Cyberwar Between Iran and Israel Out in the Open

Gil Baram[1], Yael Ram[2] & Isaac Ben Israel[3]

In 2010, Iran first reported a cyberattack against its nuclear facilities, pointing to the U.S. and Israel as the perpetrators. The attack – using the now infamous Stuxnet malicious virus – was the first known cyberattack in the world to cause physical damage beyond computer-stored data. Despite no actual proof that Israel stood behind the attack, the current consensus is that Israel will continue to act in cyberspace and in all other domains to prevent Iran from realizing its nuclear program objectives. Concurrently, Iran is steadfast in its desire to strengthen its cyber capabilities and become a major player in cyberspace.[4]

Since April 2020, the mutual cyberattacks of Israel and Iran have emerged from the shadows and become more intense, with the international news media regularly publishing reports on the trading of cyber salvos. For example, in May 2020 there were reports that Iran attempted to breach Israel's water and sewage infrastructure, and in response Israel launched a cyberattack on Iran's bustling Shaheed Rajaee port in Bandar Abbas. Subsequently, there have been numerous incidents - including explosions, power outages and blazes - at various sites including military installations, factories and industrial zones across Iran. Though these cyberattacks have not been attributed to Israel and Iran, the two countries have made declarations and displayed a clear pattern of behavior leaving little doubt of their intentions: Israel National Cyber Directorate head Yigal Unna said publicly that Israel would do whatever it could to thwart Iran's nuclear program, including cyber operations. Iran, on the other hand, stated that it would not allow Israel to challenge it on the cyber front.[4]

[1] Cyber strategy and policy expert. Head of Research at Tel Aviv University's Yuval Ne'eman Workshop for Science, Technology and Security, and a post-doctorate fellow at Stanford University.

[2] Researcher at Tel Aviv University's Yuval Ne'eman Workshop for Science, Technology and Security, and a Master's student in Security Studies at Tel Aviv University.

[3] Director of the Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University.

[4] Cohen, Matthew S., Charles D. Freilich, and Gabi Siboni. "Israel and Cyberspace: Unique Threat and Response." *International Studies Perspectives*, 2015. https://doi.org/10.1093/isp/ekv023.

[5] AP, "'Cyber winter is coming,' warns Israel cyber chief after attack on water systems", *Times of Israel*, May 28, 2020. https://www.timesofisrael.com/israeli-cyber-chief-attack-on-water-systems-a-changing-point-in-cyber-warfare/.

While cyberattacks are typically conducted in the shadows under a cloud of secrecy, the latest round of attacks between Israel and Iran has been more intense, public and out in the open than in the past. This could be what led to the latest round of escalation, with each side showing its unwillingness to absorb a blow without responding and displaying its unwavering resolve. These mutual attacks signify a new dynamic between the two countries, expanding the conflict to the cyber sphere, with each country drawing its own red lines vis-à-vis one another and the international community.

Though it could be anticipated that countries carrying out cyberattacks – or those that are victims – would prefer to maintain secrecy and ambiguity, not making any public comments, new research shows that states have a number of strategic options, with secrecy being only one choice; in many instances, countries are choosing to publicly address cyberattacks.[5]

The Israeli Response

On 24 April 2020, Iran carried out a cyberattack aimed at damaging Israel's water and sewage infrastructure, attempting to paralyze the water system and potentially harm citizens by changing the water's chemical balance. This was Iran's first public cyberattack attempt on Israel's physical infrastructure, a turning point in the cyber conflict between the two countries.[6] Though the attack did not cause significant damage to Israel, it was viewed as crossing a red line: an attempted infrastructure attack indicated that Iran was legitimizing the use of cyber force against the civilian population, which could be construed as an act of war. One month later, the *New York Times* reported that the cyber software used in the attack originated from within the Revolutionary Guards.[7]

Israel's response to this attack shows just how seriously it considered the attempted breach: on 9 May 2020, the computer system controlling traffic flow at the Shaheed Rajaee port terminal in Bandar Abbas crashed, wreaking havoc on the movement of all vessels, vehicles and goods; the port was out of commission for a few days, causing Iran significant economic

[5] Baram, Gil and U. Sommer. "Covert or not Covert: National Strategies During Cyber Conflict." 2019 11th International Conference on Cyber Conflict (CyCon) 900 (2019): 1-16. doi: 10.23919/CYCON.2019.8756682.

