Iranian Cyber Capabilities: Assessing the Threat to Israeli Financial and Security Interests

Sam Cohen

The Iranian government continues to develop and field an increasingly sophisticated range of cyber capabilities to support their strategic interests and to enable a variety of computer-based financial crime. These capabilities have directly and adversely impacted Israel, which has been the target of major cyberattacks either affiliated or directly orchestrated by the political leadership in Tehran. To assess this strategic threat, this article outlines the evolving objectives and characteristics of Iran's cyber activity targeting Israel, including attacks on banks, airlines, the Israel Defense Forces, and critical infrastructure. The article includes a brief overview of Iran's internet and telecommunications history and a technical assessment of government-linked advanced persistent threat (APT) groups. Ultimately, the article concludes that a deterrence-by-punishment strategy utilizing Israel's computer network attack and exploitation advantage could provide an impactful—albeit not risk free—approach to offsetting Iran's rapidly improving cyber posture.

Keywords: Cyberattack, Israel, Iran, offensive cyber strategy, threat actor, APT groups, computer network attack, computer network exploitation

Sam Cohen is currently a federal cybersecurity policy intern with the Telecommunications Industry Association (TIA) in Washington DC. The views and opinions expressed in this article are his own and do not represent or necessarily reflect those of his employer, university, or other affiliated organizations.

Introduction

Iran's cyber activities are responsible for some of the most costly, sophisticated, and well-organized computer attacks endured by the Israeli government and corporate sector. International sanctions have continued to deteriorate Iran's economy and its ability to project influence abroad, which has created a geopolitical incentive for launching offensive cyber operations and engaging in illicit behavior targeting its strategic adversary, Israel. At the same time, Israel's economy, military, and national infrastructure has become increasingly reliant on vulnerable digital systems and networks to move information and promote effective interconnectivity. Iran has exploited these vulnerabilities to oppose Israeli regional interests, all while maintaining a limited political footprint. Major Iranian attacks have exploited network vulnerabilities in critical infrastructure, targeted intellectual property (IP), and compromised computer systems within operational elements of the Israel Defense Forces (IDF).

Key Iranian cyber actors—such as the Ministry of Intelligence, the Basij Cyber Council, APT33, and Ashiyane—have demonstrated a relatively high degree of sophistication during past attacks against Israel. Furthermore, Tehran continues to consolidate and organize its national cyber resources into a strategy that actively searches for vulnerabilities within Israeli infrastructure, corporate, and military information systems (IS) to enable exploitation during peace and wartime. This paper will argue that Iran's offensive cyber strategy, combined with the technical computer advancements occurring across the country, represents a long-term strategic threat to Israeli economic and national security interests. Although Iranian nuclear and ballistic missile programs and Tehran's support for terrorism tend to drive the strategic discussion in Israel, this paper will highlight how Jerusalem must also prioritize a new discourse on Israeli offensive cyber capabilities and deterrence posture to adequately respond to the growing Iranian cyber threat.

Roadmap and Scope of Analysis

The first section of the paper will provide a brief background on Iran's computer and networking history. This section will look at the evolution of computer security know-how in Iran, such as how the population interacts with computer systems courses at universities, and how a workforce continues to be indigenously developed to support an information and communications technology (ICT) industry and to meet the growing demand for cybersecurity professionals.

The second part of the paper will provide a brief overview of computer network attack (CNA) and computer network exploitation (CNE) to help contextualize the technical scope and objectives of certain Iranian cyber activities discussed here later.

The third section will outline the evolution of Iran's cyber strategy. This section will look at Iranian government and government-linked attacks pre- and post-Stuxnet and how command authorities, such as the Iranian Cyber Army (ICA) and the Basij Cyber Council, have ushered in a new approach to offensive cyber operations targeting Iranian adversaries, particularly Israel. This part will also outline the unique geopolitical component of Iran's offensive cyber activities. Specifically, Iran's coordinated operations in cyberspace with regional political affiliates will be examined in Case Study 1 while Iranian cyber operations during the Joint Comprehensive Plan of Action (JCPOA) negotiation and sanctions process will be assessed in Case Study 2.

The fourth section will assess the technical capabilities of key Iranian threat actors who have targeted Israel in the past. This section will not analyze all relevant actors but rather will review the most sophisticated threats in order to evaluate the cyber risk Iran poses to Israeli information systems and data networks.

The fifth and final part will identify the need for a policy shift in Israel in which Iranian cyber activity is prioritized as a strategic threat just as Jerusalem has contextualized Tehran's nuclear and ballistic missile programs. Although the immediate physical threat is difficult to compare to nuclear weapons and their delivery systems, Iranian-linked cyberattacks continue to be active and consistently damaging, posing an ongoing threat to Israel's commercial and security interests. This section will outline a possible offensive approach that Jerusalem can implement to offset the strategic risks of growing Iranian cyber capabilities.

Contemporary Computer and ICT History in Iran

As early as 1993, Massoud Saffari, head of Iran's High Council of Informatics, had begun working on a national initiative to create a dedicated data communications network using the country's existing telephone infrastructure.[1] A few years following the launch of this initiative, Iran established its first commercial Internet Service Provider (ISP). Working with the non-profit Neda Rayaneh Institute (NRI), an affiliate of the municipal government of Tehran, the newly created ISP began offering internet access in February 1995—primarily in the national capital region. That same year, the Telecommunications Company of Iran (TCI), in collaboration with the state-controlled Telecommunication Infrastructure Company (TIC), solidified its monopoly with the purchase of international internet gateways in the country and took control of the single domestic ISP.[2]

By 1994, TCI had announced the development of a nationwide packet-switched network called IranPac.[3] A few months later, a public joint stock company called the Data Communication Company of Iran (DCI) was created to take control of IranPac and begin expanding its commercial and government usage. Although the timing is unclear, three other entities were involved in the domestic data communication market by the mid-1990s, including a private company called Pars Supaleh, the Institute for Studies in Theoretical Physics and Mathematics (IPM), and the Iranian Pek Data Outreach Center.[4]

In 1996 and 1997, DCI began to establish international connections between its growing domestic network backbone and the global internet.[5] The first key development came after DCI entered into partnership with a Canadian telecommunication company called Teleglobe, which is now VSNL International Canada. Teleglobe worked with the Luxembourg satellite company Intelsat to provide Iran with its first dedicated satellite

[1] David Banisar and Patricia Melendez, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran," *Article 19 Free Word Center: Civic Space Unit* (March 2017), p. 12, https://www.article19.org/data/files/medialibrary/38619/Iran_report_part_2-FINAL.pdf.

