Received: September 12, 2024

Revised: October 19, 2024 & November 26,2024

Published: December 31, 2024

Journal of Politics and International Studies
Vol. 10, No. 2, July–December 2024, pp.145–163

AI and Cyber Drove Warfare in the Israeli-Iran Conflict and its Impact on Gulf States' Security

Ayesha Haroon
M.Phil Scholar, Department of Political Science and International Relations (DPSIR), University of Management and Technology, Lahore, Punjab Pakistan
Corresponding: f2024353014@umt.edu.pk

Abstract

This article investigates the implication of Israel- Iran driven AI and Cyberwarfare for Gulf security states through the lense of Defensive Realism. The Isreal-Iran conflict has intensified into a highly complicated battlefield where AI driven cyberattacks and misinformation campaigns targets important infrastructure challenging regional peace and stability. Gulf states, positioned in a geopolitically suspectible zone are vulnerable to these cyber security threats.which could possibly spread into their regions and destrupt their security landscape.

Using defensive Realism this study emphasizes how Gulf states prioritize protecting their state security through defensive measures rather than adopting offensive tactics. It also discusses the importance of developing resilient cyber security posture, adopting AI powered security tools and promoting regional collaboration to counter cyber security threats effectively. Defensive Realism stresses that states intention to sustain their security without agitating unnecessary escalation, which is vital for Gulf states security equilibrium, in the amidst of increasing technological and digital challenges.

The article concludes that Gulf states must cautiously steer the evolving AI and cyber domain by fortying their defenses and collaborating with the global actors. By endorsing a defensive realist strategy, Arab states can strengthen their robustness and contribute to regional stability in the face of emerging technologies.

Key Words: Artificial intelligence, Cyber security, Structural realism, Geopolitical tension, Middle East politics.

Introduction

Since the birth of *Homo Sapiens* on Earth, they have been in a continuous race of creating ideas, tools, and methods, from the Stone Age to the discovery of fire and then the invention of the wheel, to present-day modern tools like online networks and Artificial intelligence. These all inventions have shaped and improved human civilization. Each human invention is based upon human creativity, curiosity, and innovative ideas to enhance a better understanding of societies. Thus, paving the way for advancements across, science, technology, and medicine. Correspondingly, The Iran-Israeli conflict has increasingly assimilated the technology of AI and Cyberwarfare marking a new phase in regional hostilities. Israel uses advanced and up-to-date AI technology while Iran covertly develops its cyber capabilities both aiming to gain leverage. This digital strife impacts Gulf states' security, pushing them to enhance their cyber security and AI capabilities.

Iran's approach to AI and cyberdriven warfare, shows strong alignment with the International approach of Realism, focusing on power projection, power alignment, and countering threats from Israel and the USA (Tabatabai, 2020)[1]. Iran's AI research covers fields such as robotics, 3D printing, and communications technology, particularly 5G, demonstrating a commitment to advancing domestic tech sectors despite facing international sanctions (TVBRICS, 2024)[2].

Domestically Iran uses AI for surveillance purposes such as the use of AI in facial resignation to enforce laws. Discussions and debates surrounding the utilization and significance of cyberspace and artificial intelligence in Iran primarily revolve around two key perspectives: viewing them as integral components of national security strategy, and understanding cyber capabilities and AI as essential tools for safeguarding national interests (Khorrami, 2024)[3]. Iran relies on asymmetric cyber strategies, which allow Iran to protect its interests without engaging in traditional military engagement. Iran's cyber operations include sabotage, espionage, degradation, disrupting infrastructure, and targeting governmental institutes and financial institutes. A 2021 report from the ***Atlantic Council*** notes that Iran views AI as a force multiplier, enhancing its existing cyber operations and providing tools for intelligence gathering and social control within and beyond its borders (Atlantic Council, 2021)[4]. Furthermore, Iran's development of Cyber intelligence and AI for surveillance shows its strategic intent to maintain its security and influence its regional intent, thus, following the *realist paradigm* of maximum security, the sovereignty of the state, and self-help.

Israel's approach to its cybersecurity and AI-driven warfare has positioned itself as the pioneer of cybersecurity and cyber intelligence. Israel's commitment to AI is reflected in its investment and policies engineered to support innovation across various fields including healthcare, agriculture, and defense. These efforts focus on ensuring that AI systems are free from bias, maintain human oversight, and respect personal data protection. Israel’s strong cybersecurity infrastructure also plays a crucial role in fostering trust in AI technologies, especially in sensitive applications like defense and healthcare (OECD, 2024)[5]. They have also tried to establish a framework that enhances AI research while also promoting ethical concerns like privacy and accountability. Israel's cyberwarfare policy is the foundation of its national defense strategy. Its great emphasis is on defensive as well as proactive measures to combat cyber threats. The *Israeli National Cyber Directorate (INCD)* plays a pivotal role in protecting the country's cyber infrastructure responding to real-time threats and oversight critical issues. Israel's policy also includes offensive cyber capabilities, allowing for targeted strikes against adversaries’ cyberinfrastructure in response to perceived threats or hostile actions (OECD, 2024)[6]. Israel believes in a *“preemptive”* approach which involves taking action before escalation of any perceived threats. Its policies also include relying on offensive cyber capabilities including allowing for targeted strikes against adversaries and securing countries' critical networks. Furthermore, Israel maintains strong international collaborations, particularly with the United States, to share intelligence and bolster collective cyber defense mechanisms (Israel Ministry of Defense, 2024)[7].

The technological rivalry between them has posed a significant threat to the Gulf state's security. Both developing and developed Gulf countries are focusing on artificial intelligence as part of their national defense strategies. However, the policies of underdeveloped and developing states policy tend to differ from developed and advanced states like Saudi Arabia and UAE, due to variances in infrastructure, technology, and economic efforts. Oman for instance has started integrating AI into its economy and improving the healthcare and agricultural sectors. The Omani government has invested in AI applications that can improve public administration and the efficiency of its services (Oman Vision 2040, 2024)[8]. Similarly, Bahrain is also investing in developing in sector of AI. Bahrain's emphasis on AI is evident in several successful applications, such as the BeAware Bahrain app, which leverages AI and big data for pandemic management (Bahrain Economic Vision, 2024)[9]. Similarly, AI is also enhancing its AI sectors such as health, transport, and energy. The country has created the *Saudi Data and Artificial Intelligence Authority (SDAIA)* to lead this transformation (Al-Khouri, 2024)[10]. Similarly, the UAE has launched its *National AI Strategy 2031,* aiming to become a global AI leader by investing in AI startups, creating a conducive environment for innovation, and integrating AI in public services and sectors like transportation (UAE Government, 2023)[11].

