PART 2:
IRAN'S CYBER STRATEGY, INSTITUTIONS, AND CAPABILITIES

In the early 2010s, two primary factors led Iran to rapidly develop its heretofore limited cyber capabilities. The first was the effective use of the internet by the Iranian opposition to foment and sustain the mass demonstrations following the rigged presidential elections in 2009. The regime ultimately succeeded in suppressing the protests but also gained a healthy appreciation of the threat that the new technology posed to its stature and stability.[21] The second factor was the dramatic Stuxnet attack against Iran's nuclear program in 2010, reportedly a joint US–Israeli cyber sabotage operation. Stuxnet, the first known case of a cyberattack that caused physical damage, demonstrated Iran's extreme vulnerability and led to a severe national shock. In response, Iran rapidly accelerated the development of its then only nascent cyber capabilities.[22]

Experts concur that Iran's cyber capabilities have progressed considerably ever since but they disagree on its actual level of sophistication. Some believe that Iran has not developed a sophisticated cybersecurity ecosystem, suffers from a severe brain drain, and has not achieved the level of professionalism required of an advanced actor. These experts believe that important American, European, and Israeli targets are defended at a level that exceeds Iran's

21 Collin Anderson and Karim Sadjadpour, *Iran's Cyber Threat: Espionage, Sabotage and Revenge* (Carnegie Endowment for International Peace, 2018), 10–11; Gabi Siboni and Sami Kronenfeld, "Iran and Cyberspace Warfare," in *Cyberspace and National Security – Selected Articles*, ed. Gabi Siboni (Tel Aviv: Institute for National Security Studies, 2013), 81–103; Kristina Kausch and Lior Tabansky, "Cybered Conflict in the Middle East," Mediterranean Dialogue Series No. 15 (Konrad Adenauer Stiftung, 2018), 9; Gabi Siboni, Léa Abramski, and Gal Sapir, "Iran's Activity in Cyberspace: Identifying Patterns and Understanding the Strategy," *Cyber, Intelligence and Security* 4, no. 1 (2020): 22.

22 Sanger, *The Perfect Weapon,* 46–49; Segal, *Hacked World Order*, 5; Sam Jones, "Cyber Warfare: Iran Opens a New Front," *Financial Times*, April 26, 2016; Siboni and Kronenfeld, "Iran and Cyberspace Warfare."

capabilities. Some experts believe that Israel's presumed sophisticated cyber defenses have diminished Iran's ability to cause significant damage to Israel and that it remains a third-tier cyber power. If true, this would explain why most Iranian cyberattacks to date have focused on the "low hanging fruit," i.e., poorly defended sites that it attacks with comparatively unsophisticated means.[23]

Others believe that Iran is now at the top of the second tier of global cyber powers, with aspirations to join the frontrunners. The 2022 US Worldwide Threat Assessment stated that "Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied networks and data."[24] A former head of Israel's National Cyber Directorate (INCD) maintains that Iran is one of the five most active states in the cyber realm and that it is one of the few states that conducts attacks not just for intelligence and influence purposes but for destructive ones as well.[25]

Proponents of this latter approach maintain that Iran has actually invested heavily in its cyber ecosystem, including schools and universities. By 2016 Iran was reportedly spending over $1 billion annually on its cyber capabilities, compared, for example, with $2 billion by the United Kingdom, one of the world's leading cyber powers. According to Iranian data, Iran's cyber budget jumped twelvefold during between 2013–2021 and a five-year plan discussed in 2020 raised the possibility of a further increase in Iran's digital economy from 6.5 percent of GDP to 10 percent by 2025. As of the late 2010s, some 18

23 Anderson and Sadjadpour, *Iran's Cyber Threat,* 13, 14, 31, 35–36, 52; International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," Research Papers (June 28, 2021); David Shamah, "Official: Iran, Hamas Conduct Cyber-Attacks Against Israel," *Times of Israel*, August 13, 2015.

24 Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," (2022), 1.

