# A Cyber War of Iran-Israel: A Geopolitical Rivalry

Laila Rizky Amaliya

[1] University of Indonesia, Jakarta, Indonesia
[2] Jl. Salemba Raya No.4, RT.1/RW.5, Kenari, Kec. Senen, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10430
laila.rizky31@ui.ac.id

**Abstract.** Israel and Iran have been engaged in an expanding conflict across the Middle East since the late 1990s. Following the outbreak of the Israel-Hamas war, the escalation of conflict between the two counterparts have been intensified into another level. According to reports in media, Iran and Israel have surged their cyber, influence, and cyber-enabled influence operations against one another to protect their own national securities. The *cyberwar* between Israel and Iran have also been used as a way both countries gain significant influence and hegemony in Middle East. This article provides comprehensive explanation about the dynamics of Israel-Iran cyberwars since October 7th attacks and their geopolitical rivalry in Middle East region. To analyze the topic , we use realism and hegemony theory in IR. By using qualitative study with interpretative analysis method, this article will give insights about the cyber war between Iran and Israel since October 7th conflict escalation explain about their geopolitical rivalry based on realism and hegemony perspective in International Relation. Cyber operations plays a major role in Israel and Iran conflict. Cyber operations plays a major role in Israel and Iran conflict. The two actors used cyber operations to weaken each other security in Middle East. Both countries also want to gain power standing in Middle East and want to become the only hegemon power that dominating Middle East and decrease the opponents hegemony for its own security and main interests.

**Keywords:** Cyberwar, Iran, Israel.

## 1 Introduction

Israel and Iran have been engaged in an intense conflict across the Middle East since the late 1990s. The conflict has been the most significant ‘political power war’ in Middle East and contribute largely to the increase of regional instability. Israel considers Iran to be an “existential threat” after Iran significantly accelerated its nuclear programme, support militant and independence groups that threatened Israel, and call for the destruction of Israel. Meanwhile, Iran also sees Israel as threat and sources of predominant challenge, especially for Iran’s national sovereignty and its proxies in


I. K. Rohman et al. (eds.), *Proceedings of the International Conference on Strategic and Global Studies (ICSGS 2024)*, Atlantis Highlights in Social Sciences, Education and Humanities 33,
https://doi.org/10.2991/978-94-6463-646-8_4

such as gaining nuclear programs and hold many military interventions toward Israel(Huang, n.d.-a). Iran and Israel have surged their cyber-attacks operations against one another to protect their own national securities. The cyberwar wasn't something new for Israel and Iran as both countries have been engaged in conflict in the past 30 years. Iran and Israel have exchanged blows in cyberspace, attacking each other's civilian targets since a decade (Bahgat, 2020). Furthermore, cyber warfare is conducted secretly, unless one of the sides in the confrontation has an interest in exposing it. The attacks are generally launched without claiming responsibility or with denying responsibility, if at all ascribed. In most cases, identifying the source of the attack is difficult. Attacks in cyberspace are considered to suit a "campaign between wars," since they enable the attacker to operate from afar, secretly, and avoid human casualties on both sides in order to avoid escalation. Cyberattacks allow information collection to enable cognitive warfare, send deterrent messages, increase pressure on military and civilian systems in order to achieve defense and political goals, and launch preventive actions(Syed et al., 2019).

The Israelis Stuxnet attack against Iran's nuclear facilities are one of the biggest Israelis cyberattack in Middle East. It revealed in 2010 and was a formative event regarding military cyberattacks on infrastructure. The attack on the command-and-control systems of essential civilian infrastructure is considered to be at a high level on the scale of seriousness of cyberattacks. Over 15 Iranian facilities were attacked and infiltrated by the Stuxnet worm. It is believed that this attack was initiated by a random workers' USB drive. One of the affected industrial facilities was the Natanz nuclear facility. The first signs that an issue existed in the nuclear facility's computer system in 2010. Inspectors from the International Atomic Energy Agency visited the Natanz facility and observed that a strange number of uranium enriching centrifuges were breaking(Huang, n.d.-a).