Cyberwarfare has become an increasing concern for both developing and developed Gulf nations. In developed Gulf states cyber threats have increased investments in cyber-related infrastructure. These Developed states have promoted various defense strategies including the establishment of National cyber defense agencies to tackle any lingering cyber threat. The development of smart cities and the integration of AI could increase the threat of cyber-attacks from state and non-state actors. In response, these states are effortlessly working on international partnerships and cooperation with international cybersecurity organizations to combat any susceptible cyber threat. On the other hand, underdeveloped Gulf states like Syria and Yemen don't have extensive cybersecurity frameworks and are more vulnerable to cyber threats. These states not only face risk from state-sponsored cyber actors but also from nonstate cyber actors who are capable of destabilizing the critical infrastructure of the region for instance attack on one state could amplify the effect on the neighboring states.

In conclusion, the integration of AI and cybersecurity has increased the regional tensions between Israel and Iran thus, impacting the Gulf state's security. Iran's enhancing its cyber stockpile and Israel's advanced AI and Cyber capabilities have created a composite environment for Gulf state's security posing a threat to developed and underdeveloped Gulf states. These conflicts heighten the risk of cyber spillover encouraging Gulf countries to mitigate this threat more soundly through international and regional collaborations to protect crucial infrastructure.

Research Questions

1. How are Gulf states utilizing their collaboration with global powers (for example U.S. cybersecurity backing and China artificial intelligence AI apparatus) to resist threats arising from the Israel-Iran conflict?
2. What are the economic concessions and trade-offs for Gulf states investing in cybersecurity and AI in reaction to the Israel- Iran conflict, and how does it affect their broader economic defense strategy?

The Israeli-Iran is a multifaceted conflict and a driver of geopolitical tensions in the Middle East, originating back in 1979 with the onset of the Iranian revolution. The revolution marked the overthrowing of the Shah's regime and the establishment of the Islamic Republic of Iran. Despite providing rhetorical support for an improvement in the human rights situation in Iran, the Carter administration continued military and economic support for the Shah's increasingly repressive regime, even providing fuel for the armed forces and other security services facing shortages due to the strikes (Zunes, 2009)12. Over the decades Iran's support for militant groups such as Hezbollah and Hamas, along the lines of ideological conflict and regional power dynamics. This conflict is characterized by a series of cyber-attacks, proxy wars, and political sway, making it an important factor in the geopolitics of the Middle East. Recent developments, such as preventive strikes from Israel, Iran's nuclear program, and international sanctions on Iran's atomic defense posture have posed a significant threat to Middle Eastern security.

Both Israel and Iran are increasing their technologies- cybersecurity and Artificial intelligence to assert their influence. The Gulf states security is politically and economically significantly impacted by this conflict. The Gulf states particularly Saudia Arabia, Qatar, Oman, and UAE (United Arab Emirates) have a very critically strategic position in the Middle East. Geographically adjoining Iran and its economic wealth ie vast oil refineries make them a vital key player in the Middle East. Iran also holds the world's fourth-largest proven crude oil reserves and is a major member of the Organization of the Petroleum Exporting Countries, historically producing around 3-4 million barrels per day (Rapier, 2024)13. While Gulf states make alliances with global powers, notably the USA and recently Israel had huge implications for regional security. The Gulf states navigate a strategic balance between economic opportunities and political clout to impact broader geopolitical security. This article explores how Gulf states utilize their collaboration with global powers amidst the Israeli-Iran conflict and focuses on economic tradeoffs in maintaining security under the theory of defensive realism.

Defensive Realism Theoretical Framework:

Kenneth Waltz proposed defensive realism, a branch of **neo-realism/structural realism**, emphasizing that states use security maximization and balancing strategy rather than aggressive expansionism, unlike offensive realism which asserts that states maximize power offensively. According to defensive realism, states recognize the anarchic nature of the international system and prioritize territorial integrity and protection of sovereignty. They are preventive and, at times cooperative, diplomatic, and non-expansionist. Defensive realism asserts that aggressive expansion as promoted by offensive realists upsets the tendency of states to conform to the balance of power theory, thereby decreasing the primary objective of the state, which they argue is ensuring its security (Lobell, 2010)[14]. Defensive Realism is a theoretical perspective within the broader framework of Realism that posits states are primarily security-seeking actors rather than power maximizers either by Bandwagoning or through buck-passing. This comes in the domain of negative balancing. There are several circumstances, however, where defensive realism expects states to favor short-term military preparedness over long-term economic prosperity (Taliaferro, 2001)[15].

Gulf states situated on the rim of power strife between Iran and Israel reflect this theoretical approach through their economic policies, alliance-making, and security policies. The Gulf state aims to prevent confrontation while also maintaining regional stability.

Why is this theory eligible for the topic?

1. Applicable to current topic:

Defensive realism is currently very relevant to the Israeli-Iran conflict and the emerging Gulf state's security. This theory provides a firm framework of why Gulf states form alliances to mitigate the rising threat from the Israeli-Iran conflict. Recent events include increased cyber-attacks from both sides and the assassination of Iranian nuclear scientists. Gen Fadavi, the deputy commander of the Revolutionary Guards, told a ceremony in Tehran on Sunday that a machine-gun mounted on the Nissan pick-up was "equipped with an intelligent satellite system which zoomed in on martyr Fakhrizadeh" and "was using artificial intelligence"(Kleinman, 2020)[16]. The relevance of defense realism is enhanced as Gulf states invest more in tech-oriented military pieces of equipment and make alliances with powerful states.

