dipam

DİPLOMATİK İLİŞKİLER ve POLİTİK ARAŞTIRMALAR MERKEZİ
CENTER for DIPLOMATIC AFFAIRS and POLITICAL STUDIES

ANALYSIS

IRAN NUCLEAR AGREEMENT IN THE SHADOW OF ISRAEL CYBER ATTACKS

Büşra ORAK

April 2023 No: 10

IRAN NUCLEAR AGREEMENT IN THE SHADOW OF ISRAEL CYBER ATTACKS

The developments in information and communication technology in the 20th century have led to significant changes and transformations in fourth-generation warfare technology. One of these development areas is the cyberspace. The cyberspace, which is considered as the fifth battlefield, has become one of the new battlefields for states. Especially states that have technological superiority use cyber warfare tactics, including cyber attacks, cyber espionage, and cyber intelligence to expand their maneuvering space and maintain their realpolitik interests. Israel, one of these states with advanced technological superiority, actively uses the cyber domain to minimize existing threats and ensure security.

The Stuxnet attack, which is referred to as the “Pearl Harbor” of cyber warfare, caused a significant tension between Iran and Israel in 2010. Stuxnet is a turning point in both Iran-Israel relations and cyber warfare. Israel, which has carried out numerous cyber attacks since 2010, has been seen as the primary source of cyber threat with the United States against Iran. Especially with its accelerated nuclear program in the early 2000s, Iran has become a top priority on the foreign policy agendas of the United States and Israel, and has been subject to sanctions. The majority of cyber attacks against Iran were aimed at damaging nuclear facilities, stealing documents from nuclear research institutes and archives, and shaping espionage activities. In addition, assassinations were carried out against Iranian nuclear scientists. Iranian government officials held the United States and Israel responsible for the cyber attacks that took place. In the latest cyber attacks against Iran, Israel did not deny the accusations and the cyber attacks became less secretive. (Baram, 2022)

In 2016, an agreement was signed between Iran and the P5+1, consisting of the five permanent members of the United Nations Security Council (the United States, China, Russia, the United Kingdom, and France) and Germany, which aimed to limit Iran's uranium enrichment capacity. This agreement was heavily criticized by Israel, and as a result, the Comprehensive Joint Action Plan (CJAP), which resulted in the withdrawal of the United States from the agreement in 2018, has not yet been able to be restored. The Iran Nuclear Deal that took place under the shadow of Israel has become one of the most important reasons for cyber warfare both in the real domain and cyberspace in the historical process.

Israel's Cyber Power and Capacity

The cyberspace that emerged towards the end of the 20th century has caused significant changes and transformations in many military, political, and social fields, from war technology to the state's foreign policy tools and war doctrines. Unlike traditional approaches to international relations, cyberspace has greatly changed the security-threat, attack-defense, or power-security relationships. Threats to states have begun to emerge not only at the state level but also at all levels of analysis. This has made it necessary for the state to diversify and develop its security strategies at all levels of analysis. (Choucri, Clark, & Hurwitz, 2015)

The source, type, size, and impact of threats have also changed significantly. The source of threats can be a state, but it can also be a sixteen-year-old user. Therefore, state control units and security tools have

become more complex and challenging. Types and sources of attacks have also diversified. Therefore, cyber attacks are classified according to the source and type of threat. State and non-state actors such as spyware developers, hackers, malicious software developers, terrorists, and identity thieves can be the source of the threat. Activities such as Denial of Service Attack (DoS), Distributed Denial of service (DDoS), Trojan Horse, Virus, Malicious Software, Worms, Spyware, Hacking provide us with information about the type of attack. (David, 2010)

Cyber attacks carried out by states are usually carried out by units affiliated with the state or private hacker groups. These cyber armies or private groups typically target critical infrastructure systems of states. They use cyber attacks as a deterrent element to wear down, intimidate, or threaten the enemy. Israel also frequently resorts to cyber war and attack information and tools.

Israel government is currently the world leader in information technology and the largest cyber power and capacity state in the Middle East. Israel, which pioneered the use of cyber technology as a weapon and its widespread use, returned to an active stance in the cyber field in the 1990s. The Israeli national security strategy, as outlined by cyber security expert Isaac Ben-Israel, places great importance on cyber information and technology to maintain Israel's regional and global security, balance its numerical disadvantage, and increase its qualitative advantage. This qualitative advantage is referred to as “superior weapons” based on information technology. Additionally, Ben-Israel defines Israel's cyber warfare strategy through the doctrine of deterrence.

