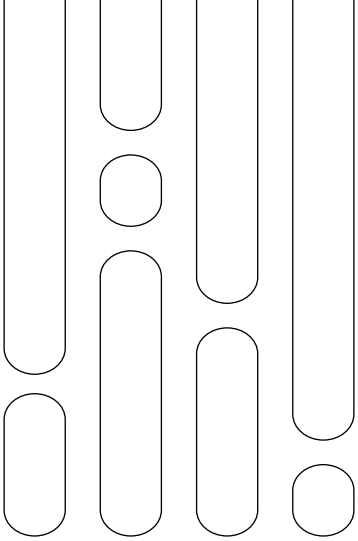
STUDY

The Impact of the Iran-Israel Cyberwar on Regional Security

Laila al-Dousari

Research Assistant

RASANAH
المعهد الدولي للدراسات الإيرانية
International Institute for Iranian Studies



Introduction 3
First: Cyber Capabilities and Israeli and Iranian Objectives Within Their Strategic Architecture..... 4
Second: Israeli-Iranian Cyberwarfare Outcomes.....13
Third: Israeli-Iranian Cyberwarfare — Regional Repercussions 20
Fourth: Future Trajectories of Cyberwarfare..... 26
Conclusion 30

www.Rasanah-iiis.org

Rasanahiiis info@rasanahiiis.com +966112166696

Introduction

Cyberwarfare has emerged as one of the most dangerous instruments of conflict employed by states and non-state actors in the 21st century. This form of warfare depends on cyberattacks targeting state networks, critical infrastructure and sensitive data for purposes ranging from espionage and sabotage to service disruption and the manipulation of public opinion and economic activity. Increasingly, it is deployed as a calculated means of reshaping the rules of regional engagement without resorting to conventional military confrontation. The objective is no longer confined to intelligence gathering or the gradual exhaustion of an adversary's resources; rather, it extends to undermining the state's very capacity to function during times of crisis. In this sense, cyberwarfare has evolved into an instrument aimed not merely at disruption, but at impairing the operational pillars of the state itself.

The cyber confrontation between Israel and Iran stands as one of the most intricate and enduring digital conflicts in the Middle East. Far from a recent phenomenon, this confrontation has developed over more than 15 years, with the Stuxnet attack marking a decisive turning point in the cyber conflict between the two sides. Despite the clear disparity in technological and operational capabilities between the two countries, Iran has succeeded in consolidating its position in confronting Israel, transforming the cyber dimension of their rivalry into a notable model of geopolitical competition.

This study examines the Israeli-Iranian cyber conflict, its impact on the cybersecurity landscape of regional states and its future trajectories. Within this framework, the study raises several key questions, most notably: what cyber capabilities do Iran and Israel possess? What impact has cyberwarfare had on both the Iranian and Israeli sides? What are the regional repercussions of this conflict? And what are the future trajectories of the Israeli-Iranian cyber confrontation?

First: Cyber Capabilities and Israeli and Iranian Objectives Within Their Strategic Architecture

Israel's cyberwarfare capabilities have undergone significant development since the emergence of the digital age, positioning the country as a leading actor in the sphere of cyberwarfare in the Middle East. On the other hand, Iran's exposure to a wide range of internal and external cyber threats has driven it to strengthen both its defensive and offensive cyber capacities with unprecedented intensity.

Israel

Israel's cyberwarfare capabilities have become a central pillar of its national strategic security architecture, reflecting an advanced combination of technological innovation and operational expertise. Among the most prominent components of these capabilities is the Electronic Dome, a system designed to safeguard critical national infrastructure. Tel Aviv first revealed the system in 2022 as part of efforts to reduce the impact of large-scale cyberattacks through the use of artificial intelligence (AI) and big data technologies, enabling the real-time detection and mitigation of cyber threats. The system is intended to secure the country's vital infrastructure against cyberattacks launched by hostile states and malicious online actors.(1)

In addition, Signals Intelligence (SIGINT) systems constitute a key element of Israel's cyber defense framework by intercepting and analyzing digital signals for intelligence-gathering purposes. These systems are designed to monitor and collect data from multiple channels of communication, including radio transmissions, satellite communications and internet traffic. Through the capture and analysis of digital signals, SIGINT systems are capable of identifying potential cyber threats, tracking malicious activities and providing critical intelligence regarding adversarial operations. (2)

---

(1)"The Electronic Dome Reflects Israel's Defensive Cyber Capabilities," *Independent Arabia,* September 18, 2024, accessed January 5, 2026, https://tinyurl.com/24ta8yal](https://tinyurl.com/24ta8yal.

(2)"Israel's Cyber Defense Capabilities," Startup Nation Central, August 11, 2024, accessed January 5, 2026. https://tinyurl.com/28t74z89](https://tinyurl.com/28t74z89.

Alongside its specialized startups, the Israeli private sector has earned a reputation as the "mother of startups," with Israel hosting hundreds of cybersecurity companies that provide globally advanced solutions for protection against digital attacks and the management of access to sensitive accounts. Among the most prominent of these firms is Check Point Software Technologies, a leading Israeli cybersecurity company established in 1993. Headquartered in Tel Aviv, with additional offices in California, the company is widely recognized for developing security software and network protection solutions, and is regarded as one of Israel's largest firms in the cybersecurity sector.[1] Another major company is CyberArk, founded in 1999. The company specializes in securing privileged accounts,[2] which are among the primary targets of cyberattacks and digital intrusions.[3]

Another major component of Israel's cyber capabilities is the Israel National Cyber Directorate, the national security and technological authority responsible for protecting Israel's national cyberspace and overseeing the establishment and development of the country's cyber force. Operating at the national level, the Cyber Directorate works to continuously strengthen the cyber defense of institutions and citizens, prevent and respond to cyberattacks and enhance emergency response capabilities in the face of digital threats.[4]

Israel also possesses a specialized military body known as the C4I Corps (Cyber Defense), the central body within the Israeli military responsible for communications planning, wireless transmission systems, computing operations, command and control functions and the protection of military and intelligence information systems.

---

(1) Shahira Badri, "Head of an Israeli Company: Foreign Investors Fear Investing in an Unstable Country," Al Bawaba News, August 15, 2024, accessed April 5, 2026, https://tinyurl.com/25lbep6y](https://tinyurl.com/25lbep6y.
(2) "Israeli Cybersecurity Company Acquires American Startup for $175 Million," Aurora Israel News, February 15, 2025, accessed April 5, 2026, https://tinyurl.com/2crghau3](https://tinyurl.com/2crghau3.
(3) "Israel's Cyber Defense Capabilities," Startup Nation Central. Ibid.
(4) "About Gov.il," Gov.il, February 21, 2024, accessed April 21, 2026, https://tinyurl.com/2d9mdp8p](https://tinyurl.com/2d9mdp8p.

