PART 4:
THE IRANIAN CYBER THREAT TO ISRAEL

Israel is Iran's primary adversary in the cyber realm, as it is in all others. Before turning to the Iranian cyber threat to Israel, it is important that we begin by placing them in the broader strategic context of the overall threat that Iran poses to Israel. For decades, the Supreme Leader Khamenei and other Iranian leaders have repeatedly called for Israel's destruction, referring to it, inter alia, as a "cancerous tumor" that must be removed.[100] In 2014 Khamenei even publicly enunciated a nine-point plan for Israel's destruction.[101]

Iranian enmity toward Israel is fundamental. Iranian enmity does not stem from any given policy, or set of policies, that Israel could change and thereby redeem itself in Iranian eyes. Iran's objection is to Israel's existence. As such, it is very different from the enmity that Iran bears toward the United States and Saudi Arabia, its two other primary adversaries, and, along with Israel, the foci of most of its cyber operations. Were the United States to "mend its ways" and make important changes to its policies toward Iran and the region, the Islamic Republic could live with it in a state of relative peace and cooperation, if not great warmth. Iran's theological, strategic, and economic differences with Saudi Arabia are historic and deeply rooted. Of late, however, they have put these differences aside and have begun at least a temporary rapprochement.

For Israel, Iranian rhetoric is anything but idle talk. To the contrary, Iran has devoted considerable efforts and resources to its anti-Israeli efforts ever since the Islamic Republic was founded. Indeed, Iran's carefully calculated

100 Amir Vahdat and Jon Gambrell, "Iran Leader Says Israel a 'Cancerous Tumor' to be Destroyed," *AP*, May 22, 2020; Tamar Pileggi, "Khamenei: Israel a 'Cancerous Tumor' that 'Must be Eradicated,'" *Times of Israel*, June 4, 2018; CNN Staff, "Iran Leader Urges Destruction of 'Cancerous' Israel," *CNN*, December 15, 2000.

101 Stuart Winer and Marissa Newman, "Iran Supreme Leader Touts 9-Point Plan to Destroy Israel," *Times of Israel,* November 10, 2014.

approach to the achievement of its objectives toward Israel, combined with its comparatively advanced society, size, resources, and distance from it, have made Iran the most sophisticated and dangerous adversary that Israel has ever faced. Certainly, no responsible Israeli official can afford to underestimate the threat.

Iran's nuclear program is the primary threat to Israel's national security today and the only potentially existential one that it faces. The likelihood of Iran ever actually using nuclear weapons against Israel is probably quite low, but the potential consequences are intolerable and Israel must, therefore, treat Iran's nuclear program with the greatest gravity. The more plausible threat, however, stems from the greatly enhanced stature and power that a nuclear capability would enable Iran and its proxies to wage an even more aggressive *sub-nuclear* confrontation against Israel. Moreover, the mere presence of nuclear weapons, even if just in the background, could risk escalating otherwise limited regional confrontations into potentially existential ones.

Furthermore, should Iran acquire nuclear weapons, additional states, such as Turkey, Saudi Arabia, Egypt, and possibly even the UAE, may seek to do so as well. A Middle East with multiple nuclear actors is a nightmare scenario with no known remedies. Unlike the nuclear rivalries between the United States and Russia, the United States and China, or India and Pakistan, Iran explicitly seeks its adversary's destruction. Whereas these nuclear powers went to great lengths to prevent or mitigate crises between them, nuclear actors in the Middle East are likely to have only limited channels of communication and crisis management. Furthermore, Iran and Saudi Arabia are theocracies and even if they are likely "rational actors," the rationality of theocracies may be different from that of other states, if only in some small but critical measure. The prospects of nuclear weapons actually being used in the Middle East, especially among multiple nuclear actors, are far greater in this region than elsewhere and are truly frightening.

In contrast to the possibility of posing a nuclear threat, Iran's conventional military capabilities are limited and unlikely to pose a major threat to Israel for some time. Iran does have a significant and growing arsenal of ballistic and cruise missiles, as well as drones, capable of striking Israel; the primary threat it poses, however, is indirect through Hezbollah, its Lebanese proxy. Iran is thought to have armed Hezbollah with a staggering arsenal of up to 150,000 rockets and mortars and over 2000 drones. In a major confrontation, Hezbollah may fire some rockets at Israel each day, for a period of weeks, causing severe damage to its civilian home front.[102]

Moreover, the rockets that Iran is now supplying to Hezbollah are increasingly precise, presenting a possible game changer from Israel's perspective. Precise rockets would provide Hezbollah with the potential to disrupt both defensive and offensive IDF operations, by targeting anti-rocket systems, mobilization centers and air bases; Israel's command-and-control processes, by targeting targets from the premier's office, down through IDF headquarters and military communications nodes; and its economy and society, by targeting critical national infrastructure and population centers. Although Israel's offensive capabilities and rocket defenses will mitigate the threat, they cannot fully neutralize an arsenal of this size. No other Arab adversary has ever had the capacity to cause disruption of this magnitude to Israel's civil and military rears.[103]

Iran is further engaged in a sustained effort to establish a permanent military presence in Syria and to turn it into a transit point for the supply of weapons to Hezbollah in Lebanon. Israel has been relatively successful so far in slowing this effort, but the buildup continues. Syria's long-term future

102 Jerusalem Post Staff, Tovah Lazaroff, "Israel is Updating Attack Plans Against Iran's Nuclear Sites – Gantz," *Jerusalem Post*, March 15, 2021; Anna Ahronheim, "Hezbollah Has Some 2,000 Unmanned Aerial Vehicles – ALMA," *Jerusalem Post*, December 22, 2021; Yonah Jeremy Bob, "IDF Intel Chief: We'll Keep Peace in North Despite Hezbollah Provocations," *Jerusalem Post*, July 11, 2023.

103 Charles D. Freilich, *Israeli National Security: A New Strategy for an Era of Change* (Oxford: Oxford Press, 2018), 154–160.

is unclear, but it is likely to remain under significant Iranian influence and to constitute at least a partial forward-operating base for Iran in its fight against Israel. The ramifications for Israel are severe and could even lead to a direct clash with Iran, over and above the indirect military confrontation already underway. Iran's presence in Syria also puts pressure on Israel's relations with Russia, the other primary player in Syria, where it has deployed its most advanced anti-aircraft system and maintains air and naval bases. Iran has also deployed missiles in Iraq and Yemen capable of reaching Israel.

In contrast with Israel's Arab adversaries in the past, Iran and Hezbollah do not seek its defeat in the near-term, which they recognize is beyond their capabilities, and have instead adopted a long-term strategy of "attrition until destruction." In so doing, they make use of a variety of weapons and tactics designed to partially neutralize Israel's technological superiority, prevent it from achieving victory, and demoralize its population. To this end, Hezbollah intentionally deploys its rockets among the civilian population, thereby leading to civilian casualties when Israel tries to destroy them, thus creating international pressure on Israel to end the fighting before it has achieved its military objectives. Hezbollah's own offensive efforts are focused overwhelmingly on Israel's civilian population, through massive and protracted rocket attacks.[104]

Iranian Cyberattacks Against Israel

The following section presents a detailed account of the primary cyberattacks that Iran has conducted against Israel. Some of the attacks were parts of broader campaigns against multiple states, others were cross-cutting (i.e., combined elements of CNA, CNE, and CNI attacks, as well as ransomware). The attacks have been categorized in accordance with their primary intent.

CNA (disruptive and destructive) attacks: In 2012 Iranian-affiliated hackers launched an attack against the computer servers of the Israel Police. External

104 Freilich, *Israeli National Security,* chapter 3.

connections to police servers had to be shuttered and each network isolated, until all intrusions could be removed from the servers. Completing this task required a large team, working 24x7 for a full week.[105]

One of the first Iranian attacks against critical national infrastructure in Israel took place in 2014, during the conflict with Hamas that year. Iranian hackers launched a large-scale attack against the civil communications system and attempted to flood Israel's DNS system.[106] A further Iranian attack against critical national infrastructure occurred sometime in 2015 or 2016. The hackers apparently believed that they had succeeded in conducting a massive attack on Israel's electric grid and possibly even a nuclear facility. In reality, the networks attacked had been decoys, known as "honey-pots," designed to deflect the attacks and expose the adversary's intentions and capabilities. Nevertheless, the attackers' willingness to launch such brazen and potentially escalatory attacks was concerning, and as will be seen, this was not the last Iranian cyberattack against nuclear-related targets in Israel.