Although Iran has not released specific details regarding the effects of the attack, it is currently estimated that the Stuxnet worm destroyed 984 uranium enriching centrifuges. By current estimations this constituted a 30% decrease in enrichment efficiency(Syed et al., 2019). In 2020, Israel also reportedly launched a cyberattack on May 9, 2020 against the Iranian port at the Shahid Raja'i port in Bandar Abbas in southern Iran. Israel's attacks toward Iran are the responses to Iranian cyberattack against water and sewage infrastructure "the water system" in Israel. The attack against the Israeli water system was carried out at a number of points throughout the country on April 24 and 25, 2020. Indeed, the Iranian cyberattacks makes Israelis forced to deal with damage to the civilian population, and even with a temporary water shortage that could have caused extensive damage and disaster(Siman-Tov & Even, 2020).

The two actors are engaged in more intense cyber struggle. Following the tension relationship between the two countries, the escalation of conflict have been intensified into another level. The *cyberwar* between Israel and Iran have also been used as a way both countries gain significant influence and hegemony in Middle East. Moreover, Israel and Iran are the main superpowers wanting to become the dominant regional power that

entrenches its influence in the Middle East. Israel and Iran are wanting to show that their military advance technology and arms capabilities can lead them as a powerful actor in Middle East. The successful *cyberattacks* as a tool to maintain Iran and Israel's superiority in the Middle East through the use of technologically advanced cyber system that can have significant dangerous and damage effects. This article provides comprehensive explanation about the dynamics of Israel-Iran cyberwars since October 7th attacks and their geopolitical rivalry in Middle East region. To analyze the topic , we use realism and hegemony theory in IR. By using qualitative study with interpretative analysis method, this article will give insights about the cyber war between Iran and Israel's conflict escalation and its their geopolitical rivalry based on hegemony and realism perspective.

## 2 Theoretical Framework

### 2.1 Theories of Realism

Realism emphasizes the importance of power, national interest, and self-help in shaping international relations (e.g., alliances, peace establishments, etc.). According to realists, the international system is chaotic and characterized by the absence of a centralized authority, and nations must pursue their own interests to ensure their survival. In particular, realists argue that conflict is inevitable in our world, and that cooperation between nations is limited and often driven by temporary interests. Realism perspective sees international relation as study that emphasize on reality "what exists" and not "what should exist". According to realist, conflict already exists closely "in front of the door" caused by violence and egoism of every human being(Rusdiyanta, 2022).

To create a path toward sovereignty and independence nation, every country most likely doesn't obey authority caused by the nature of human being which want to dominate everything. This egoism and self-centrist nature can potentially lead to conflict. Realist also believes that moral principle cannot be implemented as a tool to understand politics. As being referred to Morgenthau, political realism isn't emphasizing a morality check but only sees the interest of the nations in international politics and positioning morality as "second number"(Susilowati et al., 2022). For the realists, international relations, like the Hobbesian state of nature, represents a everlasting conflict between states and resembles a wholly zero-sum game because the most important actors in international relations are great powers whose status is mostly defined by political power, territorial size and material resources(Wu, 2018).

### 2.2 Theories of Hegemony

The concepts of hegemony and hegemon have a long pedigree in International Relations. A foundation stone for much IR theorising is Thucydides' The Peloponnesian War (431 BC), which deals with the Athenian hegemony and its implications for the Greek city-state system. By using conventional approach, the concept of hegemony has conventionally been used to highlight a condition of disequilibrium of power in the

international system, in which one state becomes so powerful that can exercise dominance over the international system. This state, often referred to as hegemon, hegemonic power that has capacity to exercise essential control over the structures of the international system, as well as the (international) behaviour of its constitutive units(Antoniades, 2018).

Superiority of the hegemon may lie include geography, natural resources, economic capacity, military capacity and preparedness, population (both quantitative and qualitative aspects such as education), morale and unity, quality of diplomacy and government, technological innovation etc. In this approach hegemony appear as a top-down, agential phenomenon, where the existence and reproduction of the hegemon / the hegemonic power is based on its ability to maintain its superiority mainly in terms and through the use of material capabilities(Antoniades, 2018). This inherently grants the hegemonic state a great capacity for coercion, influence and control over the international system structure and, consequently, the international behavior of its constituent units. Thus, the unipolar international order defines the system of hegemony for the realists(Ashraf, 2023).