The unit was established in 2003 and has since played a central role in integrating cyber defense capabilities into Israel's broader military and intelligence infrastructure.(1)

In addition to its cybersecurity education and training initiatives, Israel has developed programs targeting young people in cooperation with the Israeli Ministry of Defense and the Ministry of Education. Among the most notable of these initiatives are the two after-school Magshimim programs, which are specifically designed to identify and cultivate talent in the field of cybersecurity. Approximately 75% of participating students later join cyber and intelligence units within the Israeli military.(2)

To reinforce these capabilities, Israel has also moved toward establishing cyber alliances with major technology companies. A number of security reports suggest that ongoing conflicts have underscored for Israel the necessity of building such partnerships. Consequently, it has sought to develop strategic relationships with major firms such as Amazon, Microsoft and Google.(3) Through these partnerships, Israel aims to strengthen the security of cyberspace while benefiting from its close cooperative ties with more than 20 countries in daily exchange of information and cyber intelligence.

Israel has employed these capabilities as a means to project power, partly to safeguard the state and partly to reinforce its regional influence. In this context, three principal Israeli offensive objectives can be identified, foremost among them espionage and intelligence gathering. Within this framework, Unit 8200 has emerged as a highly advanced technological intelligence apparatus that has also served as an incubator for dozens of startups specializing in cyber espionage and cyberattacks. Widely regarded as the most important cyber

(1) Al-Khandaq.
"Directorate of Information and Communications Technology and Cyber Defense," Al-Khandaq, June 20, 2025, accessed January 10, 2026, https://tinyurl.com/2d7gqbxa](https://tinyurl.com/2d7gqbxa.
(2) Jasper Frei, "Israel's National Cybersecurity and Cyberdefense Posture," CSS Cyberdefense Report, Zürich: Center for Security Studies (CSS), ETH Zürich, September 2020, accessed January 2, 2026, https://tinyurl.com/2ck6yycv.
(3) Sami Khalifa, "The Electronic Dome Reflects Israel's Defensive Cyber Capabilities," September 18, 2024, accessed January 1, 2026, ..https://tinyurl.com/279sq8fm](https://tinyurl.com/279sq8fm.

intelligence branch within the Israeli military, Unit 8200 is known for its capabilities in intercepting communications, analyzing data, penetrating networks and conducting cyber operations.[1] Among the tools associated with these capabilities is the Graphite program, which extends beyond the scope of a conventional surveillance tool and represents a highly advanced level of cyber control. The program is reportedly capable of infiltrating mobile phones operating on both Android and iOS systems and obtaining full access to messages and conversations conducted through encrypted applications.[2] In addition, the sophisticated Flame malware —developed jointly by the United States and Israel — has been described as a complex and highly advanced cyber espionage weapon designed to collect sensitive information and intelligence data. Discovered by security researchers around 2012, Flame has been regarded as one of the most dangerous forms of malware to emerge in the cyber domain.[3] Another example is Duqu, a highly sophisticated and covert malware program specifically engineered for cyber espionage and the theft of sensitive data.[4]

The second objective involves cyber sabotage of critical infrastructure, a trend reflected in the recent escalation of cyberwarfare between the two sides. Israel's cyber capabilities have enabled it to target sensitive facilities, including nuclear installations as well as military and civilian infrastructure. These operations have included a series of financial breaches, among them attacks targeting banks and causing widespread disruptions to services.[5] The cyber arena

(1) Al Jazeera – Ahmed Antar.
Ahmed Antar, "From Unit 8200 to Paragon: How Israeli Cyber Espionage Is Manufactured," Al Jazeera, July 20, 2025, accessed January 1, 2026, https://tinyurl.com/27uww842](https://tinyurl.com/27uww842.
(2) Nesreen Kara, "The Israeli Spyware Program Graphite in the Hands of the U.S. Immigration Agency," Al Jazeera, September 9, 2025, accessed January 2, 2026, https://tinyurl.com/2bqd9f45](https://tinyurl.com/2bqd9f45.
(3) "What is Flame Malware?" Cyberpedia, ReasonLabs, accessed January 2, 2026, https://tinyurl.com/24pctcyx](https://tinyurl.com/24pctcyx.
(4) "Duqu, VPN Unlimited Help – Cybersecurity Terms and Definitions," KeepSolid Inc. accessed January 2, 2026, https://tinyurl.com/28f79hyq](https://tinyurl.com/28f79hyq.
(5) Diana Estefania Rubio, "Tools and Fronts of the Cyber War Between Iran and Israel," Al Majalla, June 24, 2025, accessed March 2, 2026, https://tinyurl.com/2yux24c2](https://tinyurl.com/2yux24c2.

also witnessed a major attack on Nobitex,[1] one of the largest cryptocurrency trading platforms in Iran. In a separate incident, cyberattacks targeted gas station networks, leading to major service disruptions in Tehran and several other Iranian cities.

The third and final objective centers on the manipulation of public opinion through psychological and cognitive cyberwarfare. Cyberattacks have increasingly become part of a broader battle over public opinion between rival actors. Their effects are no longer limited to technical disruption, such as disabling systems or damaging infrastructure; rather, they have evolved into psychological and media-driven strategies aimed at inflaming public sentiment, weakening domestic confidence in governments and fostering a pervasive sense of insecurity.

Within this context, Israeli media campaigns, alongside those of its allies and supporters, have employed disinformation and the manipulation of information as tools operating in parallel with military activities on the ground. Fact-checkers and information analysts have confronted new forms of mass information manipulation during wartime — methods that differ substantially from earlier patterns — particularly with the growing use of AI technologies to generate misleading content that is often more difficult to debunk through definitive evidence than conventional false claims.[2]

Several examples illustrate Israel's cyber capabilities in shaping the public opinion of adversarial societies. Among them is Predator Sparrow, a pro-Israel hacking group reportedly linked, directly or indirectly, to the Israeli government.[3] The group's campaigns have been marked by deliberate data destruction and the dissemination

(1) Reuters. A.J. Vicens, "Iran Crypto Exchange Hit by Hackers, $90 Million Destroyed," Reuters, June 18, 2025, accessed January 2, 2026, https://tinyurl.com/2c8l3npn](https://tinyurl.com/2c8l3npn.
(2) Shaimaa Al-Issai, "The Double Standards of Western Media Coverage of Women's Suffering in the Islamic World," Al Jazeera Media Institute, November 19, 2024, accessed January 2, 2026, https://tinyurl.com/2btsvgjd](https://tinyurl.com/2btsvgjd.
(3) Joe Tidy, Predatory Sparrow: Who Are the Hackers Who Say They Started a Fire in Iran?, BBC News, July 11, 2022, accessed January 2, 2026, https://tinyurl.com/275mu9dt](https://tinyurl.com/275mu9dt.

of provocative public messages intended to maximize psychological impact alongside operational disruption.[1]

Iran

Similarly, cyber defense capabilities represent a core component of Iran's national security strategy, as the country seeks to safeguard its critical infrastructure, governmental institutions and digital networks against external cyberattacks within a regional and international environment marked by intensifying cyber threats.

