MARCH 2017

Deterring Iran after the Nuclear Deal

PROJECT DIRECTORS AND EDITORS

Kathleen H. Hicks
Melissa G. Dalton

CONTRIBUTING AUTHORS

Melissa G. Dalton
Jon B. Alterman
Michael Connell
Michael Eisenstadt
Farideh Farhi
Kathleen H. Hicks
Thomas Karako
J. Matthew McInnis
Hijab Shah
Michael Sulmeyer
Ian Williams

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

ROWMAN & LITTLEFIELD

Lanham • Boulder • New York • London

04

Cyberspace: A Growing Domain for Iranian Disruption

Michael Sulmeyer

ROLE OF CYBER TOOLS IN IRAN'S BROADER STRATEGY

A senior Iranian Islamic Revolutionary Guard Corps (IRGC) official described a war in cyberspace as "more dangerous than a physical war."[1] This statement was likely made in 2012, in response to a wave of publicly reported cyber operations against Iran, including Stuxnet,[2] Duqu,[3] and Flame.[4] Since these operations, Iran has expanded the role of cyber capabilities in its broader national security strategy.

Iran uses its cyber capabilities to expand the regime's control over the information to which its population has access.[5] The Iranian leadership exercises its power in cyberspace to censor and block certain forms of social media content, and to surveil individuals and organizations of concern to the state.[6] Its control of information also enables the regime to leverage cyberspace to further a narrative for its domestic audience that frames Iran as a growing technological power, able to

1. "Iran Sees Cyber Attacks as Greater Threat than Actual War," Reuters, September 25, 2012, http://www.reuters.com/article/iran-military-idUSL5E8KP7HV20120925.

2. Nicolas Falliere, Liam O Marchu, and Eric Chien, "W32.Stuxnet Dossier," *Symantec Report 2011*, February 2011, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

3. Ibid.

4. Ellen Nakashima, Greg Miller, and Julie Tate, "U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say," *Washington Post*, June 19, 2012, https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html. See also Dan Goodin, "Confirmed: Flame Created by US and Israel to Slow Iranian Nuke Program," *Ars Technica*, June 19, 2012, http://arstechnica.com/security/2012/06/flame-malware-created-by-us-and-israel/.

5. Michelle Moghtader, "Iran Expands 'Smart' Internet Censorship," Reuters, December 26, 2014, http://www.reuters.com/article/us-iran-internet-censorship-idUSKBN0K40SE20141226.

6. Matthew Carrieri, Ali Karimzadeh Bangi, Saad Omar Khan, and Saffron Suud, *After the Green Movement: Internet Controls in Iran, 2009–2012* (Toronto: OpenNet Initiative, 2013), https://opennet.net/blog/2013/02/after-green-movement-internet-controls-iran-2009–2012.

defend its internal networks and exploit its rivals' vulnerabilities by compromising high-profile commercial and government institutions.[7]

The Iranian regime also considers cyberspace a domain in which it needs to defend itself, especially after the aforementioned cyber operations against Iran became publicly known.[8] Because these operations compromised Iranian nuclear, shipping, and other infrastructure facilities, the need to elevate their cyber defense strategy became a growing priority.[9]

Iran also employs cyber capabilities offensively to impose costs on its rivals in the Middle East and in the West. U.S. deputy secretary of defense Robert Work testified that "Iran very likely views its cyber program as one of many tools for carrying out asymmetric but proportional retaliation against political foes."[10] Prominent examples include destructive cyberattacks against Saudi Aramco and Qatar's RasGas, as well as disruptive denial-of-service activities against the U.S. financial sector.[11] In these and other cases, Iran employed cyber capabilities to support longer-term efforts to attack its rivals.

