

Aleksandar Bogićević*

*Strategic Research Institute, University of Defence, Belgrade,
Republic of Serbia*

ISRAEL-IRAN CYBER WARFARE: THE DIGITAL DIMENSION OF MIDDLE EASTERN CONFLICTS IN A POST-UNIPOLAR WORLD**

(Translation in *Extenso*)

Abstract

The conflict between Israel and Iran represents one of the most enduring confrontations in the Middle East. Over the past decade, its dynamics have increasingly been characterised by multidimensionality, reflected in the spillover of the conflict beyond traditional military-political frameworks into other domains, including the digital sphere. Following the Israeli Stuxnet attack on Iranian nuclear infrastructure in 2010, the cyber field has become a pivotal arena of confrontation, involving not only Israel and Iran but also affiliated cyber actors, often operating from third-party states, which adds a further layer of unpredictability and complexity to the conflict. What makes this cyber confrontation particularly significant for interstate relations in the highly sensitive Middle East is the ability of states to inflict damage on one another

* E-mail address: aleksandar.bogicevic@mod.gov.rs; ORCID: 0009-0006-7450-5193.

** This paper was presented at the conference "Perspectives of Political Sciences in Contemporary Society IV", held on December 4–5, 2025, organized by the Institute for Political Studies, Belgrade.

without resorting to armed force. On a global scale, this conflict reflects a broader transformation of relations between major actors in the international order. The support provided to Israel by the United States, coupled with the growing cooperation of Russia and China with Iran, indicates that the Iranian-Israeli cyber war is becoming an integral part of global geopolitical competition. This research aims to analyse cyber warfare between Israel and Iran, its role in their broader conflict, and its effects on both states and the regional actors who, due to their interconnectedness and complex mutual relations, also become targets. The author highlights the growing importance of the cyber dimension as a field of competition in the Middle East, where “old conflicts” are taking on a new form by shifting the struggle into the digital space, making it an inseparable part of the region’s contemporary geopolitical reality in a post-unipolar world.

Keywords: Israel, Iran, cyber warfare, cybersecurity, Middle East.

INTRODUCTION

The widespread use of new technologies and the expansion of cyberspace have significantly influenced the transformation of global relations, providing state and non-state actors with new opportunities for action while simultaneously exposing them to entirely new risks (Rid 2013), to which states often have limited capacity to respond adequately. The very characteristics of cyberspace, such as anonymity, global connectivity, high-speed information flow, and low usage costs (Liff 2012, 422), have further encouraged states in their instrumentalisation. As a result, the cyber sphere has become a space for low-intensity conflict between states that, through the theft of sensitive data, manipulation in the information space, and disruption of the normal functioning of computer networks, attempt to inflict harm on their adversaries (Bogićević 2025, 305).

The process of global networking has been accompanied by significant changes in the distribution of power in the international order that emerged after the end of the Cold War. The gradual reduction of direct U.S. presence in the Middle East and the redirection of strategic attention toward East Asia have eroded Washington’s dominant role in the region, creating conditions for increased activity

by other global and regional actors. Among the states that have shown particular ambitions to fill the power vacuum and expand their influence is Iran, which, through establishing control over numerous armed groups in Middle Eastern countries, has gained significant regional influence. However, Iran's expansion encountered a significant obstacle in the form of an irreconcilable ideological enemy and key American ally in the region, Israel. Tel Aviv's aspiration to push the defense of its territory and population as far as possible from its own borders, on one hand, and the expansion of the network of pro-Iranian proxies in the Middle East, on the other, have brought these two states into a state of permanent friction (Netolická and Mareš 2018, 418), whereby the transfer of their rivalry into cyberspace has created a new source of insecurity for all Middle Eastern countries (Amaliya 2025, 49). The discovery of the Israeli-American cyberattack on the Natanz nuclear facility in 2010 will mark the beginning of a new phase in understanding cyberspace as a domain for state conflict.

This paper aims to analyse the genesis of the cyber conflict between Israel and Iran after 2010, with particular focus on incidents that followed October 2023. The central research question concerns the extent to which cyber instruments can compensate for power asymmetry in active regional conflict. The working hypothesis is that the effects of cyber operations remain strategically limited when the technologically and organizationally stronger actor is willing and able to integrate digital operations with kinetic actions. The scholarly contribution of this paper lies in its integrated analysis of this conflict as a case study of cyber capacity asymmetry in the post-unipolar order. Unlike the existing literature, which predominantly examines the technical aspects of incidents, this work emphasises the strategic effects and structural determinants of cyber operations.

The study of cybersecurity faces a significant methodological obstacle: the limited availability of verifiable information about cyber actors, their activities, and their effects. Unlike the mutual kinetic strikes carried out in June 2025, where it was possible to determine the physical damage inflicted more directly, establishing the consequences of cyber operations is much more complex due to the immaterial nature of digital space and the limited transparency of actors. The Israel-Iran cyber conflict is characterised by a pronounced asymmetry in

information sources: most data come from Western companies and organisations specialising in cybersecurity, while information from Iranian sources is subject to far more restrictions.

This paper covers cyber incidents in the period from 2010 to the present that meet the following criteria: 1) a clear connection to interstate relations between Israel and Iran, i.e., the existence of indicators that the incident has a political or strategically motivated character; 2) the existence of publicly available technical or institutional attribution of the attack; and 3) political-strategic significance, that is, the potential to influence the behavior of actors. Only data confirmed by at least two mutually independent sources or documented through technical indicators of compromise and official reports of relevant institutions are treated as “verified facts”. In contrast, claims by actors, media interpretations, and assessments by cybersecurity companies are analysed as analytical narratives rather than empirically established facts. In this way, an effort is made to clearly separate the descriptive level of analysis from the interpretive level.

CYBERSPACE AS THE NEW FRONT: ISRAELI RESPONSES TO THE IRANIAN THREAT

The perception of a permanent existential threat (Tabansky 2020, 46) has crucially influenced Tel Aviv to adopt a proactive and preventive approach to national defense, based on the principle of the “security triangle”, whose key components are deterrence, early warning, and the swift achievement of decisive victory on the battlefield (Freilich, Cohen, and Siboni 2023, 185). Since achieving lasting peace for Israel, as the ultimate strategic goal articulated by Ben-Gurion (Baram 2017, 3), is almost unattainable due to the impossibility of the permanent military neutralization of the Arab states, Tel Aviv has focused on achieving a more modest goal: the temporary disabling of the most prominent threat before the emergence of new threats in the region and a new cycle of conflict (Freilich, Cohen, and Siboni 2023, 185).

The end of the twentieth and the beginning of the twenty-first century witnessed an evolution in the sources of threats confronting

Israel. The transformation of these threats from the regular armed forces of Arab states to non-state actors, such as terrorist groups, also altered the nature of the conflict itself. Given the asymmetric nature of conflict with non-state actors, Tel Aviv could no longer rely on swift and decisive victories on the conventional battlefield, compelling its decision-makers to reconsider the principles of the “security triangle” (Freilich 2018, 199).

Concurrently with the increased presence of terrorist organisations, the growing significance of modern digital technologies for the functioning of the economy and society exposed Israel to an entirely new set of threats. As a state whose economy depends on the application of cutting-edge technologies in both economic and administrative domains,¹ Tel Aviv is particularly vulnerable to cyber threats. A pivotal moment in the recognition of cyberspace as a new source of insecurity occurred in 2010 with the revelation of the joint US-Israeli cyberattack on Iran’s nuclear facility at Natanz.

The fear of the development of Iran’s nuclear program, combined with a belief in the efficacy of preventive strikes as a mechanism to curb regional threats, led Israel to conduct, in cooperation with the United States, a cyber operation in 2006 (Kamiński 2020, 69) code-named “Olympic Games”, to turn off the Natanz nuclear facility. Over the following four years, the virus implanted in Iran’s computer network turned off approximately 1,000 gas centrifuges, though this did not result in a significant slowdown of the nuclear program (Albright, Brannan, and Walrond 2010). Nevertheless, the consequences were of considerable regional and global significance, as this marked the first known instance of a cyber operation with direct physical effects on the critical infrastructure of a sovereign state. Globally, the “Olympic Games” operation marked the beginning of a re-examination of the vulnerabilities of critical infrastructure to an entirely new class of threats, while regionally, the discovery of the cyberattack signalled the opening of a new front in the Iran-Israel conflict, one that would soon draw in other Middle Eastern states.

¹ As much as 13% of Israel’s GDP and 31% of its exports are derived from products and services generated in the high-tech sector. For more information on the significance of this industry for the development of the Israeli economy (Razin 2018).

After 2010 and the exposure of Israeli involvement in the cyberattack, Tel Aviv radically changed its perception of Iran as a threat, both in the physical and cyber domains (Baram 2017, 1). To maintain its technological edge against regional threats and adequately respond to potential Iranian retaliation, Israel began developing cybersecurity as a new pillar of its national defence. This is evidenced by the significant efforts and resources invested by the Israeli government in building institutions and subsidising the development of new startups (Government of Israel 2011, 2; Press 2017). Relying on public-private partnerships and global economic interconnectedness, Israel has established exceptional national cyber capabilities, thereby acquiring a decisive competitive advantage over actors it perceives as regional threats.

In addition to efforts to create a national cybersecurity sector, Israel has also relied heavily on international cooperation to enhance its capacities. The United States occupies a central position in Israel's growing network of international partners, with high levels of cooperation at both the intergovernmental level (Arshad 2025, 1148) and in the economic sphere. An intensive exchange of knowledge and information, particularly regarding Iranian capabilities and intentions in the digital domain, provides Israel with significant strategic advantages, enabling the optimal utilisation of its own resources in planning cyber operations (1141).

Since 2010, cooperation with regional actors who perceive Iran as a source of regional insecurity has emerged as an increasingly important component of Israel's cyber defence. The disabling of Saudi Aramco's computer network in 2012 served as a clear indicator of Iran's progress in the cyber domain, alerting Middle Eastern states to the growing intensity of this threat. To bridge the widening gap with Iran, countries such as Egypt, Saudi Arabia, and the United Arab Emirates have turned to Israel as a provider of cybersecurity (Al-Halawany 2021; Khorrami 2021). Beyond raising the level of regional resilience to Iranian threats in the digital sphere, Tel Aviv's cyber diplomacy has also significantly influenced the process of normalising relations with regional states (Freilich, Cohen, and Siboni 2023, 275), thereby representing an important step towards achieving one of

Israel's key strategic goals – the establishment of a more stable security environment.

The outcome of efforts at both the domestic and international levels has been the development of an exceptionally sophisticated cyber defence system, founded on a large number of successful companies,² a high degree of cooperation between the private sector and institutions, and the exchange of knowledge and information with leading international actors. The organic development of cyber capabilities through economic growth has enabled Tel Aviv to rank among the top countries in its ability to respond to cyber threats (Digital Watch Observatory 2025), a proclaimed objective at the beginning of the twenty-first century. In this regard, the Israeli approach to cybersecurity does not represent a discontinuity from earlier security doctrines, but rather their functional adaptation to new technological and geopolitical conditions.

IRAN AND CYBERSPACE: ASYMMETRIC STRATEGY, PROXY WARFARE, AND THE DIGITAL PROJECTION OF POWER

Iran's approach to cyberspace, as is the case with other authoritarian powers, is marked by ambivalence: on the one hand, it serves as a mechanism for controlling the population and propagating its own values through digital media; on the other, it represents a constant source of danger in the form of Western media influence. The presence of these media as alternatives to state-run outlets poses a particular challenge for the authorities in Tehran, who frequently face mass protests (Freilich, Cohen, and Siboni 2023, 140). Additionally, the opportunities that cyberspace offers as a medium for projecting influence in the region and conducting malicious operations have led Tehran to recognise cybersecurity as a key aspect of future national security. Notably, the mass protests of 2009 and the discovery of the US-Israeli Stuxnet virus in 2010 acted as catalysts for intensified

² An illustrative indicator of Tel Aviv's success after 2010 is the remarkable growth of its cybersecurity industry. Israel is now considered the world's second-largest centre for cybersecurity software development. For a more detailed discussion (Eisenstadt and Pollock 2021).