In 2010, Ben-Israel initiated the “National Cyber Initiative” vision to increase Israel's cyber capabilities. This vision led to the publication of Israel's first national cyber strategy in 2011, which was largely not made public. By 2017, Ben-Israel had revealed Israel's national cyber security strategy for defense and offense, categorized as deterrence, persistent victory, early warning, and alliances. Israel's national cyber strategy also encompasses its international cyber strategy, which aims to create a global cyber defense mechanism through cooperation, capacity building, trust, and new technological solutions.

Beyond this strategy, an inclusive cyber security organization called the Israel National Cyber Directorate (INCD) has been established. The INCD is part of the government's cyber groups, along with UNIT-8200, the National Cyber Security Authority (NISA), and other cyber groups. In addition, the Mossad, Shin Bet, Israel National Cyber Readiness Team (CERT-IL), Israel Defense Ministry, Israel Public Security Directorate, Cyber Authority, Israel National Cyber Bureau (INCB), Israel Police, Cyber Crime Unit, and National Cyber Security Authority (NCSA) are some of the agencies working in the field of cyber security.

Not only official agencies, but also various groups such as cyber mercenaries and hacker support groups have been established. The U.S. and Israeli armies conduct joint cyber defense training processes and carry out joint exercises against cyber threats to increase their operational capabilities against possible cyber attacks. This can lead to both countries being implicated in a cyber attack. Iran has accused both Israel and the U.S. in the Stuxnet attack on its nuclear

program. Cyber attacks against Iran during the Iran nuclear agreement, also known as the Joint Comprehensive Plan of Action (JCPOA), have targeted both Israel and the U.S. The intensity of cyber attacks between Iran and Israel provides significant clues about the relationship between the two countries.

Iran Nuclear Agreement (The Joint Comprehensive Plan of Action, Jcpoa)

In 2002, which was still an early date for the cyberspace, Ali Riza Caferzade announced that Iran had two nuclear power plants in Natanz and Arak. As a result, the United States complained to the International Atomic Energy Agency (IAEA) about Iran's development of nuclear weapons. The sanctions unilaterally imposed by the US against Iran turned into multilateral sanctions with the decisions taken by the UN Security Council between 2006-2010 due to Iran's continued nuclear energy research. The Iran Sanctions Accountability and Divestment Act (ISADA), signed by H. Barack Obama in July 2010, targeted Iran's direct supply of oil energy and the oil sector (Rezaei, 2019).

In 2011-2012, the UN stopped the presence of Iranian banks and their trade in the oil sector. On March 17, 2012, states and international companies that did not comply with the sanctions and all Iranian banks were isolated from the Society for Worldwide Interbank Financial Telecommunication (SWIFT), the central point of the world's banking channels, including financial transactions.

At the end of 2015, US sanctions caused a change in Iran's policy. On June 14, 2015, an agreement was reached between 6 countries (USA, China, UK, Germany, Russia, France) and Iran, called the Comprehensive Joint Action Plan (CJAP). This agreement imposed serious limitations on Iran's nuclear activities and lifted the 1696, 1737, 1747, 1803, 1835, 1929 sanctions. (Aslan, 2018).

Although negotiations lasted more than two years, compromise and cooperation were achieved as a result of the concessions given mutually. As a result of the negotiations, the US lifted the sanctions on Iran's energy sector. Thus, the sanctions on Iran's finance and banking, insurance, energy and petrochemicals, shipping, shipbuilding and ports, gold and other metals, computer programs, and the automotive industry were lifted under the leadership of the Office of Foreign Assets Control (OFAC) (Rezaei, 2019). After being certified by the International Energy Agency (IEA), it entered into force on January 16, 2016.

Former US President Donald Trump unilaterally withdrew from the Iran Nuclear Deal, which he had referred to as the “worst deal in history,” on May 8, 2018, two years after being elected. This move, which was not accepted by China and Russia, prompted 28 EU member states, the US, and Iran to begin active diplomacy. However, Donald Trump claimed that the Joint Comprehensive Plan of Action (JCPOA) only temporarily suspended Iran's nuclear production and that negotiations failed due to Iran's continued ballistic missile production (Rezaei, 2019). As a result, the economic improvements and energy sector revitalization seen in Iran reverted back to pre-2015 levels. The US issued two calls to countries, one for 90 days and the other for 180 days, to cut off their commercial ties with Iran in the energy, manufacturing, port, industrial, and mining sectors.

