Iranian-Israeli Confrontation: The Cyber Domain

Gawdat Bahgat

Dr. Bahgat, author of 11 books on the Middle East, is a professor at the Near East South Asia Center for Strategic Studies at the National Defense University. The opinions expressed in this article are the author's alone.

Iran and Israel have been bitter foes for more than four decades. Prime Minister Benjamin Netanyahu has been the world's most outspoken leader against Iran's nuclear program, and Jerusalem has been accused of assassinating Iranian nuclear scientists. Tehran has been the main backer of Hezbollah, which has been involved in several military skirmishes against the Jewish state and has targeted Israel's cities with sophisticated rockets. Since the beginning of the civil war in Syria in 2011, Israel has been bombing Iranian and Shiite targets almost with impunity.

This intense confrontation between the two non-Arab Middle Eastern powers extends to all warfare domains, including cyberspace. Both Tehran and Jerusalem have invested substantial resources in building defensive and offensive cyber capabilities and have accused each other of using them in hostile operations. In late spring 2020, an attempt to penetrate computers that operate rural water-distribution systems in Israel was attributed to Iran. Yigal Unna, the head of the Israeli National Cyber Directorate, stated that, had his institute not detected the attack in real time, "chlorine or other chemicals could have been mixed into the water source in the wrong proportions and resulted in a 'harmful and disastrous' outcome."[1] The Israeli official added, "We will remember … May 2020 as a changing point in the history of modern cyber warfare."[2] Shortly after the incident in the Israeli water-distribution system and in apparent retaliation, Iran's Shahid Rajaee port was attacked, snarling traffic around the port for days. It was linked to Israel. Mohammad Rastad, managing director of the Ports and Maritime Organization (PMO), declared that the attack failed to penetrate the PMO's systems and was only able to "infiltrate and damage a number of private operating systems at the port."[3]

These reported attacks and counterattacks raise concerns about the two nations' cyber capabilities and how these virtual operations are likely to impact the entire Middle East. This is particularly important, given that cyber warfare lacks well-specified rules.

FROM ALLIES TO SWORN ENEMIES

Few bilateral relations have shifted as significantly as those between Tehran and Jerusalem. Iran started formulating its policy toward Israel even before the country was established. Supporting the Arab position, in 1947 Iran voted for the minority plan, which envisaged a federated state of Palestine composed of two autonomous parts, one Jewish and one Arab, and voted against the Palestine Partition Plan that led to the creation of Israel.[4] Furthermore, Iran voted against Israel's entry into the United Nations but did not disguise its unwillingness to become actively involved in the Arab-Israeli conflict. Finally, unlike Turkey, a Muslim and Middle Eastern state that granted Israel full recognition, the Iranian cabinet decided in March 1950 to grant the Jewish state de facto recognition.[5]

These seemingly contradictory moves by Tehran in its relations with the newly born Israel can be described as "calculated ambivalence,"[6] reflecting the relative weight of opposing forces that shaped Iranian policy in the aftermath of World War II. These included the growing Iranian dependence on U.S. economic and military aid to contain and neutralize Soviet threats. For many Iranian officials, granting some kind of recognition to Israel would enhance the country's image within Jewish organizations in the United States. These organizations, according to Tehran, could lobby the American administration and Congress to serve Iranian interests in Washington. Besides, the shah viewed Israel's military and agricultural expertise with great admiration. By establishing good ties with the Jewish state, Iran was able to benefit from Israeli experience. Finally, sensitivity to Arab official and public opinion, as well as domestic opposition in Iran from religious circles and leftist groups, restrained how far the shah could go in cooperating with Tel Aviv.

These forces — sometimes more, sometimes less — shaped Iran's policy toward Israel from 1948 until the 1979 Islamic Revolution. Since the fall of the Pahlavi regime, Iranian-Israeli hostility has been driven by both ideology and geopolitics. Iran, the largest and most populous country in the Persian Gulf region, along with Egypt and Turkey, has always played a leading role in Middle Eastern/South Asian history and policy. Given its advantages, the leaders in Tehran, regardless of their political orientation (imperial or Islamic), have always perceived a special role for their country in shaping Middle Eastern economic, military and political affairs.

