human or technical faults, whereas cyber-attacks gain most if not all of their success through traditional military engagement.

Meanwhile, the stuxnet attack exposed the weaknesses and vulnerabilities of a nation's cyber security system. The attack was so significant that it impacted the defensive stances of Gulf States and their collaborations with Israel under the Abraham Accords. In an attempt to mitigate the influence of Iran in the region, countries like the UAE and Bahrain, to stabilize the region, sought collaborations with Israel. This was primarily focused on the developing defensive strategies of Israel and Israel (ACW, 2023).

Iran's 2020 attack: Iran's assaults on Israeli cyberspace began in April 2020, when the Islamic Republic of Iran attempted to manipulate the chlorine levels in Israeli water treatment facilities. These attempted cyber intrusions triggered the cyber dimension of the Iran-Israel conflict. The cyber-attack on Israeli facilities resulted in a health risk and a level of chlorine is used to disinfect water. Chlorine levels to The Iranian cyber operatives accessed and manipulated the chlorine levels in the Israeli water control and data acquisition (SCADA) system. The attack was sophisticated and dominoed from an on-the-ground intelligent reconnaissance of the Israeli cyber defense (Staff, 2020).

Fortunately, these intrusions were detected in real time by the Israeli cyber national defense authority. This agency acted quickly to avert a health disaster, reflective of the evolving cyber conflict warned by Yigal Unna, the cyber defense director describing the attack as the start of a "A cyberspace attack targeting the Iranian adversaries is a challenge to Israel Iran's enemies. Water infrastructure is usually among the less vulnerable parts of a Nation's cyber defensive matrix. This cyber vulnerability of a nation constitutes a neo military strategy of cyber-attacks on economically less developed than the attacker (Al-Jazeera, 2020)

According to defensive realism, Iran's incursion shows how cyber strength can be weaponized to deter an attack. As a response, Israel has also conducted counter-measures by executing a cyber-attack on an Iranian port facility linked to trade, thus completing the cyber tit-for-tat. Since then, both Israel and Iran's cyber conflict has escalated to the targeting of strategic military and health assets, finances, and the nuclear infrastructure (Al-Jazeera, 2020).

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

Iran and Middle East

Iran's recognition of the importance of Artificial Intelligence (AI) and cyber warfare as pathways to technology advancements with counter rival powers has caused Iran to heavily invest into the tech advancements for countering rival powers. Iran's influence and power across the Middle East has been augmented due to the ability of cyber warfare.

Enhancing strategies: Cyber warfare is used to augment strategies with Middle East and the IS used with Israel (proxy) battles. Iran is able to influence and control of power hostilities without official conflict. Proxy battles with Hamas, Hezbollah and Houthis focus on Iran's control and ability to influence dynamics of the Middle East (Hassenstab, 2024).

AI-Enabled Cyber Actions

Hezbollah and some members of the Iranian Revolutionary Guard Corps (IRGC) employ artificial intelligence cyber and tools to gather intelligence, plan operations, spread propaganda, and expand their reach in the area. Iranian cyber operations most often concentrate on cyber disruption psychological warfare of minimal expense and a signal of the potential for escalation. Defacement of web pages, distributed denial of service (DDoS) attacks, misinformation, and deepfakes of political and other influential people, as well as social media campaigns, are examples of the techniques. To diffuse politically and cohesively in the region, anti-Israel and anti-Western narratives are created (VOA News, 2024).

Cyber-attacks on Regional Foes

Given the perceived threat of Israel's control of cyber systems and artificial intelligence, coupled with psychopathy, a form of cyber defense and retaliation has been developed. Among the Hackers targeting Israel's arenas of finance, including banks and stock exchanges, the target is to instigate a loss of control over monetary finances. In relation to Israel and the USA, the Gulf States, most notably the UAE, and Saudi Arabia, are regular-but- minor cyber target Fiends of Iran. The 2012 Shamoon Attack' is a classic example of targeting Saudi Arabia's Aramco. In this case, 30, 000 systems were interlinked, and with the aid of drop malware, critical documents in the target systems were permanently deleted (Incident of the Week, 2018).

Consequences and Defensive Realism

Iran's cyber strategy is determined by how defensive realism posits and explains the challenges it perceives at the regional level and how it rationalizes the application of cost effective and impactful means in neutralizing threats. At the same time, Gulf States face a security dilemma: they are more secure, but at the same time they are more exposed to Iranian cyber aggression. This illustrates the greater sophistication of cyberspace, AI, and conflict in the Middle East, where technology is clearly a game changer in determining the relative power of states and controlling their interactions.