[2] Grey E. Burkhart, "National Security and the Internet in the Persian Gulf Region," March 1988, https://web.archive.org/web/20070703041209/http://www.georgetown.edu/research/arabtech/pgi98-4.html.

[3] Ibid.

[4] Babak Rahimi, "Cyber Dissent: The Internet in Revolutionary Iran," *Middle East Review of International Affairs Journal* 7, no. 3 (September 2003): 2–3.

[5] Open Research Network, "Iran's Telecom and Internet Sector: A Comprehensive Survey," *Network Startup Resource Center: Oregon University* 1, no. 1 (June 1999): 12–13.

uplink directly integrated with the IranPac system.[6] Soon after, DCI entered into a joint venture with the Kuwaiti Ministry of Communications and the US-based Hughes Network Systems (HNS).[7] This venture centered on DCI gaining access to two very-small-aperture terminal (VSAT) hubs in Kuwait operated by HNS, which would substantially increase the geographic area within Iran supported by a dedicated internet and data transmission service, in addition to improving internet speed nationwide. The venture would eventually expand to include the Kuwait's state-controlled company Gulfsat, which—together with HNS—provided Iran's government and commercial clients with a reliable network communication service, supporting remote connections and bridges to foreign networks, including those nodes serving European, Asian, Middle Eastern, and North African markets.[8]

Iran had prioritized a well-established national internet infrastructure and it was slowly becoming accessible to the majority of the population, although network transmission services were slow and subscription fees were prohibitively costly for the country's lower socio-economic groups. DCI aimed to have 300,000 unique government users on its network by 1998, with plans to allow the public to purchase modems for private use that same year.[9] That objective had a material impact on the internet landscape in Iran, as by 2001, Tehran alone had 1,500 active internet cafes.[10] This made Iran one of the leading countries in the Middle East in terms of the number of internet cafes per major metropolitan area. Today, the ISP market has become more diversified, with government-linked providers such as Irancell and Hamrah Aval having 67 million users, with nearly 30 million of those users having access to third or fourth generation mobile data services.[11]

A nationwide internet infrastructure and a dedicated computer industry in Iran have been active and established for at least thirty years. The presence of this telecommunication backbone and the growing commercial and private accessibility to the internet after 1998 has resulted in a computer software and hardware literate population. This is evident by the technical course

[6] Ibid.

[7] Burkhart, "National Security and the Internet in the Persian Gulf Region."

[8] Open Research Network, "Iran's Telecom and Internet Sector: A Comprehensive Survey," 12, 15–16.

[9] Rahimi, "Cyber Dissent: The Internet in Revolutionary Iran," 2–3.

[10] Ibid., 4.

[11] Burkhart, "National Security and the Internet in the Persian Gulf Region."

offerings that Iran's large universities provide. For example, Sharif University of Technology in Tehran has developed its own dedicated Security and Counter-Infiltration education program where undergraduate and graduate computer science students are taught fundamentals of hacking, cybersecurity, and information security policy.[12] Courses from the curriculum include Kali and Backtrack introduction to operating systems; Infiltration tests for wireless networks; SQL Injection; Infiltrating IDS and Firewall systems; and Identifying security loopholes for XSS in web based software/ applications.[13] In 2013, Iran also launched a nationwide curriculum emphasizing scripting and hacking at the high-school level.[14] FARS News Agency, an Iranian media group, announced that certain courses would center on hacking the computer systems that supported unmanned aerial vehicles (UAVs), where technically proficient computer science students are taught remote access and authorization control techniques.[15] Many of these students are directed into cybersecurity and information assurance university programs based in Tehran.

Iran's internet and data communication infrastructure expansion in the 1990s initiated the growth of a national computer security industry. Combined with growing computer course offerings at universities and the rising demand for private industry networking, coding, and data management professionals, the country's digital sophistication and the national cyber talent pool supporting attacks will likely increase. Intellectual property theft conducted by the Iranian government will also continue to have a positive influence, as foreign computer technology will allow indigenous market developments to occur at accelerated rates.

[12] Banisar and Melendez, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran," 32, 57.

[13] Ibid., 58.

[14] Ginger Hill, "Iran Adds Hacking to Their High School Curriculum," *Security Today*, September 4, 2013, https://securitytoday.com/articles/2013/09/04/iran-adds-hacking-to-their-high-school-curriculum.aspx.

[15] Ibid; Micah D. Halpern, "Iran's Teaching Hacking in High School," *Huffington Post,* August 30, 2013, https://www.huffingtonpost.com/micah-d-halpern/iran-hacking-school_b_3836482.html.

Understanding Computer Network Attack and Exploitation

To understand how Iran has leveraged cyberspace for its geopolitical, financial, and security objectives, it is important to differentiate between different types of cyber activity. Without understanding the technical differences, it is more difficult to describe why Tehran was involved in a certain operation, which actors specifically benefited from a given attack or espionage campaign and how much technical knowledge or capability was required to launch the operation successfully. To highlight these technical differences, this section will briefly review the three primary operational components of cyber strategy or warfare: computer network exploitation (CNE), computer network attack (CNA), and computer network defense (CND)—all of which can be collectively described as computer network operations (CNO). CNO is a broad term used to describe both military and civilian computing processes that leverage digital networks and their connected information systems, assets, and data for strategic purposes. CNO enables organizations to attack and disrupt adversarial computer networks, defend friendly infrastructure connected to the internet, protect internal information systems from attack or espionage, and exploit targeted computer networks through intelligence collection.[16]

CNE is used for intelligence, surveillance, and reconnaissance (ISR) purposes to prepare for a major attack or to enable espionage activities within targeted computer systems.[17] These operations are usually conducted using tools and processes that penetrate a targeted network and then slowly search for additional security vulnerabilities to be leveraged at a later date. CNE can be a tailored operation searching for a predetermined piece of information or an operation aiming to penetrate a specific information asset—such as an employee records database or an email server distributing a network's sensitive information. When CNE activities are not tailored and are intended to be prolonged general espionage campaigns, actors will usually move throughout the targeted network by escalating user privileges, establishing

[16] Clay Wilson, "Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues," *Congressional Research Service: Report for Congress—Foreign Affairs, Defense, and Trade Division* (March 2007): 5–6.