## 3. Method

In order to explain Israel and Iran cyberwar and its geopolitical rivalry, I will use qualitative research method in this research article because it explores social science and humanities field accurately. According to Creswell, qualitative research is a post-positvism and mostly inductive research method. This qualitative method enable researcher generating meaning from data collected in the field . Qualitative research is a method that start with building an assumption and then using theoretical framework in study or research that relate to the social or human phenomenon and issue. It focuses on a naturallistic material intepretations which can be a tool to understand different perspectives in society. The methodology and procedure of qualitative research also influenced by researcher's experiences to collect and analyze datas. This article use a descriptive-analytical approach, using data and works of literature, collected various books, journals, and online resources related to the topic.

From the ontological perspective, qualitative method is a method that strongly related to the reality character and its features and also fully recognize various realities. These various realities include using various proof in a research theme with actual characteristics of man and provide different perspective. From epistemology assumption and perspective, the researchers should involve themselves with the participants whose become their research object closely. Axiologically, the researchers should recognize the added-values and actively reporting their own values and biases from the study. Generally, the qualitative method has been used to explore a problem or issue that need to be investigated. This study exploration in qualitative method is beneficiary, especially to learn a group or specific population, identify variables that bring about detail and comphrensive's understanding of the study. Moreover, qualitative method explains

about the mechanism or affinity in a theoretical or casual modes. It also beneficary for explaining partial theories or incomplexity theories in our research problems(Creswell, 2023).

## 4. Literature Review

Israel and Iran have a long and complex history of political and military tensions that date back to the 1979 Iranian Revolution. The two countries have been on opposite sides of various regional conflicts and have often viewed each other as a direct threat and frequently take military action concerning its national security. Furthermore, since the October 7th tragedy, Iran and Israel have surged their cyber-attacks operations against one another to protect their own national securities. The cyberwar wasn't something new for Israel and Iran as both countries have been engaged in military conflict over the years. The conflict escalation in October 7th makes Iran and Israel involve in greater cyberwars. As a leader of technological and digital innovation, especially in military equipments, both countries are frequently use their advanced technological cyber equipments to weaken each other security and as a way both countries gain military power in Middle East. In addition, many previous literatures had already explored about Israel and Iran cyberattacks. It can be adopted as a primary basis of this research. Otherwise, previous studies can also beneficiary for gaining new perspectives toward Israel and Iran cyberwars.

The Israel and Iran cyberwar's issue has been the most significant security challenge in Middle East region. Gawdat Bahgat's article named "Iran and its Neighbor Face Risks and Opportunities in Cyber Security" highlighting the role that cyber warfare plays in Tehran's broad defense strategy. Iranian leaders see the cyber domain as simultaneously an existential threat and an opportunity to attack their adversaries. Iran accuses the United States and its allies utilizing soft power to brainwash Iranian youth society and alienate them from the Iran's core ideology of Islamic revolution. But at the same time, Iran sees cyber as a convenient weapon to attack its adversaries. This article also explains about the growing of cyber capabilities in neighboring country, particularly the State of Israel. Israel's cyber weapon development was inspired by the domino effect of Iranian cyber development in Middle East. Iran's cyber weapon development resulting domino effect in Middle East.

It encourages the growing of cyber capabilities in neighboring countries, particularly the State of Israel and the Kingdom of Saudi Arabia. Israel, although, sees cyber warfare as one of the most critical threats to Israel's vital infrastructures in both the civil and the military-security sectors since Iranian development of cyber materials. In spite of demonstrate the cyberwars of Israel and Iran and its geopolitical rivalry dynamics in Middle East, this article only illustrates about the history and development of Israel's technological cyber equipments from years to years and its significant risks and opportunies ahead(Bahgat, 2020).

Furthermore, another research journal by Cohen etc. “Israel and Cyberspace: Unique Threat” provides insights about the dangers and opportunities on Israeli use of cyberspace and the backgrounds and factors that lead Israel develop highly advanced cyber equipments. This research also explains the development of cyber equipments based on security perspectives. As Israel experiences a constant barrage of cyberattacks, the development of cyber technology as a way to secure their national security and possibly defend them against attacks by individual and groups. Israel also has responded to these threats by developing myriad ways to use cyberspace as a platform for promoting its interests, both offensively and defensively, and also create solid policies regarding the use of cyber system and technology innovation (Cohen et al., 2015).