2. Insight into Gulf States security and survival:

The Gulf states including Saudia Arabia, Bahrain, Oman, and UAE perceive the Israel-Iran conflict as a direct threat posing an ultimatum to their regional security. Iran's cyber capability highlighted the vulnerability of Gulf security when attacked Saudi Armaco. Moreover, Saudia Arabia, UAE, and Bahrain have been actively involved in collaborating with global powers such as Britain, France, and the U.S. to collectively counter the threat of Iran, thus, allowing for greater cybersecurity collaboration and providing an intelligence-sharing platform. For Instance, the UAE's collaboration with Israel in enhancing their cybersecurity and normalization of their relations with Israel via the *Abraham Accords* are some rational and swift movements to strengthen their security design against any Iranian Indirect confrontation. This reflects the defensive realism in investing highly in cybersecurity and AI to seek security through alliances rather than involving in ornaments of maximization. raining

3. Gulf states and collaboration with global powers:

The Gulf states have increased their partnership with global powers to counter the rising threat of Iran and Israel's direct military confrontations. The cooperation in GCC has created a hegemony over its Western allies. The GCC's financial wealth is estimated to grow 4.7% annually to reach $3.5 trillion by 2027, according to research from Boston Consulting Group (BCG), and startups are poised to continue tapping into this market with innovative digital products and services (Saverin , Ganguly , & Wagle, 2024)[17].

The U.S. provides advanced cybertools, and AI defence security to its allies. For example, the Muhammad Bin Zayed University of Artificial Intelligence was established to promote research and development of RnD to counter state security threats.

The US remains one of the significant actors in the Gulf States *Abraham Accords* as moderated by the US to facilitate the normalization of relationships between Gulf status especially Bahrain, Oman, Saudi Arabia, and UAE thus fostering closer military relationships and intelligence sharing among them to counter Iran. “The UAE’s normalization with Israel allowed Saudi Arabia to avoid many pitfalls and mistakes,” according to al-Hussein (Cafiero, 2023)[18].

Similarly, Russia has strengthened its relationship with Gulf states by acting as a mediator with Iran despite Gulf countries remaining cautious of Russia's relationship with Iran. Saudi Arabia has engaged with Russia through *OPEC* to moderate oil prices in the international market. Russian crude production, which is subject to a quota under the OPEC agreement of 8.98 million b/d, has been volatile due to the sanctions, as well as airstrikes conducted by Ukraine targeting oil facilities (Wang & Griffin, 2024)[19].

China plays a complex role in the Israel-Iran conflict, maintaining economic and technological collaboration with Iran and also strengthening its relationship with Iran over Oil and energy security. For instance, Saudi Arabia and the UAE have worked with China to foster their cybersecurity domain and increase cyber espionage to counter Iranian influence. Additionally, the “Dubai 10X” initiative implemented in collaboration with Huawei and the joint venture established between Abu Dhabi and China Electronics Technology Group Corporation are exemplary models of China-UAE cooperation (Yuan, 2024)[20]. For Xi, trade with Saudi Arabia is strategically important to deepen China’s influence outside the US and Europe, where it faces rising threats of sanctions and tariffs, analysts said (White, Leng, Irwin-Hunt, & Omran, 2024)[21].

4. Economic trade-off:

Defensive realism operates on the premise that states secure themselves rather than adopting aggressive policies towards another state. These trade-offs include allocating resources to cybersecurity and military spending at the expense of strategic and economic well-being. Gulf states especially Saudia Arabia and UAE face criticism in addressing socioeconomic issues like unemployment, and social and economic inequality. Supporters of clean energy and Environmental protectionist critiques Saudi huge investments in Oil refineries which are causing an increase in carbon emissions causing fossil fuels to deplete and increasing global warming in Earth. Critics call it “*greenwashing,”* while some climate experts accuse Saudi Arabia of deliberately blurring the narratives around climate change solutions to blunt the campaign to phase out fossil fuels (Luck, 2023)[22]. Despite Saudia's massive investment in Cyber technologies they don't address domestic challenges like youth facing unemployment partly because they prioritize defense investment over social issues of the public, the same goes for UAE instead of mitigating socioeconomic issues such as affordable housing, education, and healthcare their government invests massively on country's infrastructure. Thus this high spending in the drilling of cyber technologies can lead to domestic discontent and undermine their internal security. For instance, Saudia Arabia's military budget is the highest in the world, and *Vision 2030* invests the highest in the military which could be used on other spending such as education, health, transport, or development of infrastructure. Another example is of Saudia ***Neom*** **City** which is proposed by the Crown Prince MBS and is lacking in nurturing its native people. Proposed as a harbinger of the future, the $500 billion NEOM project in Saudi Arabia has already drawn concern from human rights advocates stemming from the eviction of the indigenous Huwaitat people (university of Michigan, 2024)[23].

Another example of Gulf Strategic collaboration is with UAE with China. UAE has recently collaborated with China on G42 a tech company based in Abu Dhabi specializing in Artificial intelligence. After a data breach by Israeli-based spyware *Pegasus was* involved in the unlawful surveillance of many renowned journalists, lawyers, and media organizations. During the investigation, evidence has also emerged that family members of *Saudi journalist Jamal Khashoggi* were targeted with Pegasus software before and after his murder in Istanbul on 2 October 2018 by Saudi operatives, despite repeated denials from NSO Group (The Amnesty International, 2021)[24]

This February, in an apparent acknowledgment of these concerns, G42 announced that its investment arm had divested entirely from Chinese companies, including an estimated $100 million stake in ByteDance, owner of the controversial app *TikTok* (Clemmensen, et al., 2024)[25].

Cybersecurity is causing an economic burden for Gulf states as it is a vast and evolving field and requires contiguous allocation of funding, to stay away from the cyber-attacks arising from Iran such as ransomware or malware. Cost-benefit analysis is required as this massive funding strains their public budget. Additionally, these oil-producing countries are more vulnerable to cyberattacks adding another layer of threat to their internal security.