Iranian efforts to develop cyber capabilities (Anderson and Sadjadpour 2018, 10–11). For the survival of the ayatollah regime, cybersecurity has become as important as the development of nuclear weapons (Bucala and Pendleton 2015).

Iran's international activity in cyberspace plays a multifaceted role in its strategy to strengthen its regional position. Primarily, Tehran relies heavily on cyber means in its asymmetric actions in the Middle East, seeking to avoid escalations that could lead to armed conflict (Haroon 2024, 146) or to the depletion of resources among local proxies. At the same time, cyber instruments represent a relatively cost-effective and less visible means of gathering intelligence and targeting the institutions and businesses of other states. These activities frequently constitute the first step in information operations, which manifest through the publication of sensitive data or the articulation of specific political messages, intending to demonstrate capabilities and exploit perceived weaknesses of adversaries.

Drawing on lessons from the Stuxnet case, Iran significantly intensified its financial investments in this domain after 2010. Although precise data are not publicly available, estimates by the US Army War College indicate that Iran's cyber operations budget rose from \$76 million to \$1 billion over a four-year period, a clear indication of the importance Iran attaches to cyberspace (Shafa 2014). Particular emphasis has been placed on enhancing educational standards in information technology and on selecting personnel who have begun to fill positions in the cyber units of the Islamic Revolutionary Guard Corps and the Ministry of Intelligence (Netolická and Mareš 2018, 420; Keshavarz 2023, 122). Continuous investment has begun to yield results, as evidenced by the growing number of sophisticated attacks on critical infrastructure in other countries (such as the aforementioned 2012 attack on Saudi Aramco), which have led regional states to perceive Iran as an escalating cyber threat.

Attacks by Iranian cyber groups and their affiliated proxies on the computer networks of the Gulf states have continued in subsequent years, revealing several trends in Tehran's behaviour in cyberspace. Consistent with its strategy of relying on a network of proxy actors across the Middle East to conduct asymmetric operations and enhance its position, Iran has initiated a process of diffusing knowledge and

malicious tools from state cyber actors to affiliated non-state entities. This practice has increased Tehran's overall capacity to conduct offensive cyber operations, while simultaneously making it much more difficult to reliably identify the immediate perpetrators of attacks, thereby rendering responsibility for cyber actions diffuse and hard to attribute to a specific actor.

The low level of risk awareness and limited investment in cyber defence by Gulf states during the 2010s left them particularly vulnerable to operations by Iranian and pro-Iranian cyber actors. A telling indicator of the exposure of Middle Eastern actors to cyber threats is a study by Tenable, which found that as many as 95% of Saudi companies faced cyber threats that negatively affected their operations in 2019 (Tashkandi 2020), with Iran identified as the main source of attacks (Guzansky and Deutch 2019). In addition to targeting regional adversaries, Iranian-affiliated cyber actors have also conducted offensive operations against the United States, the main ally of Iran's regional opponents. These activities have included targeting critical infrastructure, such as the attack on the Bowman Dam in 2013 (United States Department of Justice 2016), as well as attacks on private companies and individuals, with particular focus on prominent opponents of the Tehran regime (Elgin and Riley 2014).

Like Israel, Iran has relied heavily on its network of allies as a source of technological innovation, empirical experience, and operational support in conducting cyber operations. Its primary partner in these efforts is Russia, with which Iran signed a cyber cooperation agreement in 2015 (Agence France-Presse 2015), further upgraded in 2021 with a Cyber Security Cooperation Agreement encompassing greater technology and information exchange, training, and assistance in international cyber incidents (El-Masry 2021). The Strategic Cooperation Agreement between Beijing and Tehran, concluded the same year, is also aimed at technology and information sharing, with significant Chinese investment in telecommunications infrastructure and software, enabling Iran to establish even tighter control and surveillance over its own cyberspace (Reuters 2021). Cooperation among these states is not limited to state actors in cyberspace, but also extends to non-state actors, including the exchange of stolen data and coordinated attacks on the critical infrastructure of other states. An

example of this informal cooperation was identified in joint operations by pro-Russian and pro-Iranian cyber actors during attacks on Western Balkan states in 2022 and 2023 (Oghanna 2023).

The efforts Tehran has made since 2010 in developing national cyber capabilities have made this instrument a critical component of its hybrid strategy. Alongside its reliance on proxy actors in the form of armed groups throughout the Middle East, one of the key instruments of Iran's regional activity, engagement of both state and non-state cyber actors has enabled Tehran to inflict additional damage on its adversaries with relatively limited resource expenditure. Nevertheless, unlike in Israel, where there is a broad consensus regarding cyber capabilities, this is not the case in Iran, highlighting significant differences in the capacities of the two states.

The International Institute for Strategic Studies (IISS) classifies Iran as a second-tier cyber power (International Institute for Strategic Studies [IISS] 2021b, 1), while Israel is ranked among the most advanced (International Institute for Strategic Studies [IISS] 2021a). The United States Department of Defence reached similar conclusions in its 2023 Cyber Strategy, which found that Tehran has not yet demonstrated the capability to conduct continuous, sophisticated cyber operations (U.S. Department of Defence 2023, 5). On the other hand, Siboni, Abramski, and Sapir assess that Iran's cyber capabilities have already reached the level of the most advanced countries (Siboni, Abramski, and Sapir 2020, 39–40), a view shared by Yigal Unna, former Director General of the Israel National Cyber Directorate (Israel National Cyber Directorate 2019).

Despite significant obstacles to development caused by international economic sanctions (Faris 2025, 10), brain drain, and a poorly developed private sector in cybersecurity (Freilich, Cohen, and Siboni 2023, 137), Iran has developed significant national cyber capabilities. These have provided it with an alternative mechanism of action in situations where the use of proxy armed groups is economically prohibitive, politically risky, or operationally unfeasible, a dynamic that has become particularly evident following the outbreak of conflict in Gaza in October 2023.

THE CYBER DIMENSION OF THE IRAN-ISRAEL CONFLICT AFTER OCTOBER 2023

Iran's position in the Middle East remained relatively stable until October 2023. Relying on an extensive network of allies and proxy actors, Tehran exercised influence over the Houthis in Yemen, Hezbollah in Lebanon, and Hamas in the Gaza Strip, while simultaneously projecting its power in Syria, providing crucial support to the Bashar al-Assad regime, and in Iraq, where it maintained control over numerous Shiite militias. However, following the incursion by Hamas militants into Israeli territory on October 7 and the outbreak of war in the Gaza Strip 20 days later, the Iran-Israel conflict entered a new phase, characterised by active hostilities between Israel and pro-Iranian militias and by reciprocal attacks during the Twelve-Day War of June 2025. In parallel, the cyber domain also witnessed an escalation involving both state and numerous non-state actors.

The trend of intensifying cyber operations during periods of heightened tensions between Israel and Iran was already evident in previous conflicts (2009, 2012, and 2014) in which these actors were engaged (Freilich, Cohen, and Siboni 2023, 120). The primary objectives of cyber actors included disabling or defacing government websites, targeting major financial institutions, and stealing data useful for military or further cyber operations (Brenner 2012); however, the outcomes of such operations were neither lasting nor particularly consequential for the overall course of the conflict. The outbreak of hostilities in Gaza in October 2023, however, marked the beginning of a transformation in the Iran-Israel cyber conflict, reflected in the increased sophistication of certain attacks, the expansion of the number of actors involved, and an overall intensification of cyber activity (The Economist 2024; ThreatMon 2026, 5–14).

Differences in the cyber warfare capabilities of Iran and Israel are clearly evident in an analysis of the types of operations that dominate each side, as well as the scope and nature of the damage they can inflict. Analysis of reports from cybersecurity firms (Watts 2024; Radware 2025; Reddy 2025) and government agencies (Cybersecurity and Infrastructure Security Agency 2025) reveals certain tendencies in the actions of Iranian and pro-Iranian cyber groups. The most common

is the conduct of information operations aimed at destabilising Israel by deepening social divisions, disturbing public morale, and eroding international support for Tel Aviv (Watts 2024). Iran also uses its cyber resources for intelligence purposes, primarily to collect sensitive information, such as data on members of the Israel Defence Forces, and to access surveillance camera footage for damage assessment (The Economist 2024; Newman 2025). On the other hand, despite numerous claims of successful operations (SOCRadar Cyber Intelligence 2025), there has yet to be any identified significant attack on Israeli critical infrastructure with lasting effects, an indicator of the limited reach of Iran's offensive cyber capabilities.

Israel, meanwhile, has conducted offensive operations in the Iranian cyber domain, primarily for intelligence purposes, gathering data relevant to the identification of military targets and key individuals, including nuclear scientists and senior officers of the Revolutionary Guard and Iran's regular armed forces (Zendata Cyber Security 2025), as confirmed by officials from both sides (Fassihi, Bergman, and Mazzetti 2025). Supporting this assessment is the decision by Iran's leadership, following an initial Israeli Air Force strike, to suspend internet access nationwide and instruct senior officials to set aside their mobile devices for fear they could be used for targeting and tracking (Politico 2025; Fassihi, Bergman, and Mazzetti 2025). Such measures indicate a pronounced perception of vulnerability within Iran's cyber domain and underscore the significant asymmetry in cyber capabilities between the two actors, an asymmetry Israel has leveraged as an additional instrument of its military and intelligence power.

Non-state cyber actors play a particularly distinct role in the conflict. Due to limited resources and expertise, they most often operate in the information domain (Pijpers 2023, 7). Nevertheless, both Iran and Israel employ cooperation with non-state cyber actors as a mechanism to obscure state involvement in specific activities. While examples of cooperation between Iranian state authorities and cyber actors are better documented (Sabin 2025; New Jersey Cybersecurity and Communications Integration Cell 2024), the case of the Israeli group Predatory Sparrow highlights the complexities of identifying the origins of attackers and their connections to state actors. Presenting

itself as a hacker collective opposed to the ayatollah regime, Predatory Sparrow has been responsible for highly sophisticated attacks on Iran's critical infrastructure, targeting steel plants, railways, and energy transportation systems (Miller 2025; Vicens 2023).

During the twelve-day conflict between Iran and Israel, this hacker group conducted several confirmed operations, primarily targeting the financial sector (Picus Security 2025). Particularly notable was an attack on Sepah Bank, known for its ties to the Iranian Revolutionary Guard and for financing Iran's missile program and various pro-Iranian proxies (U.S. Department of the Treasury 2007). Iranian sources confirmed that banking transactions were disrupted (The Times of Israel 2025), though there is no independent confirmation of the data destruction claimed by the hacker group (Vicens and Pearson 2025). Significant damage was also inflicted on the Iranian cryptocurrency exchange, a key institution in Tehran's efforts to circumvent sanctions-imposed trade restrictions (Zendata Cyber Security 2025). The unusual sophistication of these cyber operations has led many cybersecurity firms to categorise Predatory Sparrow as a non-state hacker group with very close ties to Israeli cyber units (Radware 2025; Miller 2025). This illustrative example underscores the growing challenge of cooperation between non-state and state actors in the cyber domain, making attribution and, subsequently, accountability significantly more difficult.

The Iran-Israel conflict since October 2023 demonstrates that cyberspace has become an integral part of contemporary armed conflict, not merely as an auxiliary tool but as an autonomous domain for projecting power. Whereas Iran has primarily used its cyber capacities for limited objectives such as intelligence gathering and information operations, Israel has succeeded in integrating its cyber operations into a broader intelligence-military apparatus, combining state and non-state actors to achieve concrete strategic effects. This practice highlights the growing role of the cyber domain in demonstrating power in asymmetric conflicts, where pronounced imbalances in cyber capabilities can have extremely detrimental consequences for states in a subordinate position, especially amid rising tensions and deepening instability in contemporary global affairs.