Shortly after the establishment of the Islamic Republic, Iran sought to "Islamize" the Arab-Israeli conflict. Instead of approaching it as a dispute between the Arabs and the Israelis, the Iranian leadership saw it as a struggle to liberate holy Muslim sites and Muslim land. This perception is in line with statements Ayatollah Khomeini made before and after rising to power as did his successor, Ayatollah Khamenei. During his exile, Khomeini supported all struggles against Israel throughout the world and accused the shah of allowing Israel a free hand in Islamic Iran. Indeed, the shah's close cooperation with Israel and the United States was a major theme of Khomeini's opposition to the Pahlavi regime. Khamenei followed the same line, arguing that the Palestinian question and the ultimate disposition of Israel were Islamic matters on which all Muslims, not just Palestinians, must have a say. In May 2020, Khamenei stated, "The struggle to liberate Palestine is a Jihad in the way of God and it is an obligation and an Islamic

goal."[7] Despite this strong ideological orientation, the Islamic Republic has been guarded in its opposition to the negotiations between Israelis and Palestinians. Iranian senior officials have repeatedly confirmed that they would accept whatever the Palestinians accept in their negotiations with the Israelis.

Meanwhile, Israel has sought to portray itself as "the West's first line of defense against the threat of both Sunni and Shiite Islamists."[8] In the last few decades, the strategic landscape in the Middle East has strongly turned in favor of Israel. Domestically, the Israeli standard of living is similar to or higher than many in Europe. The economy is one of the fastest growing in the world, and the nation has emerged as a major hub for foreign investment, particularly in the area of information technology (IT), earning it the title "start-up nation." Militarily, the country is the only nuclear power in the Middle East, and the Israel Defense Forces (IDF) are by far the strongest in the region.

There is nuclear deterrence because adversaries have a good understanding of each other's nuclear weapons. On the other hand, a cyber arsenal is usually shrouded in secrecy, for fear adversaries would develop countermeasures if even basic capabilities were known.

The balance of power between Israel and its Arab rivals has turned strongly in favor of Jerusalem. The three major traditional ones, Egypt, Iraq and Syria, have lost much of their leverage. With a population of more than 100 million and limited economic resources, Cairo faces daunting challenges. Since 1980, Baghdad has been in wars against Iran, the United States and the Islamic State (ISIS); Iraq has a long way to go before it can hope to resume its regional leadership status. Finally, since 2011, Syria has been mired in civil war and, despite the recent gains by President Bashar al-Assad, its future is uncertain. By contrast, the Gulf Cooperation Council (GCC) states of Bahrain, Saudi Arabia and the United Arab Emirates seem eager to normalize relations with Israel; some of their leaders see Iran and political Islam, not Israel, as their main enemies. Crown Prince Mohammed bin Salman needs some time to consolidate power and implement necessary economic and political reforms before Saudi Arabia can become a regional power.

Globally, Israel has always enjoyed special relations with the United States, but President Trump has proven himself the best friend Israel has ever had in the White House. Arguably, the Trump administration has given Netanyahu carte blanche, with almost no restrictions on his expansionist policies. At the same time, Netanyahu has developed close ties with other world leaders, including Vladimir Putin of Russia, Xi Jinping of China and Narendra Modi of India, among others. Additionally, Israel is building economic and diplomatic relations in Africa and Latin America.

This emerging picture does not mean everything is moving in the direction Israel prefers. Jerusalem faces serious challenges, including domestic corruption and political polarization. The nation's peace treaties with Egypt, Jordan and the Palestinian Authority are at risk due to its

plan to annex large parts of the West Bank and Jordan Valley. Equally important, the Israeli leaders have not been able to reach a consensus on how to deal with the "demographic bomb," the large and growing number of Arab-Israeli citizens.