Discussion Model:

In this modern era technology has completely transformed the idea of Traditional warfare. Countries are adopting AI and cyberwarfare in their defensive and offensive mechanisms. This transformation is more prominent in the scenario of the Israel-Iran conflict as AI and Cyber technologies have completely changed the politics of the Middle East and have transformed its global security landscape outlook. With heightened cybersecurity concerns, 83% of Middle Eastern organizations plan to deploy GenAI tools for cyber defense within the next year (House Cooper, 2024)[26] .AI and cyberwarfare have become security tools increasing the threat of state and non-state actors. In this context, the Theory of defensive realism provides the context of knowing certain behaviors and policies states adopt to secure themselves. It prevents any single state from achieving hegemony. Defensive realism posits that states act rationally avoiding conflict at the front, and maximizing their power in this anarchic international system. This theory applies to the Middle East as the balance of power has been disturbed between Israel, Iran, and Middle Eastern states due to the technological advancements in Cyber Warfare and AI. The Israel-Iran conflict is a long-standing ideological and geopolitical struggle. After the Iranian revolution, the Shah's regime was overthrown and Ayatullah Khomini established its government under Islamic principles thus, the Islamic Republic of Iran was established. This revolution was supported by many anti-western sentiments which completely changed Iran's Foreign Policy. Iran's support for non-state actors such as militant groups has further escalated the tensions as Iran supports Hamas in the Gaza Strip and Hezbollah in Lebanon. From an initial investment in training and arming the budding militia in the early 1980s, Iran now reportedly provides an estimated $700 million to Hezbollah annually, according to the U.S. Department of State (Haq, 2024)[27]

Over the years, the conflict has taken a more complex form and thus has become distended due to economic sanctions, proxy wars, and cyber wars.

The analysis is rooted in the principles of defensive realism giving a nuanced and clear understanding of the state's behaviour in the Technological era.

Section 1: Israel AI and cyberstrategy and its impact on Iran:

Israel has positioned itself at the forefront of Artificial intelligence and cybersecurity. Israel supported by the partnership of the United States and European countries has developed its industrial military complex. Israel has used state-of-the-art technology in developing highly efficient drones, intelligence algorithms, and cyberespionage and cyber decorating tools. The Israel Defence Forces (IDF) uses high-class tools for intelligence gathering, decision-making, and tasking literal strikes, such as the Iron Dome technology uses Artificial intelligence to operate its missiles. In particular, the IDF employs AI applications in its: (1) Proactive Forecasting, Threat Alert, and Defensive Systems; and (2) Intelligence Analysis, Targeting, and Munitions (Mimran & Dahan, 2024)[28]. This system has extensive threats for external threats such as shooting down missiles fired by Hamas and Hezbollah. In defensive systems, Israel has conducted various cyber operations against Iran. The most notable example is the Stuxtent operation. In this cyber operation, Israel attacked Iran's uranium plant to deter Iran and to serve as a warning to prevent Iran's aggression.

In the light of defensive realism, Israel perceives Iran as an existential threat that could destabilize the regional and geopolitical scenario of the Middle East. Israel by engaging in proactive cyber strategies and through intelligence gathering, Israel deter its enemy's aggression and also seek to survive without getting involved in military or expanding territory.

Case Study A: The Stuxtent Operation:

Operation Stuxnet was carried out by Israel in 2010. Israel and the USA joint operations against Iran with the help of a single trojan and the Ransome virus. In Cyberspace, a cyber-attack has three major themes: disruption, Espionage, and degradation.

Israel mostly uses an intermix of three ways to carry out cyber operations with the aid of Cyber disruption, Israel conducted a joint operation in Iran, it's a low-cost attack that support larger propaganda efforts. When Iran was cyber-disrupted, it was unable to identify whether the incident was caused by a human error or technological error within its nuclear plant. Iran mostly faces website defacement. Stuxnet's operation is a prime example of Israeli operations that managed to achieve its strategic interests without escalating the military confrontation. The use of cybernetic tools intended to attack the Natanz center proved to be much less costly diplomatically (Kamiński, 2020, 63-71)[29]. This cyber-attack also highlighted the vulnerabilities lying in countries' cyber defense. This attack was carried out to counter Iranian influence in the Middle Eastern region.

Israeli technological advancements significantly impacted the defense postures of Gulf states. Defensive realism emphasizes the security dilemma faced by Arab states due to this cyber-attack. After this Arab states tried to normalize reactions with Israel through ABRAHM ACCORDS significant UAE and Bahrain. The argument for supporting Arab-Israeli normalization is often couched in terms of "stabilizing" the region and facilitating economic development to offset other sources of international intervention—in particular, by Russia, China, and Iran ((ACW), 2023)[30] .For example, the UAE has collaborated with Israel to counter the rising threat coming from Iran. UAE and ISREAL have digitally collaborated to tackle the ransomware virus and have strengthened their defensive policies. However, UAE has to pay the price for this partnership, it has become vulnerable to Iranian cyber-attacks as evidenced by many Iranaina cyber hackers. They have attacked the Emairti financial institutions such as banks and also attacked their oil company.

Case Study B: Irans cyberattack on Isreal water infrastructure 2020:

In April 2020 Iran conducted a cyber-attack on Iran's water treatment facility, this attack was part of the ongoing conflict between Israel and Iran where they both wanted to undermine each other's sovereignty and contributions to the Cyber domain. The attack was targeted at increasing chlorine levels in water. Iran's objective was to raise the chlorine level to a dangerous level. Chlorine is a chemical commonly used in disinfecting water. But if added in a concentration high level it could pose a significant health threat to Israel's population.

Iran's hackers gained access to SCADA which is supervisory control of Isreal. Its main purpose is to control and treat chlorine levels in water and make it safe for human consumption. This plan was carried out and executed with a high level of resources, planning, and intelligence gathering. Fortunately, this attack was detected by Israel's National cyber control management in real time which made the authorities swiftly intervene and take prompt action to prevent any iruption of any health crises. Yigal Unna, who heads the National Cyber Directorate, did not mention Iran directly, nor did he comment on the alleged Israeli retaliation two weeks later, but he said recent developments have ushered in a new era of covert warfare, ominously warning that "cyber winter is coming (staff, 2020)[31].

A water system is mostly considered less susceptible to cyberattacks than any economic or military institution. Israeli intelligence and Western officials attributed this cyber-attack from Iran to challenge its adversaries whereas, on the other hand, Iranian officials deny any sort of cyberattack on Israel's water treatment plant. Since then the Israeli-Iran conflict has increased. Both nations engage in cyber-attacks on sites important institutions of military, finance, health, and nuclear facilities.