In 2019–2020 a series of attacks, apparently by the IRGC, again targeted Israel's critical infrastructure; this time, the water supply and waste management system. Israel's cyber defenses successfully blocked the attacks until April 2020, when an attack launched via US-based servers disrupted—or gained control over—the control systems of six water and sewage treatment stations. The attack was detected rapidly and no harm was caused, but had the attackers succeeded, they would have been able to increase the quantity of chlorine and other chemicals injected into the water supply to potentially lethal levels.[107]

105 Shamah, "Official: Iran, Hamas Conduct Cyber-Attacks"; David Shamah, "How Israel Police Computers Were Hacked: The Inside Story," *Times of Israel*, October 28, 2012.

106 Yaakov Lappin, "Iran Attempted Large-Scale Cyber-Attack on Israel, Senior Security Source Says," *Jerusalem Post*, August 17, 2014; Brewster, "Persian Paranoia."

107 Ahiya Raved, "Cyber Attack Targeted Israel's Water Supply, Internal Report Claims," *Ynet*, April 26, 2020; Ynet staff, "Report: Iran Behind Hack of Israeli Water Authority Sites," *Ynet*, May 7, 2020; Amos Harel, "With Cyberattack on Iranian Port, Tehran Gets a Warning: Civilian Installations Are a Red Line," *Haaretz*, May 20, 2020; Yonah Jeremy

Israel was so concerned that a special meeting was convened of the Ministerial Committee on Defense. The head of the Israel National Cyber Directorate defined the attack as a "turning point in the history of modern cyber warfare" and emphasized that it was the first time that Israel's adversaries had used a cyberattack to cause potentially lethal effects.[108]

Just weeks later, the water system was again targeted; this time it consisted of two, more limited, attacks. One attack targeted agricultural water pumps in the Galilee, while the other targeted infrastructure in the center of Israel. Israel's defenses again proved adequate, and neither attack succeeded. The attacks did demonstrate, however, that the counter-strikes that Israel reportedly conducted in reprisal for the earlier ones, had not achieved their intended deterrent effect.[109]

The attacks against the water system were part of an ongoing series of cyber and kinetic blows and counter-blows, which Iran and Israel reportedly exchanged from 2019 to the present. The Iranian attacks came in waves, with Iran launching 19,000 cyberattacks against Israeli firms in July 2020 and another 33,600 in November.[110] In 2020 the Hackers of Saviors, an Iranian-affiliated hacktivist group that promotes the Palestinian cause, timed the attacks to coincide with Iran's annual al-Quds (Jerusalem) Day. Despite warnings issued

Bob, "Israeli Cyber Czar Warns of More Attacks From Iran," *Jerusalem Post*, May 28, 2020; Yonah Jeremy Bob, "The Coming Cyber Winter is Worse Than all Estimates," *Jerusalem Post*, December 10, 2020; Amitai Ziv, "The Iranians Read the Reports about Israel's Cyber Error, and Succeeded to Embarrass it," *The Marker*, May 31, 2020 (Hebrew); TOI Staff, "Israel Behind Cyberattack that Caused 'Total Disarray' at Iran Port – Report," *Times of Israel*, May 19, 2020; Staff, "Iranian Cyberattacks on Israeli Facilities Thwarted for a Year – Report," *Jerusalem Post*, June 7, 2020; Tal Shahaf, "Israel Unprepared for Iranian Attack on Water Supply, Officials Warn," *Ynet*, February 17, 2021; Prime Minister's Office, National Cyber Directorate, "Annual Report" (2021).

108 Bob, "Israeli Cyber Czar."

109 TOI Staff, "Cyber Attacks Again Hit Israel's Water System, Shutting Agricultural Pumps," *Times of Israel*, July 17, 2020.

110 Meir Orbach and Golan Hazani, "Israel's Supply Chain Targeted in Massive Cyberattack," *Calcalist*, December 13, 2020.

by the INCD, the hackers successfully exploited a vulnerability in the servers of a leading hosting site and defaced thousands of Israeli websites, replacing them with vicious messages, including calls for Israel's destruction. They also sought to lure targets into downloading malware that would have completely erased their computer data. The targeted websites included municipalities, a pharmaceutical company, food chains, and other private firms, NGOs, and a regional water authority.[111]

In 2020 Static Kittens launched what initially appeared to be a ransomware attack but may have actually been the prelude to a large-scale destructive one, while Agrius, yet another Iranian-affiliated hacking group, did launch a cyber espionage campaign that evolved into destructive wiper attacks.[112] In 2021 Siamese Kittens launched a supply chain attack against Israeli computer and telecommunications firms, by posing as colleagues from similar firms so that they could lure their targets into compromising their computers, possibly in preparation for a wiper or ransomware attack.[113]

2022 saw a major upswing in attacks against Israel. Iranian hackers, possibly Charming Kittens, successfully targeted a wide range of Israeli energy firms, including power plants, oil refineries, and natural gas pipelines, as well as the National Infrastructure Protection Center. The hackers were able to steal sensitive data, including intellectual property and financial information, but they failed to disrupt the firms' ongoing operations. Just weeks later, a similar attack, apparently also by Charming Kittens, was launched against El Al airlines and the Bezeq telecommunications firm. The Tel Aviv Stock

111 Ynet reporters, "Host of Israeli Sites Targeted in Massive Cyber-Attack," *Ynet*, May 21, 2020; Ran Bar-Zik, "Thousands of Websites Defaced in Cyberattack Calling for the 'Destruction of Israel,'" *Haaretz,* May 21, 2020; Government of Israel, Prime Minister's Office, National Cyber Directorate, "Annual Report" (2021).

112 Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack"; Yuval Mann, *Ynet*, November 10, 2021.

113 Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack."

Exchange was closed for a few hours after a DDoS attack flooded its servers with traffic, making them unavailable to users.[114]

In 2022 APT34 disabled the air traffic control system at Ben Gurion Airport, disrupting airport operations and even closing it for several hours. No damage was caused to the airport's physical infrastructure, but numerous fights had to be canceled and passengers were stranded in terminals. The hackers also released a malicious file that infected the airport's computers, further disrupting operations. A DDoS attack made it impossible for passengers to book flights or check in to them.[115]

In 2022 the Hackers of Saviors disrupted the operations of a logistics firm at the port of Ashdod. The attack may have been a reprisal for an even more severe attack that Israel reportedly conducted against an Iranian port the previous year, in retaliation for the attacks on Israel's national water system.[116]

In 2022 an IRGC-affiliated attack of unprecedented size and scope led the INCD to declare a state of emergency. The DDoS attack temporarily disrupted the websites of a number of government ministries, as well as the Prime Minister's Office. Another attack by MuddyWater disrupted the websites of the Ministry of Defense and the Prime Minister's Office but failed to achieve its primary goal of disrupting Israel's critical infrastructure.[117]

An attack by Charming Kittens against the electric grid in 2022 did damage a number of power plants and substations, and hundreds of thousands of

114 Tomer Ganon, *Jerusalem Post*, March 8, 2022 and April 12, 2022; David Sanger and Ronen Bergman, *New York Times*, March 8, 2022.

115 Judah Ari Gross, *Times of Israel*, May 24, 2022 and May 25, 2022; *Haaretz*, May 11, 2022.

116 Rafael Kahan, *Calcalist*, February 1, 2022; Genia Wilenski, *The Marker*, January 31, 2022; Nevo Trebelsi, *Globes*, January 31, 2022.