[17] Kim Zetter, "Hacker Lexicon: What are CNE and CNA?" *WIRED*, July 16, 2006, https://www.wired.com/2016/07/hacker-lexicon-cne-cna/.

root or administrative level authorizations, and mapping all assets within the network to understand where relevant data is held.

CNA is defined as operations disrupting or destroying information or data processes resident in a targeted computer or being supported by a targeted network.[18] The tools used for CNA are similar to those used for computer exploitation in terms of compromising a target but configured for systems disruption rather than intelligence collection. CNA operations can be physically, financially, and strategically damaging. For example, distributed denial of service (DDoS) attacks attempt to make a network service unavailable by overwhelming it with traffic from multiple sources, which is typically facilitated by a botnet with a malicious command and control server coordinating the overall attack infrastructure.[19] This type of CNA represents more of a reputational and financial challenge for companies or governments, as a financial institution's online banking terminal or a government's social services portal may be inaccessible for a period of time. A more serious CNA can include an incident where an application containing logical malware is installed on a targeted network, which could result in major information systems becoming corrupted or data being deleted, altered, or encrypted for ransom. For example, a CNA utilizing malware that enables an attacker to have interactive remote control over an endpoint or information system can allow the attacker to signal a computer to shut off the power flow to a piece of industrial equipment, inducing a severe operating error at a critical infrastructure facility or a corporate factory.

CND is defined as defensive measures used to protect information, computers, and networks from accidental and targeted disruption, exploitation, or destruction.[20] CND can include tools that passively monitor, prevent, and respond to unauthorized computer activity, such as firewalls or adaptive data encryption, or it can include more active measures, such as monitoring adversarial computers from within to determine their capabilities and intentions or incorporating threat intelligence into corporate and government cybersecurity

[18] Ibid.

[19] Andrew Shoemaker, "How to Identify a Mirai-Style DDoS Attack," *Imperva Incapsula: Security Reports*, April 10, 2017, https://www.incapsula.com/blog/how-to-identify-a-mirai-style-ddos-attack.html.

[20] Wilson, "Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues," 5–6.

programs.[21] A core mission of CND aims to enhance organizational information integrity while also providing sufficient response capabilities for security teams containing, eradicating, and recovering from cyber incidents.

Evolution of Iranian Cyber Strategy and Command Authorities

During a 2015 interview with Iranian media outlet *Defa Press*, Behrouz Esbati, the commander of Iran's General Staff Cyber Headquarters (GSCH) stated that "cyber security and capabilities are no less important than the nuclear issue."[22] This comment summarizes the high-level strategic importance that Tehran has placed on being able to defend and attack through digital networks. Although certain hacking groups within Iran can be traced to domestic political attacks in the early 2000s, the emergence of government-linked operations specifically targeting foreign adversaries first appeared in 2007 when the Islamic Revolutionary Guard Corps (IRGC) established the Center for the Study of Organized Crime.[23] Intelligence and government officials in the West have classified this organization as Iran's first government coordinated hacking group and, with that, Iran's first official commitment to an offensive effort in cyberspace. By 2009, the IRGC began recruiting professionals for its internal cyber force and the closely linked military unit called the Iranian Cyber Army (ICA).[24] Furthermore, IRGC Commander Hossein Hamedani

[21] James Mulvenon, "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, ed. James C. Mulvenon and Richard H Yang (Santa Monica, CA: Rand Corporation, 1999), pp. 185–186; Larry Hollingsworth, "Blacking Threats With CND: Protect Your Network From Hackers & Attackers," *MIL Corporation*, June 2018, https://www.milcorp.com/service-areas/cyber-security/computer-network-defense/.

[22] Paul Bucala and Caitlan Shayda Pendleton, "Iranian Cyber Strategy: A View from the Iranian Military," *American Enterprise Institute: Critical Threats Project* (November 24, 2015), p. 7, https://www.criticalthreats.org/analysis/iranian-cyber-strategy-a-view-from-the-iranian-military.

[23] Colin Anderson and Karim Sadjadpur, "Iran's Cyber Threat: Espionage, Sabotage and Revenge," *Carnegie Endowment for International Peace* (January 4, 2018), pp. 10–11, 60, https://carnegieendowme nt.org/2018/01/04/iran-s-cyber-threat-introduction-pub-75138.

[24] Ashley Wheeler, "The Iranian Cyber Threat," *Phoenix TS: Tech Roots Project*, September 12, 2013, https://phoenixts.com/blog/the-iranian-cyber-threat-part-1-irans-total-cyber-structure/; Banisar, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran," 7.

announced in 2010 that the Basij Cyber Council—an additional cyber entity under the IRGC—had trained 1,500 cybersecurity professionals to deploy as part of its growing offensive attack and espionage outfit.[25] In 2009, leaders of this Basij cyber unit specifically called for digital attacks "against the actions of the Zionist Entity [Israel]."[26]

In 2010, Israel and the United States launched a malicious computer worm targeting Iran's nuclear program. The worm was called Stuxnet and its advanced payload utilized four different zero-day exploits affecting Windows Operating Systems (OS) and Siemens industrial control software.[27] The worm spread throughout commercial and government information systems (IS) and endpoints before eventually reaching critical nodes within Supervisory Control and Data Acquisition (SCADA) systems at Iranian nuclear production facilities. Stuxnet compromised key programmable logic controllers (PLCs) that operated the industrial equipment at these nuclear sites, which resulted in the destruction of 984 centrifuges and other machines that Iran was using to enrich uranium for an alleged weapons program.[28] Similar joint US-Israeli industrial control system attacks would occur in the following years, with the modular FLAME and WIPER variant malwares attacking PLCs at Iranian oil and natural gas production facilities and other elements of the country's critical infrastructure—such as the national financial transaction system.[29]

Iran perceived Stuxnet and similar follow-on attacks as a demonstration of how their adversaries were weaponizing cyberspace and exploiting underlying weaknesses within the country's digital security apparatus. Tehran's initial response was defensive, aiming to prevent and mitigate the network vulnerabilities that allowed Stuxnet, FLAME, and WIPER variants to be successful. For example, after the 2010 Stuxnet attack, Iran created the Cyber Defense Command and a new cybersecurity department under

[25] Michael Connell, "Deterring Iran's Use of Offensive Cyber: A Case Study," *CNA Analysis and Solutions and Defense Technical Information Center (DTIC)*, October 2014, https://apps.dtic.mil/dtic/tr/fulltext/u2/a6 17308.pdf.

