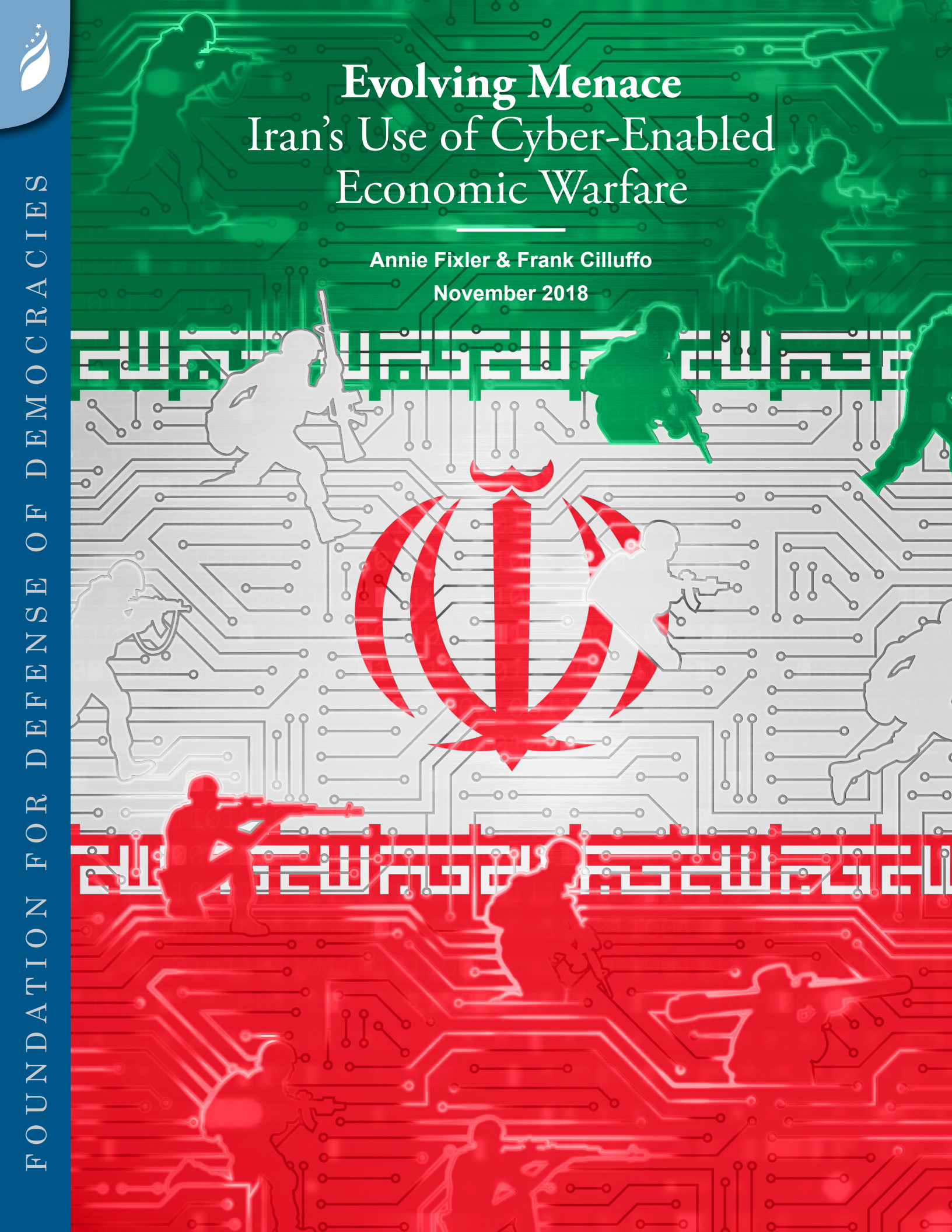


Evolving Menace
Iran's Use of Cyber-Enabled Economic Warfare

Annie Fixler & Frank Cilluffo

November 2018

FOUNDATION FOR DEFENSE OF DEMOCRACIES

Evolving Menace
Iran's Use of Cyber-Enabled Economic Warfare

Annie Fixler

Frank Cilluffo

November 2018

FDD PRESS

A division of the
FOUNDATION FOR DEFENSE OF DEMOCRACIES
Washington, DC

Table of Contents

Executive Summary

In 2016, the industrial computer security firm MalCrawler conducted an experiment: It created an elaborate network to observe the actions and gauge the intentions of malicious cyber operators. The firm concluded that hackers from different countries typically exhibit distinct behaviors. Chinese hackers pilfered "anything that looked like novel technical information." Russians penetrated systems, "mapping them and implanting hard-to-find backdoor access for potential future use." In contrast, Iranian hackers sought to do "as much damage as possible."[1] This is consistent with Iranian cyber behavior: Over the past decade, the Islamic Republic has shown it will exploit deficient cyber defenses to wreak havoc on its adversaries' networks. The regime is now bolstering its capacity to cause even greater harm in the future.