117 Amos Harel, *Haaretz*, March 15, 2022; Yaniv Kubovich and Oded Yaon, *Haaretz*, March 14, 2022; Yaniv Halperin, *Anashim Umachshevim*, March 14, 2022; Yaron Avraham and Nir Dvori, *N12*, March 14, 2022; Raphael Kahan, *Calcalist*, March 14, 2022; Stav Namer et al, *Maariv*, March 14, 2022; Daniel Salame, *Ynet*, March 14, 2022; Report by FireEye Mandiant, January 24, 2022.

people were left without power for hours. The water system and other critical infrastructure sites may also have been attacked.[118]

A broad cyber onslaught in early 2023, deliberately timed to coincide with both the annual Palestinian-affiliated #opIsrael campaign and Iran's al-Quds Day, targeted Israel's universities and an array of governmental and commercial targets. The available information is inconclusive, but the attacks may have been conducted by hackers affiliated with Russian intelligence, acting as a front for Iran, as part of the growing cooperation between the two countries following the war in Ukraine. The attacks temporarily disrupted the websites of most of Israel's banks and telecom companies, postal service, electric and water companies, Home Front Command's rocket warning system, the Israel Ports, Securities and Railways authorities, Prime Minister Netanyahu's Facebook page, Ministry of Health and emergency medical responders, a number of newspapers and TV stations, Check Point—Israel's leading cybersecurity firm—and even the public sites of the Mossad and the Shin Bet.[119]

Each year, the IDF faces hundreds of attempts to break through its defenses and penetrate military computer systems and networks, including operational ones.[120] The IDF Home Front Command's early warning system has been attacked on a number of occasions, including during some of the rounds of

118 Judah Ari Gross, *Times of Israel*, March 8, 2022; Ellen Nakashima and Adam Entous, *Washington Post*, March 9, 2022; David E. Sanger and Ronen Bergman, *New York Times*, March 8, 2022.

119 Raphael Kahan, *Haaretz*, April 5 and April 21, 2023; Daniel Salame and Raphael Kahan, *Haaretz*, April 14, 2023; Jerusalem Post Staff, "Israeli Cyber Security Website Briefly Taken Down in Cyberattack," *Jerusalem Post*, April 4, 2023; Jerusalem Post Staff, "United Hazalah Hit By Tens of Thousands of Cyberattacks Past Two Days," *Jerusalem Post*, April 5, 2023; Jerusalem Post Staff, "Israel Independence Day Cyberattack Takes Down Major News Websites," *Jerusalem Post*, April 26, 2023; Ofir Dor, "'Unsophisticated Iranian Cyberattack' Temporally Downs Israeli Bank Sites, Post Office," *Haaretz*, April 14, 2023; TOI Staff, "Website of Israeli Port Hacked; Sudanese Group Said to Claim Responsibility," *Times of Israel*, April 26, 2023.

120 Itam Elmadon, *N12,* January 21, 2021; Yoav Limor, *Israel Hayom*, February 7, 2019.

conflict with Hamas. Had the attackers succeeded, they would have been able to issue false alerts, or prevent the system from being used when actually needed. An attack in 2020 accessed the IDF's civilian supply chain, including gas and food vendors, whose activities and modus operandi can provide important insights into IDF operations.[121]

CNE (espionage) *attacks:* Iran's CNE attacks have focused on Israeli defense officials, defense industries, and even nuclear scientists. Iranian hackers have also repeatedly sought to gain insight into Israel's strategic thinking through espionage attacks against academics with links to the defense establishment. To this end, they have posed as the academics' colleagues and personal acquaintances and have sought to gain their unvarnished assessments, beyond that which appears in published papers. To make the attacks appear more credible, the hackers studied the targets' ongoing email exchanges and even participated in some.[122] In some cases, the attacks against Israeli targets were part of broader campaigns against multiple states around the world, but due to their significant Israeli component, they have been included here.

In the "Thamar Reservoir" attack, which began sometime between 2011–2014, Iranian hackers reportedly used spear phishing and social engineering techniques to lure former Israeli generals, employees of defense consulting firms, and academics into downloading malware attachments disguised in Word and Excel files. The malware contained "keyloggers," or computer code that enabled the hackers to record every keystroke made by the users, take screenshots, and copy files without their knowledge.[123]

In 2012 a spearfishing campaign targeted 800 business executives in the fields of critical infrastructure and financial services, as well as officials

121 Yoav Limor, *Israel Hayom*, February 7, 2020 and June 11, 2020.

122 Ayala Hasson, "Iranian Hackers Posed as General Yadlin and Gained Information from an Israeli Researcher," (Hebrew), *Channel 13*, November 20, 2020.

123 ClearSky Research Team, "Rocket Kitten 2 – Follow-Up on Iran Originated Cyber-Attacks," Clearsky.com, September 1, 2015.

and embassy staffs. Targets clicked on email attachments, or links to news articles, thereby downloading malware and giving the hackers access to their computers. Of the targets, 54 were Israeli.[124] Ever since 2013, Copy Kittens has targeted government agencies, defense and IT firms, academic institutions, and municipal authorities in Israel, as well as in the United States, Saudi Arabia, Turkey, Jordan, and Germany. Each of the attacks began with an infected email attachment, usually carefully chosen to match the target's interests.[125]

Between 2013–2017 Iranian hackers successfully penetrated the computer systems of 320 universities, mostly in the United States but also in Israel and elsewhere. Out of over 100,000 academic accounts targeted, approximately 8,000 were successfully breached and vast quantities of data and intellectual property stolen. A further attack—only uncovered in 2018—against 76 universities in the United States, Israel, and other countries once again sought access to unpublished research and intellectual property.[126]

In 2014 Rocket Kittens targeted Israeli academic institutions, defense contractors, and more, along with other targets in the Middle East. In some cases, the hackers impersonated Israeli engineers, including a particularly well-known one, in order to gain credibility with their targets and increase the likelihood that they would download the malware. Facebook and SMS messages, spear phishing emails, and a variety of other techniques were used. The attacks had easily identifiable errors and were generally unsophisticated but were notable for their persistence. In effect, the hackers simply sought to overwhelm the targets with attacks, until someone eventually erred and downloaded the malware.[127]

124 United Against Nuclear Iran (UANI), "The Iranian Cyber Threat," May 2020.

125 ClearSky Research Team, "Rocket Kitten 2 – Follow-Up on Iran Originated Cyber-Attacks," Clearsky.com, September 1, 2015.

126 U.S. Department of Justice, "Nine Iranians Charged"; Cuthbertson, "Iranian Hackers Attack UK."

127 ClearSky Research Team, "Rocket Kitten 2 – Follow-Up on Iran Originated Cyber-Attacks," Clearsky.com, September 1, 2015.

In 2017 Copy Kittens hackers impersonated the Prime Minister's Office and Israeli news sites, targeting Israeli embassies abroad and foreign embassies in Israel. The hackers made use of cyber infrastructure located largely outside of Iran—in the United States, Russia, and the Netherlands—in an attempt to cover their tracks.[128]

In 2017 Oil Rig masqueraded as a well-known Israeli software firm and sent malicious emails, with fake security certificates, to 120 Israeli government agencies, academic institutions, computer firms, and individuals. The phishing attack exploited vulnerabilities in Microsoft Word to access the targets' address lists, which were then used to further spread the attack.[129] In other attacks by Oil Rig, at least five Israeli IT vendors, several financial institutions, and the postal service were targeted; phony websites masqueraded as a registration page for a conference at the "University of Oxford" and as an employment site; and the website of IsraAir, an Israeli airline, was cloned and used to send targets a malicious Excel file.[130]

In 2018 Charming Kittens reportedly targeted Israeli nuclear scientists in the attempt to gain access to sensitive information. The scientists were sent emails, as part of an ongoing phishing scam with links leading to the fake "British News Agency."[131] According to one report, 11 different IRGC hacking groups were involved in the attacks, almost on a daily basis.[132] That same year, an Iranian-affiliated operation exfiltrated large quantities of information about Israeli and other targets in the Middle East, United States, Europe, and

128 Clearsky Research Team, "Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford," *Clearsky.com,* January 25, 2017.

129 Gwen Ackerman and Alisa Odenheimer, "Israeli Official Says First Wave of Cyber Hack Was Thwarted," *Bloomberg*, April 26, 2017; Anshel Pfeffer, "Why Netanyahu Failed to Mention the Iranian Link to the Cyberattack on Israel," *Haaretz*, April 27, 2017.