[26] Banisar, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran," 33.

[27] Kim Zetter, "An Unprecedented Look at the World's First Digital Weapon," *WIRED: Security Reports*, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[28] Ibid.

[29] Elinor Mills, "Behind the 'Flame' Malware Spying on Mideast Computers," *CNET*, June 4, 2012, https://www.cnet.com/news/behind-the-flame-malware-spying-on-mideast-computers-faq/.

the Passive Defense Organization (PDO) to protect domestic information systems from foreign adversaries infiltrating key networks.[30] However, Tehran also initiated a dramatic reorientation of its offensive cyber posture by directing its intelligence, security, and private industry resources to target and infiltrate adversarial networks. This was a strategic shift that emphasized not only computer-based financial crime and intellectual property (IP) theft to support the country's economy but also the leveraging of cyberspace as a new national tool for achieving geopolitical objectives.

Although an emphasis on offensive cyber capabilities and activity does not impact only Israel's economic and security interests, since Saudi Arabia, the United States, and other European and Middle Eastern powers are also considered adversaries of Tehran, it is clear that Iranian hacking groups have prioritized Israel as a prime target. For example, a 2014 CNE campaign called Operation Newscaster and a 2014 CNA campaign called Thamar Reservoir were both Iranian operations that had unique tactics, techniques, and procedures (TTPs) targeting Israeli government and military officials.[31] The security firm ClearSky Cybersecurity conducted a quantitative assessment of Thamar Reservoir and found that Israel was subjected to 14 percent of all the attacks and social engineering operations that were launched and represented the second largest targeted country after Saudi Arabia. The United States, Britain, Canada, and other Western countries all were subjected to fewer than 3 percent each of the overall coordinated Iranian effort.[32] Similar ratios were also identified during Operation Newscaster. These figures reinforce the notion that while Iran's offensive strategy has multiple objectives and targets, Israeli information systems have been labeled as a key strategic priority.

[30] Banisar, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran," 8; Connell, "Deterring Iran's Use of Offensive Cyber: A Case Study," 4.

[31] ClearSky Research Team, "Thamar Reservoir: An Iranian Cyber-Attack Campaign against Targets in the Middle East," *ClearSky Cybersecurity, Inc.*, June 2015, https://www.clearskysec.com/wp-content/uploads/2015/06/Thamar-Reservoir-public1.pdf; Jim Finkle, "Iranian Hackers use Fake Facebook Accounts to Spy on U.S., Israel and others," *Reuters*, May 29, 2014, https://www.reuters.com/article/iran-hackers/iranian-hackers-use-fake-facebook-accounts-to-spy-on-u-s-others-idUSL1N0OE2CU20140529.

[32] ClearSky Research Team, "Thamar Reservoir," 12.

Case Study 1: Regional Threat Actor Affiliates

In the years following the 2010 Stuxnet attack, Iranian officials began to aggressively leverage Israeli vulnerabilities in cyberspace. This included cooperation with Hamas and Hezbollah hacking groups who, together with Iran, conducted CNA and CNE operations against the Israeli Security Agency (Shin Bet), Home Front Command, the Office of the Prime Minister, the Defense Ministry, Bank of Jerusalem, El Al Airlines (Israel's national airline), Likud and Kadima Political Parties, and operational components of the IDF.[33] Other Iranian computer attacks have attempted to infiltrate local area networks (LANs) of "vital national systems" according to a 2013 statement by Israel's Prime Minister Benjamin Netanyahu.[34] His statement noted that Iran had begun targeting water, power, and financial transaction infrastructure, in addition to social service websites operated by the government.

According to an article in the *Jerusalem Post*, one of Hamas' preeminent hackers, Maagad Ben Juwad Oydeh, successfully infiltrated IDF data communications networks and routed data downlinks from IDF drones hovering over Gaza to Hamas commanders.[35] Beginning in 2012, the commanders had a direct real-time feed of aerial surveillance videos that were being relayed from Israeli unmanned aircraft. By 2015, Oydeh was able to extract the global positioning system (GPS) signals from the drones he was targeting, which allowed senior Hamas militants to maneuver forces and weapons away from monitored areas.[36] Israeli security forces arrested and in 2016 convicted Oydeh on charges of spying, conspiracy, contact with enemy agents, and membership in an illegal organization.

Iran has also worked with Hamas to support their cyber operations aiming to disrupt Israeli military and political activities in Gaza. For example, during the 2012 Hamas war, Israel faced a sophisticated cyber campaign

[33] Gabi Siboni, Matthew Cohen, and Charles Freilich, "Israel and Cyberspace: Unique Threat and Response," *International Studies Perspectives* 17, no. 3 (August 2016): 309–310.

[34] Jeffrey Heller and Maayan Lubel, "Iran Ups Cyber Attacks on Israeli Computers: Netanyahu," *Reuters*, June 9, 2013, https://www.reuters.com/article/us-israel-iran-cyber/iran-ups-cyber-attacks-on-israeli-computers-netanyahu-idUSBRE95808H20130609.

[35] Yonah Jeremy, "Islamic Jihad Member Convicted In Plea Bargain For IDF Drones," *Jerusalem Post*, January 2017, https://www.jpost.com/Israel-News/Islamic-Jihad-member-convicted-in-plea-bargain-for-hacking-IDF-drones-480092.