---

7. Shane Harris, "Forget China, Iran's Hackers Are America's Newest Cyber Threat," *Foreign Policy* (February 18, 2014), http://foreignpolicy.com/2014/02/18/forget-china-irans-hackers-are-americas-newest-cyber-threat/. The article explains that "Iran was motivated to ramp up its cyber security efforts, particularly the defense of its internal networks and vital infrastructure facilities, after a cyberattack on an Iranian nuclear facility by the United States and Israel that disabled 1,000 centrifuges used to enrich uranium, a key component of a nuclear weapon. Iran's defensive capabilities today are devoted to preventing another such attack, as well as monitoring and suppressing domestic political opponents who threaten the regime, Siboni wrote in a recent analysis of Iran's capabilities."

8. Lieutenant Colonel Eric K. Shafa, "Iran's Emergence as a Cyber Power," U.S. Army War College, August 20, 2014, http://www.strategicstudiesinstitute.army.mil/index.cfm/articles/Irans-emergence-as-cyber-power/2014/08/20. This article explains, "In early March 2012, Supreme Leader of Iran Ayatollah Ali Khameni publicly announced to state media the creation by decree of a new Supreme Council of Cyberspace charged 'to oversee the defense of the Islamic Republic's computer networks and develop new ways of infiltrating or attacking the computer networks of its enemies.'"

9. Researchers at Hewlett-Packard go so far as to argue that defending against cyberattacks to critical infrastructure is a "core facet of Iran's cyber doctrine." See also *Threat Intelligence Briefing: Iran Cyber Capabilities*, Episode 11 (Palo Alto, CA: Hewlett-Packard, 2013), 6, https://krypt3ia.files.wordpress.com/2014/03/companion-to-hpsr-threat-intelligence-briefing-episode-11-final.pdf.

10. *United States Security Policy and Threats: Hearing before the Senate Comm. on Armed Services*, 114th Cong., 1st sess. (September 29, 2015) (statement of United States Deputy Secretary of Defense Robert O. Work, U.S. Department of Defense), http://www.armed-services.senate.gov/hearings/15-09-29-united-states-cybersecurity-policy-and-threats.

11. Christopher Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival: Global Politics and Strategy* (April–May 2013), 81–96; U.S. Department of Homeland Security, *Joint Security Awareness Report (JSAR-12-241-01B), Shamoon/DistTrack Malware (Update B)*, by Industrial Control Systems Cyber Emergency Response Team, January 2014, https://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B; Kim Zetter, "Qatari Gas Company Hit with Virus in Wave of Attacks on Energy Companies," *Wired Magazine*, August 30, 2012, https://www.wired.com/2012/08/hack-attack-strikes-rasgas/; *United States of America v. Fathi et al.*, United States District Court: Southern District of New York, March 24, 2016, https://www.justice.gov/opa/file/834996/download.

Finally, Iran uses cyberspace to further its underwriting of proxy organizations that challenge its opponents in the Middle East, such as Syria's Electronic Army or Cyber Hezbollah.[12] The value of cyber proxies for Iran is that the "approach is indirect and soft, so as to give Iran plausible deniability of involvement."[13] Although these denials often become less plausible over time as more becomes known about specific cyber activities and their perpetrators, Iran nonetheless continues supporting these proxies to further its interests.[14]

CURRENT CAPABILITIES AND FUTURE TRAJECTORY[15]

Iran's recent offensive cyber operations indicate that it has the capability to operate along all three components of the information security triad: it can compromise the confidentiality, integrity, and availability of data.[16] Great skill is not required, and Iran has used fairly rudimentary cyber methods.[17]

Generally, before going on the offensive, hackers conduct reconnaissance to discern vulnerabilities and opportunities for exploitation.[18] While there are many forms of reconnaissance in cyberspace, in 2014 private security research company iSight reported on a sophisticated multiyear Iranian effort to reconnoiter U.S. military and government personnel online. By connecting with their U.S. targets on social media, messages sent by fake personas created by Iranian hackers were incorrectly trusted as friendly correspondence. This correspondence led to

---

12. Jordan Brunner, "Iran Has Built an Army of Cyber-Proxies," *Tower Magazine*, no. 29, August 2015, http://www.thetower.org/article/iran-has-built-an-army-of-cyber-proxies/.