130 ClearSky Research Team, "Iranian Threat Agent OilRig."

131 TOI Staff, "Iran Hackers Reportedly Tried to Phish Israeli Nuclear Scientists," *Times of Israel*, January 30, 2018.

132 NoCamels, February 1, 2018.

Russia, as well as global aerospace and telecommunications firms. The highly targeted campaign had apparently been underway for at least three years but went undetected by using a previously undiscovered Remote Access Trojan designed to evade antivirus tools and other security measures.[133]

2019 marked a dangerous change in Iranian CNE attacks. Using Facebook and messaging apps, an Iranian-led group operating out of Syria, apparently attempted to recruit people in Israel to conduct terrorist attacks. Iran may have also been behind efforts by Hezbollah and Hamas to use the internet as a means of recruiting Israeli Arabs and Palestinians for terrorism and espionage in Israel.[134]

In 2020 Pay2Key, which is apparently affiliated with Fox Kittens, targeted Israel Aircraft Industries (IAI), one of the biggest firms in Israel and a leading defense contractor. The attack may have penetrated the anti-missile systems, drones, and precision guided munitions manufactured by the firm.[135] In 2021 an attack by Fox Kittens, which took two years and spread through the systems of a large number of Israeli firms, accessing information at various levels of secrecy, was exposed.[136] It is unclear if the attack against IAI was part of this operation.

In 2020 Iranian hackers posed as General Amos Yadlin, a former head of Military Intelligence and the head of the Institute for National Security Studies (INSS) at the time. The attack masqueraded as a text message, ostensibly from Yadlin's WhatsApp account, asking an analyst at another institute to

133 Zev Stub, "Newly-Found Iranian Cyber-Espionage May Pose 'Real Threat' to Israel," *Jerusalem Post,* October 7, 2021.

134 Yoav Zitun, "Shin Bet: Iran Tried to Enlist Israelis, Palestinians for Espionage, Terror," *Ynet*, July 24, 2019.

135 Tal Shahaf, *Ynet*, March 13, 2021; Amitai Ziv, "'Iranian Attacker Impersonating Russians': Inside Recent Attacks on Israel," *Haaretz*, May 5, 2021.

136 Dolev and Siman-Tov, "Iranian Cyber Influence Operations."

comment on a still unpublished INSS study, which the attackers had clearly obtained illicitly.[137]

In 2020–2021 Charming Kittens conducted a phishing campaign against 25 senior American and Israeli experts specializing in genetic, neurological, and oncological research; the motives for the attack are unclear.[138] In 2021 Iranian intelligence masqueraded as attractive women on Instagram, in the attempt to lure Israeli businessmen into meetings abroad, ostensibly for business and/or romantic purposes but in reality to harm or kidnap them.[139] Agrius was back with a password-spraying campaign against the Office 360 accounts of Israeli and American manufacturers of satellites, drones, radar, and more. Twenty firms were successfully compromised. An attack on the databases of the postal service and various private firms in 2022 yielded the personal details of hundreds of thousands of people.[140]

Charming Kittens was behind a series of attacks on Israeli companies in 2022—including defense contractors, technology firms, and financial institutions—designed to steal sensitive data, including intellectual property and financial information.[141] In 2022 Refined Kittens (APT33) tried to breach the computer systems of several Israeli government agencies, including the Ministries of Defense and Foreign Affairs and the National Cyber Directorate, in the attempt to gain sensitive information regarding Israel's military capabilities. The hackers used a variety of methods, including phishing emails, malicious websites, and watering hole attacks. Some damage was caused to a small

137 Hasson, "Iranian Hackers Posed as General Yadlin."

138 Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack."

139 Yaniv Kubovich, "Iran Used Instagram to Try and Lure Israelis to Meetings Abroad, Shin Bet and Mossad Say," *Haaretz,* April 12, 2021.

140 Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack"; Yuval Mann, *Ynet,* November 10, 2021.

141 David E. Sanger, *New York Times*, January 24, 2022; Dan Lamothe and Felicia Sonmez, *Washington Post*, January 25, 2022.

number of Ministry of Defense servers, and the hackers were able to gain access to some of the targeted systems. Just weeks later, Refined Kittens conducted another attack against the Ministry of Defense, disrupting some websites.[142]

In 2022 Helix Kittens (a.k.a. APT34, OilRig) used spear phishing emails, social engineering, and other techniques to target Israeli financial institutions, including Bank Hapoalim and Bank Leumi. The attack successfully accessed the targeted systems and stole sensitive data, including customer information and financial records, but did not cause major financial losses. In 2022 APT36 successfully attacked the Ministry of Finance, accessing sensitive information regarding Israel's financial system.[143]

In 2023 Charming Kittens penetrated some 32 Israeli firms in the fields of insurance, medicine, communications, information technology, financial services, and more.[144] The attacks' objective is not known, but they were presumably designed to extract sensitive information and possibly also to cause Israel embarrassment.

That same year, IRGC-affiliated hacking groups, including LionTail, waged one of the more sophisticated espionage campaigns against Israel (along with Saudi Arabia and Jordan), exfiltrating large amounts of data. One of the attacks penetrated privately owned Israeli cameras along the sensitive border with Lebanon.[145]

142 Reuters, February 15, 2022; Eli Lake and Naama Stern, *Reuters*, February 25, 2022; Judah Ari Gross, *Times of Israel*, February 24, 2022; FireEye Mandiant Report, February 2022 Cyberattack on Israeli Government Websites.

143 FireEye Mandiant report, February 14, 2022; Microsoft Threat Intelligence Center, January 24, 2022; Judah Ari Gross, *Times of Israel*, April 25 and April 27, 2022.

144 Raphael Kahan, "Iranian Hackers Break Into Networks of More than 30 Companies in Israel," *Ynet*, November 9, 2023, https://www.ynetnews.com/business/article/rjrs5pn02.

145 Ronen Bergman, Aaron Krolik, and Paul Mozur, "In Cyberattacks, Iran Shows Signs of Improved Hacking Capabilities," *New York Times*, October 31, 2023.

CNI attacks: Information operations have been a primary component of Iran's overall cyber operations against Israel to date. As with its information operations against the United States and other countries, Iran's CNI operations against Israel have been designed to further stoke domestic divisions, counter Israel's positions on issues of importance, and strengthen Iran's overall deterrent posture.[146] They have also played a part in Iran's overall efforts to isolate Israel and undermine its fundamental legitimacy as a state.

The Tel Aviv Times, a fake Iranian Hebrew-language website, has tens of thousands of monthly views in Israel. In operation since 2013, the site plagiarizes articles from Israeli news media but with critical changes designed to support Iran's agenda.[147] In 2014 Iranian-affiliated hackers temporarily gained control of the IDF blog and Twitter feed and warned that the Dimona nuclear reactor had been struck by rockets and was about to explode. The IDF quickly restored control over the system relatively quickly, but in the interim many citizens feared the worst.[148]

In 2016 an even more dangerous information operation took place. An Iranian-affiliated website falsely quoted Defense Minister Moshe Yaalon as having stated that if Pakistan sent troops to Syria to fight ISIS, Israel "would destroy them with a nuclear attack." The Pakistani Defense Minister responded with a public warning that "Israel forgets (that) Pakistan is a nuclear state, too." The Israeli Defense Ministry, deeply concerned about a possible escalation with a hostile nuclear power, rapidly clarified that the story was a fabrication.[149]

146 Tabatabai, *Iran's Authoritarian Playbook*, 15–19.

147 TOI Staff, *Times of Israel*, September 6 and November 30, 2018; Stubbs and Bing, "Exclusive: Iran-Based Political Influence Operation."

148 Jerusalem Post Staff, *Jerusalem Post,* July 4, 2014; Siboni and Kronenfeld, "Iran and Cyberspace Warfare"; Kayla Ruble, "Syrian Hackers Hijack IDF Twitter Sparking Fears of Nuclear Leak," *Vice*, July 17, 2014; Mohammad J. Herzallah, "Israeli Fights Wire with Wire," *Newsweek*, July 27, 2009; TOI Staff, "Iran Hackers Reportedly Tried to Phish Israeli Nuclear Scientists."