[36] Ibid.

seeking to disable government websites and operations at private financial institutions, including a national bank that was targeted by a successful DDoS attack associated with known Iranian server infrastructure.[37] There were also incidents during Israel's 2014 campaign against Hamas, where the IDF's homeland security division experienced a temporary information system breach when the Syrian Electronic Army—an Iranian-linked hacking affiliate—was able to compromise the IDF's website and temporarily upload political messages defaming ongoing Israeli operations.[38]

Another example of Iranian coordination with regional geopolitical allies is Tehran's relationship with the Hezbollah Cyber Army (HCA). The Israeli-based cyber threat intelligence firm Check Point Software Technologies attributed a series of corporate and government breaches across Israel's defense sector from 2013 to 2015 to the HCA.[39] The group's campaign—called Volatile Cedar—was relatively advanced, well planned, and the attackers were patient while scanning for external network vulnerabilities as to limit their exposure. A custom malware variant, referred to as EXPLOSIVE, acted as a Trojan program allowing the attackers to establish remote interactive control over externally facing servers and information systems. The attackers then used these compromised assets to pivot toward internally facing servers where they could deploy other modules of the malware on network hosts.[40] The malware's technical features indicate that it was developed by Iran and subsequently distributed to the HCA, which is consistent with the overall trend of Iranian cyber authorities disseminating training and technical resources to Hezbollah-linked threat actors.[41]

In addition to foreign affiliates, Tehran has also utilized part-time domestic private hacking groups for less sophisticated cyber operations that are aligned

[37] Siboni, Cohen and Freilich, "Israel and Cyberspace: Unique Threat and Response," 312.

[38] Ibid.

[39] Ben Shaefer, "The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism," *Georgetown Security Studies Review*, March 11, 2018, http://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism/.

[40] Threat Intelligence and Research Team, "Volatile Cedar," *Check point Software Technologies*, pp. 1–2, March 30, 2015, https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf.

[41] Anderson and Sadjadpur, "Iran's Cyber Threat: Espionage, Sabotage and Revenge," 21.

with the country's foreign policy objectives. For example, in 2018 a private group called Charming Kitten was responsible for conducing Man-In-The-Browser attacks utilizing a browser exploitation framework (BEF) against multiple Jewish media outlets inside the United States who were supporters of Israel.[42] Similar attacks have also occurred against the American Israel Public Affairs Committee (AIPAC), Jewish political and academic leaders around the world, and organizations supportive of Israeli actions in Gaza or Lebanon.[43]

Case Study 2: JCPOA and an Adapting Iranian Cyber Strategy

The use of offensive cyber activity as a response mechanism to regional security developments has been a frequent policy option pursued by Tehran, specifically to counter Israeli interests. Based on the previous examples analyzed, it is clear that Iran routinely coordinates cyber operations with regional security partners to launch integrated and tailored attacks against Israeli commercial and government institutions. These attacks and espionage campaigns tend to occur during periods of security activity in the region, such as Israeli incursions into Gaza or Lebanon. This trend indicates that Iranian offensive cyber activity is intricately linked and constantly adapting to the country's geopolitical interests at any given time. This strategic approach is not necessarily an underlying characteristic of the cyber policies of other countries, such as Russia or China. For example, Moscow and Beijing, who both have access to a talent pool and technical infrastructure that greatly exceeds the sophistication of training, resources, and capability in Iran, can be described as constant systemic actors routinely launching attacks regardless of geopolitical conditions.[44] While that is true for certain cyber actors focused on financial crime in Iran, those groups tend to be less controlled and unaligned with government policy priorities, such as the independent Iranian hackers responsible for the HBO breach in 2015 after the JCPOA

[42] Oded Yaron, "Iranian Hackers Tried to Impersonate Israeli Cyber-Security Company," *Haaretz*, July 9, 2018, https://www.haaretz.com/israel-news/premium-iranian-hackers-break-into-israeli-cybersecurity-site-1.6263629.

[43] Anderson and Sadjadpur, "Iran's Cyber Threat: Espionage, Sabotage and Revenge," 35.

[44] Mark Pomerleau, "DoD Releases First New Cyber Strategy in Three Years," *The Fifth Domain,* September 18, 2018, https://www.fifthdomain.com/dod/2018/09/19/department-of-defense-unveils-new-cyber-strategy/.

agreement was signed and international sanctions were lifted.[45] The regular changes in the frequency of Iranian CNA and CNE is uncharacteristic of Chinese and Russian threat actors and highlight the uniqueness of the Iranian threat to Israel as it is fundamentally strategic and long term.

The pattern of Iranian cyber activity closely adjusting to an evolving geopolitical development has been evident throughout the JCPOA negotiation and sanctions process. US government officials have noted that in the period leading up to the negotiations in 2013 and 2014, Iran was conducting major cyber operations that caused significant financial damage to companies throughout the West and the Middle East, including in the United States, Canada, Britain, Israel, Saudi Arabia, and even Turkey.[46] Following the large-scale operations, US Attorney General Loretta Lynch stated, "These attacks were relentless, they were systematic, and they were widespread."[47] Michael Daniel, president of the Cyber Threat Alliance, explained in 2017 that "once Iran decided it really wanted to come to the table and actually negotiate something serious, they naturally took steps in a whole variety of areas to ramp back activities so that they weren't being so confrontational."[48] Iran significantly increased its offensive cyber activity during the sanctions period leading up to negotiations while it very rapidly deescalated that same policy once the deal neared agreement. It is clear that a change in geopolitical conditions between 2014 and 2015 induced the rollback of Tehran's aggressive cyber campaign during the previous two years. Levi Gundert, an Iran-focused analyst at the private intelligence firm Recorded Future noted, "Most of the destructive attacks were pre-2015. Then we had the Iran nuclear deal."[49]

[45] Andy Greenberg, "The Iran Nuclear Deal's Unraveling Raising Fears of Cyber Attacks," *WIRED*, May 9, 2018, https://www.wired.com/story/iran-nuclear-deal-cyberattacks/.

[46] Kate Brannen, "Abandoning Iranian Nuclear Deal Could Lead to New Wave of Cyber Attacks," *Foreign Policy*, October 2, 2017, https://foreignpolicy.com/2017/10/02/abandoning-iranian-nuclear-deal-could-lead-to-new-wave-of-cyberattacks/.

[47] Dustin Voltz, "U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam," *Reuters*, March 24, 2016, https://www.reuters.com/article/usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSL2N16W1I4.

[48] Brannen, "Abandoning Iranian Nuclear Deal Could Lead to New Wave of Cyber Attacks."