Despite these domestic hurdles, Israel has emerged as a major regional power. The nation faces two regional adversaries: Turkey and Iran. Like Tehran, Ankara perceives itself as a major regional power and the leader of the Islamic world. President Recep Tayyip Erdogan and Netanyahu do not trust each other, but, rhetoric aside, Israeli tourists are welcomed in Turkey and the two nations enjoy good economic relations. Erdogan opposes Israel's control of Muslim holy sites and malign treatment of the Palestinians, but he sounds much more tolerant of Israeli policies than his counterparts in Tehran. This leaves Iran and Israel as the main opponents in the Middle East.

IRAN'S CYBER PROGRAM

Iran's investment in building strong cyber capabilities is driven by several overlapping factors. First, unlike most of its adversaries (the United States, Israel, Sunni Arab countries led by Saudi Arabia and the UAE), the Islamic Republic lacks the necessary financial resources to support conventional military forces. In 2019, defense spending per capita was $207, and 3.8 percent of gross domestic product (GDP). The comparable figures for Israel are $2,254 and 5.82 percent, respectively.[9] This does not mean, however, that Iran has no options. The cyber domain is one arena in which Tehran can challenge perceived adversaries without taxing its relatively limited resources. Indeed, cyber is one of several toolkits in Tehran's asymmetrical-warfare arsenal.

Second, Iranian leaders have always perceived their country to be in a cultural war with the United States and its allies. They have always maintained that resisting Western cultural penetration of Iranian society and protecting and promoting Islamic values have been at the heart of their revolution. Stated differently, soft power is as dangerous and effective as military force. Against this background, Tehran has been building both defensive and offensive capabilities to counter the perceived adversaries' soft power. These capabilities include censorship of domestic media and active messaging to the rest of the world in multiple languages through the Islamic Republic of Iran Broadcasting (IRIB) and many other media outlets, both online and off.

Third, like other oil-producing countries, Iran has been trying to reduce its heavy dependence on petroleum revenues and to diversify its economy. Indeed, being dependent on crude and its derivative products as the main sources of public revenues has made the nation vulnerable to international sanctions and fluctuations in oil prices. Investing in human capital and information technology is one way to build a strong economy and create jobs for hundreds of thousands of young Iranians. Trade, investment, banking and all other aspects of a modern economy depend heavily on a sophisticated technological infrastructure.

Fourth, pride is a major element behind investment in cyberspace. While nuclear technology served as a symbol of technological advance and great-power status and achievement, the cyber domain is seen around the world as cutting-edge and a harbinger of the future.[10] Cyber capabilities support the official narrative that the Islamic Republic is an emerging scientific and technological force whose achieve-

ments are on par with those of other global powers. Iran was one of the first countries in the Middle East to be connected to the Internet in the early 1990s. The nation has one of the highest Internet penetration rates in its region; the majority of its young population have regular access to the World Wide Web and mobile phones. The country takes great pride in establishing and presenting itself as a major technological hub. Sharif University of Technology, for example, is among the top universities in the region.

A major turning point in Iran's ambition to build cyber capabilities was Operation Olympic Games, in which a malware agent known as Stuxnet was used to sabotage components of the Natanz uranium-enrichment facility. This sustained campaign of sabotage, unprecedented in its sophistication and preparation, was alleged to have been a joint effort by the governments of the United States and Israel. The outcome was the destruction of over 1,000 centrifuges — setting back Iran's nuclear progress by more than a year. After another three years, in July 2010, the computer virus was discovered and publicly revealed.[11] Stuxnet was the first major piece of malware to do more than harm other computers and actually cause physical destruction. Michael Hayden, former director of the CIA, argued that the Stuxnet attack "crossed the Rubicon" by attacking another country's critical infrastructure.[12] Further attacks followed. In September 2011 and again in May 2012, two forms of advanced spyware, Duqu and Flame, respectively, were discovered on computer networks in Iran. This discovery indicated that Iran was under constant cyberattack by its enemies. In Tehran, the lessons learned about the apparent vulnerability of the country's nuclear facilities and critical infrastructure became the driving force in consolidating and expanding the country's cyber capabilities.