CONCLUSION

An analysis of the development of Israel's and Iran's cyber capabilities after 2010, as well as their subsequent use during the conflict in the Gaza Strip in October 2023, demonstrates that the digital realm has become an indispensable and structurally integrated component of contemporary national security strategies, and consequently, of armed conflicts, particularly evident in complex and politically sensitive security environments such as the Middle East. In parallel with the escalation of kinetic operations and the expansion of conflict between Israel and pro-Iranian actors (eventually including Iran itself), cyberspace has functioned as an additional, though not secondary, front, one that revealed profound differences in strategies and, especially, in the available capacities for waging cyber warfare.

Israel's approach to cybersecurity, deeply rooted in the "security triangle" concept, has successfully adapted to the new technological reality. Through strategic investment of substantial financial and administrative resources, Israel has stimulated the development of a high-tech industry, exemplified by numerous successful startups, thereby consolidating its position as a global leader in the field. Further impetus for the development of national cyber capabilities has come from the expanding network of international partners, particularly in its immediate neighbourhood, who view Israel as a key provider of digital security. This synergistic effect of state incentives and private entrepreneurship has not only strengthened national resilience but has also transformed cyber capabilities into an instrument of Israeli soft power and foreign policy engagement in the region.

For Tehran, by contrast, cybersecurity has become as important as the development of its nuclear program, not only for its ability to project national power externally, but also for controlling the internal information environment, which is directly linked to the survival of a regime challenged by frequent protests. Despite systemic obstacles to the development of cyber capabilities, foremost among them international sanctions, Iran has nevertheless achieved significant results. This progress is based on strategic cooperation with Russia and China, targeted domestic investments, and a careful personnel selection process. Although, according to available data, Iran has not yet reached

the level of technical sophistication demonstrated by Israeli actors, the progress achieved has been sufficient to position Tehran as a highly potent threat to regional cybersecurity.

The empirical examples examined in this study confirm the initial hypothesis that cyber instruments cannot fundamentally compensate for power asymmetries when the stronger actor can integrate them into a broader military-intelligence apparatus. Iran primarily employed cyber means as part of an asymmetric, limited-scope strategy. Iranian and pro-Iranian cyber activities focused on information operations aimed at generating social divisions and eroding international support for Tel Aviv, as well as on intelligence gathering, without clearly observable, lasting, or systemic effects on the critical infrastructure of Israel and its allies. In contrast, the Israeli approach is characterised by a higher degree of integration of digital operations into the broader state intelligence-military apparatus, where cyber activities function as an auxiliary mechanism enabling more precise planning and execution of kinetic strikes and increasing the overall effectiveness of military operations. The reactions of the Iranian leadership, including the suspension of internet access and the restriction of mobile device use among high officials, further confirm the perception of significant vulnerability in the cyber domain and point to a pronounced asymmetry in the capabilities of the two states.

The Iran-Israel conflict after October 2023 serves as an illustrative example of the security risks produced by pronounced asymmetry in cyber capabilities in contemporary conflicts. While technologically and organizationally superior actors can integrate cyber tools into military and intelligence operations, thus achieving tangible operational and strategic effects, states in a subordinate position are limited to lower-intensity actions, whose effects are often temporary or symbolic. Such imbalances not only deepen the vulnerability of weaker actors in the context of armed conflict but also encourage the broader use of cyber tools as a component of hybrid operations below the threshold of open warfare. In an environment of increasing regional and global tensions and intensified competition among states, such forms of activity are becoming more common, further heightening the risk of instability, uncontrolled escalation, and the long-term undermining of existing security arrangements.

REFERENCES

- Agence France-Presse*. 2015. "Russia Signs Military Cooperation Deal with Iran." *Defense News*. January 20, 2015. <https://www.defensenews.com/home/2015/01/20/russia-signs-military-cooperation-deal-with-iran/>.
- Albright, David, Paul Brannan, and Christina Walrond. 2010. "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" *Institute for Science and International Security*. December 22, 2010. <https://isis-online.org/isis-reports/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/>.
- Al-Halawany, Islam. 2021. "Israel Is Becoming a Cybersecurity Guarantor in the Middle East. Here's How." *Atlantic Council*. November 18, 2021. <https://www.atlanticcouncil.org/blogs/menasource/israel-is-becoming-a-cybersecurity-guarantor-in-the-middle-east-heres-how/>.
- Amaliya, Luthfi Rahma. 2025. "A Cyber War of Iran–Israel: A Geopolitical Rivalry." In *Proceedings of the International Conference on Strategic and Global Studies (ICSGS 2024)*, 45–56. Amsterdam: Atlantis Press. DOI: 10.2991/978-94-6463-646-8_4.
- Anderson, Collin, and Karim Sadjadpour. 2018. "Iran's Cyber Threat: Espionage, Sabotage, and Revenge." *Carnegie Endowment for International Peace*. January 4, 2018. https://assets.carnegieendowment.org/static/files/Iran_Cyber_Final_Full_v2.pdf.
- Arshad, Muhammad Hammad. 2025. "U.S.–Iran Cyber War and Its Impact on Israel." *Wah Academia Journal of Social Sciences* 4 (1): 1134–1158.
- Baram, Gil. 2017. "Israeli Defense in the Age of Cyber War." *Middle East Quarterly* 24 (1): 1–10.
- Bogićević, Aleksandar. 2025. "The Influence of Non-State Cyber Actors in Conventional Armed Conflicts: A Case Study of the War in Ukraine." In *VojNa 2025: International Scientific Conference on Military Sciences*, eds. Srđan Blagojević and Dragan Trifković, 304–310. Belgrade: Military Academy.
- Brenner, Neri. 2012. "Hackers Target More Israeli Websites." *Ynetnews*. January 25, 2012. <https://www.ynet.co.il/articles/0,7340,L-4180781,00.html>.

- Bucala, Paul, and Caitlin S. Pendleton. 2015. "Iranian Cyber Strategy: A View from the Iranian Military." *Critical Threats Project*. November 24, 2015. <https://www.criticalthreats.org/analysis/iranian-cyber-strategy-a-view-from-the-iranian-military>.
- Cybersecurity and Infrastructure Security Agency. 2025. "Iranian State-Sponsored Cyber Threat: Adversaries." *Americas Cyber Defense Agency*. Last Accessed January 13, 2026. <https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/iran/publications>.
- Digital Watch Observatory. 2025. "Israel – Country Profile on Digital and Cybersecurity Landscape." *Digital Watch Observatory*. Last Accessed January 10, 2026. dig.watch/countries/israel.
- Eisenstadt, Michael, and David Pollock. 2021. "Asset Test 2021: How the U.S. Can Keep Benefiting from Its Alliance with Israel." *The Washington Institute for Near East Policy*. February 24, 2021. <https://www.washingtoninstitute.org/policy-analysis/asset-test-2021-how-us-can-keep-benefiting-its-alliance-israel>.
- Elgin, Ben, and Michael Riley. 2014. "Now at the Sands Casino: An Iranian Hacker in Every Server." *Bloomberg*. December 12, 2014. <https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas>.
- El-Masry, Ahmed. 2021. "The Abraham Accords and Their Cyber Implications: How Iran Is Unifying the Region's Cyberspace." *Middle East Institute*. June 9, 2021. <https://mei.edu/publication/abraham-accords-and-their-cyber-implications-how-iran-unifying-regions-cyberspace/>.
- Faris, Lamia. 2025. "Algorithmic Targeting in the Iranian–Israeli Confrontation: Technical Realities, Legal Thresholds, and the Boundaries of Human Control." *F1000Research* 14 (1200): 1–23 DOI: 10.12688/f1000research.169794.1.
- Fassihi, Farnaz, Ronen Bergman, and Mark Mazzetti. 2025. "Targeting Iran's Leaders, Israel Found a Weak Link: Their Bodyguards." *New York Times*. August 30, 2025. <https://www.nytimes.com/2025/08/30/us/politics/israel-iran-assassination.html>.
- Freilich, Charles D. 2018. *Israeli National Security: A New Strategy for an Era of Change*. New York: Oxford University Press.

- Freilich, Charles D., Matthew S. Cohen, and Gabi Siboni. 2023. *Israel and the Cyber Threat: How the Startup Nation Became a Global Cyber Power*. Oxford: Oxford University Press. DOI: 10.1093/oso/9780197677711.001.0001.
- Government of Israel. 2011. "Advancing National Cyberspace Capabilities: Government Resolution No. 3611." *National Security Archive*. August 7, 2011. <https://nsarchive.gwu.edu/document/22530-document-05-government-israel-resolution-no>.
- Guzansky, Yoel, and Ron Deutch. 2019. "How Prepared Is Saudi Arabia for a Cyber War?" *The Institute for National Security Studies (INSS)*. July 10, 2019. www.inss.org.il/publication/how-prepared-is-saudi-arabia-for-a-cyber-war/.
- Haroon, Ayesha. 2024. "AI and Cyber Drove Warfare in the Israeli–Iranian Conflict and Its Impact on Gulf States' Security." *Journal of Politics and International Studies* 10 (2): 145–163.
- International Institute for Strategic Studies [IISS]. 2021a. "Cyber Power – Tier Two." *IISS*. June 24, 2021. <https://www.iiss.org/research-paper/2021/06/cyber-power---tier-two/>.
- International Institute for Strategic Studies [IISS]. 2021b. "Cyber Power – Tier Two." *IISS*. June 24, 2021. <https://www.iiss.org/research-paper/2021/06/cyber-power---tier-two/>.
- Israel National Cyber Directorate. 2019. "The Israel National Cyber Directorate: Iran Is a Main Cyber Threat in the Middle East." *Israel National Cyber Directorate*. June 26, 2019. https://www.gov.il/en/pages/unna_cyber_week_2019.
- Kamiński, Michał A. 2020. "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. DOI: 10.35467/sdq/121974.
- Keshavarz, Alma. 2023. *The Iranian Revolutionary Guard Corps: Defining Iran's Military Doctrine*. London: Bloomsbury Academic.
- Khorrami, Nima. 2021. "One Year On – Israel's Cybersecurity Cooperation with the GCC States." *Middle East Institute and the National University of Singapore*. September 14, 2021. <https://mei.nus.edu.sg/publication/insight-266-one-year-on-israels-cybersecurity-cooperation-with-the-gcc-states/>.