Regional and Global Security

The expansion of AI and cyberspace technologies is a major game changer in the security of the Middle East and the world. The impetuous growth of AI is a core driver of the arms race, cyber vulnerabilities, uninhabited battlefields, and the proliferation of autonomous weapon systems. The unregulated proliferation of AI technologies, more than the potential for advanced surveillance and cyber defense, creates the greater risk of conflict, especially for weaker states (UNIDIR, 2025).

The Stuxnet operation demonstrated how poorly protected Iran's cyber systems were, which caused Tehran to rapidly improve its cyber systems to counter Israel and the United States in the following ten years (Work, 2020).

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

Iranian cyber operations increasingly expanded to the Gulf States due to their lower level of protection. Iranian cyber specialists also taught operatives to carry out attacks, such as the 2015 Yemeni cyber army, which targeted the Saudi foreign minister and subsequently leaked classified documents. These outcomes altered the regional distribution of cyber power in favor of Iran (Mohee, 2023).

The Gulf has long been a prime target for cyber-attacks, as new tech capabilities, which were also very rudimentary, introduced new weaknesses. In spite of spending on cyber security, it appeared too many of the Gulf States, Saudi Arabia being the more prominent, that they still did not have a full national system in place. Potomac Institute 2017 Report stated that Saudi Arabia has been more than out; it has been under prepared in the more primary elements of cyber readiness. Lack of cohesion on cyber strategies among ministries, corporations, and institutions severely limited the security of the country (Hathaway, Spidalieri, & Alsowailm, 2017). The phishing and malware attacks intensified cyber threats during the COVID-19 pandemic (Alexander, 2020).

Israeli-GCC Cyber Cooperation

Recognizing Israel's advanced capabilities in the cyber realm, particularly the UAE, sought to acquire such expertise to bolster the regional cyber security architecture even before the Abraham Accords. Israeli-GCC collaboration sought to address cyber gaps associated with potential Iranian threats and enhance protection to critical infrastructures (Fenton-Harvey, 2019).

There is no question that the Israeli contribution in the realms of intelligence and cyber security has begun to effect positive shifts in the cyber balance of power within the Arab World, hence altering the strategic equilibrium in the region.

Lessons for Regional Powers: Pakistan

Iran and Israel's rivalry in autonomous weapon systems (AWS) and AI military technology is particularly worrisome and poses potential threats to regional security. The AWS technology, which is a core component of modern warfare, poses numerous ethical, legal, and operational challenges on its own. The growing deployment of such systems has further Israel's and Iran's already volatile rivalry and has the potential to destabilize the Middle East and the surrounding region (Gross, 2021).

It is within Pakistan's strategic environment that impacts from conflicts in other regions of the world and the technological advancements associated with them, become sufficiently important to justify modifying an adversary's military strategy and operational concepts. Geopolitically, Pakistan is in Middle East which makes it part of the power equation, and thus the new multifaceted threats to security that come within the power equation in the Middle East. The developments and possible deployment of AWS by Israel and Iran compel Pakistan to consider changes to her defense stance and the threats she considers to be regional. From the defensive Realist perspective and within the context of the Middle East, the advent of military innovations based on Artificial Intelligence (AI), Pakistan is left with little choice if the focus is the protection of her national security. Pakistan is constrained to enhance her national security through improved surveillance mechanisms, improved collection of intelligence, and a more sophisticated level of strategic defense planning (Anwar, Mumtaz, & Mateen, 2023).

Essentially, the conflict also shows the negative security environment in which technological advancement in one region will lead to technological the advancement in defense and more sophisticated military strategy in adjacent regions and lead to a focus on a more sophisticated military defense in the region.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

AI and the Future of Warfare

Reports from the United States Department of Defense indicate military applications of Artificial Intelligence AI include autonomous weapons and cyber-talk, message and AI in military command structures. Military headship will be enhanced by AI in predictors of operations in combat and out of combat and in strategies and military command seen in Austin operations protocols of cyber security AI (Hanlon 2018).

Ethical, Legal, and Strategic Challenges

The incorporation of AI and LAWS in the military systems brings about complex problems and the rules and ethics that go with them. Different states have different algorithms, and military autonomous systems can malfunction in several ways. This could escalate the violence of a conflict and harm innocent civilians. Less human control in command-and-control systems can increase the range of unanticipated escalations in a crisis. This risk brings about the question of how autonomous systems would have acted, even in near-historic catastrophes, like the case of the Cuban Missile Crisis (Hanion, 2018).

AI Arms Race and Proliferation Risks

The rapid development of AI-integrated software and hardware indicates that the technological AI arms race has already begun. In contrast to the Cold War and the race toward nuclear armament, the tide of AI technologies will be even less controllable, as they can be developed and exploited by anyone, at very low cost, and with widespread software access, including non-state actors. This situation will intensify the global security paradox and diversify the range of techno-economic inequalities between countries that can deploy AI and those that cannot (Jamy, 2021).