In March 2012, Khamenei issued a directive establishing a centralized agency responsible for managing Iran's cyber policies. Members of the new Supreme Council of Cyber Space (SCC) include the president, the speaker of parliament, the head of the judiciary, the director of the IRIB, the minister of Information and communication technology, the minister of culture and Islamic guidance, the commander of the Revolutionary Guard Corps (IRGC) and the national policy chief.[13] All state agencies are required to cooperate with the Center. Other government entities involved in cyber warfare include IRGC Electronic Warfare and Cyber Defense Organization, Basij Cyber Council, National Passive Defense Organization and Cyber Defense Command.[14]

Stuxnet was the first major piece of malware to do more than harm other computers and actually cause physical destruction.

Have these government entities been effective in projecting Iran's cyber power and defending its critical economic infrastructure and military force? Based on open sources, it is hard to arrive at an accurate assessment. Iran has been accused of being behind several cyberattacks: assaults on the websites of major U.S. banks, attacks on the Saudi Arabian Oil Co. (Aramco) by a computer virus called Shamoon, infiltration of a large unclassified computer network used by the U.S.

Navy and Marine Corps, breaking into the command-and-control system of Bowman Avenue Dam north of New York City and stealing data from the computer network of the Las Vegas Sands Corporation.[15] Furthermore, in 2016, the United States indicted seven Iranian hackers for working on behalf of the IRGC to conduct the bank attacks, and in 2017, two Iranian nationals were charged with a criminal conspiracy related to computer fraud.[16] A year later, in 2018, the U.S. Department of Justice charged nine Iranians with conducting a massive cyber-theft campaign on behalf of the IRGC. All were tied to the Mabna Institute, an Iranian company. The victims included over 300 universities, almost 50 companies and several government agencies.[17]

On the other hand, the United States is reported to have carried out a number of cyberattacks against Iran in the last few years. For example, in mid-2019, it was reported that the U.S. Cyber Command knocked out a crucial database used by the IRGC to target oil tankers and shipping traffic in the Persian Gulf after the Iranian force shot down a U.S. surveillance drone.[18] A few months later, another cyber operation was reported to have punished Iran for the September 14 attacks on Saudi Arabia's oil facilities, which Washington and Riyadh blamed on Tehran.[19] Confronted with these alleged attacks, the Iranian minister of information and communications technology, Mohammad Javad Azari, claimed that his country's home-grown cyber-security wall, known as Digital Fortress (Dejfa), was able to neutralize 33 million cyberattacks in 2019.[20]

These claims of cyberattacks and counterattacks cannot be confirmed. Neither side has ever claimed credit for the alleged attacks and, understandably, no evidence has ever been made public. Still, these allegations suggest that Iran and its adversaries will continue to build cyber capabilities and employ them against each other in the coming years.

ISRAEL'S CYBER PROGRAM

Israel's interest in cyberspace is no different from that of Iran. Jerusalem's huge investment in cyber capabilities, both civilian and military, has been driven by economic, military and strategic impulses. Unlike some Middle Eastern countries, Israel holds limited natural resources. This has left its leaders with few options but to invest in innovation, science and technology. These policies and investments have paid off; the Israelis proudly call their country the start-up nation.[21] In the annual Bloomberg Innovation Index, the country is ranked as the world's sixth-most innovative economy after Germany, South Korea, Singapore, Switzerland and Sweden.[22]

The nation's technology sector reflects a collaboration between the government (including the military), businesses and universities. Within this framework, cybersecurity and technology in general are considered an economic growth engine. In recent years, Israel has emerged as a major hub, attracting huge investments from major hi-tech multinational companies such as Alibaba, Google, Bosch, AOL, Qualcomm, Facebook, Merck, IBM and Sony.[23] Israel has some of the best universities and research centers in the Middle East, including Technion-Israel Institute of Technology, Hebrew University of Jerusalem, the Weizmann Institute of Science and Tel Aviv University.

Innovation has been considered a major necessity for security reasons. When the country was created in 1948, Israel's founding fathers sought to establish a

qualitative edge over its vastly more populated and better endowed Arab adversaries. Within this context, Israel has become the only nuclear power in the region, its military one of the most technologically advanced in the Middle East and, indeed, the entire world. Israel is a leader in the military domains of drones, missiles, missile-defense systems and electronic warfare, among others. Jerusalem has received substantial assistance from the United States and Europe in building these capabilities.