Comparatively lacking in conventional forms of military, economic, and geopolitical power, the Islamic Republic leverages asymmetric capabilities to wage war against the United States and its allies. These methods include sponsorship of terrorists and militia forces, hostage taking, overseas assassinations, ballistic missiles, and – potentially – nuclear weapons. The latest additions to this asymmetric toolkit are cyber capabilities and, specifically, cyber-enabled economic warfare – a strategy involving cyber attacks against an adversary's economic assets in order to reduce its political and military power.[2] Consistently, the evidence reveals that the Iranian regime and its Islamic Revolutionary Guard Corps (IRGC) are sponsoring these malicious Iranian cyber operations.

The Islamic Republic accelerated its pursuit of offensive cyber capabilities in 2009-2010 after falling prey to the Stuxnet virus, reportedly engineered by the U.S. and Israel.[3] Less than two years later, the Islamic Republic retaliated against U.S. economic sanctions with cyber attacks on American banks, along with a costly attack against regional rival Saudi Arabia.[4]

After those two operations, the Islamic Republic's cyber activities appeared to shift. As Tehran sought to negotiate relief from U.S. sanctions, its malicious cyber activity focused primarily – although not exclusively – on its regional adversaries, and simultaneously, the regime also expanded its cyber infiltration operations around the world. Through these campaigns, Iranian hackers are able to hone their skills on soft targets and pre-position assets for future conflicts, both cyber and otherwise.[5]

Those battles may be around the corner. The U.S. has reinstated its sanctions on Iran after withdrawing from the controversial 2015 nuclear accord in May. These sanctions threaten to further destabilize an economy whose currency is already in free fall and appears headed for a deep recession. Reeling from sanctions, and already inclined to aggressive and destructive cyber and non-cyber related malign activities, the desperate

1. Sam Jones, "Cyber warfare: Iran opens a new front," *Financial Times* (UK), April 26, 2016. (https://www.ft.com/content/15e1acf0-0a47-11e6-b0f1-61f222853ff3)
2. Samantha F. Ravich and Annie Fixler, "Framework and Terminology for Understanding Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, February 22, 2017. (https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/MEMO_CyberDefinitions_07.pdf)
3. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014. (https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/)
4. U.S. Department of Justice, Press Release, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," March 26, 2016. (https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged); Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *The New York Times*, October 23, 2012. (https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html)
5. Courtney Kube, Carol E. Lee, Dan De Luce, and Ken Dilanian, "Iran has laid groundwork for extensive cyberattacks on U.S., say officials," *NBC News*, July 20, 2018. (https://www.nbcnews.com/news/us-news/iran-has-laid-groundwork-extensive-cyberattacks-u-s-say-officials-n893081)

regime may become a more aggressive actor both in the virtual and physical worlds.

"Reeling from sanctions, and already inclined to aggressive and destructive cyber and non-cyber related malign activities, the desperate regime may become a more aggressive actor both in the virtual and physical worlds."

To counter the Islamic Republic's malicious cyber activity, Washington must be prepared to impose significant costs on the leadership in Tehran and to use cyber and kinetic means to hold at risk the Islamic Republic's most valuable assets. Simultaneously, Washington must work with its allies and the private sector to bolster defenses so that Iranian operations are less likely to succeed. While the Islamic Republic's capabilities do not match those of China and Russia, its cyber capabilities are dangerous to U.S. national security and rapidly maturing.

List of Iranian Cyber Operations[6]

2011-2017 – social media influence operation aimed at U.S. and global audiences[7]

2012-2014, Operation Cleaver – global cyber surveillance and infiltration campaign[8]

December 2011-May 2013, Operation Ababil – distributed denial of service attacks against the U.S. financial system[9]

August 2012, Shamoon – destructive wiper malware attack against Saudi Aramco[10]

August-September 2013 – infiltration of the Bowman Avenue Dam in Rye, New York[11]

2013-December 2017 – intrusions and data theft against 176 U.S. and foreign universities, 47 U.S. and foreign private companies, and U.S. federal and state agencies[12]

2013-2014, Operation Saffron Rose – malware-based cyber espionage against Iranian dissidents and U.S. defense industrial base[13]

6. This list is not exhaustive of all Iranian cyber operations but is demonstrative of Iranian attacks. It includes all operations mentioned in subsequent sections of this report.