At the forefront of these capabilities is the Cyber Defense Command, established in November 2010 under the supervision of the Preventive Defense Organization. Its mandate is to confront organized domestic and international activities and the misuse of cyberspace against Iran, as well as other communication systems used for acts such as terrorism, cyber espionage, money laundering and cultural infiltration.[2] In addition, the National Passive Defense Organization plays a central role in infrastructure protection. One of its primary responsibilities, as outlined in its operational framework, is to mobilize all national cyber and non-cyber resources to deter, prevent, detect, respond to and counter any cyberattack originating from hostile foreign actors, whether state or non-state, targeting Iran.[3]

On the other hand, Iran has pursued the development of an "isolated internet" program, regarded as one of its strategic cyber projects initiated in early 2009. The objective of this initiative is to restructure national online activity into an internally controlled communication network separated from the global internet. This framework enables the state, on the one hand, to strengthen oversight and control over digital content and data flows while also reducing reliance on the global internet infrastructure. It further facilitates the development of indigenous technologies, including the creation of a secure

(1) Tushar Subhra Utta, "Predatory Sparrow Group Attacking Critical Infrastructure," Cyber Security News, January 11, 2026, accessed January 2, 2026, .https://tinyurl.com/23utwmbk](https://tinyurl.com/23utwmbk.
(2) Ibid
(3) Ministry of Foreign Affairs and Diplomacy of the Islamic Republic of Iran, "Iran's Cyber Capabilities: What Are They?" accessed March 11, 2026, www.irdiplomacy.ir](http://www.irdiplomacy.ir).

operating system designed to decrease dependence on foreign, particularly US operating systems.

In parallel, the aforesaid is reinforced through enhanced defensive measures within governmental institutions, including reliance on the Islamic Revolutionary Guard Corps (IRGC) to conduct intensive cyber training exercises for both civilian and military personnel in preparation for potential cyberattacks. The most recent of these exercises reportedly took place in late 2015.[1] It is also indicated that many of the individuals involved in Iran's cyber defense and offensive capabilities possess prior experience and expertise in fields such as security studies, computer science, communications and other technical and computational disciplines.[2]

In addition, Iran has engaged in international cooperation in the field of cyberwarfare. The first Russian–Iranian cyber cooperation agreement was concluded in 2015, with the head of Iran's Civil Defense Organization stating that such collaboration was necessary given that both countries face common adversaries in cyberspace. In 2017, Moscow and Tehran signed a memorandum of understanding on cooperation in information and communication technologies, covering areas such as internet governance, network security and international internet connectivity. It is also likely that Russia may supply Iran with cyber defense systems and provide training for its personnel. Similarly, the strategic cooperation agreement between China and Iran is reported to include provisions related to cyber control.[3]

---

(1) Bassem Rashid, "The Growing Development of Iranian Capabilities in Electronic Warfare," Rasanah, April 20, 2016, accessed January 11, 2026, https://tinyurl.com/25efhx2u](https://tinyurl.com/25efhx2u.
(2) Azar, Davoud. "Cyber Power Strategies of the Army of the Islamic Republic of Iran," Future Defense Studies, accessed January 11, 2026, https://tinyurl.com/23wpmhpn](https://tinyurl.com/23wpmhpn.
(3) Mohamed Farid Azzi, "Iranian Cyber Activity: Between Secrecy and Openness," Trends Research, December 5, 2021, accessed January 11, 2026, https://tinyurl.com/2ag7gb7g](https://tinyurl.com/2ag7gb7g.

Finally, Iran maintains what is commonly referred to as the Iranian Cyber Army, which is responsible for offensive operations in cyberspace. It operates under the supervision of the IRGC Cyber Command. Drawing on skilled hackers and advanced information technology expertise, it has been reported to target media outlets as well as Western interests.[1] Comprising various militias, digital factions, hackers and volunteers from academic and research institutions under IRGC oversight, this structure is often described as the "Iran Cyber Army," functioning as a digital arm of the Iranian state and used in cyber operations targeting and destabilizing external actors.

Iran has also integrated AI into its cybersecurity framework, reflecting growing investment in this field in recent years. AI applications in this domain include several key functions including the following:

• Automated threat detection: AI-based systems identify abnormal network traffic patterns and can anticipate potential cyberattacks.

• Enhanced malware analysis: Machine learning techniques are used to analyze and detect previously unknown forms of malicious activity.

• Automated incident response: AI systems are capable of delivering rapid, automated responses to complex cyber threats.

• Endpoint Detection and Response (EDR) systems: These systems are designed to defend against malware and targeted attacks. EDR is an advanced security mechanism that continuously monitors and analyzes user and system behavior, detecting and neutralizing threats in real time. Within Iran's cybersecurity architecture, EDR systems play a significant role. They enable the detection of advanced threats such as fileless malware, conduct detailed behavioral analysis of users and networked devices, integrate with AI systems to generate automated threat assessments, and provide the capacity for rapid response, including isolating compromised systems.[2]

(1) Ibid
(2) Bahrami, Katayoun
"Revealing Israel's Cyberattack Plan Against Iran: Defensive Strategies and Iran's Cyber Capabilities," Salam Digi (Technology Section), March 9, 2025, accessed January 11, 2026, hellodigi.ir.

Thus, it appears that Iran has developed advanced cyber offensive capabilities that enable it to conduct hacking and disruption operations targeting critical sectors of its adversaries. These capabilities are employed as a strategic instrument to expand influence and exert political pressure within the framework of proxy warfare. Iran's primary objective is the execution of cyber campaigns. In this context, Iranian cyber actors have carried out large-scale operations aimed at inflicting economic harm, undermining political stability, disrupting financial systems and bypassing censorship mechanisms in several countries.(1) Its secondary objective involves infiltration and intelligence-gathering operations targeting networks and infrastructure. These activities include a range of hacking operations against government systems as well as destructive cyber actions. They combine technical intrusion operations with propaganda and psychological warfare components. Iran has also disseminated stolen data and disinformation through social media and other outlets to generate fear and distrust within targeted states. In addition, it has reportedly placed forged or altered documents on compromised websites to advance its narratives, including the spread of false corruption-related reports through hacked local media platforms.(2)

The ultimate objective is the collection of tactical intelligence through cyber reconnaissance. In this regard, Iranian operatives have reportedly gained access to internet-connected surveillance camera systems in Israel, using them for battlefield observation, damage assessment and missile targeting. The exploitation of civilian infrastructure for intelligence, surveillance and reconnaissance purposes reflects a more advanced approach to cyber espionage, enabling Iran to expand its operational awareness without relying on

(1) "Iran Hack Operations: Cyberattacks and Legal Consequences," Legal Clarity Team, December 14, 2025, accessed January 14, 2026, https://tinyurl.com/296gusec](https://tinyurl.com/296gusec.
(2) "Assessment of Iran's Cyber Capabilities," Mashregh Service, September 19, 2025, accessed January 11, 2026, www.mashreghnews.ir](http://www.mashreghnews.ir.

traditional reconnaissance assets within adversary territory.[1] As part of these intelligence-gathering efforts, a cyber entity linked to the IRGC, referred to as the "Ajax Team" or "Missile Cat," was reportedly established in 2014. Its purpose was to target specific entities and individuals to collect intelligence and extract sensitive information.[2]

Second: Israeli-Iranian Cyberwarfare Outcomes

Cyberwarfare between Iran and Israel has experienced a marked escalation in recent years, with digital attacks increasingly serving as a strategic instrument for both sides to pursue their objectives without direct recourse to conventional warfare. The effects of this confrontation extend across economic systems, critical infrastructure, national security structures and civil society, underscoring the growing centrality of cybersecurity as a key dimension in the rivalry between the two countries.