After Trump, Joe Biden, who was elected US President in January 2021, stated that he was ready to start negotiations with Iran. Talks to return the US to the JCPOA began in Vienna in April 2021 and ended on August 8. However, with the protests in Iran that began in September 2022 and the increasing violence seen, along with footage emerging of Joe Biden implying that the nuclear deal was “dead” while negotiations with Iran were ongoing, it appears difficult for the parties to come back to the negotiating table (Biden, declared the nuclear deal “dead” while negotiations with Iran were ongoing, 2022).

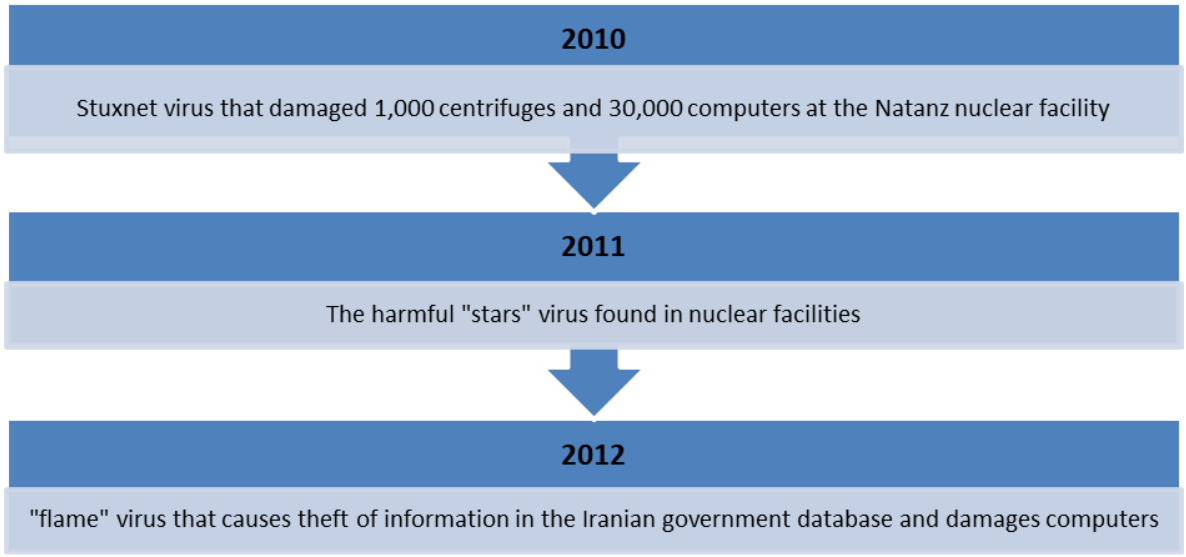
The Effect of Israel Cyber Attacks on The Iran Nuclear Agreement

Before the 1979 Iranian Islamic Revolution, Israel had good relations with the Shah's regime. However, after the revolution led by Ayatollah Khomeini, which integrated Shia-Islamic identity, Israel perceived Iran as a threat to its existence and identity. Similarly, the United States and Israel saw Iran as the biggest threat to its existence and identity due to the Iranian Revolution (Shalom, 2016). When Iran began its nuclear program and did not abandon its doctrine under Khomeini, external pressures increased, leading to sanctions and disagreements in the Iran Nuclear Agreement. Israel feared a significant threat to its state and people and the imbalance of power in the Middle East, leading to the stalemate in the Iran Nuclear Agreement (Oruç, 2016).

One of the most significant obstacles in determining whether attacks pose a security problem for states is attribution and timing. Identifying the source and type of a cyber threat can result in a significant loss of time. Not knowing who carried out the attack can put the attacking party in a more advantageous position. Mutual cyber attacks by Israel and Iran eliminate attribution issues. Although Israeli and Iranian government officials have not confirmed the attacks, their parallel statements confirm the source. Israeli cyber attacks, bombings, assassinations, and espionage against Iran since 2010 have revealed Israel's hybrid warfare tactics against Iran. The attacks were mostly aimed at Iran's nuclear program. The forms of attack include infecting nuclear facilities with computer viruses, targeting infrastructure systems, and assassinations of nuclear scientists (Timeline: Israeli Attacks on Iran, 2023).