7. Craig Timberg, Elizabeth Dwoskin, Tony Romm, and Ellen Nakashima, "Sprawling Iranian influence operation globalizes tech's war on disinformation," *The Washington Post*, August 21, 2018. (https://www.washingtonpost.com/technology/2018/08/21/russian-iran-created-facebook-pages-groups-accounts-mislead-users-around-world-company-says/?utm_term=.6051b5222fc1)

8. "Operation Cleaver," *Cylance*, December 2014. (https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf)

9. U.S. Department of Justice, Press Release, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," March 26, 2016. (https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged)

10. Jose Pagliery, "The inside story of the biggest hack in history," *CNN Money*, August 5, 2015. (http://money.cnn.com/2015/08/05/technology/aramco-hack/)

11. U.S. Department of Justice, Press Release, "Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities," March 24, 2016. (https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated)

12. U.S. Department of Justice, Press Release, "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign On Behalf Of The Islamic Revolutionary Guard Corps," March 23, 2018. (https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic)

13. Nart Villeneuve, Mike Scott, Thoufique Haq, and Ned Moran, "Operation Saffron Rose," *FireEye*, May 2014. (https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf)

February 2014 – attack against Las Vegas Sands Corporation[14]

2014-2015, **Thamar Reservoir** – cyber espionage and infiltration against Middle Eastern university researchers, defense and security companies, journalists, and human rights activists[15]

2016-2017 – APT33 cyber infiltration and trade secret theft against a U.S. aerospace company, Saudi aviation conglomerates, and a South Korean petrochemical company[16]

2016-2018 – APT OilRig global cyber espionage and data exfiltration[17]

November 2016-January 2017, Shamoon 2 – destructive malware against Saudi government ministries and companies[18]

May 2017 – data theft and extortion against HBO[19]

2017-2018 – APT Leafminer cyber infiltration against governments and businesses in the Middle East[20]

Iran's Reliance on Asymmetric Capabilities

The Islamic Republic's asymmetric mindset was forged during the Iran-Iraq War.[21] The naval battles known as the "Tanker War" crystallized Tehran's reliance on asymmetric approaches. In 1987, in response to Iranian harassment of civilian oil tankers belonging to Arab Gulf states aligned with Iraq, the U.S. Navy began escorting the tankers through the Persian Gulf. Tehran launched a conventional naval campaign against the Navy, but was quickly outgunned and lost half of its fleet. The regime then switched to the use of small boats, mines, and cruise missiles, which led to greater success.[22]

Faced with constraints on its ability to purchase conventional weapons systems (as a result of U.S. sanctions) in the decades following the Iran-Iraq War, the regime allocated its defense spending to capabilities that exploited the vulnerabilities of its regional rivals and technologically superior

14. Ben Elgin and Michael Riley, "Now at the Sands Casino: An Iranian Hacker in Every Server," *Bloomberg*, December 12, 2014. (https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas#p1)
15. "Thamar Reservoir: An Iranian cyber-attack campaign against targets in the Middle East," *Clearsky*, June 2015. (https://www.clearskysec.com/wp-content/uploads/2015/06/Thamar-Reservoir-public1.pdf)
16. Jaqueline O'Leary, Josiah Kimble, Kelli Vanderlee, and Nalani Fraser, "Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware," *FireEye*, September 20, 2017. (https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html)
17. Bryan Lee and Robert Falcone, "OilRig Targets Technology Service Provider and Government Agency with QUADAGENT," *Palo Alto*, July 25, 2018. (https://researchcenter.paloaltonetworks.com/2018/07/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/)
18. "Saudi Arabia warns on cyber defense as Shamoon resurfaces," *Reuters*, January 23, 2017. (https://www.reuters.com/article/us-saudi-cyber/saudi-arabia-warns-on-cyber-defense-as-shamoon-resurfaces-idUSKBN1571ZR)
19. U.S. Department of Justice, Press Release, "Acting Manhattan U.S. Attorney Announces Charges Against Iranian National For Conducting Cyber Attack And $6 Million Extortion Scheme Against HBO," November 21, 2017. (https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-charges-against-iranian-national-conducting)
20. "Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions," *Symantec*, July 25, 2018. (https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east)
21. Behnam Ben Taleblu, "The Long Shadow of the Iran-Iraq War," *The National Interest*, October 23, 2014. (https://nationalinterest.org/feature/the-long-shadow-the-iran-iraq-war-11535?nopaging=1)
22. J. Matthew McInnis, "Iranian Concepts of Warfare: Understanding Tehran's Evolving Military Doctrines," *American Enterprise Institute*, February 2017, pages 13-14. (http://www.aei.org/wp-content/uploads/2017/02/Iranian-Concepts-of-Warfare.pdf); see also: Michael Connell, "Iran's Military Doctrine," *The Iran Primer*, accessed September 11, 2018. (https://iranprimer.usip.org/resource/irans-military-doctrine)