Consequences and Gains for Israel

Cyberwarfare entails significant consequences for Israel, particularly in the security and military domains. Given Israel's strong dependence on advanced military technologies and a highly digitized economy, it is exposed to greater risks from cyberattacks compared to Iran, which maintains a more limited integration into the global digital environment. This dynamic makes the cyber domain an increasingly pressing security challenge for Israel, as even relatively low-cost attacks can have substantial effects on critical infrastructure and social systems.[3] In this context, cyberattacks have reportedly disrupted hospitals, including the Shamir Medical Center in

(1) Sajjad Abedi, "What Did the 12-Day War Reveal About Iran's Cyber Strategy?" Khabar Online, August 5, 2025, accessed January 2, 2026, https://tinyurl.com/26mtwz9v](https://tinyurl.com/26mtwz9v.
(2) Ahmed Ali Al-Maimouni, "An Active Front: The Repercussions of the Cyber Confrontation Between Iran and Israel," Rasanah, May 25, 2021, accessed January 22, 2026, https://tinyurl.com/2aykx5ql](https://tinyurl.com/2aykx5ql.
(3) Jay Hilotin, "Iran–Israel War: The Rise and Risks of Hybrid Warfare," Gulf News, June 25, 2025, accessed January 2, 2026, https://tinyurl.com/2da8m2fd](https://tinyurl.com/2da8m2fd.

central Israel in October 2025,[1] and have also targeted a range of companies providing computing and digital services to the economicsector.[2]

On the economic front, a recent report issued by the Israeli National Cyber Directorate provides, for the first time, an economic assessment of the cumulative costs to the Israeli economy resulting from cyberattacks. The data indicates the scale of the financial burden imposed on the country's GDP, highlighting the aggregate damage sustained by the economy over time. According to the report, Israel's total economic losses following the 12-Day War with Iran are estimated at approximately $6 billion, with critical infrastructure sectors particularly affected. The conflict is further projected to cost Israel around 1% of its GDP.[3] The report also addresses the social dimension of these cyberattacks, noting the emergence of heightened anxiety and public concern stemming from the risk of data breaches or disruptions to essential services. In addition, it highlights disruptions to daily life caused by the interruption of key digital services, including banking systems and telecommunications networks.[4]

Despite these risks and the considerable costs borne by the Israeli economy, cyberwarfare also presents a set of opportunities and advantages. Foremost among these is the consolidation of military and security superiority. In this regard, Israel has, over past decades, consistently developed its military technology to strengthen its capacity to counter security threats, particularly those posed by Iran and its regional proxies, including Hezbollah in Lebanon, Hamas and the

(1) "A Wave of Cyberattacks Hits Israel," MSN Arabic, October 22, 2025, accessed April 9, 2026, https://tinyurl.com/25v9l3zs](https://tinyurl.com/25v9l3zs.
(2) "The Economic Cost of Cyberattacks in Israel: 12 Billion NIS per Year," Gov.il – Official Website of the Government of Israel, May 8, 2024, accessed January 13, 2026, https://tinyurl.com/2b2zykm9](https://tinyurl.com/2b2zykm9.
(3) The National.
Fareed Rahman, "Israel's Economic Losses as a Result of Iran War Estimated at $6bn," The National, June 26, 2025, accessed January 13, 2026, https://tinyurl.com/22zm3e2m](https://tinyurl.com/22zm3e2m.
(4) ICliniq
Shweta Sharma, "Mental Health Impact of Cyberattacks and Data Breaches," ICliniq, July 19, 2024, accessed January 13, 2026, https://tinyurl.com/2d77h7n9](https://tinyurl.com/2d77h7n9.

Houthis. It has developed a range of advanced technological systems that play a central role in managing both air and ground defense operations.

Israel has also increasingly integrated AI into its military operations, relying on data-driven systems to analyze military targets with greater precision and identify priority targets within specific operational zones. The Gospel targeting platform is a prominent example of this approach, as it proposes targets based on strategic priorities and estimates the required amount of munitions for each strike, thereby enhancing the accuracy and effectiveness of military operations.(1)

Secondly, cyberwarfare has generated social and professional opportunities by strengthening expertise and expanding skill development. Cybersecurity has become a frontline component of both national security and economic stability, prompting states to invest heavily in training specialized personnel capable of defending against cyber threats. The Israel Cyber Campus, established in 2022, is designed to prepare students for careers in cybersecurity, both as defensive specialists and as developers. Participants gain practical experience and are trained under the guidance of leading Israeli cybersecurityexperts.(2)

Furthermore, Israel has enhanced its deterrence capabilities and strengthened its partnerships and defensive posture in this domain, particularly as cyberwarfare has become an increasingly important instrument of modern diplomacy. States now employ cyber capabilities not only for offensive operations but also to exert influence and achieve strategic objectives without direct military engagement. Cyber instruments can be used to send covert signals, deter adversaries, or project strategic dominance.(3) In parallel, the expansion of

(1) Dina Ehab Mahmoud, "A Reading of Israeli Military Technological Development," SHAF Center, September 22, 2024, accessed January 13, 2026, https://tinyurl.com/2ca56t8e](https://tinyurl.com/2ca56t8e.
(2) Nurit Yohanan & ToI Staff, "How the Israel Cyber Campus Is Preparing the Next Generation of Cyber Warriors," Times of Israel, August 25, 2024, accessed January 13, 2026, https://tinyurl.com/2c5aslta](https://tinyurl.com/2c5aslta.
(3) "Cyber Warfare and International Relations," Alpha Maneuver, 2025, accessed January 13, 2026, https://tinyurl.com/26pr48rz](https://tinyurl.com/26pr48rz.

international partnerships, including cooperation with major cybersecurity companies and foreign states, has contributed to strengthening Israel's diplomatic position. In 2022, Israel's National Cyber Directorate signed two cooperation agreements with the US Department of Homeland Security to deepen collaboration in cyber defense and advanced technologies. These agreements aimed to reinforce cyber protection for the economy and critical infrastructure, counter shared threats such as ransomware attacks, advance research and development in emerging technologies, promote cooperation between public and private sectors, and facilitate expert exchanges and professional dialogue.(1)

2-Consequences and Gains for Iran

From Iran's perspective, cyberwarfare has generated a range of significant challenges. First, it has posed a strategic challenge to the country's capabilities and nuclear infrastructure. A prominent example is the Stuxnet attack in 2010 on Iran's nuclear program, a joint US–Israeli cyber operation specifically designed for industrial sabotage. The attack caused physical damage, disrupted Iran's electronic infrastructure, and produced a profound national shock. In response, Iran rapidly accelerated the development of its then-emerging cyber capabilities.(2) On the political level, repeated accusations of Iranian involvement in cyberattacks against Western countries and international targets have contributed to the United States imposing sanctions on Iranian individuals and entities. Iran's Ministry of Intelligence also issued confidential guidelines warning ministries and major companies to prepare for the possible reactivation of UN sanctions.(3)