[49] Greenberg, "The Iran Nuclear Deal's Unraveling Raising Fears of Cyber Attacks."

While negotiations and official agreement in 2015 curbed Iranian cyber activities targeting its adversaries, President Trump's decision to officially withdraw from the JCPOA nuclear deal in May 2018 had the opposite affect. The computer security firm CrowdStrike released a report identifying a notable shift in activity associated with Iranian hacking groups, just twenty-four hours after Trump's May withdrawal announcement.[50] The activity included spear-phishing operations that had been designed with social engineering efforts, containing malicious email attachments that were tailored to breach pre-selected corporate and government cybersecurity programs. The emails were mainly delivered to US commercial executives and military officials, but the report indicates that senior military and political representatives of other US allies, such as Israel, had been specifically targeted abroad.[51] The extensive preparation that had gone into the attack suggests that Tehran was timing the operation as a geopolitical response to Trump's official statement, which reinforces the notion of Iran's offensive cyber strategy being tethered to their fluctuating strategic objectives and national security priorities.

Iran has yet to publish a comprehensive single document that outlines its overall cyber strategy or its objectives, targets, policies, and methods for offensive operations. However, official public statements from the Iranian government combined with attributed Iranian-linked CNA and CNE, which have specifically sought to exploit vulnerabilities in Israel and its allies, demonstrate how the country has moved away from its largely defensive and pre-Stuxnet cyber posture. For example, Frank Cilluffo, director of Center for Cyber and Homeland Security, stated in 2017 that "In recent years, Iran has invested heavily in building out their computer network attack and exploit capabilities. Iran's cyber budget had jumped twelvefold under President Rouhani, making it a top five cyber-power. They are also integrating cyber

[50] Nicole Perlroth, "Without Nuclear Deal, U.S. Expects Resurgence in Iranian Cyberattacks," *New York Times*, May 11, 2018, https://www.nytimes.com/2018/05/11/technology/iranian-hackers-united-states.html.

[51] Ibid; Zack Whittaker, "Iran likely to Retaliate with Cyberattacks after Nuclear Deal Collapse," *ZDNet*, May 9, 2019, https://www.zdnet.com/article/iran-poised-to-launch-cyberattacks-after-nuclear-deal-collapses/.

operations into their military strategy and doctrine."[52] This new emphasis on an offensive strategy, combined with declining security relations between Tehran and Jerusalem, has propelled Iranian cyber activities to the forefront of Israel's strategic threat landscape.

Iran's Technical Cyber Capabilities: Analyzing Key Threat Actors

It is important to review the sophistication of key Iranian threat actors to determine the technical and policy risks facing Israel. Although only a small portion of the Iranian cyber landscape will be analyzed, this section will still highlight how Iran's most experienced cyber professionals are rapidly improving their technical knowledge to support offensive behavior—including attacks targeting Israeli infrastructure, military, and commercial information systems.

First discovered by US cybersecurity firm FireEye, APT33 is an Iranian hacking group responsible for an array of breaches across infrastructure, banking, aerospace and petrochemical industries in Israel, the United States, the United Kingdom, South Korea, and Saudi Arabia.[53] An advanced persistent threat (APT) is a malicious computer attack where a person or group gains unauthorized access to a network and remains undetected for an extended period, usually mapping the network for additional vulnerabilities, escalating their user privileges, or uploading backdoors to enable remote interaction. APTs have traditionally been associated with nation-state actors due to the financial resources, talent, and infrastructure that usually support their operations, which accurately describes APT33's relationship with the Iranian government. FireEye and the Russian-based cybersecurity firm, Kaspersky Lab, have both released reports detailing the intricate connections between APT33 and the Iranian government's Nasr Institute, which is a contractor jointly operated by the IRGC's Basij cyber unit and the Ministry

[52] Eric Auchard, "Once 'Kittens' in Cyber Spy World, Iran Gains Prowess: Security Experts," *Reuters*, September 20, 2017, https://uk.reuters.com/article/us-iran-cyber/once-kittens-in-cyber-spy-world-iran-gains-prowess-security-experts-idUKKCN1BV1VA.

[53] Thomas Brewster, "Meet APT33: A Gnarly Iranian Hacker Crew Threatening Destruction," *Forbes*, September 20, 2017, https://www.forbes.com/sites/thomasbrewster/2017/09/20/iran-hacker-crew-apt33-heading-for-destructive-cyberattacks/#5b5693174a48.

of Intelligence.[54] US and Israeli government reports also indicate that many of the personnel believed to be associated with APT33 previously have worked in other Iranian hacking groups and within the Iranian government itself.

Although APT33 is not dedicated to only attacking Israel, it has conducted highly tailored and complicated operations that have disrupted and damaged Israeli information systems. The group routinely uses a complex Trojan program called DROPSHOT, which allows malware to bypass anti-virus systems and execute non-malicious programs in virtual sandbox environments to avoid detection by security teams.[55] The malware is believed to be a derivative of similar code used by another advanced Iranian hacking group called the Sword of Justice, which was responsible for developing and launching the highly capable and damaging Shamoon malware in 2012.[56] APT33 has also included new versions of NANOCORE and NETWIRE remote access trojans (RATs) as payloads for their DROPSHOT tool, which has provided the group with a full-spectrum capability to enter protected systems, locate additional vulnerabilities, extract or delete data, and remove evidence from operational and security logs.[57] This has made attribution and root cause analysis with APT33 attacks extremely difficult, which, in turn, has hindered countermeasure development for the group's operations.

APT33 is an example of one of Iran's most advanced malicious cyber groups who routinely conducts CNA and CNE operations against adversaries. The group's activity has been at the forefront of Iran's offensive cyber strategy and has had direct military impact on Israel. For example, during the 2014 Israel-Gaza war, it is believed that APT33 was behind a breach of a civilian-military communication network distributing battlespace intelligence.[58]

[54] Jacqueline O'Leary, Josiah Kimble, and Kelli Vanderlee, "Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and Has Ties to Destructive Malware," *FireEye: Threat Research Team*, September 20, 2017, https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html.

[55] Ibid.

[56] Andy Greenberg, "New Group of Iranian Hackers Linked to Destructive Malware," *WIRED*, September 20, 2017, https://www.wired.com/story/iran-hackers-apt33/.