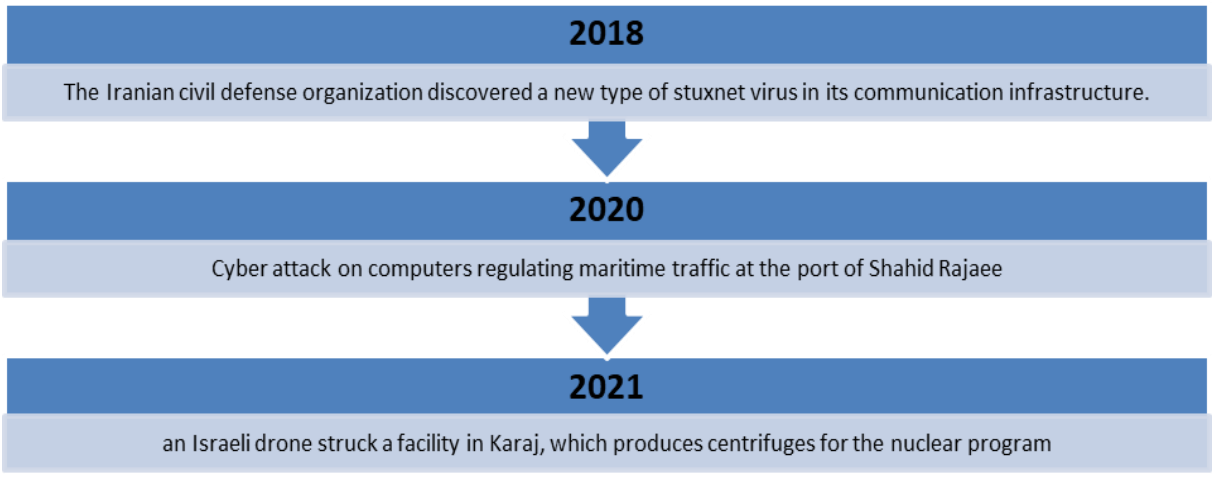
Since 2010, Israel has regularly carried out numerous cyber attacks on Iran. However, these attacks can be divided into two periods. The first period covers the years 2010-2012, when cyber attacks were particularly intense. This period predates the Iran Nuclear Deal (Israeli Sabotage of Iran’s Nuclear Program, 2021). Although there were many cyber attacks between 2010 and 2012, the most damaging cyber attacks to the other party are listed in Table 1.

Table.1: 2010-2012 Major Cyber Attacks



The second period involves the post-2018 period when the US withdrew from the Nuclear Agreement. However, this period also includes hybrid warfare methods alongside cyber warfare methods, such as Mossad raids, assassinations, and drone attacks. Numerous attacks have been carried out on Iran's nuclear facilities during this period (Israeli Sabotage of Iran's Nuclear Program, 2021). However, Table.2 shows important cyber attacks.

Table.2: 2018-2021 Major Cyber Attacks



Since 2018, the cyber attacks that have occurred are seen to be more openly carried out. Many attacks have been carried out, such as the explosion that occurred on July 2, 2020, causing great damage to Iran's main nuclear enrichment facility in Natanz, damaging the factory that produces IR-4 and IR-6 centrifuges, the drone attack on a military factory on January 29, and the targeting of Iran's unmanned aerial vehicle production center by six Israeli drones on February 14, 2022 (Iran Military Factory Drone Attack, 2023). In addition, Iran's cyber attacks are carried out as retaliation and target not only the US, Israel, and Saudi Arabia but also Turkey and Western countries. There has been a significant increase in Iran's cyber attacks in the first half of 2015 and the last six months of 2018, which is significant in terms of following the nuclear agreement process (Bulut, 2021).

Conclusion

Five years after the establishment of the State of Israel, in its national defense strategy document, it emphasized the importance of developing superior weapons technology in secret from the enemy. Half a century later, Israel has become the country with the most advanced technological weapons in the region. Its superior capabilities in cyberspace and its professional application of cyberattack-defense strategies have enabled it to carry out numerous cyberattacks and cyber espionage activities.

Israel, in collaboration with US cyber groups and non-state hacker groups, has carried out dozens of attacks and espionage activities against Iran. However, Israel's ultimate goal in its cyberattacks against Iran has been carried out within the framework of Iran's nuclear program. When analyzing cyberattacks carried out in Iran, the attacks intersect at three points: nuclear facilities, institutes and archives where nuclear work is conducted, and Iran's communication and technological infrastructure. In particular, since 2010, Israel has experienced a significant increase in cyberattacks against Iran. This period has been divided into periods according to the increasing density of cyberattacks.