Cyberwarfare has additionally affected internal stability and social cohesion. At certain points, millions of Iranians were reportedly cut

(1) "The Israeli Cyber Unit Strengthens Its Cooperation with the United States," i24NEWS, March 3, 2022, accessed January 13, 2026, https://tinyurl.com/29yyaqkg](https://tinyurl.com/29yyaqkg.
(2) Chuck Freilich, "The Iranian Cyber Threat," INSS Memorandum No. 230, February 2024, accessed January 13, 2026, https://tinyurl.com/229yzqtu](https://tinyurl.com/229yzqtu.
(3) "Sanctions Are Coming: Iranian Intel Warns Ministries," Iran International, August 11, 2025, accessed January 15, 2026, https://tinyurl.com/2a4u82wt](https://tinyurl.com/2a4u82wt.

off from external connectivity due to near-total internet blackouts in Tehran and other cities. While Iranian officials stated these measures were intended to limit cyberattacks, they also significantly affected public access to communication and information.[1]

Moreover, the scope of conflict has expanded beyond infrastructure into the psychological domain. Iran's state broadcaster was hacked, and provocative messages calling for protests were aired, while opposition-related videos circulated across social media platforms.[2] Economically, the government revised its national budget to allocate an additional $71.4 million to cyber programs for two state-controlled organizations, despite ongoing economic constraints.

Despite these challenges, Iran's cyber capabilities have also generated certain opportunities and gains, most notably through the development and consolidation of its cyber infrastructure in response to emerging threats. Iran is often described as among the early states that formulated a national cyber strategy, including the establishment of relevant governmental institutions alongside the expansion of technological capacities.

Iran's cyber operations have demonstrated an ability to disrupt, sabotage and damage civilian and commercial targets, as well as critical national infrastructure and military capabilities. Its cyber espionage activities and information operations have been particularly extensive in scope. Israel and the United States are frequently identified as the primary targets of Iranian cyber operations.[3] In this context, Iran relies heavily on asymmetric warfare strategies, employing relatively low-cost cyber tools to achieve high-impact effects as a form

(1)"Iranians Adapt to Wartime Life with No Internet," Financial Times, June 21, 2025, accessed January 13, 2026, https://tinyurl.com/272c5quy](https://tinyurl.com/272c5quy.
(2) Mohamed Makhlouf, "Artificial Intelligence and Cyberattacks: New Weapons Between Iran and Israel," Al Arabiya Net, June 20, 2025, accessed January 13, 2026, https://tinyurl.com/2apvavzm](https://tinyurl.com/2apvavzm.
(3) Chuck Freilich, "The Iranian Cyber Threat," ibid.

of defensive response, particularly in light of its disparities in conventional military preparedness compared to its adversaries.[1]

In addition to strengthening cyber cooperation with Russia and China, Iran has sought in recent years to consolidate its position by orienting its foreign relations toward Eastern powers, particularly the two mentioned countries, and India, across various fields to deepen strategic ties. Cybersecurity cooperation has been among the key areas Iran has sought to incorporate into the terms and provisions of its agreements with Eastern powers. The Iranian Ministry of Foreign Affairs has stated that such cooperation is intended to coordinate efforts in detecting cyber intrusions and to ensure a high level of cybersecurity for Iran and its partners and allies.[2]

Cyberwarfare has also contributed to enhancing Iran's technical capabilities and facilitating the integration of AI into its cyber operations. Despite international restrictions imposed over recent decades on various forms of scientific and technological research, Iranian institutions have reportedly made extensive use of AI technologies to strengthen cyberwarfare capabilities, generate synthetic or misleading content, and conduct hacking and infiltration operations within the context of national strategies and official investment programs. The rapid development of AI is reshaping the balance of power within the global cybersecurity domain,[3] while reliance on advanced technologies has also stimulated domestic research and development efforts.

From a social perspective, cyberwarfare has encouraged greater emphasis on building national expertise in technology and digital security. In this context, a clandestine cyber academy known as Ravien was reportedly established in Tehran and is operated by entities

---

(١) Mohamed Maan Mohsen, "The Future Position of Cyber Power in Regional Strategies: Iran as a Model," Political Issues, Issue 81 (2025), accessed January 15, 2026, https://tinyurl.com/27j6x3uz] (https://tinyurl.com/27j6x3uz.

(2) "The Impact of Iran's Turn to the East on Its Strategy," Arab Democratic Center, December 26, 2023, accessed January 15, 2026, https://tinyurl.com/2bkggdkj](https://tinyurl.com/2bkggdkj.

(3) "Microsoft: Iran Uses Artificial Intelligence to Enhance Cyberattacks," Iran International, October 17, 2025, accessed January 15, 2026, https://tinyurl.com/2b9rjggh](https://tinyurl.com/2b9rjggh.

linked to the state, including the Ministry of Intelligence. Its purpose is to recruit and train talented youth in cybersecurity, including skills relevant to offensive cyber operations.[1] In parallel, training programs focused on information security awareness have contributed to increasing public and institutional understanding of basic cybersecurity principles among employees and broader segments of society.[2]

It is also important to note the role of cyberwarfare between the two sides during the conflict that took place in 2025 and 2026, which witnessed a marked escalation in cyberattacks. Digital networks became an active battleground alongside conventional military operations. Both sides exchanged hacking and disruption activities targeting infrastructure and communication systems, in a technological confrontation that reflected the depth of geopolitical tensions between them.

The US-Israeli strikes on Iran, referred to as Operation Epic Fury, had several significant cyber consequences. A large-scale cyberattack reportedly disrupted Iranian communications ahead of the military strike, while extensive data analysis contributed to the identification of targets. Israeli intelligence is also reported to have spent years collecting information on Ali Khamenei through cyber means, including hacking into a network of surveillance cameras in Tehran and monitoring movements.

In response, counter-cyber operations intensified, including actions that reportedly resulted in the temporary control of approximately 12 communication towers. Another operation targeted a widely used religious application for prayer time in Iran. This cyber intrusion enabled the delivery of targeted messages directly to users,[3] while

(1) Al Arabiya Net – Ravien Academy
"A Secret Iranian Academy Recruits Talented Individuals," Al Arabiya Net, October 13, 2024, accessed January 15, 2026, https://tinyurl.com/25ykemrq](https://tinyurl.com/25ykemrq.
(2) "IT Security Awareness and Employee Training Course," Training Cred, accessed January 15, 2026, https://tinyurl.com/2alrrd89.
(3) "How Will Cyber Warfare Shape the U.S.–Israel Conflict with Iran?" Center for Strategic and International Studies (CSIS), March 3, 2026, accessed March 12, 2026, https://tinyurl.com/2c4pf999.

several official Iranian news websites were also compromised and defaced.