25 Siboni, Abramski, and Sapir, "Iran's Activity in Cyberspace," 22; Robert McMillan, "Iranian Hackers Have Hit Hundreds of Companies in Past Two Years," *Wall Street Journal*, March 6, 2019; Jones, "Cyber Warfare"; Office of the Director of National Intelligence, "Annual Threat Assessment of the US Intelligence Community," (2021), 14.

percent of Iranian university students were reportedly studying computer science, and compulsory military service was used as a means of channeling technologically sophisticated graduates to the state security apparatus, including the Ministry of Intelligence and the Islamic Revolutionary Guard Corps (IRGC).[26]

In 2012 Iran was one of the first states to establish the institutions necessary to implement a national cyber strategy. The Supreme Cyber Space Council was charged with responsibility for planning and implementing an integrated national cyber strategy.[27] The National Cyber Center coordinates Iran's overall cyber activities, gathers and disseminates relevant information and policy directives, and oversees policy implementation. The National Passive Defense Organization is responsible for defending critical national infrastructure and the Cyber Defense Command coordinates the military's (Artesh) cyber operations. The Maher Information Security Center is Iran's computer emergency response team. The Committee for Identifying Unauthorized Sites and FATA (Persian acronym for the Police for the Sphere of the Production and Exchange of Information) serve as cyber police, monitoring internet usage both for purposes of domestic suppression and countering cybercrime.[28] All of the above is in

26 Jones, "Cyber Warfare"; Siboni, Abramski, and Sapir, "Iran's Activity in Cyberspace," 22; International Institute for Strategic Studies, "Cyber Capabilities"; Pierre Pahlavi, "Digital Hezbollah and Political Warfare in Cyberspace," *National Interest*, October 31, 2022; Michael Sulmeyer, *Cyberspace: A Growing Domain for Iranian Disruption* (Washington DC: Center for Strategic and International Studies, 2017), 38.

27 The Council's membership includes the president, speaker of the Parliament, head of the Islamic Republic of Iran Broadcasting, commander of the Armed Forces, commander of the IRGC, minister of defense, minister of information and communications technologies, and others.

28 Congressional Research Service, "Iranian Offensive Cyber Attack Capabilities" (January 13, 2020); Jordan A. Brunner, "The (Cyber) New Normal: Dissecting President Obama's Cyber National Emergency," *Jurimetrics Journal* 57 no. 3 (2017): 397–431; Ersin Cahmutoğlu, *Iran's Cyber Power* (Ankara: iRAM: Center for Iranian Studies, April 2021), 14–15; Giacomo Spadoni, "IRGC Cyber-Warfare Capabilities," (International Institute for Counterterrorism, 2019).

addition to the long-existing Ministry of Intelligence and Security, responsible for signals intelligence and the Ministry of Information and Communications Technology.

By 2015 the IRGC had reportedly recruited thousands of personnel and had become the dominant cyber actor in Iran. Its Electronic Warfare and Cyber Defense Organization bears primary responsibility for offensive cyber operations. The IRGC also provides operational direction and support for the cyber operations of Iranian proxies, such as Hezbollah.[29]

The Basij, a paramilitary force under the IRG and that is responsible for domestic order, claims to have 1,000 cyber battalions around the country. The Basij outsources cyberattacks to some 50 different hacktivist groups, which operate independently, compete for contracts, and have their own modus operandi and targets. Some of the better known of these groups are the Iranian Cyber Army, Islamic Cyber Resistance Group, and the Ashiyane Digital Security Team. Other examples are the various "Kittens" groups.[30] Flying Kittens gather intelligence on foreign governments and corporations of interest; Magic Kittens target domestic dissidents; Domestic Kittens target dissidents in Iran, the United States, United Kingdom, and more; Charming Kittens use social networking platforms to reach various targets; and Cutting Kittens produce website penetration tools. Basij cyber activities are coordinated by the Basij Cyber Council. Some of these activities are also conducted through three "institutes": Mabna, Rana, and Nasr. Mabna assists Iranian universities

29 Congressional Research Service, "Iranian Offensive Cyber Attack Capabilities"; Brunner, "The (Cyber) New Normal"; Siboni and Kronenfeld, "Iran and Cyberspace Warfare," 82, 87–88; Cahmutoğlu, *Iran's Cyber Power*, 14–15.

30 The "Kittens" names, like those of most cyberattacks, have been assigned by the leading global cyber security firms as a means of identification. Most of these groups are also known by various other terms. Charming Kittens, for example, are referred to as APT 35, and other groups have different APT numbers. Static Kittens are also known as MuddyWater.

and scientific and research organizations to gain access to foreign scientific resources.[31]