- Liff, Adam P. 2012. "Cyber War: A New 'Absolute Weapon'? The Proliferation of Cyber Warfare Capabilities and Interstate War." *Journal of Strategic Studies* 35 (3): 401–428. DOI: 10.1080/01402390.2012.663252.
- Miller, Maggie. 2025. "Here's How the War between Israel and Iran Is Playing Out in Cyberspace." *Politico*. June 22, 2025. <https://www.politico.com/news/2025/06/22/us-israel-iran-war-cyber-attacks-00417782>.
- Netolická, Veronika, and Miroslav Mareš. 2018. "Arms Race 'in Cyberspace' – A Case Study of Iran and Israel." *Comparative Strategy* 37 (5): 414–429. DOI: 10.1080/01495933.2018.1526568.
- New Jersey Cybersecurity and Communications Integration Cell. 2024. "Increase in Cyber Threat Activity Associated with Iranian State-Sponsored and State-Affiliated Threat Groups." *Office of Homeland Security and Preparedness*. August 29, 2024. <https://www.cyber.nj.gov/Home/Components/News/News/1440/>.
- Newman, Lily Hay. 2025. "Israel Says Iran Is Hacking Security Cameras for Spying." *WIRED*. June 21, 2025. <https://www.wired.com/story/israel-says-iran-is-hack-security-cameras-for-spying/>.
- Oghanna, Ayman. 2023. "How Albania Became a Target for Cyberattacks." *Foreign Policy*. March 25, 2023. <https://foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran/>.
- Picus Security. 2025. "Predatory Sparrow: Inside the Cyber Warfare Targeting Iran's Critical Infrastructure." *Picus Security*. November 4, 2025. <https://www.picussecurity.com/resource/blog/predatory-sparrow-inside-the-cyber-warfare-targeting-irans-critical-infrastructure>.
- Pijpers, Patrick B. M. J. 2023. "Revisiting the Stability/Instability Paradox in Cyberspace: Lessons from the Russo-Ukraine War." *SSRN Electronic Journal*. DOI: 10.2139/ssrn.4514908.
- Politico*. 2025. "Iran Orders Officials to Ditch Connected Devices." *Politico*. June 17, 2025. <https://www.politico.eu/article/iran-orders-officials-to-ditch-connected-devices/>.
- Press, Gil. 2017. "6 Reasons Israel Became a Cybersecurity Powerhouse Leading the \$82 Billion Industry." *Forbes*. July 18, 2017. <https://>

- www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/.
- Radware. 2025. "Hybrid Warfare Unfolded: Cyberattacks, Hacktivism and Disinformation in the 2025 Israel–Iran War." *Radware*. June 18, 2025. www.radware.com/security/threat-advisories-and-attack-reports/cyberattacks-hacktivism-and-disinformation-in-the-2025-israel-iran-war/.
- Razin, Assaf. 2018. *Israel and the World Economy: The Power of Globalization*. Cambridge: MIT Press.
- Reddy, Pagilla Manohar. 2025. "Part 1: The Iran-Israel Cyber Standoff – The Hacktivist Front." *CloudSEK*. June 19, 2025. <https://www.cloudsek.com/blog/part-1-the-iran-israel-cyber-standoff--the-hacktivist-front>.
- Reuters. 2021. "Iran and China Sign 25-Year Cooperation Agreement." *Reuters*. March 27, 2021. <https://www.reuters.com/world/china/iran-china-sign-25-year-cooperation-agreement-2021-03-27/>.
- Rid, Thomas. 2013. *Cyber War Will Not Take Place*. Oxford: Oxford University Press.
- Sabin, Sam. 2025. "Iran Leans on Hacktivist Proxies in Wake of Israeli, U.S. Strikes." *Axios*. July 1, 2025. <https://www.axios.com/2025/07/01/iran-hacktivist-israeli-us-strikes>.
- Shafa, Eric K. 2014. "Iran's Emergence as a Cyber Power." *Strategic Studies Institute, U.S. Army War College*. August 20, 2014. <https://ssi.armywarcollege.edu/SSI-Media/Recent-Publications/Display/Article/3614420/irans-emergence-as-a-cyber-power/>.
- Siboni, Gabi, Lea Abramski, and Gal Sapir. 2020. "Iran's Activity in Cyberspace: Identifying Patterns and Understanding the Strategy." *Cyber, Intelligence and Security* 4 (1): 21–40.
- SOCRadar Cyber Intelligence. 2025. "Reflections of the Israel–Iran Conflict on the Cyber World." *SOCRadar Blog*. June 19, 2025. <https://socradar.io/blog/reflections-of-israel-iran-conflict-cyber-world/>.
- Tabansky, Lior. 2020. "Israel Defense Forces and National Cyber Defense." *Connections* 19 (1): 45–62. DOI: 10.11610/Connections.19.1.05.

- Tashkandi, Hala. 2020. "Cyberattacks Hit 95% of Saudi Businesses Last Year, Says Study." *Arab News*. August 12, 2020. <https://www.arabnews.com/node/1718596/saudi-arabia>.
- The Economist*. 2024. "Iran's Electronic Confrontation with Israel." *The Economist*. August 15, 2024. <https://www.economist.com/middle-east-and-africa/2024/08/15/irans-electronic-confrontation-with-israel>.
- The Times of Israel*. 2025. "Iranian news site confirms banking issues due to cyberattack after hacking claim." *The Times of Israel*. June 17, 2025. https://www.timesofisrael.com/liveblog_entry/iranian-news-site-confirms-banking-issues-due-to-cyberattack-after-hacking-claim/.
- ThreatMon. 2026. "The Cyber Front of Iran-Israel." *ThreatMon*. Last Accessed January 13, 2026. <https://threatmon.io/the-cyber-front-of-iran-israel/>.
- U.S. Department of Defense. 2023. "Summary 2023 Cyber Strategy of The Department of Defense." *Department of Defense*. September 12, 2023. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf.
- U.S. Department of the Treasury. 2007. "Iran's Bank Sepah Designated by Treasury; Sepah Facilitating Iran's Weapons Program." *U.S. Department of the Treasury*. January 9, 2007. <https://home.treasury.gov/news/press-releases/hp219>.
- United States Department of Justice. 2016. "Seven Iranians Working for Islamic Revolutionary Guard Corps—Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks against U.S. Financial Sector." *Office of Public Affairs*. March 24, 2016. <https://www.justice.gov/archives/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged>.
- Vicens, A. J. 2023. "Savvy Israel-Linked Hacking Group Reemerges amid Gaza Fighting." *CyberScoop*. October 10, 2023. <https://cyberscoop.com/predatory-sparrow-israel-gaza-cyber/>.
- Vicens, A. J., and James Pearson. 2025. "Suspected Israeli hackers claim to destroy data at Iran's Bank Sepah." *Reuters*. June 17, 2025. <https://www.reuters.com/world/middle-east/suspected-israeli-hackers-claim-destroy-data-irans-bank-sepah-2025-06-17/>.

Watts, Clint. 2024. "Iran accelerates cyber ops against Israel from chaotic start." *Microsoft*. February 6, 2024. <https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/>.

Zendata Cyber Security. 2025. "Zendata's Cyber Analysis of the Iran-Israel Conflict." *Zendata Cyber Security*. June 24, 2025. <https://zendata.security/2025/06/24/zendatas-cyber-analysis-of-the-iran-israel-conflict/>.

Александар Богићевић*

*Институт за стратегијска истраживања,
Универзитет одбране, Београд, Република Србија*

САЈБЕР РАТ ИЗРАЕЛА И ИРАНА: ДИГИТАЛНА ДИМЕНЗИЈА БЛИСКОИСТОЧНИХ СУКОБА У ПОСТ-УНИПОЛАРНОМ СВЕТУ**

Резиме

Овај рад анализира еволуцију сајбер сукоба између Израела и Ирана од 2010. године, са посебним освртом на период након избијања сукоба у Гази у октобру 2023. године, у контексту транзиције од америчке униполарности ка мултиполарном међународном поретку. Централно истраживачко питање односи се на то у којој мери сајбер инструменти могу компензовати асиметрију моћи у условима активног регионалног сукоба. Рад заступа став да ефекти сајбер операција остају стратешки ограничени када је технолошки надмоћнији актер способан да интегрише дигиталне операције са кинетичким дејствима. Иранско-израелски сајбер сукоб започео је откривањем вируса *Stuxnet* (рачунарски црв) 2010. године, у оквиру заједничке израелско-америчке операције усмерене против нуклеарног постројења у Натанзу, која је означила први познати пример сајбер напада са директним физичким ефектима на критичну инфраструктуру. Овај догађај навео је обе државе да суштински преусмере своје политике сајбер безбедности и офанзивне сајбер стратегије. Израел је, ослањајући се на доктрину „безбедносног троугла” која наглашава одвраћање, рано упозорење и одсудну победу, развио софистициран национални сајбер екосистем кроз стратешка јавно-приватна улагања и ширење мреже међународних

* Имејл адреса: aleksandar.bogicevic@mod.gov.rs; ORCID: 0009-0006-7450-5193.

** Овај рад представљен је у оквиру конференције „Перспективе политичких наука у савременом друштву IV”, одржане 4–5. децембра 2025. године у организацији Института за политичке студије, Београд.

партнера, учврстивши тако своју позицију глобалног лидера у области сајбер безбедности. За Иран је сајбер безбедност постала подједнако важна као и нуклеарни програм, служећи како пројекцији моћи према споља, тако и контроли унутрашњег информационог простора. Упркос системским препрекама, укључујући међународне санкције, ограничена финансијска средства и одлив мозгова, Техеран је остварио значајан напредак кроз стратешку сарадњу са Русијом и Кином и пажљиву селекцију кадрова унутар сајбер јединица повезаних са Револуционарном гардом. Емпиријска анализа потврђује централну претпоставку рада: Иран је сајбер инструменте превасходно користио у оквиру асиметричне стратегије ограниченог домета, усмерене на операције у информационом простору са циљем генерисања друштвених подела и ерозије међународне подршке Израелу, као и на прикупљање обавештајних података, без јасно уочљивих, трајних или системских ефеката по критичну инфраструктуру. Израел је, насупрот томе, интегрисао сајбер операције у шири војно-обавештајни апарат као допунски механизам који омогућава прецизније планирање и извођење кинетичких удара. Иранско-израелски сукоб након октобра 2023. године тако представља илустративну студију случаја безбедносних ризика које производи изражена асиметрија сајбер способности, у којој технолошки надмоћнији актери остварују конкретне стратешке ефекте, док су слабије државе ограничене на облике деловања нижег интензитета, чији су домети неретко привремени или симболични.

Кључне речи: Израел, Иран, сајбер ратовање, сајбер безбедност, Блиски исток.

* This paper was received on January 21, 2026, and accepted for publication at the Editorial Board meeting on February 27, 2026.

*Александар Божићевић**

*Институт за стратегијска истраживања,
Универзитет одбране, Београд, Република Србија*

САЈБЕР РАТ ИЗРАЕЛА И ИРАНА: ДИГИТАЛНА ДИМЕНЗИЈА БЛИСКОИСТОЧНИХ СУКОБА У ПОСТ-УНИПОЛАРНОМ СВЕТУ**

Сажетак

Конфликт између Израела и Ирана представља један од најистрајнијих сукоба на Блиском истоку, чију динамику током последње деценије све више одликује мултидимензионалност оличена у преливању сукоба изван традиционалних војно-политичких оквира и на друга поља, међу којима је и окршај у дигиталном простору. Након израелског *Stuxnet* (рачунарски црв) напада на иранску нуклеарну инфраструктуру 2010. године, сајбер поље постаје једна од кључних сфера сукобљавања, како између Израела и Ирана, тако и са њима повезаних сајбер актера, неретко из трећих држава, што уноси додатни степен непредвидивости и сложености у овом сукобу. Оно што чини овај сајбер сукоб посебно значајним за односе између држава на веома осетљивом Блиском истоку јесте могућност држава да нанесу другој штету без употребе оружане силе. Посматрано глобално, овај сукоб одражава ширу трансформацију односа између главних актера у међународном поретку. Подршка коју Сједињене Државе пружају

* Имејл адреса: aleksandar.bogicevic@mod.gov.rs; ORCID: 0009-0006-7450-5193.

** Овај рад представљен је у оквиру конференције „Перспективе политичких наука у савременом друштву IV”, одржане 4–5. децембра 2025. године у организацији Института за политичке студије, Београд.

Израелу и растућа сарадња Русије и Кине са Ираном указују на чињеницу да иранско-израелски сајбер рат постаје део глобалног геополитичког надметања. Циљ истраживања јесте анализирање сајбер рата Израела и Ирана, улоге коју он има у њиховом сукобу, као и ефеката које остварује, како на ове две државе, тако и на државе у региону, које услед повезаности и сложених међусобних односа, такође бивају таргетиране. Аутор указује на растућу важност сајбер димензије као поља надметања актера на Блиском истоку, где „стари сукоби” добијају нову димензију кроз премештање борбе у дигитални простор и постају неодојиви део савремене геополитичке реалности региона у пост-униполарном свету.

Кључне речи: Израел, Иран, сајбер ратовање, сајбер безбедност, Блиски исток.