adversaries.[23] Instead of a conventional air force, Iran developed ballistic missiles. Instead of traditional naval capabilities, Iran relied on swarms of small, fast-attack speedboats. Instead of conventional land forces, Iran built up terrorist proxies like Hezbollah and the Islamic Revolutionary Guard Corps' (IRGC) expeditionary Quds Force, both of which the regime created in the immediate wake of the 1979 Revolution.[24] Iran's current strategy focuses on the ability to develop a nuclear weapons capability, conduct terrorist activities around the world, threaten missile attacks, and hold hostage global oil markets by threatening to close the Strait of Hormuz – a vital waterway for global oil trade.[25]

"U.S. State Department concluded, 'The Islamic Republic has developed its cyber capabilities with the intent to surveil and sabotage its adversaries, undermining international norms and threatening international stability'."

Testifying before Congress, then-Director of National Intelligence (DNI) James Clapper explained that Iran "views its cyber program as one of many tools for carrying out asymmetric but proportional retaliation against political foes."[26] After reaching the nuclear deal with Iran, some officials in the Obama administration noted to *The New York Times* that the regime views cyber as "a tool to seek the kind of influence that some hard-liners in Iran may have hoped its nuclear program would eventually provide."[27] More recently, in September, the U.S. State Department concluded, "The Islamic Republic has developed its cyber capabilities with the intent to surveil and sabotage its adversaries, undermining international norms and threatening international stability."[28]

Cyber operations have also become an increasing part of Iran's arsenal because they provide "less risky opportunities to … retaliate against perceived enemies at home and abroad."[29] In February 2014, in retaliation for Las Vegas Sands Corporation CEO Sheldon Adelson's recommendation that the United States drop a nuclear bomb in the Iranian desert to convince the Islamic Republic to relinquish its own nuclear ambitions,[30] suspected Iranian hackers

23. Michael Eisenstadt, "The Strategic Culture of the Islamic Republic of Iran: Religion, Expediency, and Soft Power in an Era of Disruptive Change," *Marine Corps University*, November 2015, pages 7-8. (https://www.washingtoninstitute.org/uploads/Documents/pubs/MESM_7_Eisenstadt.pdf)

24. For an in depth look at the Islamic Republic of Iran's concepts and doctrines of warfare, see: J. Matthew McInnis, "Iranian Concepts of Warfare: Understanding Tehran's Evolving Military Doctrines," *American Enterprise Institute*, February 2017. (http://www.aei.org/wp-content/uploads/2017/02/Iranian-Concepts-of-Warfare.pdf)

25. Michael Eisenstadt, "The Strategic Culture of the Islamic Republic of Iran: Religion, Expediency, and Soft Power in an Era of Disruptive Change," *Marine Corps University*, November 2015, pages 7-8. (https://www.washingtoninstitute.org/uploads/Documents/pubs/MESM_7_Eisenstadt.pdf)

26. James Clapper, "Statement for the Record: Worldwide Cyber Threats," *Hearing before the House Permanent Select Committee on Intelligence*, September 10, 2015, page 4. (https://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf)

27. David E. Sanger and Nicole Perlroth, "Iranian Hackers Attack State Dept. via Social Media Accounts," *The New York Times*, November 24, 2015. (https://www.nytimes.com/2015/11/25/world/middleeast/iran-hackers-cyberespionage-state-department-social-media.html)

28. U.S. Department of State, "Outlaw Regime: A Chronicle of Iran's Destructive Activities," September 25, 2018, page 31. (https://www.state.gov/documents/organization/286410.pdf)

29. Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," *Carnegie Endowment for International Peace*, January 2018, page 12. (https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf)

30. Maya Shwayder, "Adelson: US Should Drop Atomic Bomb on Iran," *The Jerusalem Post* (Israel), October 24, 2013. (https://www.jpost.com/Diplomacy-and-Politics/Adelson-US-should-drop-atomic-bomb-on-Iran-329641); Micah Halpern, "Did Iran Try to Get Lucky by Hacking Sheldon Adelson's Casino Company?" *Observer*, March 13, 2015. (http://observer.com/2015/03/did-iran-try-to-get-lucky-by-hacking-sheldon-adelsons-casino-company/)

penetrated the systems of Adelson's company. The attack caused computers to flat-line, knocked corporate e-mail offline, and crippled phones and other business operations platforms that ran the $14-billion company.[31] The result: an estimated $40 million in damages.[32] And it took the company a week to restore its networks.[33] Then-DNI Clapper called the incident the first destructive cyber attack "carried out on U.S. soil by [a] nation-state entit[y]."[34]