As in other areas of asymmetric warfare, Iran takes a variety of measures to camouflage its cyber operations and maintain plausible deniability. Malware that has been publicly attributed to Iran is frequently abandoned upon exposure. Membership in the above groups changes continually, leading to a blurring of the lines between them. The IRGC reportedly employs trusted intermediaries to outsource contracts to them, as a means of further masking its tracks, at times employing several contractors for a single operation. The command structure between the IRGC, Basij, and hacktivist groups is fluid, making their activities particularly unpredictable and difficult to assess. This obscurity is further exacerbated by the opaque nature of Iran's decision-making processes and of the control the regime exercises over the security apparatus. At a minimum, the hacktivist groups appear to enjoy tacit approval from Iran's political and security establishments.[32]

Iran's cyber strategy evolved in three primary stages. Stage 1, from 2009–2011, was the wake-up call and initial response to the demonstrations following the 2009 elections and to the Stuxnet attack the year after. Stage 2, from 2012–2018, saw the establishment of the above cyber institutions, the beginning of cyber cooperation with Russia and China, and the transitioning from largely defensive cyber operations to offensive ones—primarily for intelligence purposes. In Stage 3, from 2019 to the present, Iran built a bank

31 Jones, "Cyber Warfare"; Congressional Research Service, "Iranian Offensive Cyber Attack Capabilities"; Anderson and Sadjadpour, *Iran's Cyber Threat,* 17; International Institute for Strategic Studies, "Cyber Capabilities and National Power"; Tom Brewster, "Persian Paranoia: America's Fear of Iranian Cyber Power," *The Guardian*, August 29, 2014; Cahmutoğlu, *Iran's Cyber Power*, 15; Gordon Corera, "Iran 'Hides Spyware in Wallpaper, Restaurant and Games Apps,'" *BBC News*, February 8, 2021.

32 Jones, "Cyber Warfare"; Sulmeyer, *Cyberspace*, 39; Dorothy Denning, "Explainer: How Iran's Military Outsources its Cyberwarfare Forces," *Navy Times*, January 23, 2020; Anderson and Sadjadpour, *Iran's Cyber Threat,* 13.

of infrastructure, defense-related, and other targets around the world, and further expanded its offensive operations. This has been especially true in the areas of information operations and in many cases of combined CNA, CNE, CNI, and ransomware attacks.[33] As will be seen, much of Iran's cyber activities over the years have been of a reactive nature, in response to attacks it attributed to Israel or the United States.

For Iran, the United States has posed the greatest threat to its national security and the only existential threat to the future of the Islamic Republic. Israel is perceived as a severe and particularly active threat, but not an existential one.[34] Other states in the region, especially in the Gulf, are also considered significant threats, although somewhat mitigated by the recent easing of tensions in the spring of 2023. Iran's threat perception and national security strategy are rooted in a nearly all-pervasive sense of weakness and vulnerability, stemming from the failed chapters of Iranian and Persian history, and the recognition that Iran's limited conventional capabilities are no match for those of its primary adversaries.

This deep-seated sense of weakness has led to the resolve not only to deter and defend Iran against its enemies but also to develop effective offensive capabilities with which to promote its interests and to extend its influence abroad. Asymmetric warfare has long comprised a critical component of Iran's national security strategy, designed to offset the advantages of its more powerful adversaries, and cyber has gained an important role therein. Cyber is particularly suited to Iran's strategic culture, which emphasizes ambiguity,

33 Danny Citrinowicz and Jason Brodsky, "Iran's Cyberspace Evolution," *The Dispatch*, April 12, 2022; Boaz Dolev and David Siman-Tov, "Iranian Cyber Influence Operations Against Israel Disguised as Ransomware Attacks," INSS Special Publication, January 27, 2022.

34 Ali Akbar, "Iran's Regional Influence in Light of its Security Concerns," *Middle East Policy* 28 no. 3–4 (2021); Raz Zimmt, "The Israeli Threat—The View From Iran," *Bein HaKtavim*, Dado Center for Interdisciplinary Military Research, forthcoming fall 2023.

deniability, and the use of proxies.[35] To this end, Iran has developed offensive cyber capabilities for purposes of disruption and destruction, espionage, and information operations.