From a defensive realism perspective, this attack shows that Iran wants to show its capabilities and readiness to wage a cyber-attack to counter its adversary. When Iran conducted a cyber-attack on a water facility, Isreal relying on the "tit for tat" phenomenon conducted a cyber-attack on Iran's airport in response to its water attack. The Post quoted intelligence and cybersecurity officials familiar with the situation as saying the computer strike was carried out by Israeli operatives, "presumably in retaliation for an earlier attempt to penetrate computers that operate rural water distribution systems in Israel" (Al-Jazeera, 2020)[32].

Section 2: IranAI and cyber strategies and its effect on the Middle East:

Iran has recognized the strategic importance of AI and cyber warfare and has heavily invested in progressing its technologies to counter rival global powers. Iran's hackers have conducted several cyber-attacks on enemies to enhance its strategic posturing instead of direct military confrontation. The current conflicts in the Middle East involving Hamas, Hezbollah, and the Houthis all demonstrate the control that Iran exerts over conflicts in the region—without ever becoming officially involved in the conflicts. (Hassenstab, 2024)[33]. Iran uses proxy groups such as Hezbollah which uses AI and cyber tactics to gather intelligence, carry out operations, spread propaganda, and extend their influence in the Middle Eastern region. Iran's cyber warfare focuses more on cyber disruption which is more of a psychological warfare. It is low cost, low pay-off, and dangerousness bargaining context. It signals escalation risk and supports larger propaganda efforts. Mostly carried out through website development and DDOS (distributed denial of service).

Iranian groups such as *IRGC Islamic Revolutionary Guard Corps* use cyber tools to carry out cyber-attacks through multiple means such as website defacement, spreading disinformation, attacking critical information, and spreading propaganda.

The key example of Iran's cyber technology logo is the creation of fabricated videos of political and influential personalities using DEEPFAKE technology. Similarly, Iran AI AI-based social media campaigns try to construct Westerners and anti-Israel narratives to destabilize the Regional outlooks further. Another example of an AI attack is Iran's attack on the UAE while live streaming on a news network. "This marked the first Iranian influence operation Microsoft has detected where AI played a key component in its messaging and is one example of the fast and significant expansion in the scope of Iranian operations since the start of the Israel-Hamas conflict," a Microsoft blog post said (VOA news, 2024)[34]

According to *defensive realism,* Iran perceives Israel's cyber and AI capabilities as existential threats and adopts many defensive strategies to counter its enemy. In contrast, Israel is adopting offensive strategies to counter Iran's cyber commitments. An example of this is that Iran's hackers have attacked Israel's economic sector, banks, and stock market to destabilize them financially.

Similarly, these attacks significantly impact Gulf states, particularly UAE and Saudi Arabia. These nations as the rivals of Iran are recurring targets of Iran's cyber-attacks. In 2012, Iran carried out a cyber-attack known as SHAMOON attack on Saudia ARMACO. Hacking 30,000 Saudi computers. It spreads to computers on a network through a dropper, according to TechTarget, and can compile lists of files, send information back to the attacker and erase some or all of the compromised files

(*Incident Of The Week: Shamoon Virus Cripples Hundreds Of Computers*, 2018)[35]. If seen from a defensive realist perspective, a security dilemma is faced by Gulf states, when they strengthen their relationship with global powers such as Israel and the US they become more susceptible to Iranian aggression.

Case Study: Iran's involvement in SYRIA:

Iran plays a significant role in the Syrian civil war which demonstrates its potential use of AI and cyber capabilities. Iran's support of the Assad regime, aimed to counter the Saudi and Israeli conflict. Iran assisted Hezbollah employed high-tech cyber capabilities to support the Assad regime. This establishes opposition and alters the dynamics of regional powers by not directly involving them in any military confrontation. For other militias, Iran pays salaries between $200 to $300, and, for local militias, such as Nubl and Zahra Brigades, it gives less than $100 a month (Saban, 2020)[36]. Similarly, Iran's presence in Syra established a gateway to Lebonan, building up its capability to supply weapons to Hezbollah. Hezbollah has supported Assad with a robust, well-trained force whose involvement in the conflict aligns with Iranian strategic interests as Secretary General Hassan Nasrallah acknowledged on April 30 in Tehran. (Fulton, Holliday, & Wyer, 2013)[37]. Thus the increased Iran's influence in Syria posed a significant threat to its rival state Israel, which in return resulted in massive airstrikes against Iranian holdings in Syria.

This reflects the quest for power and the struggle to maintain hegemony in the region.

Section 3: Israel Cybernetics and AI Warfare Impact on the Middle Eastern Region

Israel has tried to make its influence on the Middle Eastern region through overt and covert operations and collaboration on AI and Cybernetics to maintain its supremacy in the Gulf.

This partnership has bolstered intelligence sharing, using AI technology in military reforms, and cyber strategies among the nations. From a defensive realism standpoint, Israel wants to deter Iranian aggression and to be a hegemon in the Middle Eastern region. Another factor is that Israel wants to dominate in this region to prevent any Gulf state from having that region's power. This approach emphasizes one of the core principles of defensive realism.

For Middle Eastern region especially Saudia Arabia views Iran's cyber capabilities as a forthright threat to Saudi security. To counter this Saaudia has expanded its partnership with the US purchasing highly advanced AI-driven defense systems and cyber abilities. However, this limits Saudia's dependence on external threats. The Abraham Accords of 2020 appeared to pave the way for further reconciliation between Israel and the Arab World, which, while still divided over the Palestinian question, is increasingly drawn to economic opportunities provided by Israel, such as access to cutting-edge technology in agriculture, defense, artificial intelligence, and cybersecurity (Alcamo, 2024)[38].

The ***UAE's*** normalization of relations with Israel has made both collaborate toward defense structure. This collaboration has also shifted the geopolitics of the Middle East. UAE aims to enhance its cyber and AI capabilities which make it more susceptible to Iranian aggression. For Israel, the UAE represents a leading market for Israeli technologies, a source of investment in capital-intensive technologies, and a launching pad for Israeli exports and partnerships in the rest of the region (Gause, Alghashian, & Leshem, 2025)[39].