In contrast, Iran's state-led cyber campaign, within the broader ideological framework of Islamic cyber resistance, relies on psychological operations, espionage, and service-disruption activities aimed at generating confusion within Israeli society and collecting intelligence. These operations have reportedly targeted the water, energy, and utilities sectors, manipulated industrial control systems, infiltrated encryption networks, and conducted data scanning, data leakage, phishing attempts, and gathered information on sites impacted by Iranian missiles within Israel.(1) The Israeli National Cyber Directorate reported detecting dozens of Iranian intrusions into surveillance camera systems for espionage purposes,(2) as well as more than 1,300 attempted Iranian cyberattacks since the beginning of the war with Iran, including operations targeting Israeli civilians through fraudulent phone calls and text messages.(3)

The Iranian group Handala is a cyber hacking organization associated with Iran. Active between late 2025 and 2026, it concentrated on carrying out multiple cyberattacks against Israeli and Western targets. Its activities included targeting Israeli officials through phone hacking and the publication of sensitive information, issuing threats against the Israeli intelligence agency Mossad and launching a new website while releasing more than 100,000 classified documents linked to Israeli intelligence sources.(4)

Third: Israeli-Iranian Cyberwarfare — Regional Repercussions

The cyber conflict between Iran and Israel represents one of the most significant forms of unconventional rivalry in the Middle East,

(1) "Cyber Threat Bulletin: Iranian Cyber Threat Response to US/Israel Strikes," Government of Canada, Canadian Centre for Cyber Security, February 2026, accessed March 10, 2026. https://tinyurl.com/29wuxds3.
(2) "Israel Detects an Iranian Breach of Surveillance Cameras," Asharq Al-Awsat, March 12, 2026, accessed March 10, 2026, https://tinyurl.com/2dmp9oou](https://tinyurl.com/2dmp9oou.
(3) "Have Cyberattacks Escalated with the Outbreak of the War Against Iran?" Euronews, March 10, 2026, accessed March 10, 2026, https://tinyurl.com/2xzkhdey](https://tinyurl.com/2xzkhdey.
(4) "New Website of the Hanzalah Cyber Group Launched," Safir, April 9, 2026, accessed June 10, 2026, https://tinyurl.com/23rvhyqa](https://tinyurl.com/23rvhyqa.

as the exchange of cyberattacks has gone beyond the two sides and has affected regional security and stability. Among these effects are:

1-Competition and Attempts to Enhance Capabilities Amid Lack of Digital Self-sufficiency

Developing cyber capabilities at the regional level depends primarily on participation in international events and alliances, as well as on the conclusion of partnership and investment agreements and memoranda of understanding among regional countries and between these countries and other states worldwide in the field of cyberspace.(1) Accordingly, the Kingdom of Saudi Arabia, represented by the National Cybersecurity Authority, participated in the Gulf Cooperation Council (GCC) meeting held in Kuwait, which addresses all cybersecurity-related issues. The GCC held an annual meeting at the level of cybersecurity ministers from member states, with the aim of contributing to the creation of a secure Gulf cyberspace, harmonizing efforts, enhancing coordination and cooperation among GCC countries and protecting their interests in international cybersecurity organizations.(2) The Saudi Federation for Cybersecurity, Programming and Drones also signed a memorandum of understanding with the Arab League Educational, Cultural and Scientific Organization (ALECSO) for cooperation in the field of cybersecurity.(3)

In the context of digital competition, cybersecurity investment in the Middle East is undergoing a significant strategic shift, as governments increasingly prioritize this domain within their national development plans to protect digital infrastructure and address rising cyber threats. Cybersecurity expenditure in the Gulf region is projected to double by 2030, reaching more than AED 120 billion

(1) Ahmed Mohi Mohamed Ahmed Ali, "The Impact of the Israeli–Iranian Cyber War on Arab Regional Security," Journal of the Higher Institute for Qualitative Studies, Vol. 3, No. 8, July 2023, accessed January 17, 2026, https://tinyurl.com/245jsqv2](https://tinyurl.com/245jsqv2.
(2) "The Kingdom Participates in the Fourth Meeting of the Ministerial Committee on Cybersecurity," National Cybersecurity Authority (Saudi Arabia), September 2025, accessed January 17, 2026, https://nca.gov.sa/ar/news/1930/](https://nca.gov.sa/ar/news/1930/.
(3) Government of Canada, Canadian Centre for Cyber Security, ibid.

(approximately $32.7 billion).[1] The cybersecurity market in Saudi Arabia reached SAR 15.2 billion, reflecting total government and private sector spending on cybersecurity products and services in 2024, marking a 14% increase compared to the previous year.[2] Egypt ranked first in the Middle East and North Africa in terms of the number of investment deals supporting emerging cybersecurity companiesduring2023.[3]

2-The Impact on Security and Regional Balance of Power

Some view Israel as the most advanced country in the Middle East in the field of cybersecurity. This has been demonstrated in the wars it has conducted since October 7 on multiple fronts, where its technological and cyber superiority has provided it with a significant military advantage that has influenced the course of its operations. This superiority is considered one of the manifestations of power that gives Israel an edge in the region and may offer it greater opportunities to pursue its ambitions of reshaping the regional balance of power in its favor, at the expense of Arab states whose capabilities are seen as imported and relatively limited compared to Israel's.[4]

The use of cyber instruments has extended beyond the binary nature of the Israel–Iran conflict, as attacks targeting digital environments in neighboring Arab countries have also been observed, whether directly or through non-state actors such as hacktivists. In Qatar, for example, several residents of Doha reported unusual changes in their mobile phone location data, which were incorrectly showing activity originating from Iran. In the UAE, there were widespread attempts at cyberattacks targeting government entities and companies.[5] There

(1) Kath Young, "Gulf Cybersecurity Spend to Exceed AED120bn by 2030," Arabian Business, November 21, 2025, accessed January 17, 2026, https://tinyurl.com/2yv3nzep.
(2) "Saudi National Cybersecurity Authority Released Key Economic Indicators in the Cybersecurity Sector in the Kingdom 2025," National Cybersecurity Authority, September 17, 2025, accessed January 17, 2026, https://tinyurl.com/24h8lq52.
(3) Ahmed Ghoneim, "Electronic Risks Support the Growth of Emerging Cybersecurity Companies," Al Borsa, February 3, 2025, accessed January 17, 2026, https://tinyurl.com/22ksrdpx](https://tinyurl.com/22ksrdpx.
(4) Government of Canada, Canadian Centre for Cyber Security, ibid.
(5) "The UAE Thwarts 200,000 Cyberattacks Daily," Al Khaleej, February 18, 2026, accessed March 12, 2026, https://tinyurl.com/24ng7nmk](https://tinyurl.com/24ng7nmk.

are also reports indicating that Iranian-linked actors leaked data related to visitors and games associated with an event in Saudi Arabia, suggesting cyber espionage or data breaches.[1] This expansion of cyberwarfare implies that any future confrontation between major regional powers could quickly spill over into third countries without warning or preparation, creating a new security reality in which neutrality no longer provides protection from digital involvement.[2]

3-The Region Becoming a Cyberwarfare Arena

Several regional countries continue to face persistent cybersecurity threats due to weak infrastructure and limited national coordination, which leaves them vulnerable to digital espionage and proxy attacks, particularly from Israel. Lebanon's strategic location has also made it a testing ground for Israel's regional cybersecurity tactics, with some attacks on its national networks functioning as trials for broader operations. In addition, Israeli intelligence has treated Lebanon as a live environment for testing cyber operations. Jordan's geographic position could turn it into a data hub that may be exploited in wider regional conflicts, reinforcing the need for stronger cyber cooperation at both the domestic and regional levels.[3] Cyberwarfare has also revived proxy conflicts in fragile states such as Lebanon, Syria and Iraq, significantly disrupting the fragile balance in the Middle East. Iran, for its part, has relied on state-affiliated or state-supported hacktivist groups to conduct cyberattacks, particularly following US-Israeli strikes, seeking to expand its cyber influence while officially denying responsibility.