149 TOI Staff, "Cyber Firm Says Three Iran-Run Sites are Targeting Israelis With Fake News," *Times of Israel,* September 6, 2018; TOI Staff, "Iran Duped Pakistan into Israel Nuke Threat

In 2019 at least 350 fake accounts on Facebook, Twitter, and Telegram were traceable to Countdown 2040, an Iranian website that claims Israel will cease to exist by that year. Masquerading as legitimate news websites, the fake ones disseminated fictitious information to as many as half a million people in Israel each month. Countdown 2040 often rephrases genuine news articles in a manner designed to promote divisive discourse in Israel, on such controversial issues as criticism of Prime Minister Netanyahu, wealth inequality, sexual harassment, poverty, and the judicial system. The campaign was originally designed to inflame tensions in Israel over the Israeli–Palestinian conflict, but in a demonstration of considerable operational agility, following the announcement of early elections, the attackers rapidly shifted gears to an attempt to influence the electoral outcome.[150]

In 2019, in a further attempt to sow discord in Israel, the website of Harvard's Belfer Center carried a report ostensibly based on a talk that the former head of the Mossad, Tamir Pardo, had actually given there. The report quoted him as having said that Russian-born Defense Minister Avigdor Lieberman had been dismissed after having been exposed as a Russian mole. In reality, the Center's website had been cloned, Lieberman had been dismissed for entirely different reasons, and the article was a complete fabrication.[151]

Since 2020, if not earlier, Emennet Pasargad, the same Iranian hacktivist group that attacked the American presidential elections that same year, has repeatedly conducted information operations against Israel. Between 2020–2022 it masqueraded as the Hackers of Savior Pro, a Palestinian hacktivist group, and conducted four cyber campaigns against multiple sectors in Israel, mostly around the annual al-Quds Day. It has also posed as cyber criminals

as Tiny Part of Huge Fakery Campaign," *Times of Israel*, November 30, 2018.

150 Roi Rubenstein, "Report: Iranian Bot Army Trying to Influence Israeli Elections," *Ynet*, January 31, 2019; Ron Shamir and Eli Bahar, "Defending Israel Elections from Cyber Attack – What Should Be Done?" *Israel Democracy Institute*, January 2019, 12 (Hebrew).

151 Scott Shane and Ronen Bergman, "New Report Shows How a Pro-Iran Group Spread Fake News Online," *New York Times*, May 14, 2019.

to conduct a lock-and-leak operation against an Israeli call center. To further amplify the impact of its attacks, Emennet Pasargad makes extensive use of its own websites, Telegram, and fake personas on social media, as well as online hacking and illicit trading forums. In so doing, it seeks to undermine confidence in the targets' networks, cause them reputational damage and financial loss, demonstrate the weakness of Israel's cyber defenses, and promote anti-Israeli messaging.[152]

In 2020 Iranian hackers sought to exacerbate tensions between the Netanyahu government and the public over the government's handling of the COVID-19 crisis. The hackers created official-looking Facebook and Instagram accounts, which were followed by 1,100 and 9,500 Israelis respectively; however, little effort was devoted to making the accounts look authentic.[153]

When the coronavirus crisis diminished, Iranian hackers turned their attention in 2020–2021 to an information campaign designed to further aggravate the political crisis underway in Israel at the time. The identities of American Jewish philanthropists were hacked to collect information about the opposition to Prime Minister Netanyahu. This information was then used on phony Facebook, Twitter, Instagram, and Telegram accounts to disseminate inflammatory and even violent messages designed to taint the opposition. After Netanyahu was forced out of office, a Telegram account urged that he be imprisoned, with a photoshopped image of him behind bars. The similarity between the techniques used by both these hackers and Russian hackers during the attack on the American elections suggests possible collaboration.[154]

152 Anna Ribeiro, "FBI Reveals Iranian Cyber Group Emennet Pasargad Executing Hack-and-Leak Operations Using False-Flag Personas," *Industrial Cyber*, October 21, 2022; Dennis Fisher, "FBI Warns of Attacks From Iranian Threat Group Emennet Pasargad," *Decipher*, October 21, 2022.

153 Facebook, *Threat Report The State of Influence Operations 2017–2020*, May 2021.

154 Sheera Frenkel, "Iranian Disinformation Effort Went Small to Stay Under Big Tech's Radar," *New York Times*, June 30, 2021; Omer Benjakob, "Iranian Accounts, Russian Tactics and Q: Israel Has Become a Disinformation Battlefield," *Haaretz*, April 21, 2021.

Other hackers posed as members of Israel's opposition movement, setting up a false website and seeking to disrupt WhatsApp groups. Facebook removed three accounts of allegedly opposition activists who had posted inflammatory content, including comparisons between Israel's right and Hitler. Another attack on Facebook had 1,800 followers, mostly Israeli citizens who had been made followers by the hackers themselves. In 2021 an Instagram account used bots to tag tens of thousands of Israeli citizens with opposition messages. In 2021 10 Facebook and Twitter accounts, active in more than 90 mostly right-wing groups, posted content critical of the Bennet-Lapid government then in office and called for anti-government demonstrations. In some cases, the hackers sought to make direct contact with political activists close to the prime minister; in others they masqueraded as real political activists.[155]

Iranian hackers sought to interfere in the 2022 elections in Israel. Prior to the elections, some 40 fake Twitter accounts called for a split among the right-wing parties, presumably to weaken them. During the campaign, thousands of Tweets, by profiles ostensibly belonging to left-wing Israelis, called for an electoral boycott. The profiles also posted hate messages against the right wing and Haredim (ultra-Orthodox). Similar messaging took place on election day itself, in an attempt to try and suppress voter turnout.[156] In this case, the hackers' objective may have been to weaken the center-left, leading to a right-wing victory that would harm Israel's international standing and weaken its strategic posture, as, indeed, occurred. The attempts to affect the elections do not appear to have succeeded.[157]

In 2022 another Iranian information campaign again sought to stoke internal divisions in Israel. Hackers on Facebook, Telegram, and other social

155 Frenkel, "Iranian Disinformation Effort"; FakeReporter, "Rolling in the Deep: An Iranian Cross-Platform Influence Operation Summary."

156 Omer Benjakob, "Israel Election: Twitter Purges Foreign Influence Op to Suppress Voting," *Haaretz*, November 1, 2022; FakeReporter, "Rolling in the Deep."

157 Amos Harel, *Haaretz*, June 11, 2023.

media platforms posed as an ultra-Orthodox nationalist group, seeking to encourage anti-government protests by the far right; promote anti-police sentiment among the ultra-Orthodox community; and spread the belief that the inclusion of an Islamist party in the governing coalition meant that Israel was being taken over by Muslims. The attackers went to considerable lengths to make the phony website look genuine, creating a page for a fictitious bakery in an ultra-Orthodox town, using the identity of a real ultra-orthodox man who had died a few years earlier, and more.[158]

In 2022 the Iranian hacker group Moses Staff posted personal pictures and tax documents on the internet, taken from the cell phone belonging to the head of the Mossad's wife, along with some of his medical records. The attack was presumably designed to cause him embarrassment, as he was the senior official charged with Israel's efforts to contain Iran, and to further magnify the attack's public impact. The same hacker group also posted bloody pictures of a terrorist attack in Jerusalem, which it had hacked from unencrypted security cameras, to amplify the attack's impact.[159]

Between June 2022 and May 2023, 24 Iranian-affiliated influence operations took place, compared to just 7 in 2021, mostly by Emennet Pasargad. The operations focused primarily on Israel, as well as Iran's Gulf adversaries and the US. Most of the operations were designed to bolster Palestinian resistance, sow fear among Israelis, and counter normalization of Arab-Israeli ties.[160] The Hunters and No Voice groups used social media, including WhatsApp, Facebook,

158 Tom Bateman, "Iran Accused of Sowing Israel Discontent With Fake Jewish Facebook Group," *BBC*, February 3, 2022.

159 Haim Golditch, *Ynet*, December 24, 2022; Yaniv Kubovich, "Iranian Hackers Post Footage of Jerusalem Bombing, Taken by Large Security Agency," *Haaretz*, November 24, 2022; Michael Horovitz, "Report: Iran Hacked Israeli Cameras a Year Ago; Defense Officials Knew, Didn't Act," *Times of Israel*, December 19, 2022; Itamar Eichner and Yuval Mann, *Ynet*, April 4, 2022.