Whereas ***Bahrain*** which is a smaller oil-producing Gulf state with a significant Shia population is more susceptible to Iranian aggression due to its strong alliance and friendly relationship with the US, Saudia, and Israel. Additionally, three of them are collaborating on joint military drills to counter Iranian aggression. He pointed to a collaboration with Israel's Sheba Medical Center, where Bahraini doctors will work in Israel and Sheba aims to open an innovation center in Bahrain (Scheer, 2023)[40]. Iran could destabilize the region through erupting propaganda among Shias which would ultimately destabilize the region.

Qatar does not have any direct relationship with Israel but collaborates on creating mediated peace in Gaza. Qatar acts as a mediator between Israel and the Gulf States by maintaining regional stability. For example, **Qatar** mediated peace talks between Israel and Hamas enhancing its diplomacy and soft power also maintaining its regional influence. Qatari authorities have acknowledged difficulties in their attempts at negotiation, raising the possibility that an end to the fighting may not come soon (y Teran, 2024)[41]. Qatar's engagement in Iran, despite its views of Iran as an existential threat, Qatar has regional ties with Iran through a pipeline of oil known as the "*NORTH DOME gas field"*. Both countries are currently producing 650,000 to 700,000 barrels of gas condensate (ultra-light oil) daily from these four layers. (Khatinoglu & Shokri, 2024)[42]. Qatar also tries to maintain diplomatic ties with Iran to avoid confrontation with Iran. By maintaining this relationship Qatar reduces the likelihood of becoming a victim of Iranian aggression through any military confrontation or becoming susceptible to any cyber-attack. Despite maintaining ties with Iran Qatar became a victim of Iran cyberattacks in 2017 when Iran carried out a cyber-attack on its news Agency which escalated regional conflicts.

Jordan a geopolitically important country of the Gulf shares Syria and Isreal as its neighboring countries, its policies show extensive realism they try to mitigate any external threat while focusing on maintaining internal stability. Jordan signed a peace treaty with Israel in 1944 to maintain closer relations with Israel to minimize the direct threat arising from Iillegaly occupied Isreal and to address the Palestinian issue as its majority population comprises of Palsetianin refugees coming from *Gaza strip*. But due to Israel's hostile policies and illegal intervention in Jersuluam particularly the *AL AQSA* mosque, it is susceptible to anger the Muslim population and destabilize regional stability which could be a potential threat to the current regime. Jordan doesn't comply with direct relations with Israel but in 2021 proposed a spying technology for eradicating militants on Jordanian soil. Israeli NSO came under fire from critics that the Jordanian government was using that spying technology to surveil the civilians. The *Israeli cyber intelligence firm NSO* has been in talks with the Jordanian government regarding the sale of new spy technology to Amman, Axios report (Times of Israel, 2021)[43].

Jordan views Iran as an existential threat because Iran supported the militant groups such as Hezbollah and Houthis which pose a direct threat to its borders. Jordan due to being an economic and resource country tries to maintain normal and peaceful relations with Iran Unlike Gulf states like UAE and Saudia fully engage in aggressive ties with Iran.

Israel's illegal occupation in Palestine and mass killing of innocent civilians with the aid of AI. In addition to talking about their use of the AI system, called Lavender, the intelligence sources claim that Israeli military officials permitted large numbers of Palestinian civilians to be killed, particularly during the early weeks and months of the conflict (Sarfraz, 2024)[44]

Yemen is a key player in the Israeli-Iran conflict, the outgoing civil war in Yemen has provided an environment where both Iran and Israel compete for their influence. Iran provides significant financial and military aid to HOUTIS, which dominates Northern Syria and the Arabian Peninsula. Houthis have launched significant missiles against Saudia Arabia and the UAE to counter their regional influence. The BAB-UL MANDAB or the GATE OF TEARS strait is present in Yemen connecting to the Arabian Peninsula. Houts tries to assert their control over that strait which is an important neckpoint for oil trading. Houts gives importance to Inran on this strait creating a regional threat to the USA and Gulf countries. LONDON, Dec 19 (Reuters) - Yemen's Houthis have been targeting vessels in the southern Red Sea and the Bab al-Mandab Strait in attacks that the Iran-aligned group says aim to support the Palestinians as Israel and Hamas wage war (Ghaddar, 2023)[45]. The Gulf views HOUTIS as an arm of Iranian power, which creates a threat to them. The GCC GULF COUNTRIES COOPERATION especially Saudia and UAE militarily intervened to counter Iranian influence but it resulted in civil war creating resource constrain and Humanitarian crises.

While Israel is not directly involved in Yemen it still sees Iran as an existential threat that could target the oil/trade ships and can exercise their control over the RED sea.

EQYPT an important and the largest ARAB nation adopts a very pragmatic approach toward the Isreal-Iran conflict. Egypt was the first country to sign a peace treaty with Isreal in 1979 in the light of defensive realism the main points of the treaty were that treaty allowed for: enhancing relations with the US and its alliances, to prevent the lurking threat of Israeli military confrontation and to reclaim the Sinai Peninsula concerning its relation with Iran Eqypt adopts neutrality to avoid direct contact with Proxy groups like Hamas, they see Hamas as a destabilizing force which could destabilize the regional stability of Gulf states. Still, Jerusalem and Cairo will never be able to completely decouple their relationship from the Israeli-Palestinian conflict and therefore must continue working together to prevent future rounds of violence and the deterioration of the status quo (Dagres, 2021)[46].

For ***Syria***, its situation is quite the opposite, Syria being the battleground of the Israeli-Iran conflict. Iran's financial and military support has just short termed benefited the Assads Regime, as they were supporting military aid to Hezbollah. Syria relies on decreasing Israeli influence in Syria. Israel wants to counter the ASSADS regime by attacking Iran's assessed assets and weakening its power within Syria.

Case study: The impact of Arabs regional stability

Proxy wars in Lebanon, Syria, and Yemen are mostly conducted by the ongoing Israeli--- Iran cyber conflict. These conflicts have adverse effects that destabilize the regional balance and security of Arab states. Israel and Iran both try to leverage their influence on each other making the Gulf states their victim of spillover of Regional instability. For the first instance, Yemen-based Houthis rebels are using cyber tactics and technological warfare to spread propaganda in Saudia to destabilize its government. On the other hand, the Israeli cyber war front is trying to counter the Yemni influence by gathering intelligence on any technological advancement and preventing their way of spreading propaganda. This case study illustrates that the impact of the ongoing Israeli-Iran conflict could severely destabilize the regional stability and peace of Gulf nations.