The Architecture of Cyber Warfare

Experts assess that the IRGC and security services oversee the majority of the Islamic Republic's offensive cyber capabilities,[35] but the government bodies that determine the regime's policies in cyber space also include representatives of other power centers, including the president, the supreme national security council, and relevant cabinet ministers. The regime also has an extensive censorship apparatus, which blocks access to traditional media, social media sites, and online content more generally. The entities responsible for censorship include the Ministry of Information and Communications Technology, which is responsible for deploying the regime's censored, national internet infrastructure,[36] as well as the state-owned media firm Islamic Republic of Iran Broadcasting (IRIB), which jams foreign satellite broadcasts.[37] Sitting atop this bureaucracy is Supreme Leader Ali Khamenei. He is the "single most powerful individual in a highly factionalized, autocratic regime. Though he does not make national decisions on his own, neither can any major decisions be taken without his consent," scholar Karim Sadjadpour observes.[38]

"IRGC and security services oversee the majority of the Islamic Republic's offensive cyber capabilities… Sitting atop this bureaucracy is Supreme Leader Ali Khamenei."

31. Corey Bennet, "Iranian hackers downed Adelson's casino empire," *The Hill*, December 12, 2014. (http://thehill.com/policy/cybersecurity/226915-iranian-hackers-downed-us-casino-empire); "Sands Casino Website Hacking: Some Customers' Data Was Stolen," *Associated Press*, February 28, 2014. (https://www.nbcnews.com/tech/security/sands-casino-website-hacking-some-customers-data-was-stolen-n41601); Ben Elgin and Michael Riley, "Now at the Sands Casino: An Iranian Hacker in Every Server," *Bloomberg*, December 12, 2014. (https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas#p1); "Las Vegas Sands' network hit by destructive malware in Feb – Bloomberg," *Reuters*, December 11, 2014. (https://www.reuters.com/article/lasvegassands-cybersecurity-idUSL3N0TW16920141212)

32. Russell Brandon, "Iran hacked the Sands Hotel earlier this year, causing over $40 million in damage," *The Verge*, December 11, 2014. (https://www.theverge.com/2014/12/11/7376249/iran-hacked-sands-hotel-in-february-cyberwar-adelson-israel)

33. "Sands Casino Website Hacking: Some Customers' Data Was Stolen," *Associated Press*, February 28, 2014. (https://www.nbcnews.com/tech/security/sands-casino-website-hacking-some-customers-data-was-stolen-n41601)

34. James Clapper, "Hearing to Receive Testimony on Worldwide Threats," *Hearing before the Senate Armed Services Committee*, February 26, 2015, page 11. (https://www.armed-services.senate.gov/imo/media/doc/15-18%20-%202-26-15.pdf)

35. Michael Connell, "Deterring Iran's Use of Offensive Cyber: A Case Study," *CNA*, October 2014, page 4. (https://www.cna.org/CNA_files/PDF/DIM-2014-U-008820-Final.pdf)

36. Tzvi Kahn, "U.S. Should Sanction Iran's ICT Minister," *The Cipher Brief*, July 26, 2018. (https://www.thecipherbrief.com/column/opinion/u-s-should-sanction-irans-ict-minister)

37. Saeed Ghasseminejad and Richard Goldberg, "The Case for Designating Iran's State Media," *Foundation for Defense of Democracies*, February 6, 2018. (https://www.fdd.org/analysis/2018/02/06/the-case-for-designating-irans-state-media/)

38. Karim Sadjadpour, *Reading Khamenei: The World View of Iran's Most Powerful Leader* (Washington, DC: Carnegie Endowment for International Peace, 2009), page 1. (http://carnegieendowment.org/files/sadjadpour_iran_final2.pdf)

Main Actors and Organization of Iran's Cyber Aggression Campaigns[39]

Supreme Leader Ali Khamenei – the ultimate decision-maker on all domestic and national security issues;[40] exercises direct control over the IRGC, armed forces, and security services.

- **The Supreme National Security Council** – the highest national security policymaking body; coordinates and implements the supreme leader's directives; led by the president; members also include speaker of parliament, chief justice, ministers, military chiefs, and appointees of the supreme leader.[41]

Supreme Cyberspace Council – oversees internet and cyber space policy;[42] reports to Supreme Leader Ali Khamenei; members include the president, cabinet ministers, the commander of the IRGC, and other high-ranking officials from the intelligence and security agencies;[43] responsible for "protecting the country from negative content of cyberspace."[44]

- **National Cyberspace Council** – defends the Islamic Republic against the "culture war" online.[45]

Islamic Revolutionary Guard Corps (IRGC) – oversees offensive cyber activities;[46] overseas quasi-independent cyber groups (discussed below; see graphic for a list of prominent groups).