13. Ibid.

14. Ibid.

15. Alleged activity includes Twitter (2007) Iranian Cyber Army; Baidu (Chinese search engine) (2010) Iranian Cyber Army; Diginotar hack (June 2011); Operation Ababil (December 2011–May 2013); Anchorman (2011–2014); Saudi Aramco (August 2012) Cutting Sword of Justice; Operation Cleaver (2012–2014) (includes National Marine Corps Intranet hack); NASA (June 2013) Islamic Cyber Resistance Group; NY Dam (August–September 2013); Sands Casino (February 2014); U.S. Department of State social engineering (2015); see also "Iran Cyber Capabilities," *HP Security Research Threat Intelligence Briefing*, Episode 11 (Palo Alto, CA: Hewlett-Packard, 2013), for a full list through early 2014.

16. "CIA Triad," *CIPP Guide*, August 3, 2010, https://www.cippguide.org/2010/08/03/cia-triad/.

17. Ellen Nakashima, "Iranian Hackers Are Targeting U.S. Officials through Social Networks, Report Says," *Washington Post*, May 29, 2014, https://www.washingtonpost.com/world/national-security/iranian-hackers-are-targeting-us-officials-through-social-networks-report-says/2014/05/28/7cb86672-e6ad-11e3-8f90-73e071f3d637_story.html. This article explains that "the Iranians are not among the elite or most sophisticated of hackers. The United States, Russia, Israel and China still are leagues ahead. But the Iranians are working hard to catch up, experts say."

18. Patrick Engebretson, "The Basics of Hacking and Penetration Testing," in *Ethical Hacking and Penetration Testing Made Easy* (2011), 15–41, http://www.sciencedirect.com/science/article/pii/B9781597496551000027: "Reconnaissance (also known as information gathering) plays a vital role in the success or failure of the overall PT [penetration testing] or hack."

"spear-phishing"—malicious emails appearing to come from a familiar contact—which offered the perpetrators one avenue through which they could begin an intrusion.[19]

To compromise the confidentiality of data, a system, or a network, one generally needs to gain unauthorized access to a system or to a network.[20] Iran has demonstrated its ability to gain unauthorized access on multiple occasions (referenced earlier in this chapter) as a precursor to mounting disruptive or destructive attacks. Iran also established a presence inside a network connected to the Bowman Avenue Dam in Rye, New York, although it evidently did not proceed any further than this internal network reconnaissance.[21]

Iran has also shown the ability to compromise the integrity of information through a series of cyber operations that deleted data and forced victims to abandon compromised computing infrastructure.[22] In August 2012, Iran unleashed a destructive virus called Shamoon against Saudi Aramco, which "erased data on three-quarters of Aramco's corporate PCs—documents, spreadsheets, e-mails, files—replacing all of it with an image of a burning American flag."[23] The same attack was quickly replicated against Qatar's natural gas authority, RasGas. More recently, in February 2014, Iranian hackers cyberattacked the Las Vegas Sands Corporation, in what *Business Insider* described as "likely the first time hackers had targeted American corporate infrastructure on a large scale with the primary goal of destroying it (as opposed to stealing from it or spying on it)."[24]

Finally, Iran has conducted denial-of-service activities that compromise the availability of the target's information. These activities do not destroy or steal information, but they render it at least temporarily inaccessible to the data's legitimate owners. In 2013 and 2014, Iranian hackers targeted U.S. financial institutions in a campaign that disrupted multiple public-facing systems.[25] Cybersecurity research firm Arbor Networks also linked denial-of-service activities against Israel to Iranian hackers during and after Operation Protective Edge in 2014.[26]

The governmental structure in Iran that oversees most cyberspace-related activities is the Supreme Council of Cyberspace. Ayatollah Khamenei established this council in March 2012, and its membership includes representatives from a variety of Iran's intelligence and security agencies.