4-Threatening Infrastructure and Disrupting Regional Energy Supplies

Should the conflict escalate, existing trade relations with Tehran or even Tel Aviv could be negatively affected, with broader repercus-

(1) "Iran-Linked Threat Actors Leak Visitors and Athletes' Data from Saudi Games," Resecurity, June 22, 2025, accessed March 2, 2026, https://tinyurl.com/2dh28nnp.
(2) Ahmed Fathy, "The Future of Cyber Conflicts in the Middle East," Aton Center, April 30, 2025, accessed January 17, 2026, https://tinyurl.com/2ctdhm7r](https://tinyurl.com/2ctdhm7r.
(3) "Middle East Cyber War: Strategy Failures Leave Arab States Vulnerable," Shafaq News, January 16, 2026, accessed January 16, 2026, https://tinyurl.com/2ar7v25y.

sions for the region as a whole.[1] Within the context of the Iranian–Israeli crisis, three main economic sectors — energy, transportation and financial markets — have been particularly exposed. In the energy sector, attacks on critical Iranian infrastructure have contributed to a sharp decline in oil and gas exports, while the shutdown of production at Israel's Leviathan and Karish gas fields, both major suppliers of gas to Egypt and Jordan, has disrupted regional energy supplies.[2] Cyber infrastructure plays a central role in both targeting and defending these sectors.

5-Changing the Dynamic Between Israel and Regional Countries

The cyberwar between Israel and Iran has influenced the pattern of relations among regional countries. The increase in cyberattacks against targets in the GCC member states, along with Israel's relative superiority in the cyber domain, has accelerated the formation of cooperative frameworks between some countries and Israel.[3] Following the Abraham Accords between Israel and both the UAE and Bahrain, cooperation among these states in cybersecurity has expanded notably, particularly in light of shared concerns over Iranian cyber threats targeting regional infrastructure.

At the CyberTech conference in Tel Aviv, senior cybersecurity officials from Israel, the UAE, Bahrain and Morocco met to discuss expanding cybersecurity cooperation within the framework of the Abraham Accords, with a focus on protecting critical infrastructure and exchanging information on cyber threats. This form of cooperation illustrates how shared cyber challenges have encouraged countries to strengthen technological and security partnerships with Israel following normalization of diplomatic relations.[4] In efforts to adjust the regional balance of cyber power and reduce cybersecuri-

(1) Zaid Aslim, "What Are the Repercussions of Turkey Suspending Its Trade Relations with Israel?" Al Jazeera Net, May 3, 2024, accessed January 17, 2026, https://tinyurl.com/2yw49ljz](https://tinyurl.com/2yw49ljz.
(2) "What Geopolitical Effects Does the Iran–Israel War Have?" *Euronews Persian,* June 21, 2025, accessed March 1, 2026, "https://tinyurl.com/2732lv7c](https://tinyurl.com/2732lv7c.
(3) Government of Canada, Canadian Centre for Cyber Security, ibid.
(4) "DHS Expands Abraham Accords to Cybersecurity," Department of Homeland Security (DHS), February 2, 2023, accessed January 17, 2026, https://tinyurl.com/25ejx85w.

ty vulnerabilities, access to Israeli expertise in intelligence and cyberwarfare has become an important factor.

6-Cyber Investment in Light of Financial Disparities

With the rise of cyberattacks and the growing complexity of digital threats, investment in cybersecurity human capital has become a cornerstone of national digital security. This investment is centered on developing and training personnel and equipping them with advanced skills to counter breaches and protect critical infrastructure. A notable example is the Saudi program Qualifying Future Cybersecurity Experts, which provides national talent with training and practical experience to contribute to the protection of Saudi Arabia's cyberspace and to strengthen the kingdom's cybersecurity capabilities.(1) This aligns with the strategic objectives of the National Cybersecurity Authority, which focus on developing human capital in the cybersecurityfield.(2)

Egypt has also launched the Cyber Skills initiative, aimed at building a new generation of cybersecurity professionals. However, cybersecurity in some regional countries faces financial constraints, which increases vulnerability to digital threats compared to states with larger budgets and more advanced programs. This situation calls for greater investment. For instance, Jordan's cybersecurity budget is approximately $70 million annually, which is relatively small compared to countries with more advanced capabilities, such as the UAE, which allocates around $1.5 billion to cybersecurity. This disparity affects Jordan's capacity to build strong defenses against cyberattacks.(3)Limited cybersecurity funding may place economic pressure on smaller countries in comparison with countries that allocate significantly larger resources to the cyber domain. Additional invest-

(1) "Future Cybersecurity Experts Qualification Program," National Cybersecurity Authority (Saudi Arabia), accessed January 17, 2026,
https://tinyurl.com/2bogjtmq](https://tinyurl.com/2bogjtmq.
(2) "Minister of Communications: Qualifying 1,000 University Students Annually Through the Cyber Skills Initiative," Masrawy, May 4, 2025, accessed April 1, 2026, https://tinyurl.com/253qpx5j](https://tinyurl.com/253qpx5j.
(3) Saudi National Cybersecurity Authority, ibid.

ment is required to strengthen digital defenses and counter threats, potentially affecting other sectors, thus increasing overall financial expenditures and burdens.

Fourth: Future Trajectories of Cyberwarfare

The foregoing indicates a strategic transformation in the nature of the conflict. Israel and Iran have shifted their confrontation from conventional military domain to cyberspace, which is characterized by low cost, high impact and plausible deniability, and by a clear overlap between defensive, offensive and psychological dimensions of warfare. This conflict is reshaping the balance of cyber power in the Middle East, particularly in light of Israel's growing role as a leading technological power and the consequent move by some Gulf states to strengthen cybersecurity cooperation with Israel.

Cyberwarfare also suggests a qualitative Israeli cyber advantage at both the regional and international levels. Israel possesses advanced cyber capabilities that provide it with a qualitative edge based on innovation, AI and the integration of military and private sector capacities, including units such as Unit 8200 and companies such as Check Point and CyberArk.