- **IRGC Electronic Warfare and Cyber Defense Organization** – operates training courses; censors content and access.[47]
- **Basij Cyber Council** – non-professional, inexperienced operators; conducts simple hacking or infiltration operations against the regime's internal enemies.[48]
- **Center to Investigate Organized Crime** (aka Gerdab) – conducts "defensive" operations focused

39. This list highlights only the government bodies with jurisdiction over the capabilities most relevant to cyber-enabled economic warfare. However, it should be noted that Tehran views as fluid the defense of the state, the export of the ideology of the revolution, and attacks against Iran's adversaries, and also does not distinguish between domestic and foreign enemies.
40. "Iran's Decider: Supreme Leader Ayatollah Khamenei," *NPR*, February 23, 2012. (https://www.npr.org/2012/02/23/147277389/meet-irans-decider-supreme-leader-khamenei)
41. Kenneth Katzman, "Iran: Internal Politics and U.S. Policy and Options," *Congressional Research Service*, October 17, 2018, page 4. (https://fas.org/sgp/crs/mideast/RL32048.pdf); "The Islamic Republic's Power Centers," *Council on Foreign Relations*, January 5, 2018. (https://www.cfr.org/article/islamic-republics-power-centers); "The Structure of Power in Iran," *PBS Frontline*, accessed October 28, 2018. (https://www.pbs.org/wgbh/pages/frontline/shows/tehran/inside/govt.html#snsc)
42. Eric Shafa, "Iran's Emergence as a Cyber Power," *Strategic Studies Institute*, August 20, 2014. (http://ssi.armywarcollege.edu/index.cfm/articles/Irans-emergence-as-cyber-power/2014/08/20); Michael Connell, "Deterring Iran's Use of Offensive Cyber: A Case Study," *CNA*, October 2014, page 4. (https://www.cna.org/CNA_files/PDF/DIM-2014-U-008820-Final.pdf)
43. "Structure of Iran's Cyber Warfare," *BBC* (UK), accessed September 21, 2018. (https://nligf.nl/v1/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf); "Iran's supreme leader calls for new Internet oversight council," *The Los Angeles Times*, March 7, 2012. (https://latimesblogs.latimes.com/world_now/2012/03/iran-internet-council-khamenei.html)
44. U.S. Department of the Treasury, Press Release, "Treasury Sanctions Individuals and Entities for Human Rights Abuses and Censorship in Iran, and Support to Sanctioned Weapons Proliferators," January 12, 2018. (https://home.treasury.gov/news/press-releases/sm0250)
45. "Iranian Internet Infrastructure and Policy Report," *Small Media*, February 2014, page 4. (https://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb2014.pdf)
46. Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," *Carnegie Endowment for International Peace*, January 2018, page 17. (https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf)
47. U.S. Department of the Treasury, Press Release, "Treasury Sanctions Individuals and Entities for Human Rights Abuses and Censorship in Iran, and Support to Sanctioned Weapons Proliferators," January 12, 2018. (https://home.treasury.gov/news/press-releases/sm0250)
48. "Structure of Iran's Cyber Warfare," *BBC* (UK), accessed September 21, 2018. (https://nligf.nl/v1/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf); Michael Rubin, "Basij Organization Enters Cyber Operations," *American Enterprise Institute*, December 1, 2014. (http://www.aei.org/publication/basij-organization-enters-cyber-operations/); Dorothy Denning, "Following the developing Iranian cyber threat," *The Conversation*, December 11, 2017. (https://theconversation.com/following-the-developing-iranian-cyberthreat-85162)

on censoring content, targeting dissident websites, and identifying opposition activists.[49]

Armed Forces General Staff – coordinates policies and operations between the IRGC and the regular military (Artesh).[50]

- **Cyber Headquarters** (aka Cyber Defense Command) – coordinates cyber policy (primarily defensive policy) within the Iranian armed forces; identifies and eliminates threats to Iran's cyber infrastructure; conducts offensive cyber attacks in cooperation with the Basij Cyber Council.[51]

Ministry of Intelligence and Security (MOIS) – responsible for signals intelligence.[52]

Ministry of Interior – oversees Iran's police and domestic security forces.[53]

- **Iran Cyber Police** (aka FATA) – filters web content; monitors online behavior; hacks email accounts of political dissidents.[54]