УВОД

Све шира употреба нових технологија и експанзија сајбер простора значајно су утицале на трансформацију глобалних односа, пружајући државним и недржавним актерима нове могућности деловања, истовремено их излажући потпуно новим ризицима (Rid 2013) на које државе често имају ограничене капацитете за адекватан одговор. Саме карактеристике сајбер простора као што су анонимност, глобална повезаност, велика брзина кретања информација и ниски трошкови коришћења (Liff 2012, 422) додатно су подстакле државе у процесу његове инструментализације. Тиме је сајбер сфера постала простор сукобљавања ниског интензитета између држава које, кроз крађу осетљивих података, манипулације у информационом простору и ометање нормалног функционисања рачунарских мрежа, покушавају нанети штету противнику (Bogićević 2025, 305).

Процес глобалног умрежавања праћен је значајним променама у расподели моћи у међународном поретку насталом након краја Хладног рата. Постепено смањење директног присуства САД на Блиском истоку и преусмеравање стратешке пажње ка Источној Азији довели су до ерозије доминантне улоге Вашингтона на том простору, чиме су створене околности за појачано деловање других глобалних и регионалних актера. Међу државама које су показале посебне амбиције у жељи

да попуне вакуум моћи и прошире свој утицај јесте Иран, који је успостављањем контроле над бројним оружаним групама у државама Блиског истока стекао значајан регионални утицај. Међутим, експанзија иранског присуства наишла је на значајну препреку у виду непомирљивог идеолошког непријатеља и кључног америчког савезника у региону, Израела. Тежња Тел Авива да помери одбрану територије и становништва што даље од сопствених граница, са једне, и ширење мреже проиранских проксија на Блиском истоку са друге стране, довели су ове две државе у стање перманентног трвења (Netolická and Mareš 2018, 418), при чему је преношење њиховог ривалства у сајбер простор изазвало настанак новог извора небезбедности за све државе Блиског истока (Amaliya 2025, 49). Управо ће откриће израелско-америчког сајбер напада на нуклеарно постројење у Натанзу 2010. године означити почетак нове фазе у разумевању сајбер сфере као простора сукобљавања држава.

Циљ овог рада јесте анализа генезе сајбер сукоба између Израела и Ирана након 2010. године, са посебним освртом на инциденте који су уследили након октобра 2023. године. Централно истраживачко питање односи се на то у којој мери сајбер инструменти могу компензовати асиметрију моћи у условима активног регионалног сукоба, при чему полазна претпоставка рада јесте да ефекти сајбер деловања остају стратешки ограничени када је технолошки и организационо јачи актер спреман и способан да интегрише дигиталне операције са кинетичким дејствима. Научни допринос рада огледа се у интегрисаној анализи овог сукоба као студије случаја асиметрије сајбер капацитета у пост-униполарном поретку, при чему се, за разлику од постојеће литературе која се претежно бави техничким аспектима инцидентата, нагласак ставља на стратешке ефекте и структурне детерминанте сајбер деловања.

Проучавање сајбер безбедности суочено је са значајном методолошком препреком у виду ограничене доступности проверљивих информација о сајбер актерима, активностима које они спроводе и њиховим ефектима. За разлику од међусобних кинетичких удара изведених током јуна 2025. године, код којих је било могуће непосредније утврдити нанету физичку штету, утврђивање консеквенци сајбер операција знатно је сложеније услед нематеријалне природе дигиталног простора

и ограничене транспарентности актера. Сајбер сукоб Израела и Ирана обележен је израженом асиметријом извора информација: највећи део података потиче од западних компанија и организација специјализованих за сајбер безбедност, док су информације из иранских извора са знатно више ограничења.

Овај рад обухвата сајбер инциденте у периоду од 2010. године до данас који испуњавају следеће критеријуме: 1) јасну повезаност са међудржавним односима Израела и Ирана, односно постојање индикатора да инцидент има политички или стратешки мотивисан карактер; 2) постојање јавно доступне техничке или институционалне атрибуције напада; и 3) политичко-стратешки значај, односно потенцијал утицаја на понашање актера. Као „проверене чињенице” третирају се искључиво подаци који су потврђени из најмање два међусобно независна извора или који су документовани кроз техничке индикаторе компромитације и званичне извештаје релевантних институција. Насупрот томе, тврдње актера, медијске интерпретације и процене компанија за сајбер безбедност анализирају се као аналитички наративи, а не као емпиријски утврђене чињенице. На тај начин настоји се јасно разграничити дескриптивни ниво анализе од интерпретативног.

САЈБЕР ПРОСТОР КАО НОВИ ФРОНТ: ИЗРАЕЛСКИ ОДГОВОР НА ИРАНСКУ ПРЕТЊУ

Перцепција перманентне угрожености опстанка (Tabansky 2020, 46) кључно је утицала на Тел Авив да прихвати проактивно и превентивно деловање у националној одбрани које се темељи на принципу „безбедносног троугла” чије су кључне компоненте одвраћање, рано упозорење и брзо остваривање одсудне победе на бојном пољу (Freilich, Cohen and Siboni 2023, 185). Како је постизање трајног мира за Израел, као коначног стратешког циља који је артикулисао Бен Гурион (*David Ben-Gurion*) (Baram 2017, 3), скоро недостижно услед немогућности трајног војног неутралисања арапских држава, Тел Авив се фокусирао на достизање скромнијег циља у виду привременог онеспособљавања најистакнутије претње пре појаве других претњи у региону и новог циклуса сукобљавања (Freilich, Cohen, and Siboni 2023, 185).

Крај XX и почетак XXI века довео је до еволуције извора претњи са којима се Израел суочавао у свом окружењу. Њихова

трансформација из регуларних оружаних снага арапских држава у недржавне актере као што су терористичке групе утицала је и на саму природу сукоба. Услед асиметричне природе сукоба са недржавним актерима, Тел Авив се више није могао ослањати на брзе и одлучујуће победе на конвенционалном бојном пољу што је приморало његове доносиоце одлука да преиспитају принципе „безбедносног троугла” (Freilich 2018, 199).

Упоредо са појачаним присуством терористичких организација, растући значај савремених дигиталних технологија за функционисање економије и друштва открио је потпуно нови скуп претњи којима је Израел постао изложен. Као држава чија се привреда ослања на примену најсавременијих технологија у привреди и администрацији,¹ Тел Авив је посебно осетљив на сајбер претње. Кључан моменат у процесу препознавања сајбер простора као новог извора небезбедности догодио се 2010. године са откривањем америчко-израелског сајбер напада на иранско нуклеарно постројење у Натанзу.

Страх од развоја иранског нуклеарног програма, заједно са уверењем у ефикасност превентивног удара као механизма за сузбијање регионалних претњи, навео је Израел да већ 2006. године, заједно са САД, спроведу сајбер операцију (Kamiński 2020, 69) под називом „Олимпијске игре” са циљем онеспособљавања нуклеарног постројења у Натанзу. Током наредне четири године, вирус који се налазио у иранској рачунарској мрежи онеспособио је око 1.000 гасних центрифуга, што није довело до радикалног успоравања нуклеарног програма (Albright, Brannan, and Walrond 2010). Међутим, консеквенце су биле од изузетног регионалног и глобалног значаја, будући да је реч о првом познатом примеру сајбер операције са директним физичким ефектима на критичну инфраструктуру једне државе. Посматрана глобално, операција „Олимпијске игре” означила је почетак преиспитивања рањивости критичне инфраструктуре на потпуно нову врсту претњи, док је на регионалном нивоу откриће сајбер напада означило отварање новог фронта у иранско-израелском сукобу, које ће убрзо увући и друге државе Блиског истока.

¹ Чак 13% БДП и 31% извоза Израела потиче из производа и услуга насталих у области примене високих технологија. За више информација о важности ове привредне делатности на развој израелске економије (Razin 2018).

Након 2010. године и открића израелске умешаности у сајбер напад, Тел Авив је радикално променио перцепцију Ирана као претње, како у физичком, тако и у сајбер простору (Baram 2017, 1). Како би одржао технолошку предност у односу на регионалне претње и адекватно одговорио на могућу иранску реталијацију, Израел је приступио развоју сајбер безбедности као новом стубу будуће одбране државе о чему сведоче значајни напори и ресурси које је уложила израелска влада у изградњу институција и субвенционисању развоја нових стартапова (Government of Israel 2011, 2; Press 2017). Ослањајући се на јавно-приватно партнерство и глобалну економску повезаност, Израел је изградио изузетне националне сајбер капацитете чиме је стекао одлучујућу конкурентску предност над актерима које перципира као регионалну претњу.

Поред настојања да се креира национални сектор компанија усмерених ка сајбер безбедности, Израел се у значајној мери ослонио и на међународну сарадњу као механизам за унапређење капацитета. Централно место у растућој мрежи међународних партнера заузимају САД, са којима је остварен висок ниво сарадње како на међувладином плану (Arshad 2025, 1148), тако и у домену привреде. Интензивна размена знања и информација, посебно у погледу иранских способности и намера у дигиталном простору, обезбеђује Израелу значајну стратешку предност, омогућавајући му оптималну употребу сопствених ресурса у планирању сајбер операција (1141).

Као све значајнија компонента израелске сајбер одбране након 2010. године постепено се развија и сарадња са регионалним актерима који у Ирану препознају извор регионалне небезбедности. Онеспособљавање рачунарске мреже компаније Арамко (*Aramco*) 2012. године био је јасан показатељ напретка који је Иран остварио у сајбер домену, указујући блискоисточним државама на растући интензитет ове претње. Како би премостили настајући јаз у односу на Иран, државе попут Египта, Саудијске Арабије и Уједињених Арапских Емирата окренуле су се Израелу као провајдеру безбедности у сајбер простору (Al-Halawany 2021; Khorrami 2021). Поред подизања нивоа регионалне отпорности на иранске претње у дигиталном простору, сајбер дипломатија Тел Авива имала је значајан утицај и на процес нормализације односа са државама региона (Freilich, Cohen, and Siboni 2023,

275), чиме је остварен важан корак ка реализацији једног од кључних стратешких циљева Израела – успостављања стабилнијег безбедносног окружења.

Производ напора на унутрашњем и међународном плану јесте развој изузетно софистицираног система сајбер одбране заснованог на великом броју успешних компанија,² високом степену кооперације привреде са институцијама и размени знања и информацијама са водећим међународним актерима. Органски развој сајбер капацитета кроз привредни развој омогућио је Тел Авиву да се нађе у самом врху држава у погледу њихових способности да одговоре на сајбер претње (Digital Watch Observatory 2025), што је и био прокламовани циљ постављен током почетка XXI века. У том смислу, израелски приступ сајбер безбедности не представља дисконтинуитет у односу на раније безбедносне доктрине, већ њихову функционалну адаптацију новим технолошким и геополитичким условима.

ИРАН И САЈБЕР ПРОСТОР: АСИМЕТРИЧНА СТРАТЕГИЈА, ПРОКСИ ДЕЛОВАЊЕ И ДИГИТАЛНА ПРОЈЕКЦИЈА МОЋИ

Однос Ирана према сајбер простору, као и у случају других ауторитарних сила, означен је амбивалентношћу: са једне стране, он представља механизам контроле становништва и пропагирања сопствених вредности кроз дигиталне медије, док са друге представља сталан извор опасности у виду продора утицаја западних медија. Присуство ових медија, као алтернативе државним гласилима, представља посебан проблем за власти у Техерану које се учестало суочавају са масовним протестима (Freilich, Cohen, and Siboni 2023, 140). Такође, могућности које сајбер простор пружа као медијум за ширење утицаја у региону и вршење малициозних операција утицале су на Техеран да препозна сајбер безбедност као једну од кључних аспеката националне безбедности у будућности. Управо ће масовни протести 2009.

² Илустративан показатељ успеха који је постигао Тел Авив након 2010. године јесте процват његове индустрије сајбер безбедности. Израел се сматра другим највећим центром за развој софтвера за сајбер заштиту на свету (Eisenstadt and Pollock 2021).