Moreover, the convergence of cyberwarfare with psychological and cognitive warfare and its impact on the conflict is evident. Operations are no longer limited to system disruption but extend to influencing public opinion through disinformation, data leaks, information manipulation, and the use of AI to amplify psychological effects. Cyberattacks on critical infrastructure have also contributed to humanitarian consequences, including disruptions to essential services and the emergence of new waves of displacement, placing additional pressure on neighboring countries and humanitarian response systems.

Undoubtedly, the Iranian–Israeli cyberwar has significantly reshaped the nature of conflict, with its effects extending to infrastructure, society, the economy and politics, while simultaneously strengthening the national capabilities of both sides.

More importantly, cyberwarfare is no longer confined to a bilateral Iran–Israel confrontation, but has expanded to include neighboring Arab states, either directly or through digital proxies. This reflects the risks of third-party exposure and the impact of cyberwarfare on their digital security, making traditional neutrality insufficient as a protective measure. Participation in international blocs and forums such as the GCC, as well as regional memoranda of understanding, may help states enhance coordination and safeguard their digital interests.

With the increasing reliance on technology and digitalization, Israel and Iran are now engaged in a cyberwar that extends their broader regional conflict through the targeting of critical infrastructure and digital systems. Accordingly, examining the trajectories of this conflict is necessary to understand its implications for regional security and the defensive capabilities of both sides. It appears that there are three scenarios for the future of cyberwarfare between Israel and Iran.

Scenario One: Sustaining the Status Quo

This scenario assumes the continuation of the current situation through limited and reciprocal strikes between Iran and Israel, aimed at containing the conflict and preventing its escalation into a broader regional cyberwar. Both sides continue to rely on indirect methods to undermine each other's interests and to conduct intelligence operations intended to obstruct the activities of the opposing side. Within this framework, the confrontation takes on the characteristics of a prolonged war of attrition in which neither party is capable of achieving a decisive victory, resulting in mounting cumulative damage for both.

Iran, which is facing a severe economic crisis, comes under increasing pressure to meet the basic needs of its population while also experiencing growing social instability. Israel, despite possessing stronger economic capabilities, also bears substantial costs due to the continuation of the conflict, the heavy expenditure on defense

systems and the decline in foreign investor confidence caused by heightened uncertainty.

The effects of this scenario would extend beyond the two direct parties and affect the broader region as well. A deterioration of conditions inside Iran could trigger large-scale displacement toward neighboring countries such as Türkiye, Iraq and Pakistan, potentially creating a complex humanitarian and regional crisis. Continued instability and disorder could also provide favorable conditions for the re-emergence of extremist groups and the intensification of insurgent activities among certain ethnic minorities opposed to Iran, including the Kurds and the Baloch.

This scenario remains a source of concern for major international powers because it reflects a state of chronic instability in the Middle East, with the possibility that the conflict could expand into multiple arenas and generate wide-ranging security and political consequences. The likelihood of this scenario is considered relatively high, and it may continue for a prolonged period, with the intensity of the conflict fluctuating between limited escalation and temporary de-escalation, reflecting the enduring instability of the region.

Scenario two: Escalation and Regional Conflagration

An unintended escalation resulting from miscalculation or unplanned military entanglements could lead to a costly regional confrontation opposed by most international and regional actors. Three indicators point to the possibility of such an escalation.

The first relates to the Iranian nuclear program. Iran's strong defenses surrounding its nuclear facilities, together with its advanced levels of uranium enrichment, could encourage Israel to adopt more aggressive policies. At the same time, developments in AI and automation may contribute to more sophisticated cyber operations, including automated hacking, large-scale data analysis, and covert attacks that are difficult to trace or counter. Such developments could draw the United States, as the dominant international power, more directly into the conflict, thereby intensifying the confronta-

tion. Some Arab and Gulf states could also become involved. Within this scenario, it is difficult to envision the conflict ending before the United States and Israel launch attacks on Iran's remaining nuclear facilities, which could subsequently contribute to regime change within a few years.

The second indicator concerns the possible collapse of the Iranian political system. Such a collapse would create a major power vacuum in the region, with negative consequences for regional political and security balances. In addition, the intensification of cyberwarfare between Israel and Iran would carry serious implications for both regional and international stability.

The third indicator is Iran's military weakness, which may push it to rely more heavily on cyberattacks as a less costly and more flexible instrument for escalation and confrontation.

The likelihood of this scenario is assessed as moderate, while its level of risk is considered high, making it a medium-probability, high-impact scenario.

Scenario Three: Curbing Cyberwarfare Through Forcing the Iranian Establishment to Change Course

The third scenario centers on the continuation of the ruling establishment in Iran. This scenario does not assume the overthrow of the establishment or a radical transformation in leadership, but rather envisages a tactical or reform-oriented adjustment in the leadership's behavior while it remains in power. Several indicators could drive such a behavioral shift. **First**, the escalation of cyberattacks targeting Iranian infrastructure; **second**, the declining effectiveness of Iran's offensive cyber capabilities; **third**, the mounting economic and technological pressures facing the country; and fourth, the growing domestic and media pressures.

Taken together, these factors could push the Iranian regime toward recalibrating its behavior rather than collapsing or being overthrown. Under this scenario, it is possible that Mojtaba Khamenei, as the new supreme leader of Iran, could agree to concessions related

to the nuclear and missile programs, as well as to reducing or suspending support for certain regional proxy groups, such as Hezbollah. Such measures could contribute to containing the cyberwar and maintaining it within manageable limits. Nevertheless, the likelihood of this scenario materializing in the short to medium term is still regarded as low.

Conclusion

In conclusion, the status quo scenario appears to be the most likely outcome, based on a number of structural and strategic considerations. The possibility that the conflict could escalate from an Iranian–Israeli confrontation into a comprehensive regional war remains relatively limited. This is largely due to the distinctive nature of cyberspace, where accurately identifying or conclusively proving responsibility for attacks is often difficult. Such ambiguity reduces the likelihood of direct military retaliation and constrains the dynamics of conventional escalation.

In addition, the states involved in this form of conflict, particularly Israel and Iran, have become increasingly aware of the dangers and strategic implications of cyberwarfare. This awareness has driven both sides to invest heavily in the development of their defensive and offensive cyber capabilities. As a result, the resilience of critical infrastructure has been strengthened and its vulnerability to attacks reduced compared to the earlier phases of this type of conflict, making decisive breakthroughs more difficult to achieve.

This growing awareness is not confined to the direct parties involved in the confrontation, but also extends to regional states, which have become more conscious of the serious implications of cyberwarfare for national security and domestic stability. Consequently, these states have intensified efforts to strengthen cybersecurity, develop defensive capabilities and enhance the preparedness of vital institutions to confront any potential repercussions arising from such conflicts.

By contrast, the scenario involving the containment of the conflict through the modification of the existing Iranian political order appears unlikely, particularly in the near term. Moreover, the appointment of Mojtaba Khamenei as supreme leader of Iran sends clear signals of continuity and defiance, indicating that the Iranian establishment has chosen a figure closely associated with the IRGC to reinforce the latter's influence over the centers of power, especially amid the continuing confrontation with the United States and Israel.

info@rasanahiiis.com
@rasanahiiis
www.rasanah-iiis.org