[57] O'Leary, Kimble, and Vanderlee, "Insights into Iranian Cyber Espionage: APT33."

[58] Yaakov Lappin, "Iran Attempted Large-Scale Cyber Attack On Israel, Senior Security Source Says," *Jerusalem Post*, August 17, 2014, https://www.jpost.com/Arab-Israeli-Conflict/Iran-attempted-large-scale-cyber-attack-on-Israel-senior-security-source-says-371339.

Private security firms have linked APT33 to the attacks due to the TTPs and malware variants used during the operation. The compromised network, however, only experienced a short period of data relay disruptions between command and control entities, which resulted in an extremely minor impact on the overall war effort.[59] Although the attack was not entirely successful, it demonstrates how Iran is creating the technical capability to induce real costs to IDF operations and Israeli military posture.

There are also advanced Iranian threat actors inducing significant financial harm to Israel and affecting its economic interests. For example, an Iranian APT called COBALT DICKENS conducted a CNA operation in 2018 targeting research institutes, universities, and professors around the world.[60] Over fifteen billion pages of intellectual property (IP) were stolen from the databases and information assets of facilities in twenty-two different countries. Security firms estimate that the IP is worth 3.4 billion dollars.[61] Universities in Israel were successfully targeted during this operation, although the exact losses suffered by specific universities have not been made public.[62] COBALT DICKENS has also been identified as a partner group to the Iranian Mabna Institute, who has strong ties to another Iranian-linked firm called the Nasr Institute. These groups have been linked to DoS and other computer attacks on Israeli banks, in addition to stealing trade secrets from Israeli and allied companies.[63]

[59] Ibid.

[60] John Kuhn, "COBALT DICKENS Targets Universities," *IBM X-Force Threat Exchange*, August 29, 2018, https://exchange.xforce.ibmcloud.com/collection/COBALT-DICKENS-Targets-Universities-4bdbb7eff5196b24ce4981abcffec11e.

[61] Victoria Bekiempis and Larry McShane, "Iranian Hackers Stole $3.4B in Intellectual Property from Hundreds of Universities across the World," *NY Daily News*, March 23, 2013, https://www.nydailynews.com/news/crime/iran-hackers-breached-5-u-s-gov-computer-systems-prosecutors-article-1.3891703.

[62] "Israeli University Compromised in Iran Hack," *Times of Israel*, March 24, 2018, https://www.timesofisrael.com/israeli-university-accounts-compromised-in-iran-hacking-scheme/.

[63] Pierluigi Paganini, "Iran-linked COBALT DICKENS Group Targets Universities in New Phishing Campaign," *Security Affairs*, August 28, 2018, https://securityaffairs.co/wordpress/75710/cyber-warfare-2/cobalt-dickens-iran-attacks.html; Charlie Osborne, "Iranian Hackers Target 70 Universities Worldwide to Steal Research," *ZDNet*, August 24, 2018, https://www.zdnet.com/article/iran-hackers-target-70-universities-in-14-countries/; Brewster, "Meet APT33: A Gnarly Iranian Hacker Crew Threatening Destruction."

Another APT group that has specifically targeted Israel and has been a generally active component of Iran's offensive cyber strategy is OilRig. Initially active in 2015, OilRig has conducted successful spear phishing and domain name system (DNS) spoofing attacks against multiple law firms, banks, and third-party information technology (IT) vendors that serve the financial industry in Israel.[64] Although the metrics of these attacks and resulting financial costs are extremely vague and underreported, Israeli media and government statements indicate that certain attacks have compromised critical payment card industry (PCI), market trading, and index reporting information systems. Palo Alto Networks reported that OilRig also successfully attacked financial institutions and technology organizations within Saudi Arabia.[65]

OilRig is an example of an increasingly capable Iranian threat actor. One of the TTPs the group utilizes involves sending malicious Microsoft Excel attachments to an employee at the target organization. Once the employee opens the attachment, the file displays decoy content within the spreadsheet and installs a variant of HELMINTH malware. This malware opens up a backdoor linking the endpoint to a command and control server, which then provides the group with remote functional control of the infected endpoint.[66] The attackers have also used advanced obfuscation techniques to mask their attack infrastructure and certain details of the HELMINTH malware itself, which has impeded security investigations and created challenges for corporate cybersecurity programs in Israel's financial industry.

The last actor that is important to the technical assessment of Iranian cyber capabilities is the Ashiyane Digital Security Team, also referred to as Ashiyane or NEST. Ashiyane is a unique actor within the overall Iranian threat landscape as, in addition to their malicious operations, they also act as one of the largest online educational and training resources for the

[64] ClearSky Research Team, "Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford," *ClearSky Cybersecurity Inc.*, January 5, 2017, https://www.clearskysec.com/oilrig/.

[65] Robert Falcone and Bryan Lee, "The OilRig Campaign: Attacks on Saudi Arabian Organizations Deliver Helminth Backdoor," *Palo Alto Networks*, May 26, 2016, https://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/.

[66] Ibid.

hacking and computer security community in Iran.[67] For example, members of Ashiyane have attended hackathons and security conferences in Qom as keynote speakers.[68] During closed seminars at these events, members of the group review TTPs for Linux server infiltration, DDoS operations, and SQL Injection attacks. As of 2017, there were allegedly 363,949 unique members participating in the group's online tutorials, which ranged from instructional videos and interactive labs focusing on Access Control, Privilege Escalation, OS Analysis and Scanning, Network Management and Infiltration, Cryptography, Email Security, and RAT Development.[69]

Ashiyane's malicious CNA and CNE activities are not as advanced, dedicated, or resource intensive as other major threat actors such as APT33. In 2017, cybersecurity firms attributed to Ashiyane the defacement and service interruption of 500 Israeli and other Western websites during the 2009 Israeli incursion into Gaza.[70] The group was also responsible for widespread DDoS attacks that targeted 1,000 websites in the United States, Britain, and France in 2010 for supporting anti-Iranian activist groups.[71] Although these operations have been politically and financially impactful, their technical sophistication has not been similar to Iran's predominant threat actors. However, since the group is the most technically proficient and up-to-date educational resource for hackers within the country, it is clear that Ashiyane has been a major facilitator of the growing Iranian offensive cyber threat through their training and lab-based education network. The Iranian government itself has recognized the impact the group has had within the hacking community, with entities such as the Grand Ayatollah Makarem Shirazi—a Shiite religious authority—the FATA Police and leaders within the IRGC praising their work.[72]

[67] Dorothy Denning, "Following the Developing Iranian Cyberthreat," *Scientific American*, December 12, 2017, https://www.scientificamerican.com/article/following-the-developing-iranian-cyberthreat/.