године и откриће присуства америчко-израелског *Stuxnet* вируса – сајбер оружаног малвера, 2010. године бити катализатори појачаних иранских напора у правцу развоја сајбер капацитета (Anderson and Sadjadpour 2018, 10–11). За опстанак режима ајатолаха, сајбер безбедност постала је подједнако важна као и питање развоја нуклеарног наоружања (Bucala and Pendleton 2015).

Међународно деловање Ирана у сајбер простору заузима вишеструку улогу у његовој стратегији оснаживања регионалне позиције. Првенствено, Техеран се у свом асиметричном деловању на Блиском истоку у значајној мери ослања управо на сајбер средства како би се избегла ескалација тензија која би могла водити у оружане сукобе (Haroony 2024, 146) или трошење ресурса локалних проксија. Са друге стране, сајбер инструменти представљају релативно економичан и мање видљив метод за прикупљање обавештајних података, као и за таргетирање институција и привредних субјеката других држава. Ове активности неретко представљају први корак у спровођењу операција у информационој сфери, које се манифестују кроз објављивање осетљивих података или артикулисање одређених политичких порука, са циљем истицања сопствених способности, али и експлоатације уочених слабости противника.

Поучени случајем *Stuxnet*, Иран је након 2010. године значајно интензивирао финансијска улагања у овај домен. Иако тачни подаци нису јавно доступни, процене Ратног колеџа Војске САД (*US Army War College*) о расту иранског буџета за сајбер операције са 76 милиона америчких долара на једну милијарду четири године касније, представљају јасан индикатор значаја који носи сајбер простор за Иран (Shafa 2014). Посебан акценат стављен је на унапређење стандарда образовања у области информатичких технологија и селекцију кадрова који су почели попуњавати позиције у сајбер јединицама Иранске републиканске гарде и Министарства информисања (Netolická and Mareš 2018, 420; Keshavarz 2023, 122). Континуирано улагање почело је давати резултате што се могло уочити кроз растући број софистицираних напада на критичну инфраструктуру других држава (као што је поменути случај саудијске компаније Арамко 2012. године) које су почеле перципирати Иран као растућу сајбер претњу.

Напади од стране иранских сајбер група и њима блиских проксија на рачунарске мреже заливских држава наставили су се

и у наредним годинама, што је указивало на неколико трендова у понашању Техерана у сајбер простору. У складу са стратегијом ослањања на мрежу прокси актера широм региона Блиског истока и вођења асиметричне борбе зарад унапређења позиције, Иран је започео процес дифузије знања и малициозних алата са својих сајбер актера на повезане, недржавне субјекте. Оваква пракса омогућила је повећање укупних капацитета Техерана за вођење офанзивних сајбер операција, али је истовремено значајно отежала поуздану идентификацију непосредних извршилаца напада, чиме је одговорност за сајбер дејства постала дифузна и тешко приписива конкретном актеру.

Низак ниво свести о ризицима и ограничена улагања заливских држава у заштиту од сајбер претњи током 2010-их година учинили су их изразито рањивим на деловање иранских и проиранских сајбер актера. Индикативан показатељ степена изложености блискоисточних актера сајбер претњама јесу резултати истраживања компаније Тенебл (*Tenable*) који показују да је чак 95% саудијских компанија било суочено са сајбер претњама које су негативно утицале на њихово пословање током 2019. године (Tashkandi 2020), а као главни извор напада је управо идентификован Иран (Guzansky and Deutch 2019). Поред деловања усмереног ка метама у непосредном регионалном окружењу, сајбер актери повезани са Ираном спроводили су офанзивне операције и против САД, као главног савезника иранских регионалних опонената. Ове активности обухватале су таргетирање критичне инфраструктуре, попут напада на брану Боуман (*Bowman Dam*) 2013. године (United States Department of Justice 2016), као и нападе на приватне компаније и појединце, где се посебан фокус ставља на осведочене противнике званичног Техерана (Elgin and Riley 2014).

Као и у случају Израела, Иран се у значајној мери ослонио на своју мрежу савезника као извору технолошких иновација, емпиријских искустава и оперативне подршке у спровођењу сајбер операција. Примарни партнер у овим напорима јесте Русија, са којом Иран од 2015. године има потписан споразум о сајбер кооперацији (Agence France-Presse 2015), а који је додатно унапређен 2021. године када је склопљен Споразум о сарадњи на пољу сајбер безбедности (*Cyber Security Cooperation Agreement*), који обухвата још виши степен размене технологије и

информација, обуке и помоћ у међународним сајбер инцидентима (El-Masry 2021). Споразум о стратешкој кооперацији између Пекинга и Техерана склопљен исте године такође је усмерен ка размени технологије и информација, са значајним кинеским инвестицијама у телекомуникациону инфраструктуру и софтвере, омогућавајући Ирану да успостави још чвршћи надзор и контролу над сопственим сајбер простором (Reuters 2021). Сарадња између поменутих држава није ограничена искључиво на државне актере у сајбер простору већ се она пренела и на недржавне где се кооперација осликава у размени украдених података и координисаним нападима на критичну инфраструктуру других држава. Пример таквог облика неформалне сарадње идентификован је у заједничком деловању проруских и проиранских сајбер актера током сајбер напада који су погодили државе Западног Балкана 2022. и 2023. године (Oghanna 2023).

Напори које је уложио Техеран након 2010. године у развој националних сајбер капацитета учинили су овај инструмент критичном компонентом његове стратегије хибридног деловања. Паралелно са ослањањем на прокси актере у облику оружаних група широм Блиског истока, које чине један од кључних инструмената иранског регионалног деловања, ангажовање државних и недржавних сајбер актера омогућило је Техерану да, уз релативно ограничен утрошак ресурса, нанесе додатну штету својим противницима. Ипак, за разлику од Израела, где је у значајној мери присутан консензус у погледу сајбер способности, на примеру Ирана то није случај што указује на постојање значајних разлика у способностима ових држава.

Међународни институт за стратешке студије (*International Institute for Strategic Studies* – IISS) сврстава Иран међу другоразредне сајбер силе (International Institute for Strategic Studies [IISS] 2021b, 1), док се Израел налази у групу најнапреднијих (International Institute for Strategic Studies [IISS] 2021a). До сличних закључака дошао је и Департман одбране Сједињених Држава (*United States Department of Defence*) у њиховој Сајбер стратегији 2023. године где је дата процена да Техеран још увек није демонстрирао могућности спровођења континуираних и софистицираних сајбер операција (U.S. Department of Defense 2023, 5). Са друге стране, Сибони (*Gabi Siboni*), Абрамски (*Léa Abramski*) и Сапир (*Gal Sapir*) оцењују да су ирански сајбер капацитети већ

достигли ниво најнапреднијих држава (Siboni, Abramski, and Sapir 2020, 39–40), у чему је сагласан и Јигал Уна (*Yigal Unna*), бивши директор-генерал Националног сајбер директората Израела (Israel National Cyber Directorate 2019).

Упркос значајним препрекама у развоју изазваних међународним економским санкцијама (Faris 2025, 10), одливом мозгова и слабо развијеним приватним сектором у области сајбер безбедности (Freilich, Cohen, and Siboni 2023, 137), Иран је успео да развије значајне националне сајбер капацитете који су му омогућили алтернативни механизам деловања у ситуацијама у којима је употреба прокси оружаних група економски прескупа, политички ризична или оперативно неизводљива, што је посебно дошло до изражаја након избијања сукоба у Гази у октобру 2023. године.

САЈБЕР ДИМЕНЗИЈА ИРАНско-ИЗРАЕЛског СУКОБА НАКОН ОКТОБРА 2023. ГОДИНЕ

Позиција Ирана на Блиском истоку била је релативно стабилна до октобра 2023. године: ослањајући се на разгранату мрежу савезника и прокси актера, Техеран је остваривао утицај над Хутима у Јемену, Хезболахом у Либану и Хамасом у Појасу Газе, док је истовремено пројектовао своју моћ у Сирији, пружајући кључну подршку режиму Башара ал-Асада, као и у Ираку, где је под својим окриљем држао бројне шиитске милиције. Међутим, након упада припадника Хамаса на територију Израела 7. октобра и почетка рата на територији Појаса Газе 20 дана касније, иранско-израелски сукоб ушао је у нову фазу, која ће се одликовати како активним сукобом између Израела и проиранских милиција, тако и међусобним нападима током Дванаестодневног рата јуна 2025. године. Паралелно са овим догађајима, у сајбер домену је такође дошло до заоштравања сукоба који је обухватао како државне, тако и бројне недржавне актере.

Тренд интензивирања сајбер дејстава током ескалација тензија између Израела и Ирана био је присутан и током ранијих сукоба (2009, 2012. и 2014. године) у којима су ови актери били укључени (Freilich, Cohen and Siboni 2023, 120). Циљ деловања сајбер актера били су онемогућавање рада или нарушавања изгледа сајтова државне администрације, великих финансијских

институција, као и крађа података корисних за извођење војних или даљих сајбер операција (Brenner 2012), али резултати таквих операција нису били трајни или од већег значаја по исход сукоба. Међутим, избијање сукоба у Гази у октобру 2023. године означило је почетак трансформације иранско-израелског сајбер сукоба која се огледа у повећаној софистицираности појединих напада, ширењу броја укључених актера и интензивирању укупних сајбер активности (The Economist 2024, ThreatMon 2026, 5–14).

Разлике у погледу способности Ирана и Израела за вођење борбе у сајбер домену јасно се уочавају кроз анализу врста операција које су доминирале код сукобљених страна, као и кроз обим и карактер штете проузроковане њиховом применом. Анализирајући извештаје компанија из области сајбер безбедности (Watts 2024; Radware 2025; Reddy 2025) и државних институција (Cybersecurity and Infrastructure Security Agency 2025), могу се идентификовати одређене тенденције у деловању иранских и проиранских сајбер група међу којима је најучесталија извођење операција у информационом простору са циљем дестабилизације Израела кроз продубљивање друштвених подела, узнемиравање јавности и ерозију међународне подршке Тел Авиву (Watts 2024). Такође, Иран је своје сајбер ресурсе користио у обавештајне сврхе, пре свега ради прикупљања осетљивих информација, као што су подаци о припадницима Одбрамбених снага Израела, као и приступа снимцима надзорних камера, који су служили за процену штете (The Economist 2024; Newman 2025). Са друге стране, упркос бројним наводима о успешним операцијама (SOCRadar Cyber Intelligence 2025), до сада није идентификован ниједан значајнији напад на израелску критичну инфраструктуру са трајним последицама, што може бити индикатор ограниченог домета офанзивних сајбер капацитета Ирана.

Израел је истовремено спроводио офанзивне операције у иранском сајбер простору, пре свега у обавештајне сврхе, са циљем прикупљања података релевантних за идентификацију војних циљева и кључних појединаца, укључујући нуклеарне научнике и високе официре Револуционарне гарде и регуларних оружаних снага Ирана (Zendata Cyber Security 2025), о чему сведоче званичници са обе стране (Fassihi, Bergman, and Mazzetti 2025). У прилог овој тврдњи говори и одлука иранског државног врха да, након иницијалног ваздушног удара израелског ваздухопловства,

суспендује интернет на националном нивоу и наложи високим званичницима одлагање мобилних уређаја, услед страха да би они могли послужити за лоцирање и праћење мета (Politico 2025; Fassihi, Bergman, and Mazzetti 2025). Такве мере указују на перцепцију изражене рањивости Ирана у сајбер домену и сведоче о постојању значајне асиметрије у сајбер способностима између два актера, коју је Израел интензивно користио као додатни инструмент своје војне и обавештајне моћи.