---

19. For more on this campaign, which iSight dubbed Operation Newscaster, see the archived version of the report's overview: http://cyber-peace.org/wp-content/uploads/2014/08/NEWSCASTER-An-Iranian-Threat-Inside-Social-Media-iSIGHT-Partners.pdf. The full version of the report is now behind the FireEye paywall.

20. See "CIA Triad."

21. See U.S. Department of Justice Indictment 2016, *United States of America v. Ahmad Fathi, et al.* [hereafter, "DOJ Indictment 2016"] available at https://www.justice.gov/usao-sdny/file/835061/download.

22. See ibid.

23. Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, October 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=0.

24. Natasha Bertrand, "Iranian Hackers Paralyzed Billionaire Sheldon Adelson's Las Vegas Casino," *Business Insider*, December 15, 2014, http://www.businessinsider.com/iranian-hackers-shut-down-sheldon-adelsons-casino-in-las-vegas-2014-12.

25. See DOJ Indictment 2016.

26. Kirk Soluk, "DDoS and Geopolitics—Attack Analysis in the Context of the Israeli-Hamas Conflict," *Arbor Networks Report*, August 5, 2014, https://www.arbornetworks.com/blog/asert/ddos-and-geopolitics-attack-analysis-in-the-context-of-the-israeli-hamas-conflict/.

A June 23, 2008, image of Saudi Aramco's Al-Khurais central oil processing facility in the Saudi Arabian desert, just 160 kilometers east of Riyadh. On August 16, 2012, the U.S. technology company Symantec discovered the malware Shamoon, which wiped out 35,000 work stations. The malware was traced back to the hacker group "Cutting Sword of Justice," linked to Iran.
Source: Photo by Marwan Naamani, AFP, available at http://www.gettyimages.com/license/168967544.

Beyond operational control, it appears the Iranian leadership has heavily invested its resources in fostering a technologically savvy population.[27] As an example, it expended significant resources in building IT infrastructure at schools, including the IRGC-affiliated Malek Ashtar University.[28] Iran's compulsory military service requirement allows it to channel graduates with technology specialties to support the state's security operations. The threat of incarceration for refusing to serve provides an additional motivation for the country's tech-savvy youth to lend their skills to the security services.[29]

27. Michael Eisenstadt, "Iran's Lengthening Cyber Shadow," *Research Notes* no. 34, Washington Institute for Near East Policy, July 2016, http://www.washingtoninstitute.org/uploads/Documents/pubs/ResearchNote34_Eisenstadt.pdf.

28. Geof Hancock, "Recent Report on Iranian Cyber Threat," *Security Insights*, April 23, 2015, http://www.securityinsights.org/2015/04/recent-report-on-iranian-cyber-threat-two-notable-findings/.

29. Nikoloz Kokhreidze, "Cyberspace of Iran," LinkedIn, December 8, 2014, https://www.linkedin.com/pulse/20141208113146-180372024-cyberspace-of-iran. This article states that the Iranian "government's policy is harsh

Observers could expect to see a refinement of Iranian cyberspace operational capabilities in three areas. First, Iranian hackers will likely try to evolve beyond the exploitation of commonly known vulnerabilities, which is how they conducted distributed denial-of-service (DDoS) activities against the U.S financial sector.[30] Second, if Iran develops the ability to exploit zero-day vulnerabilities on a recurring basis, it would mark an evolution from exploiting vulnerabilities known to the security research community that may be patched at any time. Third, Iranian hackers may try to build on their success of breaking into a network connected to the Bowman Dam in Rye, New York,[31] by refining their targeting to achieve unauthorized access to other, more vulnerable and more consequential components of U.S. infrastructure. To that end, Iranian hackers may seek to capitalize on better targeting by developing more sophisticated means to ensure they can maintain their unauthorized access once they compromise a targeted network.

LINKAGE TO OTHER ACTORS AND INSTITUTIONS IN IRAN

The degree of explicit command and control exercised by Iran's political leaders over its security services and, in turn, over the countries' hackers is murky. In part, this is due to the opaque nature of how the security services integrate into the political workings of the regime. In addition, Iran's use of proxy actors to conduct at least a portion of its cyber operations further complicates the ability to understand precisely whom does what on whose behalf.[32] Nonetheless, it seems there is, at the very least, tacit approval from Iran's political and security leaders of its hackers' activities.