Impact on Nuclear Stability

There are new strategic risks as a result of the new AI technologies that affect delivery systems, and dominate the command, control, and control of nuclear weapons systems. Machine learning improvements that are even on the nuclear balance of power will either destroy or stabilize the balance; however, the most opaque and problematic area is the influence of machine learning on nuclear systems. As a result of the opposition of the Great Powers (USA, Russia, India, and Israel), attempts to create international control AI warfare norms, including the CCW under the UN, have simply collapsed (Boulanin & Saalman, 2020).

Conclusion

The implementation of AI technology such as computer-driven predictive analysis, surveillance, and targeting has improved the response time and accuracy of attacks. The innovations that characterized this technology have also made the responses and attacks of both sides faster, regardless of the human consequences of the war. The automated targeting and combat system accelerate the response and the attacks with no human consequences or warfare considerations to slow the combat down.

The use of AI tools in warfare systems has led great increased operational accuracy on both side of the conflict; it has increased the strategic uncertainty dramatically. The absence of systemic adaptation and the lack of transparency have made AI combat systems more error prone. The risk of collateral damage has increased greatly and the expectation that systems will work as described is, in fact, adding to the risk greatly. This is particularly true in Iran and Israel proxy warfare with direct cyber-attacks and covert warfare. In this case, the incorporation of AI is almost certain to cause even more impreciseness and defiance of deterrence.

Smart warfare can also significantly aid in peacekeeping and in the reduction of civilian collateral. The increased operational efficiency offers improved opportunities to create safe civilian zones during combat. New routes of peacekeeping will, however, open new routes of conflict as traditional diplomatic routes will no longer fit the global ecosystem of warfare. The continued conflict between Iran and Israel and the introduction of combat AI tools will, however, open new routes of confinement. Peacekeeping will certainly require new frameworks to avoid inadvertent conflict.

References

ACW, 2023. Assessing the Abraham accords, three years on. Retrieved from https://arabcenterdc.org/resource/assessing-the-abrahamaccords-three-years-on/ retrieved on 11 August 2025.

Adams, R. G., 2020. The impact of artificial intelligence on decision-making processes in healthcare. *Journal of Healthcare Management*, 65(3), 187-195.

Alexander, K. 2020. Israeli-Gulf cyber cooperation. *Modern diplomacy*, *23*.

Al-Jazeera. (2020, May 19). Israel cyberattack caused 'total disarray' at Iran port: Report. Al Jazeera news. Retrieved 1 07, 2025, from https://www.aljazeera.com/news/2020/5/19/israel-cyberattack-caused-totaldisarray-at-iran-port-report retrieved on 7 October 2025.

Al-Jazeera. (2020, May 19). Israel cyberattack caused 'total disarray' at Iran port: Report. Al Jazeera news. Retrieved 1 07, 2025, from https://www.aljazeera.com/news/2020/5/19/israel-cyberattack-caused-totaldisarray-at-iran-port-report retrieved on 15 July 2025.

Anwar, A., Mumtaz, T., & Mateen, M. (2023). Evolution of Security Paradigms in Pakistan: Assessing Contemporary Challenges to National Security. *Asian Innovative Journal of Social Sciences and Humanities*, *7*(4).

Binns, R. (2018). Fairness in machine learning: Lessons from political philosophy. In Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency (pp. 149-158). ACM.

Boulanin, V., & L., Saalman, 2020. "Artificial Intelligence, Strategic Stability, and Nuclear Risk" SIRPI, June 2020, Available at: https://www.sipri.org/sites/default/files/2020-06/artificial_intelligence_strategic_stability_and_nuclear_risk.pdf retrieved on 22 Decemer 2021.

Cummings, M. L. (2017). Artificial Intelligence and the Future of Warfare (Research Paper). *International Security Department and US and the Americas Programme-January*.

Cummings, M. L. (2017). Automation and accountability in the digital age. *Journal of Military Ethics*, 16(3), 177-197.

Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. *Harvard Business Review*, 96(1), 108-116.

Dayal, M., Garg, S., & Shrivastava, R. (2014). Big Data: Road Ahead for India. *Indore Management Journal*, *6*(2), 1-14.

Fallãhnejãd, A., 2002. Iran-Israel Relations under the Second Pahlavi (Tehran: Islamic Revolution Document Center, 120.

Farhang, M. (1989). The Iran-Israel Connection. *Arab Studies Quarterly*, 85-98.

Fenton-Harvey, J. (2019). UAE-Israel Cyber-Spying aids Emirati influence and repression. *Inside Arabia*, *27*.

Giannopoulos, G. A. (2021). AI in military operations: Potential and risks. *Journal of Defense Studies and Resource Management*, 9(1), 45-60.