Conclusion

The thorough analysis of AI and cyber-driven warfare within the Israeli-Iran conflict has a keen impact on the broader regional stability of the Middle East. This research paper utilizing the framework of Defensive realism navigates how nations engage in technological warfare in an anarchic global system to enhance their national security posture to maintain peace and serenity.

Israel's advanced AI and cyber capabilities such as Irom Dome technology and Stuxnet operation have strengthened its ability to deter Iranian Influence. Iseal aims to protect its security from external and internal threats, without territory seeking Expansion. On the Other hand, its Rival Iran tries to maintain its hegemony through assisting militant and proxy groups such as Hezbollah and Houthis. This approach helps Iran maintain its influence in Gulf states without involving any direct military conformation. This side-by-side retaliation has created regional instability in the Middle East making both Iran and Israel in a phenomenon of security Delimma less secure for their capabilities.

The Middle East has broader implications for this AI and cyber-driven warfare making them caught between the two states trying to maintain security in their region. The Abraham Accords facilitated the UAE, and Saudia to extend and facilitate cooperation with Israel and the U.S. to improve their defensive measure and highlight that collaborative efforts can be made to counter a single threat of Iran. Gulf states Qatar and Oman adopt a neutral approach without being directly involved. Similarly, Syria and Yeyemen at the forefront of proxy groups tried to stick with Iran escalating the conflict.

With the rise of AI and cyber technologies the idea of traditional warfare has completely changed, it has added more complexities to warfare. While these technologies provide a majority of benefits they also undermine the sovereignty and national security of states. If not managed carefully it could potentially destabilize the region and could lead to further escalation and ultimately war.

In a nutshell, the Israeli conflict and its impact on Gulf states need an intricate balance between countries as these emerging technologies such as AI and Cyberwarfare have advantages such as postering defensive structures but there are distances between them as well which could lead to cyber and AI-generated warfare. Countries should try to ensure regional cooperation, peace, and diplomacy among themselves and should mindfully tackle any lurking threat defensively rather than opting for offensive means.

References

[1] Tabatabai, A. M**.** (2020). Iran's Cyber Strategy and Its Role in National Defense. *Middle East Institute*. Available at: https://www.mei.edu/publications/irans-cyber-strategy.

[2] TVBRICS. (2024, November 02). *Iran ranks among top 100 global leaders in AI readiness for government services. Retrieved* 11 12, 2024, from Iran ranks among top 100 global leaders in AI readiness for government services Text copied from https://tvbrics.com/en/news/iran-ranks-among-top-100-global-leaders-in-ai-readiness-for-government-services/.

[3] Khorrami, N. (2024, March 29). Navigating Cybersecurity and Surveillance: Iran's Dual Strategy for National Security. *Policy analysis*, (nil), 01. https://www.washingtoninstitute.org/policy-analysis/navigating-cybersecurity-and-surveillance-irans-dual-strategy-national-security

[4] Atlantic Council. *AI and Cyber Warfare in the Middle East: Iran's Strategic Adaptations*. 2021.

[5] OECD. (2024). *Artificial Intelligence Policy Review*. Organisation for Economic Co-operation and Development. Retrieved from https://www.oecd.org/

[6] OECD. (2024). *Israel's Cybersecurity Strategy: A Review.* Organisation for Economic Co-operation and Development. Retrieved from https://www.oecd.org/digital/cybersecurity/

[7] Israel Ministry of Defense. (2024). *Israel's Cyber Warfare Capabilities*. https://www.idf.il/en/ministry-of-defense/cyber-warfare/

[8] Oman Vision 2040. (2024). *Oman's AI and Technological Development Plans*. from https://www.oman.om/

[9] Bahrain Economic Vision 2030. (2024). *AI and innovation in Bahrain*. from https://www.bahrain.bh

[10] Al-Khouri, N. (2024). Saudi Arabia's Vision 2030 and the AI revolution. Saudi *Gazette*. Retrieved from https://www.saudigazette.com

[11] UAE Government. (2023). National Artificial Intelligence Strategy 2031. *UAE Government Website*. Retrieved from https://www.uae.gov.ae

[12] Zunes, S. (2009, April). *The Iranian Revolution* (1977-1979). ICNC. https://www.nonviolent-conflict.org/iranian-revolution-1977-1979/

[13] Rapier, R. (2024, October 2). Iran Missile Strike On Israel Sparks Fears In Global Oil Markets. *Forbes*.

https://www.forbes.com/sites/rrapier/2024/10/01/iran-missile-strike-on-israel-sparks-fears-in-global-oil-markets/

[14] Lobell, S. E. (2010). Structural realism/offensive and defensive realism. Retrieved from https://oxfordre.com/internationalstudies/internationalstudies/abstract/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-304

[15] Taliaferro, J. W. (2001). Security seeking under anarchy: Defensive realism ... Retrieved from http://www.rochelleterman.com/ir/sites/default/files/taliaferro%202001_0.pdf

[16] Kleinman, Z. (2020). Mohsen Fakhrizadeh: “machine-gun with ai” used to kill Iran scientist. Retrieved from https://www.bbc.com/news/world-middle-east-55214359

[17] Saverin , E., Ganguly , R., & Wagle, K. (2024). Unlocking deep tech potential in the Gulf Cooperation Council (GCC). Retrieved from https://b.capital/unlocking-deep-tech-potential-in-the-gulf-cooperation-council-gcc/

[18] Cafiero, G. (2023, September 17). *Three years on, how have the Abraham Accords helped the UAE?* Al Jazeera. Retrieved December 28, 2024, from https://www.aljazeera.com/news/2023/9/17/three-years-on-how-have-the-abraham-accords-done-for-the-uae

[19] Wang, H., & Griffin, R. (2024, 07 18). *Saudi Arabia, Russia to maintain 'close coordination' on OPEC+: Kremlin*. S&P Global. Retrieved 12 28, 24, from https://www.spglobal.com/commodity-insights/en/news-research/latest-news/crude-oil/071824-saudi-arabia-russia-to-maintain-close-coordination-on-opec-kremlin