Against this background, Israel has developed a multilayered cyber strategy leveraging automated computerized systems and highly trained personnel that combine intelligence, early warning, and both defensive and offensive capabilities across civil-military domains. In 1997, Tehila (Government Infrastructure for the Internet Age, Israel's e-government project) was launched with the goal of protecting the connection of government offices to the Internet and providing secure hosting for the governmental sites.[24] The IDF identified the enormous potential of computers and engaged in various types of computer warfare as early as the 1990s. In 2002, the government issued a resolution titled "Responsibility for the Defense of Computerized Systems in the State of Israel" (Resolution 84/B), which outlined the defense principles for Israel's critical computer-supported infrastructure.[25]

In August 2011, the government issued Resolution 3611, "Advancing National Cyberspace Capabilities," in which strengthening the country's scientific and technological cyber capabilities and innovation processes was considered a critical priority.[26] A few months later, in January 2012, the Israeli National Cyber Bureau (INCB) was established. It was tasked with promoting and regulating government cyber activity, improving cyber defense for the non-defense-related sectors of the government, and expanding the state's capabilities to secure critical infrastructure systems against cyber terrorism, whether carried out by foreign nations or terrorist groups.[27] Other tasks include recommending policy changes to the government regarding cyberspace, promoting cyberspace industry, funding cyber research and development, advancing national cyber-educational programs, and articulating a cyberspace security doctrine.[28] Three years later, in February 2015, the National Cyber Security Authority (NCSA) was established, and in 2017, the Israeli National Cyber Directorate was created as the highest national authority for strategic cyber-policy planning. It consists of two arms: the INCB, which is responsible for overall strategic policy planning in the realm of capacity building, and second, the NCSA, which is responsible for national-level implementation and regulation of critical infrastructures. In short, the Israel National Cyber Directorate is responsible for all aspects of cyber defense in the civilian sphere, from formulating policy and building technological power to managing operational defense in cyberspace.[29]

In addition to the civilian sphere, cyber operations play a prominent role in the military domain. Initially, cybersecurity was conceptualized along the lines of information warfare. Understandably, specific details of military cyber units and capabilities are not publicly available. Still, since the late 2000s, the IDF has considered cyberspace a strategic and operative combat zone. The Intelligence Corps Unit 8200, which deals with national signals intelligence (SIGINT) and code decryption, plays a leading role in military cyber

operations.[30] A cyber unit within 8200 was established in 2009, entrusted with developing and deploying offensive cyber weapons.[31] The C41 Directorate (command, control, computers, communications and intelligence) is responsible for preventing and detecting infiltration into military networks.

THE WAY FORWARD

Several conclusions can be drawn from Iranian and Israeli policies in cyberspace. They are likely to shape their strategic rivalry as well as economic and political stability in the broader Middle East. First, there is no way to provide an accurate assessment of the two countries' cyber power. Unlike they do for traditional military forces (air, naval and ground), nation states do not disclose information on their cyber weapons. Because they are rarely acknowledged publicly, cyber strikes are much like covert operations. Rather, a close examination of Tehran's and Jerusalem's cyber policies shows the huge investments they have made in building their capabilities and underscores their determination to use them, both defensively and offensively. Stated differently, cyber warfare has been integrated into the broad defense strategies of both the Islamic Republic and the Jewish state.

Second, the digital confrontation between the two is likely to intensify in the coming years. A key element of deterrence is ensuring that an adversary knows the other side's basic capabilities. There is nuclear deterrence because adversaries have a good understanding of each other's nuclear weapons. On the other hand, a cyber arsenal is usually shrouded in secrecy, for fear adversaries would develop countermeasures if even basic capabilities were known. Thus, in the absence of cyber deterrence and a lack of internationally recognized regulations, both Tehran and Jerusalem are likely to further employ their capabilities against each other and against other countries.