However, this article isn’t addressing the dynamics of Iran and Israel cyberwars and its impact on geopolitical rivalry in Middle East. In fact, Iran and Israel cyberwars in Middle East should be mentioned in this research because of its significant impacts on Middle East geopolitics. The cyberwars between Iran and Israel are the most important thing to potray the complex relation between two superpowers in Middle East and explain the two countries competition for hegemonic power. Existing academic research regarding Israel has largely focused on limited aspects of Israeli-Iran cyberwar. This article addresses gaps in existing studies by focusing the research on comprehensive analyses about Iran and Israel’s cyberwars and its geopolitical rivalry.

## 5. Result and Analysis

### 5.1 Cyberwars in Middle East and Geopolitical Rivarly: The Case Study of Iran and Israel

The relationship between Iran and Israel has been deteriorating since the era of Iranian Islamic revolution in 1979. The Islamic Republic of Iran, established after the revolution, adopted a strong anti-Israel ideology and has since been a vocal opponent of Israel's existence as a state(Dryden, 2024). The main sources of tension between the two countries have been Iran's support for various militant groups that significantly make Israel unsecured. Iran has provided financial, military, and logistical support to groups such as Hezbollah in Lebanon and Hamas in Gaza, which have carried out attacks against Israeli targets. Furthermore, Israel sees Iran's support for these groups as a direct threat to its national security and has taken military action against them(Hamdi, n.d.). Another source of tension between Israel and Iran has been Iran's nuclear program. Israel consider Iran as a predominant security challenge as Iran develop its nuclear weaponization and gain power at the regional level (Huang, n.d.-a).

Iran also has a different standpoint of the Palestinian’s issue . Iran’s support for the independence of Palestine and its state establishment of Palestine has been critical for Israel's security. As one of the key player in Middle East, Iran is the predominant challenge for Israel’s security. Moreover, Iran also sees Israel as threat, especially for Iran’s national sovereignty and its proxies in Middle East region. Israel and Iran’s concern of

security lead them to strengthen its arms capabilities and hold many military interventions (Huang, n.d.-a) Overall, the historical problems between Israel and Iran are complex and multifaceted, and they reflect broader tensions in the region. The conflict between Iran and Israel has been escalated significantly and contributed largely to the increase of regional instability.

The two superpowers have involved in many military activities such as airstrike, constrained warfare, cyberattacks, and land strike to weaken each other's power, making it as a zero-sum game. One of the main military invasions that surged between the two couterparts are cyberattacks. Iran and Israel have surged their cyber-attacks operations against one another to protect their own national securities. The Israelis Stuxnet attack against Iran's nuclear facilities are one of the biggest Israelis cyberattack in Middle East. It revealed in 2010 and was a formative event regarding military cyberattacks on infrastructure. The attack on the command-and-control systems of essential civilian infrastructure is considered to be at a high level on the scale of seriousness of cyberattacks. Over 15 Iranian facilities were attacked and infiltrated by the Stuxnet worm. It is believed that this attack was initiated by a random workers' USB drive(Netolická & Mareš, 2018).

One of the affected industrial facilities was the Natanz nuclear facility. The first signs that an issue existed in the nuclear facility's computer system in 2010. Inspectors from the International Atomic Energy Agency visited the Natanz facility and observed that a strange number of uranium enriching centrifuges were breaking. Israel's cyber capabilities were considered as technologically advanced military capabilities which could damage one of the most Iranian's important assets, nuclear facility. Iran's nuclear program had became existential threat for Israel's security. Israel's attack toward Iran's main nuclear facility led the conflict between two counterparts escalated. Those attacks have a significant effect to Iran which could weaken Iran's security(Huang, n.d.-b). Clearly, Israel wants to become the only 'powerful state' in Middle East to ensure the security of itself.