[6] "Cyber Attack on Israel's Water Facilities: Iran Attempted to Increase Chlorine Levels," *YNET* 01 June 2020, https://www.ynet.co.il/articles/0,7340,L-5740087,00.html [Hebrew]

[7] Bergman, Ronen and Halbfinger, David. "Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks.", *New York Times*. May 19, 2020. https://www.nytimes.com/2020/05/19/world/middleeast/israel-iran-cyberattacks.html

damage and harming its reputation. The *Washington Post* attributed the incident to Israel, claiming the cyberattack was in response to the Iranian attack in April.[8] Israel's disproportionate response, causing significantly more damage than the Iranian attack – seemingly was intended to display Israel's military and technological superiority to deter the Iranian regime from attempting similar attacks in the future.[9]

On the heels of the port incident, there was a string of unusual mishaps and explosions at a number of military installations and facilities: on 26 June 2020, there was a large explosion at a site where weapon systems related to the nuclear program (allegedly) were being tested and missiles were being produced. The explosion also caused a power outage in the nearby city of Shiraz. Claiming the site of the blast was a "public area" in a report on Iran state TV, an Iranian Ministry of Defense spokesman maintained the explosion was caused by a gas leak, there were no casualties and the fire had been contained.[10] Yet, those claims are not consistent with the fact that army personnel, as opposed to firefighters, extinguished the blaze.

Quoting a source familiar with the area, a local BBC correspondent said that , the explosion occurred on a base of the Revolutionary Guards or other military base.[11] Israel, for its part, denied any involvement in the attack.[12] Four days later, there was an explosion at a missile manufacturing facility near a base used for development of fuels for the Revolutionary Guards missile program. Once again, Israel denied involvement.[13]

On 2 July 2020, there was an explosion at a uranium enrichment facility using advanced centrifuges. Western sources believed the blast was caused by an Israeli cyberattack, and that

[8] Warrick, Joby, and Ellen Nakashima. "Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility," *Washington Post*, 18 May 2020. https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

[9] Yonah Jeremy Bob, "The Goal of the Attack Attributed to Israel – Get the Other Side to Think Twice Before Acting." *Ma'ariv Online*, 19 May 2020. https://www.maariv.co.il/news/military/Article-766345 [Hebrew]

[10] "Iran Reports Gas Explosion at Gas-Storage Tank Near Sensitive Military Site ,"*Radio Free Europe*, 26 June 2020 https://www.rferl.org/a/iran-explosion-military-site-gas-tank/30691489.html

[11] Gambrell, Jon. "Satellite Image: Iran Blast Was near Suspected Missile Site." *Associated Press*, 27 June 2020. https://apnews.com/8d2517ff364bb395f0385859f0fa9d0f

[12] "American, Israeli Officials Deny Sabotage of Iranian Missile Site, Report Says." *Ha'aretz*, 30 June 2020. https://www.haaretz.com/middle-east-news/iran/.premium-american-israeli-officials-deny-sabotage-of-iranian-missile-site-report-says-1.8958009

[13] Intentional Destruction or an Accident? Israeli & American Officials Say They Had Nothing to Do with the Explosion in Tehran," *Ha'aretz*, 4 July 2020. https://www.haaretz.co.il/news/world/middle-east/.premium-1.8957964 [Hebrew]

it would lead to a delay of months or even years in the Iranian nuclear program. Despite the attempts to attribute the attack to Israel, Israel's response was ambiguous.[14] Senior Israeli officials did not take responsibility, instead giving vague answers and refocusing attention on the Iranian nuclear program. When asked about the attack, Defense Minister Benny Gantz neither confirmed nor denied the reports, stating: "Not every incident that transpires in Iran necessarily has something to do with us...."[15]

Senior Iranian officials claimed they had identified the attackers but preferred not to expose them.[16] Nonetheless, Iranian Foreign Ministry spokesman Abbas Musawi issued an unveiled threat, saying that "if we conclude that a regime or government had a hand in the explosion, either directly or indirectly, there will be a very serious response from us."[17]

In parallel with these mysterious explosions at Iranian military installations, there were random blasts and power outages nationwide, such as a power station explosion in Ahvaz on 4 July 2020, and the next day a chlorine leak at a petrochemical plant in which 70 people were hospitalized.[18] On 7 July 2020, nearby what was claimed by Iran to be a data storage center, two scientists from the Iranian nuclear program were killed in an explosion; this was the same facility that Israel breached in 2018, stealing a huge archive of Iranian nuclear plans.[19] That same week, explosions were heard in western Tehran, perhaps in an area where missiles were

[14] Fassihi, Farnaz, Richard Pérez-Peña, and Ronen Bergman. "Iran Admits Serious Damage to Natanz Nuclear Site, Setting Back Program." *New York Times*, 5 July 2020. http://www.nytimes.com/2020/07/05/world/middleeast/iran-Natanz-nuclear-damage.html

[15] "Major Damage to Natanz, Could Lead to Delay in Centrifuge Development." *Walla! News*, 6 July 2020 https://news.walla.co.il/item/3371786 [Hebrew]

[16] Farnaz, Pérez-Peña, and Bergman, "Iran Admits Serious Damage to Natanz Nuclear Site, Setting Back Program." *New York Times*, 5 July 2020.