For Iran, the internet and cyber realm, as a whole, are a mixed blessing. They constitute subversive instruments for the propagation of Western values and domestic opposition, and thus pose potential threats to the regime's stability and survival—Iran's foremost objective. At the same time, the internet has also proven to be an effective means of shaping public opinion and of exerting popular control. To this end, and much like its authoritarian models—China, Russia, and North Korea—Iran has created a sizable and effective cyber propaganda machine for disseminating regime policies and Shiite dogma in Iran and abroad.[36]

Iran has succeeded in gaining relatively effective control over its national cyberspace. Following the Chinese model, Iran established a separate national intranet, the National Information Network (NIW). The NIW project began in 2009, when the regime directed domestic companies to begin moving network activities to servers and data centers situated in Iran itself, with the objective of ultimately hosting all Iranian websites there. Iran reportedly also developed an independent email service, operating system, search engine, and other tools for use on the NIW. Although the NIW was formally completed

35 Ariane M. Tabatabai, *Iran's Authoritarian Playbook: The Tactics, Doctrine, and Objectives behind Iran's Influence Operations* (Washington DC: Alliance for Securing Democracy, 2020), 3, 8; Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Rowman and Littlefield, 2017), 41; Kausch and Tabansky, "Cybered Conflict in the Middle East," 8; Micah Loudermilk, "Iran Crisis Moves Into Cyberspace," Policy Watch 3151, *Washington Institute for Near East Policy* (July 9, 2019); Siboni and Kronenfeld, "Iran and Cyberspace Warfare," 81–82; Anderson and Sadjadpour, Iran's Cyber Threat, 12.

36 Loudermilk, "Iran Crisis"; Sulmeyer, *Cyberspace*, 34–35; Siboni and Kronenfeld, "Iran and Cyberspace Warfare," 81–103; Siboni, Abramski, and Sapir, "Iran's Activity in Cyberspace," 35.

in 2016, the work is ongoing, and a new cloud infrastructure project and data center were inaugurated in 2020.[37]

The NIW has enabled Iran to more effectively counter foreign cultural and political influences, monitor and identify sources of malicious activity, and reduce its vulnerability both to external cyberattack and domestic opposition. In 2019, at the height of the protests that year—possibly the greatest challenge the regime had faced until then—the NIW shut down internet access throughout Iran for a week. In so doing, the regime prevented the opposition from further mobilizing and was able to hide evidence of the extraordinary measures taken to suppress it, including the reported killing of hundreds and jailing of thousands.[38] The NIW was used once again, to considerable effect, in suppressing the even more severe protests in late 2022, following the killing of a young woman who had refused to cover her hair with a scarf, as required by Iranian law. The internet and cellular access of millions of Iranians was disrupted to frustrate efforts in organizing the protests and to slow their momentum.[39]

Iran has conducted cyber operations designed to promote its primary national objectives, the most important of which, by far, is ensuring the stability and longevity of the Islamic Republic. Additional objectives include preserving Iran's Islamic values and strictures; defense of its territorial integrity and population; promoting socioeconomic growth and the welfare of the Iranian people; propagating Iran's theology and influence throughout the region; achieving regional hegemony; maintaining strong international ties

37 Mahsa Alimardani, "Iran Declares 'Unveiling' of its National Intranet," *Advox*, September 2, 2016; Siboni and Kronenfeld, "Iran and Cyberspace Warfare," 81–103.

38 Lily Hay Newman, "How the Iranian Government Shut Off the Internet," *Wired*, November 17, 2019; Carol Morello and Missy Ryan, "U.S. Says Iranian Forces May Have Killed More Than 1,000 Protestors," *Washington Post*, December 5, 2019.

39 Vivian Lee, "Despite Iran's Efforts to Block Internet, Technology Has Helped Fuel Outrage," *New York Times*, September 29, 2022; Benoit Faucon, "Iran Restricts Internet Access as Women's Rights Protests Spread," *Wall Street Journal*, September 22, 2022.

and recognition as an important global power; countering US efforts to contain Iran, especially regarding the nuclear issue; undermining American influence in the region;[40] and countering, weakening, and ultimately destroying Israel.

International Cooperation

Cooperation with foreign actors, chiefly Russia and China, has contributed significantly to Iran's cyber capabilities. In 2015 Russia and Iran concluded their first cyber cooperation agreement, soon followed by a number of more substantive ones. An IRGC cyber defense system, reportedly developed with Russian and possibly Chinese assistance, may have become operational in 2015.[41] In 2016 Russia and Iran agreed to cooperate on "de-monopolizing…unilateral Western domination" of software, a possible indication of Iran's interest in a Russian alternative to Microsoft's Windows and Office software. In 2017 a memorandum of understanding (MoU) on information and communications technology (ICT) cooperation included "internet governance, network security… and international internet connection." At Iran's initiative, a bilateral committee on media cooperation was established in 2018 to combat "Western media terrorism." The committee had been formed as part of another MoU that provided measures designed to promote favorable mutual media coverage, increase coproduction of content, counter Western media narratives, and broaden cooperation on means of targeting foreign audiences.[42]