Gross, J. A. (2021). Israel's Artificial Intelligence and Autonomous Weapon Systems Strategy. *The Jerusalem Post*. https://www.jpost.com retrieved on 12 September 2025.
Hanion, M. O., 2018, "The role of AI in future warfare" Brookings, November 29, 2018. https://www.brookings.edu/research/ai-and-future-warfare/ retrieved on 22 December 2021.
Hanion, M. O., 2018, "The role of AI in future warfare" Brookings, November 29. https://www.brookings.edu/research/ai-and-future-warfare/ retrieved on 22 December 2021.
Hanion, M. O., 2018. "The role of AI in future warfare" Brookings, November 29, 2018. https://www.brookings.edu/research/ai-and-future-warfare/ retrieved on 22 December 2021.
Hassenstab, N. (2024, February 5). Understanding Iran's Use of Terrorist Groups as Proxies. American University. Retrieved on 8 January 2025. https://www.american.edu/sis/news/20240205-understanding-irans-use-ofterrorist-groups-as-proxies.cfm retrieved on 18 October 2025.
Hathaway, M., Spidalieri, F., & Alsowailm, F., 2017. *Kingdom of Saudi Arabia cyber readiness at a glance*. Potomac Institute for Policy Studies.
Incident of the Week, 2018. Incident of The Week: Shamoon Virus Cripples Hundreds of Computers. (2018, December 14). Cyber security hub. Retrieved on 01 August 2025. https://www.cshub.com/attacks/news/incident-of-the-week-shamoon-viruscripples-hundreds-of-computers retrieved on 5 October 2025.
Jamy, S., 2021. "US National Security Commission on Artificial Intelligence Report: A Call to Arms in the AI Era," Institute of Strategic Studies Islamabad, June 16. https://issi.org.pk/wpcontent/uploads/2021/06/Final_IB_Shayan_June_16_2021.pdf retrieved on 22 December 2021.
Kamiński, M. A. (2020, May 06). Operation "Olympic Games". Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear program. Security and Defence Quarterly, 29, 63-71. https://securityanddefence.pl/Operation-Olympic-Games-nCyber-sabotageas-a-tool-of-American-nintelligence-aimed,121974,0,2.html retrieved on 9 January 2025.
Kaye, D. D., Nader, A., & Roshan, P., 2011. Israel and Iran: A dangerous rivalry.
Kott, A., & Linkov, I., 2021. To improve cyber resilience, measure it. *arXiv preprint arXiv:2102.09455*.
Mohee, A., 2023. The Impact of the Israeli-Iranian Cyberwar on Arab Regional Security.
Molaei, H., 2016. "A History of Pahlavi-Zionist Regime Relations," Islamic Revolution Document Center, February 9, 2016, https://www.irdc.ir/fa/news/194/ retrieved on 2 October 2025.
Roberts, P., 2022. *Intelligence, Surveillance and Reconnaissance in 2035 and Beyond*. Royal United Services Institute (RUSI). https://static.rusi.org/201602_op_isr_in_2035_and_beyond.pdf retrieved on 7 October 2025.
Saniabad, E. R., 2012. "Understanding Iran's Identity Based on Constructivism," *Political Science Journal* 15(58), 191.
Scharre, P., 2018. *Army of none: Autonomous weapons and the future of war*. WW Norton & Company.
Science & Technology Organization, 2020. Science & Technology Trends 2020-2040. Brussels, Belgium. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf retrieved on 30 October 2025.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

Silver, D., Schrittwieser, J., Simonyan, K., Antonoglou, I., Huang, A., Guez, A., & Hassabis, D., 2017. Mastering the game of Go without human knowledge. Nature, 550(7676), 354-359.
Sobhani, S. C., 1989. *The pragmatic entente: Israeli-Iranian relations, 1948-1988*. Georgetown University.
Sparrow, R., 2007. Killer robots. Journal of Applied Philosophy, 24(1), 62-77.
Staff, T. (2020, June 1). Iran cyberattack on Israel's water supply could have sickened hundreds – report. The Times of Israel. Retrieved January 8, 2025, from https://www.timesofisrael.com/iran-cyberattack-on-israels-watersupply-could-have-sccckened-hundreds-report/ retrieved on 12 June 2025.
UNIDIR, 2025. The impact of AI on regional security in the Middle East, https://www.youtube.com/watch?v=tKGYu0HmSn0&t=103s retrieved on 07 November 2025.
VOA News. (2024, February 8). Iranian Hackers Interrupt UAE Broadcasts with Deepfake News. VOA. Retrieved January 8, 2025. https://www.voanews.com/a/iranian-hackers-interrupt-uae-broadcasts-withdeepfake-news-/7480126.html retrieved on 8 October 2025.
Work, J. D., 2020. Troubled Vision: Understanding Recent Israeli-Iranian Offensive Cyber Exchanges.