Iran couldn't maximalize its nuclear development as the main source of its national security. Therefore, Iran wouldn't acquire the nuclear power. The conflict escalation and geopolitics rivalry between Iran and Israel also become the main reasons why Israelis afraid of the potential risks and dangers that Iran can do with its nuclear weaponization program. Iran's support and encouragement of armed hostilities against Israel, and its effort to sabotage the peace process has turned Iran into one of Israel's staunchest enemies. In line with that, many military activities that Israelis do to prevent Iran acquire its nuclear weaponization. Israeli international diplomatic efforts against Iranian nuclearization and the implied military threats to destroy the Iranian nuclear facilities have enhanced Iranian hostility toward Israel (Evron, 2024).

Regarding to this matter, Israel could not let Iran's power dominated in Middle East. Israel strives to acquire more power to weaken Iran's and damage its nuclear because Israel's ambition to remain as a superpower that dominating the Middle East. If Iran

acquire more power over the Israel, Israel would be in a dangerous situation. Iran's power in the Middle East could prevent Israel to achieve their interest in Middle East such as Israel's military expansion at Gaza and Lebanon and its ambition through the great of Israel that wanted to enlarge Israel's territory based on Zionism ideology. That's why Israel has continuously sought to degrade Iran- linked nuclear infrastructure through frequent cyberattacks. Israel has the most significant cyber capabilities in the MENA region, on eye level with the world's first-tier cyber powers United States, Russia, and China(Bahgat, 2020).

However, In 2011, Iran took revenge toward Israel by reportedly launched "Newscaster" against Israel. Iran making a series of false virtual identities with ties to government officials and reporters. With its technological power, Iran could compromised over 2,000 computers. Moreover, Iran have been able to penetrate defenses in several government agencies and to have successfully accessed restricted information from Israel's system. During the 2014 Gaza, Iran also attacks exceeded all previous ones, both in scope and breadth of the targets selected. The Islamic Republic has been identified as the author of 19 state-sponsored offensive cyber operations since 2010(Cohen et al., 2015).

Iran, as one of the regional power use its advanced cyber technology to attack civilian infrastructure, including financial networks, government security systems, including, an attempt to seize control of Israeli drones. Iran's cyber ability making Iran as one of the most technological power house in Middle East. Iran is using cyberspace to develop and deploy asymmetric tools against its own regional rivals, Israel. The cyber's technology would become Iran's main source of power to combat superpowers like Israel. The growth of Iran's cyber technology also could actually beneficiary for Iran to strengthen its state security from many existential threats. Iran would make it as chance to prove that its military, technology and political power would change the positioning of Israel as a hegemonic power in Middle East. With its technological power which could destroy Israel's most advanced digital system that would make Iran counterbalancing the hegemony of Israel and western countries in Middle East.

Israel reportedly also launched a cyberattack on May 9, 2020 against the Iranian port at the Shahid Raja'i port in Bandar Abbas in southern Iran, in response to an Iranian cyberattack against water and sewage infrastructure ("the water system") in Israel. In early May 2020, networks supporting shipping and cargo handling operations within the Iranian port of Shahid Rajaei at Bandar Abbas allegedly suffered disruptions following a cyber intrusion. The state-owned Rajaei facility has remained one of the country's key logistics hubs, handling over 85 percent of Iranian import-export cargos. Although downplayed by the Iranian Ports and Maritime Organization, satellite imagery showed continued disruption suggesting extensive delays at the container terminals' eight vehicle entry and exit lanes(*A New Level in the Cyber War between Israel and Iran.Pdf*, n.d.).

Western and Israeli media reporting has linked this incident to offensive action by the government of Israel, allegedly in direct response to an attempted Iranian intrusion in late April 2020 against multiple Israeli water utility networks. These alleged Iranian attacks sought to alter industrial control systems in a manner that may have been intended to create lethal effects. The alleged water treatment attack could also have been operational preparation of the environment for action timed as part of annual campaigns associated with Qods Day. While this date typically sees attempted intrusions and disruptive attacksfrom multiple ideologically motivated actors, in prior years these attempts have usually had only limited or merely symbolic impact.