Third, an all-out war between Iran and Israel is not likely but cannot be ruled out. Global powers (i.e., the United States, Russia, China and Europe) and neighboring states understand that an Iranian-Israeli war would deal a heavy blow to economic and political stability in the broader Middle East/South Asia region and trigger immigrant and refugee crises. Being under an American "maximum pressure" campaign and trying to recover from the coronavirus, Iran does not wish to start a war. Meanwhile, Israeli leaders, with strong support from Washington, Riyadh and Abu Dhabi, seem satisfied to mount economic and military pressure on Tehran, hoping for a "regime change." This low-cost strategy seems a better option than a costly and uncertain full-scale war. However, history teaches us that wars usually start because of miscalculation by one or both sides. Given this uncertain strategic environment, both Tehran and Jerusalem are likely to further employ low-cost cyber operations.

Fourth, the digital confrontation between Iran and Israel is not likely to be restricted to the two of them. Neighboring countries are likely to become involved. The GCC states — Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the UAE — are trying to implement economic reform and reduce their heavy dependency on oil revenues. Thus, the more digital their economies and societies become, the more vulnerable they are to cyberattacks. The GCC states have already reported numerous cyberattacks on their critical economic infrastructure.

Finally, given the rhetoric from both Ira-

nian and Israeli leaders in the last several years, it is hard to imagine peace or détente between the two regional rivals. Therefore, neighboring Sunni-Arab countries and global powers need to invest in diplomacy to reduce the hostility between Tehran and Jerusalem. The ongoing tension is being felt and played out in Lebanon, Iraq, Syria and other countries. In recent years, there have been signs of warming relations between Israel, on one side, and Bahrain, Oman, Saudi Arabia and the UAE, on the other. This growing cooperation should not be used to form a new axis against Iran, while there are no credible signs of regime collapse in Tehran. Diplomatic efforts to reduce tension among the regional powers and acknowledge their legitimate security concerns would reduce incentives for a destructive cyber confrontation.

[1] "Israeli Cyber Chief Says Major Attack on Country's Water Systems Foiled," *Haaretz*, May, 28, 2020, https://www.haaretz.com/misc/article-print-page/israeli-cyber-chief-says-major-attack-on-country-s-water-systems-foiled-1.8878952.
[2] Yonah Jeremy Bob, "Israeli Cyber Czar Warns of More Attacks From Iran," *Jerusalem Post,* May 28, 2020 https://www.jpost.com/israel-news/israeli-cyber-czar-warns-of-more-attacks-from-iran-629577.
[3] Joby Warrick and Ellen Nakashima," Cyberattack on Iranian Port is Attributed to Israel," *Washington Post,* May 18, 2020, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html.
[4] Michael Brecher, *The Foreign Policy System of Israel: Setting, Images, Process* (New Haven: Yale University Press, 1972).
[5] Gawdat Bahgat, *Israel and the Persian Gulf: Retrospect and Prospect* (Florida: University Press of Florida, 2006).
[6] R.K. Ramazani, "Iran and the Arab-Israeli Conflict," *Middle East Journal* 32, no.4 (Fall 1978): 413-28.
[7] "Leader Offers Seven Guidelines to Liberate Palestine: Continuing Resistance and Resisting Normalization," IRNA News Agency, May 22, 2020, https://en.irna.ir/news/83797090.
[8] Anoushiravan Ehteshami and Raymond A. Hinnebusch*, Syria and Iran: Middle Powers in a Penetrated Regional System,* (London: Routledge, 1978)
[9] International Institute for Strategic Studies, *The Military Balance* (London: Routledge & Taylor & Francis, 1978).
[10] Michael Eisenstadt, "Iran's Cyber Capabilities," *Iran Primer,* August 5, 2016, http://iranprimer.usip.org/blog/2016/aug/05/report-iran%E2%80%99s-cyber-capabilities. Accessed August 5, 2016.
[11] Eric K. Shafa, "Iran's Emergence as a Cyber Power," Strategic Studies Institute, August 20,2014, https://www.hsdl.org/?view&did=757312.
[12] Barbara Slavin and Jason Healey, "Iran: How a Third Tier Cyber Power Can Still Threaten the United States," Atlantic Council, July 29, 2013, http://www.atlanticcoundil.org/publications/issue-brief.
[13] "The Supreme Council of Cyberspace: Centralizing Internet Governance in Iran," Iran Media Research Organization, April 13, 2008, https://asl19.org/en/blog/2013-04-09-the-supreme-council-on-cyberspace-centralizing-internet-governance-in-iran.html. http://www.iranmediaresearch.org/en/blog/227/13/04/08/1323.
[14] Catherine Theohary, "Iranian Offensive Cyber Attack Capabilities," Congressional Research Service, January 13, 2020, https://crsreports.congress.gov/product/pdf/IF/IF11406.
[15] "Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad," Cybersecurity & Infrastructure Security Agency, January 6, 2020, https://www.us-cert.gov/ncas/alerts/aa20-006a.
[16] "Two Iranian Nationals Charged in Hacking of Vermont Software Company," Department of Justice, July 17, 2017, https://www.justice.gov/opa/pr/two-iranian-nationals-charged-hacking-vermont-software-company.