160 Clint Watts, "Rinse and Repeat: Iran Accelerates its Cyber Influence Operations Worldwide," *Microsoft.com,* May 2, 2023.

Twitter, Instagram and Telegram, to try to exacerbate the domestic political divide in Israel over the controversial "judicial overhaul" underway at the time. One attack called on the opponents of the proposed reforms to attack both police officers and demonstrators. It also disseminated photographs of police violence, along with the police officers' names, addresses and more, as part of a shaming campaign. In another attack, the hackers used WhatsApp groups of Likud activists to stoke confrontations and encourage violence against anti-judicial reform protesters. Other attacks, to the contrary, sought to promote opposition to pro-government demonstrators.[161]

Combined attacks: Most of the destructive CNA attacks that Iran had conducted up to that time were directed at countries other than Israel, with few exceptions, primarily the failed attack against Israel's water system in 2020. The attacks against Israel were primarily intended for purposes of disruption or espionage, with some information operations. Mid-2020, however, marked a turning point, as most of the attacks shifted to mixed ones, combining disruption, espionage, information operations, and ransomware.

Since mid-2022, in particular, Iran has leveraged cyber information operations to amplify its offensive cyber capabilities and to try to undermine Israel's sense of security. Fundamentally, it has sought to use information operations to foster political and strategic change in accordance with regime objectives.[162] Attacks masquerading as ransomware were employed primarily for purposes of information operations.

In 2020 Sapiens, an Israeli software firm, was forced to pay $250,000 following a Bitcoin ransomware attack, in which Iranian-affiliated hackers threatened to

161 David Siman-Tov, "Attempted Foreign Influence as a Challenge to Israel's National Resilience: Using the Judicial Overhaul Protests to Deepen Internal Rifts," *INSS Insight* No. 1741, June 26, 2023; Bar Peleg, Josh Breiner, and Omer Benjakob, "Iran, Russia or Both, A Foreign Influence Operation to Incite Violence in Israel is Reemerging," *Haaretz,* July 3, 2023.

162 Microsoft Threat Intelligence, "Iran Turning to Cyber-Enabled Influence Operations For Greater Effect," May 2, 2023; Dolev and Siman-Tov, "Iranian Cyber Influence Operations."

shut down its entire system. Tower Semiconductors paid a ransom of several million dollars, rather than lose a single day of manufacturing time. The attack may have been part of a broader campaign against prominent Israeli firms by Static Kittens that was designed to look like ransomware, but which was actually similar to the highly destructive Shamoon attack against Saudi Aramco. The attack damaged Tower Semiconductor's operating systems, the "holy grail" of cyberattacks, not just its information systems.[163]

That same year, Black Shadow (a possible alias for Agrius, or APT36) conducted a ransomware attack against Shirbit, an insurance firm that caters largely to government employees, including those from sensitive defense agencies, such as the Shin Bet. In this case, the hackers intentionally presented unrealistic deadlines for payment of the ransom and then posted the stolen data on the internet when Shirbit refused to do so. The data posted included the names of those insured; the agencies they worked for; confidential hospital records; contents of WhatsApp conversations; home and email addresses; ID, phone, license plate, and credit-card numbers, and more.[164]

Hacker group Pay2Key used the remote connection systems of employees at seven Israeli firms to conduct a sophisticated ransomware attack. Four of the firms paid the ransom.[165] Pay2Key then targeted Amital, which provides specialized software to 70 percent of the logistics firms in Israel. After penetrating

163 Meir Orbach, *Calcalist*, June 14, 2020 and September 7, 2020; Omer Benjakob, "'Operation Quicksand': Iran-Linked Hackers Target Israel in 'New Cyberwar Phase,'" *Haaretz*, October 19, 2020; Amitai Ziv, "Cash-Strapped Over Coronavirus, Crime Organizations Unload Cyberattacks," *Haaretz*, September 21, 2020.

164 Bernard Brode, "The Shirbit Data Hack Was an Attack on National Security. Now What?" *Times of Israel*, December 18, 2020. According to one source, the attack against was conducted by Hezbollah. See Tal Shahaf, *Ynet*, October 29, 2021.

165 Omer Benjakob, "'It's Not About Money': Destructive Cyberattack Proves Israel Lacks One Key Thing," *Haaretz,* December 9, 2020; Hagay HaCohen, "Check Point Unveils New Iranian Cybercrime, Ransoming Companies' Data," *Jerusalem Post*, November 12, 2020; Meir Orbach, "Israeli Cybersecurity Giant Tracks Ranson Payments From New Cyber Attack to Iranian Nationals," *The Algemeiner*, November 12, 2020.

Amital's computer system, Pay2Key spread to the systems of at least 40 of its clients and infected them with ransomware, thereby placing a significant part of Israel's entire air and maritime cargo traffic at risk. Some of the firms targeted were providers of logistics services to the defense establishment, with potentially sensitive information on weapons imports and exports. At least three were providers of the highly complex logistics services required to distribute the coronavirus vaccine.[166]

In still another attack, Pay2Key stole proprietary information about new semiconductors then under development by Havana Labs, an Israeli subsidiary of Intel, which was critical to Intel's future business plans.[167] Once Pay2Key's CNE attack against Israel Aircraft Industries was exposed in 2021, it switched to a hack and leak attack, releasing the details of approximately 1,000 users. By this point, Pay2Key had attacked over 80 Israeli firms, many for the purpose of ransomware-based information operations. Twitter and Telegram were used to dump stolen information, as was a specially designed website, while a myriad of threats against Israel were posted on social media.[168]

In 2021 Black Shadow launched a ransomware attack against KLS Capital, a car leasing firm. As with the attack against Shirbit, one of the primary motives may have been to demonstrate the weakness of Israel's defenses and to cause it reputational damage. The hackers succeeded in erasing much of the firm's servers and then dumped personal data on the internet on a scale

166 Tal Shahaf, *Ynet*, December 13, 2020 and December 15, 2020; Raphael Kahan, *Calcalist*, December 13, 2020; Orbach and Hazani, "Israel's Supply Chain Targeted in Massive Cyberattack."

167 Tal Shahaf, *Ynet*, December 13, 2020, December 15, 2020, and December 17, 2020; Raphael Kahan, Calcalist, December 13, 2020; Amitai Ziv, "Iran Suspected After Massive Cyberattack on Israeli Firms Revealed," *Haaretz*, December 13, 2020; Amitai Ziv, *Haaretz*, December 31, 2020; Tal Schneider, *Ynet*, December 20, 2020.

168 Tal Schneider, *Ynet*, December 20, 2020; Yonah Jeremy Bob, "Suspected Iranian Cyberattack Targets Israel Aerospace Industries," *Jerusalem Post*, December 20, 2020; Omer Benjakob, "Iranian Hackers Hit Top Israeli Defense Contractor, Data Leaked as Cyberattack Continues," *Haaretz*, December 20, 2020; Dolev and Siman-Tov, "Iranian Cyber Influence Operations."

that dwarfed the Shirbit attack, even while the ransom negotiations were still under way. Black Shadow then hacked the website of Israel's leading LGBTQ organization. After initially demanding a ransom, the hackers posted the names of the organization's entire membership, along with explicit pictures, sexual orientations, chats, and health history, including exposure to HIV. Another attack leaked the personal data of 1.5 million patients of a private health network.[169] Networm, likely just a new name for Pay2Key, conducted ransomware attacks against Veritas, another Israeli logistics firm, as well as the Israeli franchise of the H&M clothing chain. Once again, the primary motivation appears to have been to cause embarrassment and reputational damage, as well as to deter Israel.[170]

In 2021, in a significant security breach, Moses Staff succeeded in hacking and dumping the personal details of an entire IDF combat brigade on the internet, including each of the soldiers' names, addresses, phone numbers, training, role, mental health and socioeconomic status. Footage posted on Telegram showed the surroundings of Israel's top secret defense contractor, Rafael.[171]

In 2022 Black Shadow sent spear phishing emails to employees at some of Israel's largest medical centers, demanding a ransom of $10 million in Bitcoin and threatening to release patients' medical records, financial data, and other sensitive information, if its demands were not met. The emails were disguised as legitimate ones from trusted sources but contained malicious attachments.