In 2019–2020 bilateral Russian and Iranian working groups were established to provide Iran with capabilities designed to track citizens through facial recognition and other technologies; promote cooperation in 5G networks and AI; and increase Russian investment in Iranian cyber firms, including possible multilateral investments with Turkey and Azerbaijan. In 2020 an

40 Tabatabai, *Iran's Authoritarian Playbook*, 3, 6–8; Anderson and Sadjadpour, *Iran's Cyber Threat,* 42.

41 Cyber Threat Brief, *Flash Critic*, November 29, 2015.

42 John Hardie and Annie Fixler, "Russia-Iran Cooperation Poses Challenges for US Cyber Strategy, Global Norms," *C4ISR*, February 8, 2021.

agreement was reached to counter "increasing information pressure from the West…designed to discredit Russia and Iran."[43]

An even broader bilateral "Information Security Cooperation Pact" was signed in 2021. The pact reportedly covered cybersecurity and technology transfers, including measures to detect cyberattacks; suppression of domestic dissent; diplomatic coordination in the UN and other multilateral forums to promote international cyber norms and law that were in accord with Russian and Iranian interests; and possible provision of advanced Russian surveillance software to Iran for hacking phones and computers of dissidents and adversaries. Without direct evidence, it was thought that Iran may have passed some of the technologies and methodologies acquired from Russia to Hezbollah and other allied militias.[44]

The war in Ukraine has led to a further deepening of strategic cooperation between Iran and Russia, and various reports indicate that this may encompass the cyber area as well. Details are scarce, and it is unclear to what extent this cooperation goes beyond previously existing agreements. One possible indication is the apparent involvement of Russian-affiliated hackers in Iranian cyberattacks against Israel, as part of the annual #OpIsrael and Jerusalem Day campaign (see below).[45]

Chinese firms have also invested heavily in Iran's cyber infrastructure. In 2021 China and Iran concluded a major 25-year strategic cooperation agreement that provides, inter alia, for Chinese assistance in building

43 Hardie and Fixler, "Russia-Iran Cooperation"; Setareh Behroozi, "We are in Iran for Cooperation, not to Sign Memorandums: Russian Official," *Tehran Times*, June 24, 2019.

44 Omree Wechsler, "The Iran-Russia Cyber Agreement and U.S. Strategy in the Middle East," *Council on Foreign Relations*, March 15, 2021; Morgan Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack Landscape," *IronNet*, September 15, 2021; Hardie and Fixler, "Russia-Iran Cooperation"; Dov Lieber, Benoit Faucon, and Michael Amon, "Russia Supplies Iran With Cyber Weapons as Military Cooperation Grows," *Wall Street Journal*, March 27, 2023.

45 Lieber, Faucon, and Amon, "Russia Supplies Iran"; Avi Davidi, "Iranian-Russian Cooperation on Hack Attacks May Challenge Israeli Cyber Supremacy," *Times of Israel*, April 18, 2023.

Iran's 5G telecommunications infrastructure; access to China's new global positioning system, Beidou; and help in asserting greater Iranian control over its cyberspace, possibly by further strengthening the NIW. China may have also agreed to provide Iran with new cyber capabilities, including those necessary for intelligence collection.[46] Chinese firms have sold camera and AI capabilities to the IRGC and Basij militia. The technology was initially designed for traffic enforcement but was repurposed during the mass demonstrations in late 2022 to enforce Iran's dress code for women and to identify and arrest demonstrators.[47]

46 Farnaz Fassihi and Steven Lee Myers, "Defying U.S., China and Iran Near Trade and Military Partnership," *New York Times*, July 11, 2020; Farnaz Fassihi and Steven Lee Myers, "China, With $400 Billion Iran Deal, Could Deepen Influence in Mideast," *New York Times*, March 27, 2021; Eyal Pinko, "Iranians Developing the Cyber Capabilities of Hezbollah," *Israel Defense*, March 30, 2021; Golnaz Esfandiari, "Iran to Work With China to Create National Internet System," *Radio Free Europe*, *Radio Liberty*, September 4, 2020.

47 Benoit Faucon and Liza Lin, "U.S. Weighs Sanctions for Chinese Companies Over Iran Surveillance Buildup," *Wall Street Journal*, February 4, 2023; Michael Lee, "Chinese Facial recognition Technology Helping Iran to Identify Women Breaking Strict Dress Code: Report," *Fox News*, January 12, 2023.