[17] Dorothy Denning, "Explainer: How Iran's Military Outsources its Cyberwarfare Forces, *Navy Times,* January 23, 2020, https://www.navytimes.com/news/your-navy/2020/01/23/explainer-how-irans-military-outsources-its-cyberwarfare-forces.
[18] Julian E. Barnes and Thomas Gibbons-Neff, "U.S. Carried Out Cyberattacks on Iran," *New York Times*, June 22, 2019, https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html.
[19] Idrees Ali and Phil Stewart, "Exclusive: U.S. Carried Out Secret Cyber Strike on Iran in Wake of Saudi Oil Attack: Officials," Reuters, October 16, 2019, https://www.reuters.com/article/idUSKBN1WV0EK.
[20] "Minister: Iran Repels Massive State-Sponsored Cyberattack Against Infrastructures," *Fars News Agency,* December 11, 2019, https://en.farsnews.com/print.aspx?nn=13980920000464.
[21] Dan Senor and Saul Singer, *Start-Up Nation: The Story of Israel's Economic Miracle* (Washington DC: Council on Foreign Relations).
[22] Michelle Jamrisko and Wei Lu, "Germany Breaks Korea's Six Year Streak as Most Innovation Nation," *Bloomberg,* January 18, 2020, https://www.bloomberg.com/news/articles/2020-01-18/germany-breaks-korea-s-six-year-streak-as-most-innovative-nation.
[23] "Foreigners Made 77% of Investments in Israeli Tech Firms in Past Two Years," *Times of Israel,* November 27, 2018, https://www.timesofisrael.com/foreigners-made-77-of-investments-in-israeli-tech-firms-in-past-two-years/.
[24] "Background For the Establishment of the Bureau," April 19, 2019, http://www.pmo.gov.il/english/primeminstersoffice/divisionandauthorities/cyber/pages/background.aspx.
[25] Gil Baram, "Israeli Defense in the Age of Cyber War," *Middle East Quarterly* 24, no.1 (Winter 2017): 1-10.
[26] Lior Tabansky, "Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defense Strategy," Rajaratnam School of International Studies, January 20, 2015, https://www.rsis.edu.sg/wp-content/uploads/2015/01/PR150108_-Israel_Evolving_Cyber_Strategy_WEB.pdf.
[27] "The Partnership," Ben-Gurion University, accessed June 10, 2020, https://cyber.bgu.ac.il/israel-national-cyber-bureau.
[28] Matthew S. Cohen, Charles D. Freiligh and Gabi Siboni, "Israel and Cyberspace: Unique Threat and Response," *International Studies Perspective* 17, no.4 (2016): 307-321.
[29] "About the Directorate", Israel National Cyber Directorate, accessed June 10, 2020, https://www.gov.il/en/departments/israel_national_cyber_directorate.
[30] Geoffrey Ingersoll, "The Best Tech School on Earth is Israeli Army Unit 8200, "*Business Insider,* October 13, 2013, https://www.businessinsider.in/the-best-tech-school-on-earth-is-israeli-army-unit-8200/articleshow/21813110.cms.
[31] Michael Raska, "Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defense Strategy," Rajaratnam School of International Studies, January 2015, https://www.michaelraska.de/download/Israel's_Evolving%20Cyber%20Strategy_Raska.pdf.