169 Adir Yanko, Tal Shahaf, and Hadar Gil-Ad, *Ynet*, November 1, 2021; Farnaz Fassihi and Ronen Bergman, "Israel and Iran Broaden Cyberwar to Attack Civilian Targets," *New York Times*, November 27, 2021.

170 Tal Shahaf, *Ynet*, March 13, 2021; Ziv, "Iranian Attacker Impersonating Russians."

171 Tal Shahaf and Nina Fuchs, *Ynet*, October 26, 2021; Tal Shahaf, *Ynet,* October 26, 2021; Michael Horovitz, *Times of Israel*, December 19, 2022.

The hackers also tried to exploit vulnerabilities in the hospitals' computer systems to disrupt their operations, including medical supply systems.[172]

In 2023 Static Kittens launched what initially seemed to be a ransomware attack against the Technion, Israel's equivalent of MIT, encrypting servers and disrupting critical systems. The malware was specifically tailored to the Technion's systems, likely only possible after having first mapped out its entire network. The Technion was forced to disconnect its computers from the internet, limit computer use by faculty and students, and postpone some examinations. The harsh anti-Israel and pro-Palestinian rhetoric the hackers used on Telegram suggests that their primary motivation may have been political, not financial.[173]

Hezbollahs Cyberattacks Against Israel

In the early 1980s Iran established Hezbollah as a proxy organization in Lebanon, with the dual objective of strengthening the Shiite community there and of creating a forward base of operations against Israel. Ever since, Iran has provided Hezbollah with a mammoth rocket arsenal, advanced anti-aircraft, drone and electronic warfare capabilities, and more.[174]

The IRGC, according to one source, has provided Hezbollah with massive technical, material and financial support for its cyber capabilities. Another source believes that Iran has turned Hezbollah into the most sophisticated and influential terrorist organization in the cyber realm today, as a means of gaining deniability, deflecting attention from itself, and strengthening

172 Judah Ari Gross, *Times of Israel*, April 25, 2022 and April 27, 2022; Tomer Ganon, *Jerusalem Post*, April 12 and April 26, 2022.

173 TOI Staff, "Israel Publicly Blames Iran for Cyberattack on Major University Last Month," *Times of Israel*, March 7, 2023; Roei Hahn and Yuval Mann, "Leading Israeli Research Institute Falls Prey to Cyberattack," *Ynet*, December 2, 2023; Israel National Cyber Directorate, "Iranian Government Sponsored Threat Actor Muddy Water Conducts Cyber Attack Against Israel," March 9, 2023.

174 Yonah Jeremy Bob, "Iran Hackers Closer to Penetrating Israel US Drones Cyberdefense CEO," *Jerusalem Post*, November 21, 2022.

Iran's hold on Lebanon.[175] Despite these assessments, the publicly available information on Hezbollah's cyber capabilities is limited and thus difficult to make an informed judgment. Whether this paucity of information reflects the limits of Hezbollah's cyber capabilities, or the efficacy of its operational secrecy, is unknown. It is reasonable to presume that the latter is at least partly the case.

CNA attacks: A sophisticated multi-year Hezbollah attack against the IDF was uncovered in 2015. The attack sought to circumvent the IDF computers' built-in protections, by targeting the firms that supply it with software.[176]

CNE attacks: In 2010, in what may have served as a model for a number of later attacks by Hamas, Hezbollah hackers created a phony Facebook profile of an attractive young woman, who sent "friendship" requests to IDF soldiers. Approximately 200 responded, along with information about the names of other personnel and, in some cases, detailed descriptions of bases and even codes. It took almost a year before the attack was discovered.[177]

In 2012 the Hezbollah Cyber Army launched Volatile Cedar, an espionage campaign that used custom-built malware to target military suppliers, telecommunications firms, media outlets, and universities in Israel, the United States, United Kingdom, a number of Middle Eastern states, and more. In 2015 Hezbollah hackers participated in the above-mentioned "Thamar Reservoir" attack, which employed social engineering techniques against a variety of Israeli targets, including retired generals and defense consulting firms.[178]

175 Pahlavi, "Digital Hezbollah"; Benjamin R. Young, "How Iran Built Hezbollah into a Top Cyber Power," *National Interest*, April 11, 2022.

176 Oded Yaron, "Has Hezbollah's Cyber Spy Ring Been Exposed?" *Haaretz*, April 8, 2015.

177 Rid, *Cyber War Will Not Take Place*, 103.

178 Jeff Moskowitz, "Cyberattack Tied to Hezbollah Ups The Ante for Israel's Digital Defenses," *Christian Science Monitor*, June 1, 2015; Pahlavi, "Digital Hezbollah"; Lucas Ropek, "Hezbollah-Linked Cyber Unit Has Been Hacking Into Internet Companies for Years," *Gizmodo*, January 29, 2021; TOI Staff, "Iran Spying on Israel, Saudi Arabia with Major Cyberattacks," *Times of Israel*, June 14, 2015.

In 2016 Hezbollah hacked closed-circuit security camera systems in government buildings in Haifa and Tel Aviv, including the IDF's General Staff Headquarters and the Ministry of Defense, and released the images on social media platforms. Although not a particularly sensitive breach, it provided Hezbollah with a propaganda coup and did enable it to monitor those entering the buildings.[179]

A more serious campaign that same year employed social media to recruit Israeli Arabs and West Bank Palestinians for intelligence and terrorist purposes. One of those reportedly involved was the son of Hezbollah leader, Hassan Nasrallah. In one attack, an online recruit was enlisted to kidnap Israelis and transfer the hostages to Lebanon; in another, to conduct a suicide bombing. The attacks, which were thwarted by Israel, typically began with contact on Facebook and then switched to encrypted communications platforms.[180]

In 2021 Hezbollah's Cedars of Lebanon used vulnerabilities in Oracle and Atlassian servers to attack approximately 250 telecommunications, web hosting, and infrastructure firms in Israel, the United States, United Kingdom, Egypt, Jordan, Saudi Arabia, the UAE, Palestinian Authority, and elsewhere. Once the attacks penetrated the targeted systems, most proceeded manually, but some provided the attackers with remote control. The code used was similar to that employed by various Iranian hacker groups, indicating close cooperation. The Cedars of Lebanon were first discovered in 2015 but were able to continue operating under the radar by taking measures designed to avoid leaving a unique footprint.[181]

179 Ryan De Souza, "Israeli Security Camera Systems Targeted by Pro-Hezbollah Hackers," *Hackread*, February 21, 2016; Sagi Cohen, *Ynet*, June 15, 2015.

180 Michael Shkolnik and Alexander Corbeil, "Hezbollah's 'Virtual Entrepreneurs': How Hezbollah is Using the Internet to Incite Violence in Israel," *CTC Sentinel* 12, no. 9 October 2019.

181 Amichai Stein, *Kan Hadashot*, January 28, 2021; Tal Shahaf, *Ynet*, January 28, 2021; Raphael Kahan, *Calcalist*, January 28, 2021; Yossi Hatoni, "Hezbollah Cyberattacked Hundreds of Companies, Also in Israel," *People and Computers*, January 28, 2021(Hebrew).