Academic and research institutions also provide training and recruit talent to support the Islamic Republic's cyber operations. According to some experts, the science and technology departments of Shahid Beheshti University and Imam Hossein University may be key recruitment grounds for Iran's government cyber forces.[55] Both of these universities have strong connections to the regime's military and security apparatus.[56] For example, Fereidoun Abbasi-Davani, former head of the Atomic Energy Organization of Iran, was a professor at Shahid Beheshti,[57] and the European Union sanctioned the university in 2011 for its involvement in Iran's nuclear and ballistic missile activities.[58] Similarly, the U.S. Treasury Department sanctioned Imam Hossein University in 2012 for being

49. Levi Gundert, Sanil Chohan, and Greg Lesnewich, "Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations," *Recorded Future*, May 9, 2018, page 5. (https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf); U.S. Department of the Treasury, "Fact Sheet: Sanctions on Iranian Government and Affiliates," November 8, 2012. (https://www.treasury.gov/press-center/press-releases/Documents/Fact%20Sheet%20-%20Sanctions%20on%20Iranian%20Govt%20and%20Affiliates%20-%20November%208,%202012.pdf); "Iran's Guards increase monitoring of social media: state TV," *Reuters*, March 2, 2015. (https://www.reuters.com/article/us-iran-internet-idUSKBN0LY1YC20150302)

50. U.S. Navy, Office of Naval Intelligence, "Iranian Naval Forces: A Tale of Two Navies," February 2017, pages 13-14. (https://www.oni.navy.mil/Portals/12/Intel%20agencies/iran/Iran%20022217SP.pdf)

51. Paul Bucala and Caitlin Shayda Pendleton, "Iranian Cyber Strategy: A View from the Iranian Military," *American Enterprise Institute*, November 24, 2015. (https://www.criticalthreats.org/analysis/iranian-cyber-strategy-a-view-from-the-iranian-military); "Structure of Iran's Cyber Warfare," *BBC* (UK), accessed September 21, 2018. (https://nligf.nl/v1/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf); Farzin Nadimi, "Iran's Passive Defense Organization: Another Target for Sanctions," *The Washington Institute for Near East Policy*, August 16, 2018. (https://www.washingtoninstitute.org/policy-analysis/view/irans-passive-defense-organization-another-target-for-sanctions)

52. Library of Congress, Federal Research Division, "Iran's Ministry of Intelligence and Security: A Profile," December 2012. (https://fas.org/irp/world/iran/mois-loc.pdf)

53. Kenneth Katzman, "Iran: Internal Politics and U.S. Policy and Options," *Congressional Research Service*, October 17, 2018, page 6. (https://fas.org/sgp/crs/mideast/RL32048.pdf)

54. U.S. Department of the Treasury, Press Release, "Treasury Announces Sanctions Against Iran," February 6, 2013. (https://www.treasury.gov/press-center/press-releases/Pages/tg1847.aspx)

55. Levi Gundert, Sanil Chohan, and Greg Lesnewich, "Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations," *Recorded Future*, May 9, 2018, page 7. (https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf)

56. "Shahid Beheshi University," *IranWatch*, May 12, 2009. (https://www.iranwatch.org/iranian-entities/shahid-beheshti-university)

57. U.S. Department of the Treasury, "Fact Sheet: Treasury and State Department Actions Target Iran's Nuclear Enrichment and Proliferation Program," December 13, 2012. (https://www.treasury.gov/press-center/press-releases/Documents/121312%20Iran%20Enrichment%20Designations%20Fact%20Sheet.pdf)

58. Council Implementing Regulation (EU) No 503/2011 of 23 May 2011 implementing Regulation (EU) No 961/2010 on restrictive measures against Iran, *Official Journal of the European Union*. (https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:136:0026:0044:EN:PDF)

controlled by the IRGC and supporting its operations. Sanctioned Iranian telecommunications producer and software developer PeykAsa grew out of an initiative at another university, Sharif University of Technology.[59] The regime reportedly partners with major universities to advance Tehran's strategic objectives in a broad range of fields including cyber. This arrangement also funnels graduating students – whom Supreme Leader Khamenei has called Iran's "cyber-war agents"[60] – into companies and projects that further these same objectives.[61]