Посебно улогу у сукобу имају недржавни сајбер актери који, услед ограничених ресурса и знања, најчешће спроводе операције у информационом простору (Pijpers 2023, 7). Међутим, Иран и Израел користе кооперацију са недржавним сајбер актерима као механизам за прикривање умешаности државе у одређеним активностима. Иако су примери на страни сарадње иранских државних органа са сајбер актерима боље документовани (Sabin 2025; New Jersey Cybersecurity and Communications Integration Cell 2024), случај израелске групе Предаторски врабац (*Predatory Sparrow*) указује на све сложености идентификације порекла нападача и његове повезаности са државним актерима. Представљајући се као хакерска група која се противи режиму ајатолаха у Ирану, Предаторски врабац је заслужна за извођење изузетно сложених напада на критичну инфраструктуру Ирана, таргетирајући железаре, железнички саобраћај и системе за транспорт енергената (Miller 2025; Vicens 2023).

Током трајања дванаестодневног сукоба између Ирана и Израела, ова хакерска група извела је неколико до сада потврђених операција таргетирајући примарно финансијски сектор (Picus Security 2025). Посебно важна мета сајбер напада била је Сепак банка (*Sepah Bank*), позната по њеним везама са Иранском републиканском гардом и финансирањем иранског ракетног програма и различитих проиранских проксија (U.S. Department of the Treasury 2007). Ирански извори потврдили су да су банкарске трансакције онемогућене (The Times of Israel 2025), али истовремено изостају информације о деструкцији података коју је пријавила хакерска група (Vicens and Pearson 2025). Значајну штету претрпела је и иранска берза криптовалута, кључна институција у напорима Техерана да заобиђе ограничења у међународној трговини која су му наметнута санкцијама (Zendata Cyber Security 2025). Необична софистицираност сајбер

операција навели је бројне сајбер компаније да Предаторски врабац сврстају међу недржавне хакерске групе са врло блиским везама са израелским сајбер јединицама (Radware 2025; Miller 2025). Илустративан пример ове хакерске групе указује на растући проблем кооперације недржавних и државних актера у сајбер домену чиме је процес идентификације одговорних, а потом и процес њиховог кажњавања, значајно отежан.

Иранско-израелски сукоб након октобра 2023. године указује да је сајбер простор постао интегрални део савремених оружаних сукоба, не само као помоћно средство, већ и као самосталан домен пројекције моћи. Док је Иран сајбер капацитете превасходно користио у сврхе ограниченог домета као што су прикупљање обавештајних података или операције утицања у информационом простору, Израел је успео да своје сајбер операције интегрише у шири обавештајно-војни апарат, комбинујући државне и недржавне актере ради постизања конкретних стратешких ефеката. Оваква пракса указује да сајбер домен све чешће служи као инструмент демонстрације моћи у асиметричним сукобима, при чему изражена неравнотежа у сајбер способностима може имати изузетно погубне последице по државе које се у таквим односима налазе у подређеном положају, нарочито у условима растућих напетости и продубљивања нестабилности у савременим глобалним односима.

ЗАКЉУЧАК

Анализа развоја сајбер капацитета Израела и Ирана након 2010. године, као и њихова потоња употреба током сукоба који је уследио у Појасу Газе октобра 2023. године показује да је дигитални простор постао незаобилазан и структурно интегрисан део савремених националних стратегија безбедности, а последично и оружаних сукоба, што је посебно видљиво у комплексним и политички осетљивим безбедносним окружењима као што је регион Блиског истока. Паралелно са ескалацијом кинетичких дејстава и ширењем сукоба између Израела и проиранских актера (на крају и самог Ирана), сајбер простор је функционисао као додатни, али не и споредни фронт, на коме су се испојиле дубоке разлике у стратегијама, а посебно доступним капацитетима за вођење сајбер борбе.

Израелски приступ сајбер безбедности, дубоко утемељен у концепту „безбедносног троугла”, успешно се прилагодио новој технолошкој стварности: кроз стратешко улагање значајних финансијских и административних ресурса, Израел је подстакао развој високотехнолошке индустрије оличене у бројним успешним стартаповима чиме је учврстио своју позицију глобалног лидера у овој области. Додатан подстрек развоју националних сајбер капацитета проистекао је из ширења мреже међународних партнера, нарочито у непосредном окружењу, који у Израелу препознају кључног провајдера безбедности у дигиталном простору. Овај синергијски ефекат државних подстицаја и приватног предузетништва није само ојачао националну отпорност, већ је трансформисао сајбер капацитете у инструмент израелске меке моћи и спољнополитичког деловања у региону.

Са друге стране, за Техеран, сајбер безбедност постала је подједнако важно питање као и развој нуклеарног програма, не само због њене способности да пројектује националну моћ споља, већ и због контроле унутрашњег информационог простора која се директно везује за опстанак режима погођеног учесталим протестима. Упркос системским препрекама у развоју сајбер капацитета, првенствено међународним санкцијама, Техеран је успео остварити значајне резултате. Овакав напредак заснован је на стратешкој сарадњи са Русијом и Кином, али и на фокусираним домаћим улагањима и пажљивом процесу селекције кадрова. Иако, према доступним подацима, Иран још увек није досегао ниво техничке софистицираности израелских актера, остварени напредак је био довољан да се Техеран позиционира као изузетно потентна претња по регионалну сајбер безбедност.

Емпиријски примери разматрани у овом раду потврђују полазну претпоставку да сајбер инструменти не могу суштински компензовати асиметрију моћи када је јачи актер способан да их интегрише у шири војно-обавештајни апарат. Иран је сајбер средства превасходно користио у оквиру асиметричне стратегије ограниченог домета. Иранске и проиранске сајбер активности биле су усмерене на операције у информационом простору са циљем генерисања друштвених подела и ерозије међународне подршке Тел Авиву, као и на прикупљање обавештајних података, без јасно уочљивих, трајних или системских ефеката по критичну инфраструктуру Израела и његових савезника. Са друге стране,

израелски приступ одликује се вишим степеном интеграције дигиталних операција у шири обавештајно-војни апарат државе, где сајбер активности служе као допунски механизам који омогућава прецизније планирање и извођење кинетичких удара и повећање укупне ефикасности војних операција. Реакције иранског државног врха, укључујући суспензију интернета и ограничење употребе мобилних уређаја међу високим званичницима, додатно потврђују перцепцију значајне рањивости у сајбер домену и указују на постојање изражене асиметрије у способностима две државе.

Иранско-израелски сукоб након октобра 2023. године представља илустративан пример безбедносних ризика које производи изражена асиметрија сајбер способности у савременим сукобима. Док технолошки и организационо надмоћнији актери могу интегрисати сајбер инструменте у војне и обавештајне операције, остварујући тиме конкретне оперативне и стратешке ефекте, државе које се налазе у подређеном положају остају ограничене на облике деловања нижег интензитета, чији су домети често привремени или симболични. Оваква неравнотежа не само да продубљује рањивост слабијих актера у условима оружаног сукоба, већ истовремено подстиче све ширу употребу сајбер средстава као компоненте хибридног деловања испод прага оружане борбе. У условима растућих регионалних и глобалних напетости и интензивiranог надметања између различитих држава, овакви облици деловања постају све учесталија пракса, што додатно повећава ризик од нестабилности, неконтролисане ескалације и дугорочног подривања постојећих безбедносних аранжмана.

РЕФЕРЕНЦЕ

- Agence France-Presse*. 2015. "Russia Signs Military Cooperation Deal with Iran." *Defense News*. January 20, 2015. <https://www.defensenews.com/home/2015/01/20/russia-signs-military-cooperation-deal-with-iran/>.
- Albright, David, Paul Brannan, and Christina Walrond. 2010. "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" *Institute for Science and International Security*. December 22, 2010. <https://isis-online.org/isis-reports/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/>.

- Al-Halawany, Islam. 2021. "Israel Is Becoming a Cybersecurity Guarantor in the Middle East. Here's How." *Atlantic Council*. November 18, 2021. <https://www.atlanticcouncil.org/blogs/menasource/israel-is-becoming-a-cybersecurity-guarantor-in-the-middle-east-heres-how/>.
- Amaliya, Luthfi Rahma. 2025. "A Cyber War of Iran–Israel: A Geopolitical Rivalry." In *Proceedings of the International Conference on Strategic and Global Studies (ICSGS 2024)*, 45–56. Amsterdam: Atlantis Press. DOI: 10.2991/978-94-6463-646-8_4.
- Anderson, Collin, and Karim Sadjadpour. 2018. "Iran's Cyber Threat: Espionage, Sabotage, and Revenge." *Carnegie Endowment for International Peace*. January 4, 2018. https://assets.carnegieendowment.org/static/files/Iran_Cyber_Final_Full_v2.pdf.
- Arshad, Muhammad Hammad. 2025. "U.S.–Iran Cyber War and Its Impact on Israel." *Wah Academia Journal of Social Sciences* 4 (1): 1134–1158.
- Baram, Gil. 2017. "Israeli Defense in the Age of Cyber War." *Middle East Quarterly* 24 (1): 1–10.
- Bogićević, Aleksandar. 2025. "The Influence of Non-State Cyber Actors in Conventional Armed Conflicts: A Case Study of the War in Ukraine." In *VojNa 2025: International Scientific Conference on Military Sciences*, eds. Srđan Blagojević and Dragan Trifković, 304–310. Belgrade: Military Academy.
- Brenner, Neri. 2012. "Hackers Target More Israeli Websites." *Ynetnews*. January 25, 2012. <https://www.ynet.co.il/articles/0,7340,L-4180781,00.html>.
- Bucala, Paul, and Caitlin S. Pendleton. 2015. "Iranian Cyber Strategy: A View from the Iranian Military." *Critical Threats Project*. November 24, 2015. <https://www.criticalthreats.org/analysis/iranian-cyber-strategy-a-view-from-the-iranian-military>.
- Cybersecurity and Infrastructure Security Agency. 2025. "Iranian State-Sponsored Cyber Threat: Advisories." *Americas Cyber Defense Agency*. Last Accessed January 13, 2026. <https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/iran/publications>.
- Digital Watch Observatory. 2025. "Israel – Country Profile on Digital and Cybersecurity Landscape." *Digital Watch Observatory*. Last Accessed January 10, 2026. dig.watch/countries/israel.

- Eisenstadt, Michael, and David Pollock. 2021. "Asset Test 2021: How the U.S. Can Keep Benefiting from Its Alliance with Israel." *The Washington Institute for Near East Policy*. February 24, 2021. <https://www.washingtoninstitute.org/policy-analysis/asset-test-2021-how-us-can-keep-benefiting-its-alliance-israel>.
- Elgin, Ben, and Michael Riley. 2014. "Now at the Sands Casino: An Iranian Hacker in Every Server." *Bloomberg*. December 12, 2014. <https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas>.
- El-Masry, Ahmed. 2021. "The Abraham Accords and Their Cyber Implications: How Iran Is Unifying the Region's Cyberspace." *Middle East Institute*. June 9, 2021. <https://mei.edu/publication/abraham-accords-and-their-cyber-implications-how-iran-unifying-regions-cyberspace/>.
- Faris, Lamia. 2025. "Algorithmic Targeting in the Iranian–Israeli Confrontation: Technical Realities, Legal Thresholds, and the Boundaries of Human Control." *F1000Research* 14 (1200): 1–23 DOI: 10.12688/f1000research.169794.1.
- Fassihi, Farnaz, Ronen Bergman, and Mark Mazzetti. 2025. "Targeting Iran's Leaders, Israel Found a Weak Link: Their Bodyguards." *New York Times*. August 30, 2025. <https://www.nytimes.com/2025/08/30/us/politics/israel-iran-assassination.html>.
- Freilich, Charles D. 2018. *Israeli National Security: A New Strategy for an Era of Change*. New York: Oxford University Press.
- Freilich, Charles D., Matthew S. Cohen, and Gabi Siboni. 2023. *Israel and the Cyber Threat: How the Startup Nation Became a Global Cyber Power*. Oxford: Oxford University Press. DOI: 10.1093/oso/9780197677711.001.0001.
- Government of Israel. 2011. "Advancing National Cyberspace Capabilities: Government Resolution No. 3611." *National Security Archive*. August 7, 2011. <https://nsarchive.gwu.edu/document/22530-document-05-government-israel-resolution-no>.
- Guzansky, Yoel, and Ron Deutch. 2019. "How Prepared Is Saudi Arabia for a Cyber War?" *The Institute for National Security Studies (INSS)*. July 10, 2019. www.inss.org.il/publication/how-prepared-is-saudi-arabia-for-a-cyber-war/.
- Haroon, Ayesha. 2024. "AI and Cyber Drove Warfare in the Israeli–Iranian Conflict and Its Impact on Gulf States' Security." *Journal of Politics and International Studies* 10 (2): 145–163.