[20] Yuan, S. (2024). China-UAE relations in Artificial Intelligence. Retrieved from https://mepei.com/china-uae-relations-in-artificial-intelligence/

[21] White, E., Leng, C., Irwin-Hunt, A., & Omran, A. A. (2024). China’s ties with Saudi Arabia buoyed by Green Tech. Retrieved from https://www.ft.com/content/f0babafc-57e6-434f-9d94-013c312dc0f9

[22] Luck, T. (2023). Can the oil industry help address climate change? Saudi Arabia says yes. Retrieved from https://www.csmonitor.com/World/Middle-East/2023/0523/Can-the-oil-industry-help-address-climate-change-Saudi-Arabia-says-yes

[23] University of Michigan. (2024, May 16). *NEOM’s Shadow: The Dispossession of the Huwaitat People*. NEOM’s Shadow: The Dispossession of the Huwaitat People. Retrieved December 27, 2024, from https://limos.engin.umich.edu/deitabase/2024/05/16/neoms-shadow/

[24] The Amnesty International. (2021, 08 21). *Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally*. Amnesty International. Retrieved 12 27, 2024, from https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

[25] Clemmensen,, A. G., Redlich,, R., & Rumley, G. (2024, 04 03). G42 and the China-UAE-U.S. Triangle. *The Washington policy for near East policy*. https://www.washingtoninstitute.org/policy-analysis/g42-and-china-uae-us-triangle

[26] House cooper, P. (2024). Tech advancements in the region heighten cyber-threats as Middle East Leaders act, according to new PWC report. Retrieved from https://www.pwc.com/m1/en/media-centre/2024/tech-advancements-in-the-region-heighten-cyber-threats-as-middle-east-leaders-act-according-to-new-pwc-report.html

[27] Haq, I. u. (2024, 03 26). Iran and Hezbollah: *Proxy powerplay*. Institue for Security and development policy. Retrieved 01 07, 2025, from https://www.isdp.eu/iran-and-hezbollah-proxy-power-play/

[28] Mimran, D. T., & Dahan, G. (2024, 04 20). *Artificial Intelligence in the Battlefield: A Perspective from Israel*. OpinioJuris. Retrieved 01 07, 2025, from http://opiniojuris.org/2024/04/20/artificial-intelligence-in-the-battlefield-a-perspective-from-israel/

[29] Kamiński, M. A. (2020, 06 05). 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-sabotage-as-a-tool-of-American-nintelligence-aimed,121974,0,2.html

[30] (ACW), A. C. W. D. (2023). Assessing the Abraham accords, three years on. Retrieved from https://arabcenterdc.org/resource/assessing-the-abraham-accords-three-years-on/

[31] 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-water-supply-could-have-sccckened-hundreds-report/

[32] 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-total-disarray-at-iran-port-report

[33] Hassenstab, N. (2024, February 5). *Understanding Iran's Use of Terrorist Groups as Proxies*. American University. Retrieved January 8, 2025, from

https://www.american.edu/sis/news/20240205-understanding-irans-use-of-terrorist-groups-as-proxies.cfm

[34] VOA news. (2024, February 8). Iranian Hackers Interrupt UAE Broadcasts with Deepfake News. VOA. Retrieved January 8, 2025, from https://www.voanews.com/a/iranian-hackers-interrupt-uae-broadcasts-with-deepfake-news-/7480126.html

[35] *Incident of The Week: Shamoon Virus Cripples Hundreds of Computers*. (2018, 14 12). Cyber security hub. Retrieved 01 08, 2025, from https://www.cshub.com/attacks/news/incident-of-the-week-shamoon-virus-cripples-hundreds-of-computers

[36] Saban, N. (2020, November 5). Factbox: *Iranian influence and presence in Syria*. Atlantic Council. Retrieved January 8, 2025, from https://www.atlanticcouncil.org/blogs/menasource/factbox-iranian-influence-and-presence-in-syria/

[37] Fulton, W., Holliday, J., & Wyer, S. (2013). Iranian strategy in Syria. Retrieved from https://www.understandingwar.org/report/iranian-strategy-syria

[38] Alcamo, I. (2024, December 2). *The future of Israeli-Saudi relations: opportunities and challenges* -. IARI. Retrieved January 8, 2025, from https://iari.site/2024/12/02/the-future-of-israeli-saudi-relations-opportunities-and-challenges/

[39] Gause, F. G., Alghashian, A., & Leshem, O. A. (2025). How tech is cementing the UAE-Israel alliance. Retrieved from https://www.mei.edu/publications/how-tech-cementing-uae-israel-alliance

[40] Scheer, S. (2023). Bahrain aims to use closer ties to tap Israel's tech expertise Reuters. Retrieved from https://www.reuters.com/world/middle-east/bahrain-aims-use-closer-ties-tap-israels-tech-expertise-2023-09-07/

[41] y Teran, A. M. (2024, 5 15). *Handling Israel-Hamas war mediation: The role of Qatar*. unav. Retrieved 01 08, 2024, from https://www.unav.edu/web/global-affairs/handling-israel-hamas-war-mediation-the-role-of-qatar

[42] Khatinoglu, D., & Shokri, U. (2024, march 11). *Qatar's Gas Ambition Affects Iran's Reserves*. Iran international. Retrieved 1 8, 2024, from https://www.iranintl.com/en/202403118957

[43] Times of Israel. (2021, April 21). *Israeli cyber-firm NSO said in talks with Jordan over sale of new spy technology*. times of Israel. Retrieved 1 8, 2024, from https://www.timesofisrael.com/liveblog_entry/israeli-cyber-firm-nso-said-in-talks-with-jordan-over-sale-of-new-spy-technology/

[44] Sarfraz, M. (2024). How Israel Harnesses technology to advance its offensive in the Middle East. Retrieved from https://www.dawn.com/news/1862118

[45] Ghaddar, A. (2023). Houthi attacks in the bab al-mandab strait hit global trade reuters. Retrieved from https://www.reuters.com/world/bab-al-mandab-shipping-lane-target-israel-fights-hamas-2023-12-12/

[46] Dagres, H. (2021). Lessons from Israel and Egypt's lukewarm peace. Retrieved from https://www.atlanticcouncil.org/blogs/menasource/lessons-from-israel-and-egypts-lukewarm-peace.