The U.S. Justice Department's 2016 indictment of seven Iranian hackers contains the most concrete evidence of this linkage.[33] The indictment alleged that "[the accused groups] performed work on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps."[34]

---

against hackers too[;] when they identify a professional hacker, authorities contact and threaten him with imprisonment, if he does not cooperate."

30. See DOJ Indictment 2016. "At certain times relevant to this Indictment, the ITSec Team Defendants and Mersad Defendants conducted extensive computer network exploitation and computer network attacks against victim corporations in the United States."

31. See DOJ Indictment 2016.

32. Kenneth Corbin, "Iran Is a More Volatile Cyber Threat to U.S. than China or Russia," *CIO*, March 21, 2013, http://www.cio.com/article/2387362/government/iran-is-a-more-volatile-cyber-threat-to-u-s--than-china-or-russia.html. This article notes that "in considering attacks emanating from foreign actors . . . attribution and the involvement of a foreign government are often murky at best." Also, Frank Cilluffo, former director of Homeland Security Policy Institute at George Washington University, testified to the cybersecurity subcommittee in 2013, "The bad news is what they [Iran] lack in capability they more than make up for in intent." Moreover, even if Iran's capacity to launch an attack is a far cry from that of Russia or China, Cilluffo pointed out that the nation can fairly easily turn to proxies or rent out low-cost botnets: "The bar to entry when we talk about cyber is not very high," he said.

33. "Four Companies and Five Individuals Indicted for Illegally Exporting Technology to Iran," U.S. Department of Justice, April 17, 2015, https://www.justice.gov/opa/pr/four-companies-and-five-individuals-indicted-illegally-exporting-technology-iran.

34. See DOJ Indictment 2016. "At all times relevant to this Indictment, ITSec Team and Mersad Co. ('Mersad') were private computer security companies based in the Islamic Republic of Iran ('Iran') that performed work on behalf of the

Specifically, one of the suspects, Amin Shokohi,[35] received credit toward his mandatory military service obligation in exchange for his computer intrusion services.[36] This arrangement is significant because it suggests a level of state awareness of his exploits.[37] Although the Department of Justice stopped short of accusing the Iranian government of directing these activities, publicizing Shokohi's military credit indicates that the U.S. government strongly suspected state involvement in his activities.[38]

Sometimes a degree of political approval can be inferred from the nature of the cyber operation itself. The cyberattack on the Las Vegas Sands Casino is an instructive example.[39] In October 2013, the CEO of Sands, Sheldon Adelson, spoke out about the Iran nuclear negotiations and publicly proposed detonating a nuclear weapon in the Iranian desert to demonstrate U.S. resolve.[40] This call to action generated a strong rebuke from Supreme Leader Khamenei, who warned the United States to "slap these prating people in the mouth and crush their mouths."[41] In February 2014, Sands experienced a destructive cyberattack, as its networks were compromised and data destroyed on some systems.[42] A similar kind of leadership sanctioning or direction can be inferred for domestic surveillance activities within Iran that intensify before and during key political events, especially national elections.[43] Finally, due to the IRGC's control of a significant portion of Iran's

---

Iranian Government, including the Islamic Revolutionary Guard Corps ('IRGC'), which is one of several entities within the Iranian Government responsible for Iranian intelligence."

35. Federal Bureau of Investigation, "Amin Shokohi, FBI Most Wanted," https://www.fbi.gov/wanted/cyber/amin-shokohi/@@download.pdf.

36. See DOJ Indictment 2016.

37. Ibid.

38. See "Amin Shokohi"; see also DOJ Indictment 2016, which states, "Shokohi helped to build the ITSec Team botnet used in the U.S. Financial Industry DDoS Attacks, and created malware used to direct the botnet to engage in those attacks. During the time in which he worked in support of the U.S. Financial Industry DDoS Attacks, Shokohi received credit for his computer intrusion work for the Iranian Government towards completion of his mandatory military service in Iran."