From 2010 to the present, Israel has conducted a hybrid war against what it sees as the biggest security threat: Iran's nuclear program. This has included cyberattacks, cyber espionage, assassination, drone attacks, and explosions, thus weakening Iran's nuclear activities and causing delays. Iran has also carried out cyberattacks against Israel, especially targeting Israel's allies. Cyberattacks between Iran and Israel are shaped by their foreign policy strategies and security perceptions. Therefore, the cyber domain can provide important insights into the future of the Iran Nuclear Deal and how the process will proceed. Since 2018, the increasing number of cyberattacks has increased uncertainty about the future of the Iran Nuclear Deal and cast a shadow over nuclear negotiations.

REFERENCES

(2020). *Israel's National Cybersecurity and Cyberdefense Posture.* Zürich: Center for Security Studies (CSS).

Israeli Sabotage of Iran's Nuclear Program. (2021). https://iranprimer.usip.org/blog/2021/apr/12/israeli-sabotage-iran%E2%80%99s-nuclear-program

Kasım Süleymani suikastı üzerinden bir yıl geçti ancak İran ile ABD arasındaki gerginlik azalmadı. (2021). anadolu ajansı: https://www.aa.com.tr/tr/dunya/kasim-suleymani-suikasti-uzerinden-bir-yil-gecti-ancak-iran-ile-abd-arasindaki-gerginlik-azalmadi/2096165

Biden, İran ile müzakereler devam ederken nükleer anlaşmayı "ölü" ilan etmiş. (2022, aralık 20). https://www.hurriyet.com.tr/dunya/biden-iran-ile-muzakereler-devam-ederken-nukleer-anlasmayi-olu-ilan-etmis-42190798

İran Askeri Fabrikasına Drone Saldırısı. (2023). https://www.voaturkce.com/a/iran-askeri-fabrikasina-drone-saldirisi/6938909.html

Timeline: Israeli Attacks on Iran. (2023). https://iranprimer.usip.org/blog/2022/aug/11/timeline-israeli-attacks-iran

Aslan, M. (2018). ABD'nin Nükleer Anlaşmadan Çekilmesinin Ekonomik Sonuçları. *İran Araştırma Merkezi(İRAM)*, 5-18.

Baram, G. (2022, july 25). *How the cyberwar between Iran and Israel has intensified*. https://www.washingtonpost.com/politics/2022/07/25/iran-israel-cyber-war/

Bulut, S. (2021). İran'ın Siber Alan Faaliyetleri: Kapsamlı Ortak Eylem Planı (KOEP) SürecineDair Bulgular. *Gaziantep Unıversıty Journal OF Socıal Scıences*, 166-191.

Choucri, N., Clark, D. D., & Hurwitz, R. (2015). *exploration in cyber international relation.* Cambridge: Massachusetts Institute of Technology.

Çağla Gül Yesevi. (2015). İran'ın Enerji Sektörü: İran'ın Yumuşak ve Akıllı Gücü. *İstanbul Kültür Üniversitesi*, 441-467.

David, C. (2010). Characterizing,cyberspace:,past,,present,and,future. *MIT,CSAIL*, 1-18.

McCreanor, K. (2021). The Theory, Pursuit, and Practice of Cyber power in Israel. *Centre of Military and Strategic Studies*, 2-21.

Oruç, H. (2016). ran Nükleer Anlaşması ve İsrail'in Anlaşmaya Yönelik Tepkisi. *ORTADOĞU YILLIĞI* , 484-500.

Rezaei, F. (2019). *Iran's Foreign Policy After the Nuclear Agreement.* Ankara: Palgrave Macmillan.

Shalom, Z. (2016). Israel, the United States, and the Nuclear Agreement with Iran:Insights and Implications. *Strategic Assessment*, 18-28.

dipam
DİPLOMATİK İLİŞKİLER ve POLİTİK ARAŞTIRMALAR MERKEZİ
CENTER for DIPLOMATIC AFFAIRS and POLITICAL STUDIES

+90 216 310 30 40
info@dipam.org
+90 216 310 30 50
www.dipam.org
Merdivenköy Mah. Nur Sok. Business İstanbul
A Blok Kat:12 No:115, Kadıköy/İstanbul

ABOUT THE AUTHOR

Büşra ORAK graduated from Niğde Ömer Halisdemir University, Department of Political Science and International Relations, and continues her Master's Degree in International Relations at Hacı Bayram Veli University. Orak also works as a Focus Working Group Intern at DIPAM.
orakbusra09@gmail.com