- International Institute for Strategic Studies [IISS]. 2021a. "Cyber Power – Tier Two." *IISS*. June 24, 2021. <https://www.iiiss.org/research-paper/2021/06/cyber-power---tier-two/>.
- International Institute for Strategic Studies [IISS]. 2021b. "Cyber Power – Tier Two." *IISS*. June 24, 2021. <https://www.iiiss.org/research-paper/2021/06/cyber-power---tier-two/>.
- Israel National Cyber Directorate. 2019. "The Israel National Cyber Directorate: Iran Is a Main Cyber Threat in the Middle East." *Israel National Cyber Directorate*. June 26, 2019. https://www.gov.il/en/pages/unna_cyber_week_2019.
- Kamiński, Michał A. 2020. "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. DOI: 10.35467/sdq/121974.
- Keshavarz, Alma. 2023. *The Iranian Revolutionary Guard Corps: Defining Iran's Military Doctrine*. London: Bloomsbury Academic.
- Khorrami, Nima. 2021. "One Year On – Israel's Cybersecurity Cooperation with the GCC States." *Middle East Institute and the National University of Singapore*. September 14, 2021. <https://mei.nus.edu.sg/publication/insight-266-one-year-on-israels-cybersecurity-cooperation-with-the-gcc-states/>.
- Liff, Adam P. 2012. "Cyber War: A New 'Absolute Weapon'? The Proliferation of Cyber Warfare Capabilities and Interstate War." *Journal of Strategic Studies* 35 (3): 401–428. DOI: 10.1080/01402390.2012.663252.
- Miller, Maggie. 2025. "Here's How the War between Israel and Iran Is Playing Out in Cyberspace." *Politico*. June 22, 2025. <https://www.politico.com/news/2025/06/22/us-israel-iran-war-cyber-attacks-00417782>.
- Netolická, Veronika, and Miroslav Mareš. 2018. "Arms Race 'in Cyberspace' – A Case Study of Iran and Israel." *Comparative Strategy* 37 (5): 414–429. DOI: 10.1080/01495933.2018.1526568.
- New Jersey Cybersecurity and Communications Integration Cell. 2024. "Increase in Cyber Threat Activity Associated with Iranian State-Sponsored and State-Affiliated Threat Groups." *Office of Homeland Security and Preparedness*. August 29, 2024. <https://www.cyber.nj.gov/Home/Components/News/News/1440/>.

- Newman, Lily Hay. 2025. "Israel Says Iran Is Hacking Security Cameras for Spying." *WIRED*. June 21, 2025. <https://www.wired.com/story/israel-says-iran-is-hack-security-cameras-for-spying/>.
- Oghanna, Ayman. 2023. "How Albania Became a Target for Cyberattacks." *Foreign Policy*. March 25, 2023. <https://foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran/>.
- Picus Security. 2025. „Predatory Sparrow: Inside the Cyber Warfare Targeting Iran’s Critical Infrastructure.” *Picus Security*. November 4, 2025. <https://www.picussecurity.com/resource/blog/predatory-sparrow-inside-the-cyber-warfare-targeting-irans-critical-infrastructure>.
- Pijpers, Patrick B. M. J. 2023. "Revisiting the Stability/Instability Paradox in Cyberspace: Lessons from the Russo-Ukraine War." *SSRN Electronic Journal*. DOI: 10.2139/ssrn.4514908.
- Politico*. 2025. "Iran Orders Officials to Ditch Connected Devices." *Politico*. June 17, 2025. <https://www.politico.eu/article/iran-orders-officials-to-ditch-connected-devices/>.
- Press, Gil. 2017. "6 Reasons Israel Became a Cybersecurity Powerhouse Leading the \$82 Billion Industry." *Forbes*. July 18, 2017. <https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/>.
- Radware. 2025. "Hybrid Warfare Unfolded: Cyberattacks, Hacktivism and Disinformation in the 2025 Israel–Iran War." *Radware*. June 18, 2025. www.radware.com/security/threat-advisories-and-attack-reports/cyberattacks-hacktivism-and-disinformation-in-the-2025-israel-iran-war/.
- Razin, Assaf. 2018. *Israel and the World Economy: The Power of Globalization*. Cambridge: MIT Press.
- Reddy, Pagilla Manohar. 2025. "Part 1: The Iran-Israel Cyber Standoff – The Hacktivist Front." *CloudSEK*. June 19, 2025. <https://www.cloudsek.com/blog/part-1-the-iran-israel-cyber-standoff---the-hacktivist-front>.
- Reuters*. 2021. "Iran and China Sign 25-Year Cooperation Agreement." *Reuters*. March 27, 2021. <https://www.reuters.com/world/china/iran-china-sign-25-year-cooperation-agreement-2021-03-27/>.
- Rid, Thomas. 2013. *Cyber War Will Not Take Place*. Oxford: Oxford University Press.

- Sabin, Sam. 2025. "Iran Leans on Hacktivist Proxies in Wake of Israeli, U.S. Strikes." *Axios*. July 1, 2025. <https://www.axios.com/2025/07/01/iran-hacktivist-israeli-us-strikes>.
- Shafa, Eric K. 2014. "Iran's Emergence as a Cyber Power." *Strategic Studies Institute, U.S. Army War College*. August 20, 2014. <https://ssi.armywarcollege.edu/SSI-Media/Recent-Publications/Display/Article/3614420/irans-emergence-as-a-cyber-power/>.
- Siboni, Gabi, Lea Abramski, and Gal Sapir. 2020. "Iran's Activity in Cyberspace: Identifying Patterns and Understanding the Strategy." *Cyber, Intelligence and Security* 4 (1): 21–40.
- SOCRadar Cyber Intelligence. 2025. "Reflections of the Israel–Iran Conflict on the Cyber World." *SOCRadar Blog*. June 19, 2025. <https://socradar.io/blog/reflections-of-israel-iran-conflict-cyber-world/>.
- Tabansky, Lior. 2020. "Israel Defense Forces and National Cyber Defense." *Connections* 19 (1): 45–62. DOI: 10.11610/Connections.19.1.05.
- Tashkandi, Hala. 2020. "Cyberattacks Hit 95% of Saudi Businesses Last Year, Says Study." *Arab News*. August 12, 2020. <https://www.arabnews.com/node/1718596/saudi-arabia>.
- The Economist*. 2024. "Iran's Electronic Confrontation with Israel." *The Economist*. August 15, 2024. <https://www.economist.com/middle-east-and-africa/2024/08/15/irans-electronic-confrontation-with-israel>.
- The Times of Israel*. 2025. "Iranian news site confirms banking issues due to cyberattack after hacking claim." *The Times of Israel*. June 17, 2025. https://www.timesofisrael.com/liveblog_entry/iranian-news-site-confirms-banking-issues-due-to-cyberattack-after-hacking-claim/.
- ThreatMon. 2026. "The Cyber Front of Iran-Israel." *ThreatMon*. Last Accessed January 13, 2026. <https://threatmon.io/the-cyber-front-of-iran-israel/>.
- U.S. Department of Defense. 2023. "Summary 2023 Cyber Strategy of The Department of Defense." *Department of Defense*. September 12, 2023. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf.
- U.S. Department of the Treasury. 2007. "Iran's Bank Sepah Designated by Treasury; Sepah Facilitating Iran's Weapons Program." *U.S.*

- Department of the Treasury*. January 9, 2007. <https://home.treasury.gov/news/press-releases/hp219>.
- United States Department of Justice. 2016. "Seven Iranians Working for Islamic Revolutionary Guard Corps—Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks against U.S. Financial Sector." *Office of Public Affairs*. March 24, 2016. <https://www.justice.gov/archives/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged>.
- Vicens, A. J. 2023. "Savvy Israel-Linked Hacking Group Reemerges amid Gaza Fighting." *CyberScoop*. October 10, 2023. <https://cyberscoop.com/predatory-sparrow-israel-gaza-cyber/>.
- Vicens, A. J., and James Pearson. 2025. "Suspected Israeli hackers claim to destroy data at Iran's Bank Sepah." *Reuters*. June 17, 2025. <https://www.reuters.com/world/middle-east/suspected-israeli-hackers-claim-destroy-data-irans-bank-sepah-2025-06-17/>.
- Watts, Clint. 2024. "Iran accelerates cyber ops against Israel from chaotic start." *Microsoft*. February 6, 2024. <https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/>.
- Zendata Cyber Security. 2025. "Zendata's Cyber Analysis of the Iran–Israel Conflict." *Zendata Cyber Security*. June 24, 2025. <https://zendata.security/2025/06/24/zendatas-cyber-analysis-of-the-iran-israel-conflict/>.

Aleksandar Bogićević*

*Strategic Research Institute, University of Defence, Belgrade,
Republic of Serbia*

THE ISRAEL-IRAN CYBER WAR: THE DIGITAL DIMENSION OF MIDDLE EASTERN CONFLICTS IN A POST-UNIPOLAR WORLD**

Resume

This paper analyses the evolution of cyber conflict between Israel and Iran since 2010, with emphasis on the period following the Gaza conflict in October 2023, against the backdrop of the transition from American unipolarity toward a multipolar international order. The central research question addresses the extent to which cyber instruments can compensate for power asymmetry in conditions of active regional conflict. The paper argues that the strategic effects of cyber operations remain limited when the technologically superior actor can integrate digital operations with kinetic action. The Israeli-Iranian cyber conflict began with the discovery of the Stuxnet virus in 2010, a joint Israeli-American operation targeting Iran's Natanz nuclear facility, marking the first cyberattack to produce direct physical effects on critical infrastructure. This event prompted both states to fundamentally reorient their cybersecurity policies and offensive cyber strategies. Israel, drawing on its "security triangle" doctrine emphasising deterrence, early warning, and decisive victory, developed a sophisticated national cyber ecosystem through strategic public-private investment and an expanding network of international partnerships, cementing its position as a global leader in cybersecurity. For Iran, cybersecurity became equally important as its nuclear program, serving both to project power externally and to control the domestic information space. Despite systemic obstacles, including international sanctions,

* E-mail address: aleksandar.bogicevic@mod.gov.rs; ORCID: 0009-0006-7450-5193.

** This paper was presented at the conference "Perspectives of Political Sciences in Contemporary Society IV", held on December 4–5, 2025, organized by the Institute for Political Studies, Belgrade.

limited financing, and brain drain, Tehran achieved significant progress through strategic cooperation with Russia and China and by carefully selecting personnel within cyber units linked to the Revolutionary Guard. Empirical analysis confirms the paper's central hypothesis: Iran primarily employed cyber instruments as part of an asymmetric strategy of limited reach, focused on information operations aimed at generating social divisions and eroding international support for Israel, as well as intelligence gathering, without producing clearly observable, lasting, or systemic effects on critical infrastructure. Israel, by contrast, integrated cyber operations into its broader military and intelligence apparatus as a complementary mechanism enabling more precise planning and execution of kinetic strikes. The Iranian-Israeli conflict after October 2023 thus represents an illustrative case study of the security risks produced by pronounced asymmetry in cyber capabilities, in which technologically superior actors achieve concrete strategic effects while weaker states remain confined to lower-intensity, often symbolic forms of action.

Keywords: Israel, Iran, Cyber warfare, Cybersecurity, Middle East.

* Овај рад је примљен 21. јануара 2026. године, а прихваћен за штампу на састанку Редакције 27. фебруара 2026. године.