39. Benjamin Elgin and Michael Riley, "Now at the Sands Casino: An Iranian Hacker in Every Server," *Bloomberg*, December 12, 2014, http://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas.

40. See ibid. quoting Sheldon Adelson: "What are we going to negotiate about?" Adelson asked. "What I would say is, 'Listen. You see that desert out there? I want to show you something.'" He would detonate an American warhead in the sand, he said, where it "doesn't hurt a soul. Maybe a couple of rattlesnakes and scorpions or whatever."

41. See ibid., which states, "Iran's Supreme Leader Ayatollah Ali Khamenei responded two weeks later, according to the country's semiofficial Fars News Agency, saying America 'should slap these prating people in the mouth and crush their mouths.'"

42. Riley Walters, "Cyber Attacks on U.S. Companies since November 2014," Heritage Foundation, November 18, 2015, http://www.heritage.org/research/reports/2015/11/cyber-attacks-on-us-companies-since-november-2014. The article states, "In February 2014, the Sands Casino was hacked by a group out of Iran. The hackers brought the $14 billion operation to a standstill as they shut down PCs, [and] servers, and wiped hard drives clean. The attack was suspected to be in retaliation for comments that Sands CEO Sheldon Adelson made about the Iranian government."

43. Abbas Milani, "The Green Movement," in *The Iran Primer*, ed. Robin Wright (Washington, DC: United States Institute of Peace, 2010), http://iranprimer.usip.org/sites/default/files/The%20Green%20Movement.pdf. This piece explains that

networks, it is reasonable to assume that activities originating from that system are tolerated, if not sponsored, by the IRGC.[44]

Iran's employment of and reliance upon proxies to conduct activities for the state in cyberspace complicate efforts to attribute malicious activity to the state. Not only is it difficult to know if a particular hacker or group of hackers is acting as a free agent, but the degree of oversight or control from central authorities may change over time. Iran is believed to have lent support both financially and technologically to Cyber Hezbollah (implicated in a cyber-espionage campaign targeting Israel and Lebanon),[45] the Syrian Electronic Army, the Yemen Cyber Army, and Hamas.[46] Yet, identifying the degree of Iranian control over these groups, especially for specific activities, has remained an elusive goal for the security research community.

IMPLICATIONS FOR THE REGION AND U.S. INTERESTS

With the implementation of the Joint Comprehensive Plan of Action (JCPOA), the United States will need to determine whether malicious Iranian cyber activities will continue as before. As recently as this past year, former director of National Intelligence James Clapper called out Iran for its aggressive use of cyber espionage, propaganda, and attacks against U.S. allies in the region.[47] If Iran continues on the current trajectory, a question for the United States and its partners will be how far to let Iranian cyber developments proceed before taking action. A further difficulty will be modulating any deterrent actions or response so as to demonstrate the unacceptability of Iranian hacking without jeopardizing the overall goals of the JCPOA.

Alternatively, Iran may reduce the scope of its external cyber operations against the United States, and instead focus on the development of more skilled personnel and less overtly aggressive forms of activity throughout the Gulf and the Middle East. Even this level of activity could provoke Iran's

---

during the turmoil of the 2009 Green Revolution, "the regime also shut down newspapers, magazines and websites close to the Green Movement. Iran became the country with the most imprisoned journalists. To help fight the reform movement's use of the Internet, the Revolutionary Guards became majority owner of Iran's telecommunications giant."

44. Frederick W. Kagan and Tommy Stiansen, "The Growing Cyberthreat from Iran: The Initial Report of Project Pistachio Harvest," American Enterprise Institute, April 17, 2015, http://www.criticalthreats.org/sites/default/files/Growing_Cyberthreat_From_Iran_AEI_Norse_Kagan_Stiansen.pdf. Other cybersecurity researchers take issue with the methodology and conclusions of the AEI/Norse report and argue that the evidence presented therein is highly circumstantial if not speculative. See, for example, Robert Lee et al., "Analysis of a Recent Iranian Cyber Attack Intelligence Report by Norse and the American Enterprise Institute," Industrial Control Systems (ICS), Defense Use Case (DUC) no. 3, SANS, April 23, 2015.