In 2022 a joint Iranian and Hezbollah cyberattack reportedly targeted UNIFIL, the UN peacekeeping force stationed in Lebanon. The attack was designed to steal materials regarding UNIFIL's activities and deployment.[182]

CNI attacks: The Hezbollah Cyber Army reportedly conducts training camps in Lebanon, designed to create "electronic armies" around the region. Thousands of Iranian-affiliated social media activists from Iraq, Saudi Arabia, Bahrain, Syria, and elsewhere have undergone intensive training on propaganda and disinformation campaigns, including digital manipulation of photographs, management of fake social media accounts, video production, and means of circumventing the censorship techniques employed by social media firms.[183]

As with Iran, information operations have long been a critical part of Hezbollah's multi-decade strategy of asymmetric warfare. To this end, Hezbollah has used social media such as Facebook, Twitter, YouTube, Telegram, WhatsApp, and Signal to reach a Muslim and international audience on a previously unprecedented scale and to brand itself as the leader of the anti-Israel "Resistance Front." It has further used these media to amplify information campaigns designed to adversely affect Israel's international standing and to promote international pressure on it to cease military operations before it is able to achieve its objectives.[184] Hezbollah's leader, Hassan Nasrallah, reportedly believes that cyber information campaigns are even more effective for Hezbollah's purposes than military operations.

182 Amos Harel, Yaniv Kubovich, and Reuters, "Israel Accuses Iran, Hezbollah of Hacking UN Force in Lebanon," *Haaretz,* June 29, 2022; Emanuel Fabian, "Gantz Says Iran and Hezbollah Tried to Hack UN Peace Force, Steal Deployment Data," *Times of Israel*, June 29, 2022.

183 Wil Crisp and Suadad al-Salhy, "Exclusive: Inside Hizbollah's Fake News Training Camps Sowing Instability Across the Middle East," *The Telegraph*, August 2, 2020; Pahlavi, "Digital Hezbollah."

184 Anshel Pfeffer, "Israel Suffered Massive Cyber Attack During Gaza Offensive," *Haaretz*, June 15, 2009, Oded Yaron, "Palestinians Behind Cyber Attacks on Israeli Army and Government Targets," *Haaretz*, February 16, 2015; Paul J. Springer, *Encyclopedia of Cyberwarfare* (ABC-Clio, 2017), 220–221.

Hezbollah has long blended asymmetric warfare and information campaigns. Its TV station, al-Manar, has a Twitter feed followed by half a million people. It also runs more than 20 websites in seven languages (Arabic, Azeri, English, French, Hebrew, Persian, and Spanish), as well as the above-noted social media network. Social media platforms are also used as a means of recruiting fighters and hackers from around the Arab and international worlds.[185] Hezbollah has reportedly joined Iranian information campaigns designed to sow discord in Western countries. It is also suspected of conducting information operations targeting populations of Lebanese descent in several West African countries.[186]

Palestinian Islamic Jihad (PIJ)'s Cyberattacks Against Israel

An Iranian proxy based in Gaza, PIJ successfully hacked the (unencrypted) communications of IDF drones operating over Gaza for two full years, between 2012–2014. The attack enabled it to monitor the intelligence gathered by the drones in real-time and facilitated both its efforts and those of Hamas in hiding their rockets. Live feeds from Israeli road cameras were also hacked in order to ascertain where rockets had fallen and to monitor the movement of IDF forces, thereby improving PIJ's rocket targeting. Another attack tracked aircraft landings and departures at Ben Gurion Airport, to better target rocket attacks during times of conflict and to disrupt Israel's civil aviation. In contrast, PIJ's attempts to intercept phone conversations on Israeli telecommunications were reportedly unsuccessful. PIJ cyber operatives have been trained in Gaza by Iran and, in some cases, in Iran itself.[187] Beyond this, little is known about PIJ's cyber activities.

185 Ron Ben-Yishai, *Ynet*, July 24, 2021; Pahlavi, "Digital Hezbollah."
186 Pahlavi, "Digital Hezbollah."
187 Gili Cohen, *Haaretz*, March 23, 2016; Yonah Jeremy Bob, *Jerusalem Post*, March 23, 2016.

The War in Gaza 2023

Fifteen hacking groups affiliated with Iran, Hezbollah, and Hamas were active in the first weeks of the war with Hamas that began in October 2023, all of which cooperated with each other to some degree. The Iranian hackers do not appear to have had preplanned cyber attacks aligned with Hamas's surprise attack; rather, it appears they operated largely reactively, exploiting opportunities as they arose. The war began primarily with CNE attacks and rapidly pivoted to CNA and CNI operations.[188] As of the end of the third month of the war, these attacks do not appear to have had a significant impact.

CNA: Vast numbers of relatively simple DDoS attacks were launched, designed to disrupt Israeli websites, especially those belonging to media and software firms, as well as banks, financial institutions, and government sites. During the first six days of the war, DDoS attacks reached one million attempted logons per second, before decreasing to under 100,000 in the following two weeks (an average website is able to process up to 10,000 at a time). Short-lived attempts were also made to disrupt Israel's rocket alert systems.[189]

At the onset of the war, the website of the *Jerusalem Post* was knocked off line for 2–3 days, presumably as part of an effort to prevent Israel from presenting its side of the conflict abroad.[190] Of somewhat greater consequence, the Iranian-affiliated hacking group Agrius, with the involvement of Hezbollah's Lebanese Cedar, sought to disrupt operations at the Ziv Hospital. The attack was

188 Israel National Cyber Directorate, "The Cyber Dimension of the 'Iron Swords' War: Insights and Means of Coping," December 24, 2023, https://www.gov.il/he/departments/news/published24122 (Hebrew); "Reactive and Opportunistic: Iran's Role in the Israel–Hamas War," *Microsoft.com*, November 9, 2023, https://www.microsoft.com/en-us/security/blog/2023/11/09/microsoft-shares-threat-intelligence-at-cyberwarcon-2023.

189 Raphael Kahan, "Hamas Hackers Are Trying to Scare Israelis with Fake SMS Messages and News Sites," *Ynet*, October 25, 2023, https://www.ynetnews.com/business/article/hjoy4f8mp.

190 Kahan, "Hamas Hackers."

thwarted before it succeeded in disrupting hospital operations, but sensitive patient information was stolen.[191] A separate phishing attack, impersonating emails from a cybersecurity firm, urged recipients to make urgent security updates to their software. To make the emails appear genuine, they included real information about the equipment used by the target organization. Once downloaded, the attached malware collected information from the targeted system and then used wiper software to erase the organization's entire information system. The attack was preceded by a careful study of the appropriate technical people to approach in each organization, in order to maximize the damage.[192]

CNI: In order to undermine Israel's standing and cast blame on the United States for Israel's alleged war crimes, Iran promoted highly charged, slanted, and at times even false information on social media, reaching a vast global audience in support of Hamas. Iranian accounts on Facebook and Twitter glorified Hamas atrocities against Israeli civilians and encouraged further attacks against them.[193]

Prewar incitement and disinformation campaigns targeting opponents of the "judicial overhaul" continued unabated during the early weeks of the war. Accounts on Facebook, Twitter, Instagram, Telegram, and WhatsApp were also used to stoke and exacerbate societal tensions surrounding sensitive

191 Israel National Cyber Directorate, "Iran and Hezbollah Stand Behind the Cyberattack against the Ziv Hospital during the Iron Swords War," December 18, 2023, https://www.gov.il/he/departments/news/ziv181223 (Hebrew).

192 Israel National Cyber Directorate, "A New Fishing Attack from Iran Tries to Erase Information in Organizations," December 26, 2023, https://www.gov.il/he/departments/news/iranf5_2612 (Hebrew).

193 Steven Lee Myers and Sheera Frenkel, "In a Worldwide War of Words, Russia, China and Iran Back Hamas," *New York Times*, November 3, 2023, https://www.nytimes.com/2023/11/03/technology/israel-hamas-information-war.html.

topics, such as the status of Israeli Arabs and radical positions identified with the extreme Israeli right.[194]

CNE: Tens of fake Iranian accounts on social media, especially Telegram, sought to provide Hamas with useful intelligence. In some cases, the fake profiles ostensibly pursued romantic relationships with IDF soldiers, as a means of tempting them into providing information about their units and operations. Thousands of IDF soldiers were targeted.[195]

194 Raphaela Goichman, "The Iranian Cyber attacks – More Sophisticated and Destructive," *The Marker*, November 6, 2023, https://www.themarker.com/captain-internet/2023-11-06/ty-article/.premium/0000018b-a44b-dc41-af9f-ef6bdcca0000 (Hebrew).

195 Raphael Kahan, *Ynet*, November 9, 2023.