[17] Roi Case, "Revolutionary Guards Quds Force Commander Threatens – Difficult Days Ahead for the U.S. and Israel," *Kan 11*, July 2020. https://www.kan.org.il/item/?itemid=74249 [Hebrew]

[18] "Fire at Power Plant, Chlorine Leak at Petrochemical Plant in Iran." *JPost.com*, 5 July 2020. https://www.jpost.com/breaking-news/explosion-heard-at-a-power-plant-in-ahvaz-iran-633841

stored, and there were also reports of power outages.[20] On 15 July 2020, Iranian vessels caught fire in the Bushehr port; there were no injuries, but significant damage was caused to the ships.[21]

Based on its vague and ambiguous reactions to these latest incidents in Iran, it is clear that Israel is not responding to all attributions for carrying out cyberattacks on Iranian infrastructure or military sites. At the same time, based on its pattern of behavior and declarations by senior Israeli representatives, it is clear what the Israeli red lines are vis-à-vis Iran: on all matters related to the Iranian nuclear program, Israel is trying to create an asymmetrical equation based on its superior military and technological capabilities.

With regards to attempts to harm civilian infrastructure, Israel is operating under the "eye for an eye" law of retaliation, responding in kind to Iran's attempted attacks.[22]

The Iranian Response

The Iranian cyberattack on Israel's water and sewage infrastructure on 24 April 2020 led to an escalation in the cyber warfare between the two countries. Even though Iran never publicly claimed responsibility for the attack, American media attributed the attack to Iran, and Israel confirmed the attempt to attack its water infrastructure via cyberspace.[23] As stated above, this attack was seen by Israel as crossing a red line; Israel chose to respond in a disproportionate, broad-ranging manner, damaging Iranian civilian infrastructure and possibly its armed forces in a series of nationwide explosions, fires and power outages.

The Iranian response has largely consisted of denial of the origin, nature and extent of these attacks, providing a partial and limited narrative to the outside world. Accordingly, most of the latest attacks have been attributed to human error or technical mishaps without giving

[19] Joffre, Tzvi. "Explosion near Iran's Capital Kills Two, Damages Factory - IRNA." *JPost.com*, 8 July 2020. https://www.jpost.com/middle-east/2-killed-in-explosion-at-factory-south-of-tehran-report-634114

[20] "Report in Iran: Explosions Were Heard in Western Tehran; Power Outages in the Region." *Ha'aretz*, 16 June 2020. https://www.haaretz.co.il/news/world/middle-east/1.8984571 [Hebrew]

[21] "Seven Ships Damaged after Fire Breaks out at Iran's Bushehr Port.". *Al Jazeera*, July 15, 2020 https://www.aljazeera.com/news/2020/07/ships-damaged-fire-breaks-iran-bushehr-port-200715144227617

[22] Alon Ben-David: Explosions in Iran: Israel Also Investigating Who is Responsible," *Channel 13 News*, 21 July 2020. https://13news.co.il/item/news/politics/security/iran-fire-1097704 [Hebrew]

[23] "Report: Iran Responsible for Last Month's Cyberattack on Israel's Water Infrastructure" *Ha'aretz*, 7 May 2020. https://www.haaretz.co.il/news/politics/1.8828864 [Hebrew]

details on what happened and where. Explosions on military bases, for example, were attributed to a gas leak in a civilian area.[24]

As for the attack on the Natanz uranium enrichment facility, Iran's response was vague and contradictory: in the immediate aftermath, Iran said it was an accident, and that Israel was attempting a propaganda coup by assuming responsibility. But afterwards, the Iranian regime warned that if it discovers that foreign states were trying to cross red lines – naming the Zionist regime and the U.S. – it would reconsider its strategy and response.[25]

On the one hand, partial and vague retorts by the Iranian regime help maintain ambiguity with regards to its own cyberattacks against Israel. On the other hand, this nebulousness may paint Iran as a country not controlling its national sovereignty and not responding decisively to the threats it is facing. Accordingly, Iran is likely to continue strengthening and developing its already impressive cyber warfare capabilities, challenging Israel on this front with additional physical infrastructure attacks.

Acknowledgment

The authors would like to thank the Yuval Ne'eman Workshop for Science, Technology and Security at Tel Aviv University for supporting the research on which this paper is based.

A Hebrew version of this paper was published in *"Ha'uma"* 220, November 2020.

[24] Satellite Images: Origin of Mysterious Explosion in Tehran – Near Missile Production Facility," *Ha'aretz*, 27 June 2020. https://www.haaretz.co.il/news/world/middle-east/1.8951785 [Hebrew]

[25] "Iran Reports 'Accident' at Nuclear Site, Warns Enemies." *France 24,* 2 July, 2020. https://www.france24.com/en/20200702-iran-reports-accident-at-nuclear-site-warns-enemies