45. Jeff Moskowitz, "Cyberattack Tied to Hezbollah Ups the Ante for Israel's Digital Defense," *Passcode*, *Christian Science Monitor*, June 1, 2015, http://www.csmonitor.com/World/Passcode/2015/0601/Cyberattack-tied-to-Hezbollah-ups-the-ante-for-Israel-s-digital-defenses.

46. See Brunner, "Iran Has Built an Army of Cyber-Proxies."

47. *Worldwide Threat Assessment of the US Intelligence Community: Hearing before Senate Comm. on Armed Services Committee*, 114th Cong., 2nd sess. (February 9, 2016) (statement of Former Director of National Intelligence James R. Clapper), https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.

regional rivals, who might look to the United States for support or leadership. A united front against disruptive and certainly destructive Iranian actions in cyberspace, and a willingness to publicly expose and attribute these actions, will help prevent unnecessary strains in the United States' relationships in the region.

If Iran perceives a low likelihood that its cyber activities will prompt retaliation, two risks may emerge. The first is that Iranian actions in cyberspace could overreach, perhaps by purposefully or accidentally targeting or disrupting a system that is perceived to cross a redline by its owner. Inadvertent escalation, both within and outside of cyberspace, becomes a possibility. The second risk is that of further escalation when supplying resources and tools to proxies, who may operate from distinct (and perhaps even conflicting) interests, such that they may be more willing to absorb the risks of collateral damage than their Iranian sponsors. It is also possible that proxies might be less meticulous in concealing their state-sponsored affiliation, thereby galvanizing the victim to retaliate against the most likely culprit.

RECOMMENDATIONS FOR THE UNITED STATES AND ITS PARTNERS

The fundamental challenge for policymakers, and especially the Trump administration, is to be clear eyed about the threats that Iranian cyber activities do (and importantly, do not) pose, and to align responses within a broader understanding of Iran's actions under the JCPOA. The United States and its partners should be postured to respond promptly and proportionally to aggressive Iranian cyber operations. The more time that elapses between an unacceptable cyberattack and a Western response, the harder it is to signal credibly that cost will be, and will continue to be, imposed.

A second priority is to improve the cybersecurity of critical infrastructure, such as electricity and water, in the Gulf and Middle East. There is no need to aim for erecting a perfect defense. Rather, as evidenced in the Justice Department's 2016 indictment, detecting and patching known vulnerabilities, such as SQL injections (insertion of malignant code to manipulate or steal data) and others in the Common Vulnerabilities and Exposures database, would complicate Iranian efforts to compromise the confidentiality, integrity, and availability of important infrastructure.[48] The goal is to decrease the attack surface in the region, which would block most low-level nuisances while allowing network defenders to focus on the most critical threats.

Finally, to deter malicious Iranian cyber activities, the United States and its partners should be mindful of Iran's changing priorities and sensitivities. Deterrence by cost-imposition succeeds only if cost is imposed in an area of importance to one's rival. Although cyberspace is a core area of importance for the United States and its partners, threatening to retaliate outside of cyberspace may send a more compelling signal to the Iranians that their activities in cyberspace are unacceptable. For example, the opportunity to use the so-called cyber sanctions authority, highlighted in

48. See DOJ Indictment 2016.

Executive Order 13694 signed by President Obama in April 2015, gives a U.S. administration the ability to respond to malicious cyber activities without retaliating with in-kind cyber activities.[49] This will require a clear understanding of Iran's broader geopolitical vulnerabilities and interests to ensure that sanctions or other costs imposed are appropriately calibrated for their intended effects.

49. U.S. Department of the Treasury, *Periodic Report on the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities*, by Jacob Lew, October 1, 2015.