[68] Banisar and Melendez, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran," 34.

[69] Ibid.

[70] Denning, "Following the Developing Iranian Cyberthreat."

[71] Ibid.

[72] Banisar and Melendez, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran," 34.

Although the sophistication of the actors discussed in this section represent the minority of the overall Iranian threat landscape, it is clear that certain groups linked to the Iranian government or working for the government directly are becoming increasingly advanced. Further, the scale, complexity, and scope of the 2018 COBALT DICKENS attack—although not solely aimed at Israeli institutions—demonstrated how Iran's overall cyber ambitions are rising concurrently with the nation's technical capabilities and resources. The specific economic and military objectives of future Iranian offensive operations will likely adapt and evolve as key threat actors become more technically proficient, but the general aim of using cyberspace as a strategic tool to pressure Israel will remain constant.

Strategic Policy Shift: Offsetting the Iranian Cyber Threat

Rapid digitalization of critical infrastructure and the increasing use of susceptible information and communications technology (ICT) throughout Israel has created a large attack surface vulnerable to Iranian threat actors. In 2011, Israel's Prime Minister Benjamin Netanyahu told a Tel Aviv cybersecurity conference, "The more computerized we get, the more vulnerable we become. There is therefore no choice but to deal with this in a more systematic and focused manner."[73] At the same conference the Israeli Security Service's Cyber Task Force chief stated that "Israeli networks critical to communications, transport systems, finance, and the supply of electricity and water are all wide open to attack. This constitutes a major threat to national security."[74] These comments indicate that a strategic perspective of cyberspace had already been active in Israel for several years. For example, major policy reforms in 2015 strengthened the roles and capabilities of the National Cybersecurity Authority, the National Cyber Directorate, the Information Security Agency, and the now terminated Cyber Command project.[75] However, in 2016, Israel's Energy Authority responsible for national electric grids still experienced

[73] Matthew Kalman, "Israel Vulnerable To Cyber Attack, Leaders Warn," *MIT Technology Review*, June 15, 2011, https://www.technologyreview.com/s/424302/israel-vulnerable-to-cyber-attack-leaders-warn/.

[74] Ibid.

[75] Deborah Housen-Couriel, "National Cyber Security Organization: Israel," C*yber Defense Center of Excellence NATO* 2, no. 4 (February 2017): 11–12.

a two-day information system shutdown after a systemic APT attack.[76] Regardless of the commitment to cybersecurity expressed in 2011 by the prime minister, this attack indicates that the threat to the country has only worsened and that previous responses have failed to mitigate the technical and strategic cyber threat.

An underlying feature of why a traditional detection and protection approach will not address evolving Iranian capabilities and intent is due to the geopolitical nature of the threat. For example, Russia is a financially motivated cyber actor in Israel, primarily conducting intellectual property (IP) theft, identity fraud, and computer-based transaction crime.[77] Adding barriers to Russian cyber operations with a computer network defense (CND) strategy reduces the financial return Russian actors receive due to the additional time, talent, and technical costs that would need to be put into attack preparation and execution. Alternatively, Iran's cyber motivations in Israel are largely strategic and geopolitically driven. Although there are numerous instances of Iranian actors, such as COBALT DICKENS, focusing on financial and IP objectives, the threat landscape is overwhelmingly targeted at Israeli security and economic interests that hurt and pressure the Israeli government at a strategic level—not at a specific company level—and not necessarily to the financial benefit of Tehran. Although a deterrence-by-denial strategy seeking to leverage Israel's advanced cybersecurity industry is useful to ensure less sophisticated Iranian groups are not incentivized to target Israel, Jerusalem must also develop and implement a cyber centric deterrence-by-punishment strategy.

The key aspect of a deterrence-by-punishment strategy is that it threatens unacceptable costs in response to an adversary's first strike action, or in this case, a major Iranian CNA or espionage campaign. The massive reorientation of Iran's cyber forces after the 2010 Stuxnet attack indicates that Tehran is likely to view an openly communicated deterrence-by-punishment strategy from Jerusalem as a highly credible strategic threat to Iranian interests—including the integrity of its energy infrastructure, military apparatus, and commercial enterprises. Further, the WIPER variants and FLAME attacks

[76] Danna Harman, "Israel's Electrical Grid Targeted by 'Severe Cyberattack'" *Haaretz*, January 26, 2016, https://www.haaretz.com/israel-news/.premium-israel-s-electrical-grid-targeted-by-severe-cyberattack-1.5396042.

[77] Ronen Bergman, "Israel is under Massive Chinese, Russian Cyber Espionage Attack," *Ynet*, July 31, 2018, https://www.ynetnews.com/articles/0,7340,L-5320392,00.html.

that followed Stuxnet reinforced the notion that Israel maintains a clear qualitative edge in offensive cyber activities over Iran. Israel would likely reduce the cyber risk stemming from Iran if a publicly communicated—non-covert—retaliatory policy was enacted as a guaranteed reprisal for major cyberattacks launched by Iranian groups.

Focusing on a strictly denial strategy will have a minimal impact on the geopolitical imperative that Tehran has placed on cyber operations targeting Israel. For example, Israel will never be able to completely rid its national infrastructure, military, or key commercial entities from cyber risk, which means that Tehran will always be committing financial, technical, and talent resources to search for vulnerabilities and create exploits—regardless of the cost. Although it is important for Israel to leverage its national cyber talent and cybersecurity industry to protect against non-strategic threats from other countries, such as Russia and less experienced attackers within Iran itself, a new offensive strategy is required for Jerusalem to mitigate the capability improvements Iran continues to experience. This cyber-based deterrence-by-punishment approach would be the most direct, financially conservative, and sustainable model for Israel to offset Iran's strategic objectives in cyberspace.