The conflict between the two actors is heating up again in 2023(Dekel, n.d.). Hamas' attack on 7 October 2023 tightened linkages between the enduring occupation of Palestine and the regional standoff between Israel and Iran04/12/2024 14:47:00. Political tensions and high conflict escalation makes the war become inevitable between the two superpowers in Middle East as Israel and Iran's prioritize military actions as its primary drivers. The international anarchist system makes Iran and Israel compete with each other to deliberately strengthen their power in Middle East. Iran and Israel make various efforts without even focusing on moral values and seek to gain control and strengthen their power among other countries. Based on The Economist, the intensity between Iran and Israel's cyberattacks rose three-fold than before(Huang, n.d.-b).

Iran's targeting of Israel in the cyber realm has spiked dramatically since the wider regional conflict sparked. After Hamas-Israel war on 2023, Iran have striked Israeli radar systems in the weeks(Barnea, n.d.; Ji-Hyang, n.d.; Mercan, 2023). Similarly, Iran also has launched many social media operations with the aim of destabilizing Israel's cyber security. An account called "Tears of War" impersonated Israeli activists critical of Prime Minister Benjamin Netanyahu's handling of a crisis over scores of hostages taken by Hamas, according to the report. An account called "KarMa", created by an Iranian intelligence unit, claimed to represent Israelis calling for Netanyahu's resignation. Iran also began impersonating partners after the war started. Likewise, Iranian services created a Telegram account using the logo of the military wing of Hamas to spread false messages about the hostages in Gaza and threaten Israelis. Iran's targeting of Israel in the cyber realm has spiked dramatically since the wider regional conflict sparked. Iran sees Israel as threat and sources of predominant challenge, especially for Iran's national sovereignty and its proxies in Middle East region. Iran's concern of security lead them to attacks Israel in numerous way. In this context, Iran shows its cyberattack capabilities which could reach one of the most advanced Israel radar and national systems in the world.

Since a decade ago, Iran has focused to expand its cyber and technology capabilities and invested in numerous arms development. Iran's government allocated $1 billion in July 2011 to enhance its cyber capabilities by acquiring new technologies and hiring cyber specialists. The growing attention of cyber technology make Iran developed its newest advanced cyber technology equipment. Furthemore, Iran develop many cyber technologies such as surveillance gear, intelligence tools, covert photographic

equipment, and lying detectors that could have attacking digital and infrastructure systems effectively to combat Israel. Iran also have been developing technologies designed by Microsoft-backed OpenAI to improve their cyber espionage skills. Iran's acquisition of cyber warfare features is a powerful complement to carry out espionage against and attack more powerful adversaries in support its national security goals and to combat Israel and western countries attempt to attack Iran's digital infrastructure.

Cyber equipments plays a major role in Iran's asymmetric defence strategy for streghtening its security by increasing cyberattacks abilities. These cyber capabilities have enabled Iran launched attack at Israeli radar and national systems within weeks. Moreover, Iran sees this operation as a way to weaken Israel's national security and its military power. Furthermore, by attacking Israelis radar and security system, Iran could possibly launched military attacks toward Israel, destablizing Israelis national security, and gain its power over Middle East states. By increasing its cyber technology system and military power, Iran would gain its significant influence and hegemony in Middle East. The development of cyber technology equipments can be seen as Iran's hegemonic strategy to become progressive regional power. The improvement of Iran's cyber security would actually influence Iran's position in Middle East. Iran would become the superpower challenging Israel's position as the most powerful country in Middle East. Iran would likely to eliminating Israel and Western influence in the Middle East and advancing its philosophy of Islamic revolution based on "anti-Imperialism"(Bahgat, 2020).

## 6. Conclusion

Israel and Iran have been engaged in an expanding conflict across the Middle East since the late 1990s. The relationship between Iran and Israel has been deteriorating since the era of Iranian Islamic revolution in 1979. Following the outbreak of the Israel-Hamas war, the escalation of conflict between the two counterparts have been intensified into another level. Iran and Israel have surged their cyber, influence, and cyber-enabled influence operations against one another to protect their own national securities. One of the most important operations between the two countries are cyber-attack operations. Cyber operations plays a major role in Israel and Iran conflict. The two actors used cyber operations to weaken each other security in Middle East. Both countries also want to gain powerful influence in Middle East and want to become the only hegemon power that dominating Middle East. It would lead to decrease the opponents power for its own security and main interest.

**Acknowledgments.** I sincerely thank Indonesia Education Scholarsip from Ministry of Education for providing me with financial support during my study and research. I would also like to express my gratitude to dean and lectures of Middle East and Islamic Studies, University of Indonesia for their kind technical/consultative assistance.

**Disclosure of Interests**: This research grants from Indonesia Maju Scholarship from Ministry of Education, Indonesia. The research support including salaries, equipment, supplies, reimbursement for attending symposia, and research by Indonesia Maju Scholarship that may gain or lose financially through publication of this manuscript.

## References

1. A New Level in the Cyber War between Israel and Iran.pdf. (n.d.).
2. Antoniades, A. (2018). Hegemony and international relations. International Politics, 55(5), 595–611. https://doi.org/10.1057/s41311-017-0090-4
3. Ashraf, N. (2023). Revisiting international relations legacy on hegemony: The decline of American hegemony from comparative perspectives. Review of Economics and Political Science, 8(6), 410–426. https://doi.org/10.1108/REPS-05-2019-0061
4. Bahgat, G. (2020). Iran and Its Neighbors Face Risks and Opportunities in Cyber Security. Orbis, 64(1), 78–97. https://doi.org/10.1016/j.orbis.2019.12.006
5. Cohen, M. S., Freilich, C. D., & Siboni, G. (2015). Israel and Cyberspace: Unique Threat and Response. International Studies Perspectives, ekv023. https://doi.org/10.1093/isp/ekv023
6. Creswell, J. (2023). Penelitian Kualitataif dan Desain Riset: Memilih Di Antara Lima Pendekatan (1st ed.). Pustaka Pelajar.
7. Dryden, J. (2024). IRAN, ISRAEL, AND THE STRUGGLE FOR THE SKIES OVER THE MIDDLE EAST.
8. Evron, Y. (2024). An Israel-Iran Balance of Nuclear Deterrence:
9. Hamdi, W. (n.d.). The Abraham Accords: Reasons, Contexts, and Implications.
10. Huang, X. (n.d.-a). THE IRANIAN NUCLEAR ISSUE AND REGIONAL SECURITY: DILEMMAS, RESPONSES AND THE FUTURE.
11. Netolická, V., & Mareš, M. (2018). Arms race "in cyberspace" – A case study of Iran and Israel. Comparative Strategy, 37(5), 414–429. https://doi.org/10.1080/01495933.2018.1526568
12. Rusdiyanta, R. (2022). Pengantar Ilmu Hubungan Internasional (Cetakan ke-1). PT. Rajagrafindo Persada.
13. Siman-Tov, D., & Even, S. (2020). A New Level in the Cyber War between Israel and Iran. Institute for National Security Studies. https://www.jstor.org/stable/resrep25542
14. Susilowati, I., Fauzi, M., Virqiyan, S., & Zahidin, A. E. (2022). Eksistensi Realisme dalam Aneksasi Israel Terhadap Palestina. JOURNAL of LEGAL RESEARCH, 4(5), 1155–1172. https://doi.org/10.15408/jlr.v4i5.28514
15. Syed, R., Khaver, Ahmad Awais, & Yasin, M. (2019). Cyberwarfare. Sustainable Development Policy Institute. http://www.jstor.com/stable/resrep24376.7
16. Wu, Z. (2018). Classical geopolitics, realism and the balance of power theory. Journal of Strategic Studies, 41(6), 786–823. https://doi.org/10.1080/01402390.2017.1379398
17. Barnea, A. (n.d.). Israeli Intelligence Was Caught Off Guard: The Hamas Attack on 7 October 2023—A Preliminary Analysis. 0(0).
18. Dekel, U. (n.d.). *The Israel-Hamas War: Israel Needs a Political Idea*.
19. Ji-Hyang, J. (n.d.). Israel-Hamas War: Analysis and Prospects.
20. Mercan, M. H. (2023). Operation al-Aqsa Flood: A Rupture in the History of the
21. Palestinian Resistance and Its Implications. Insight Turkey, 25(Fall 2023), 79–90. https://doi.org/10.25253/99.2023254.6