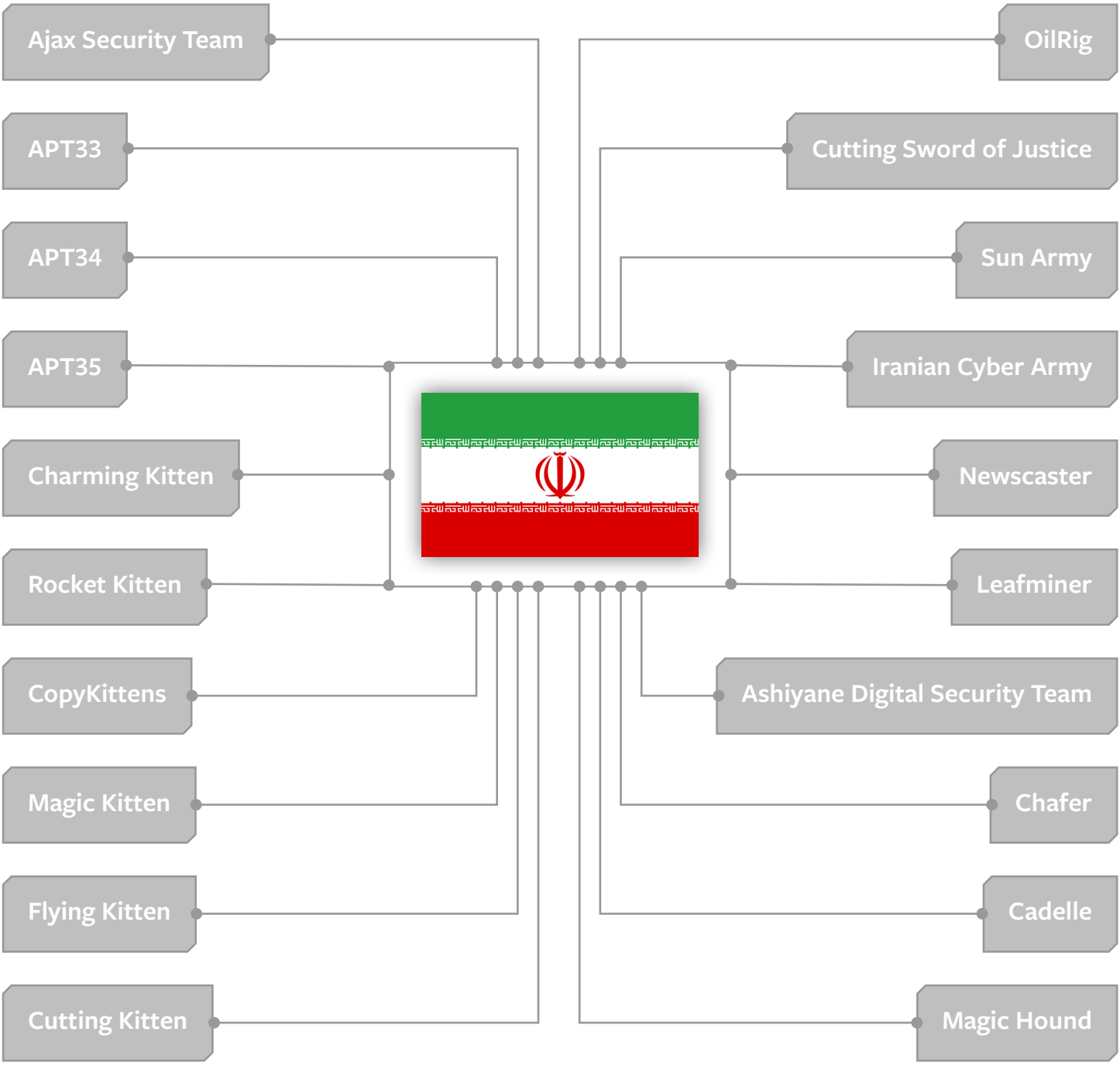
It is often difficult to identify Iranian cyber threat actors because they are not static. What at first appear to be distinct groups will later use the same network infrastructure or tactics in subsequent operations. For example, researchers initially identified separate hacker groups they labeled "Flying Kitten" and "Rocket Kitten" in 2013 and 2014. Then, in 2015, researchers noted the two groups employed similar modes of operation and shared domain names, leading them to conclude that "the ecosystem of Iranian actors is chaotic and ever-changing, making disambiguating different campaigns and groups a troublesome process."[62] The affiliation of individual hackers may also be fluid.[63]

Further complicating the challenge of attribution, these groups often use publicly available malware tools.[64] For example, even though the Shamoon 2 attacks in 2016-17 against Saudi Arabia described below shared characteristics with campaigns launched by the group labeled APT33, cyber security firm FireEye could not conclusively link ATP33 to those attacks because of "differences in both targeting and tactics, techniques and procedures (TTPs) associated with the group using SHAMOON and APT33."[65]

Nevertheless, a list of names of prominent Advance Persistent Threat (APT) groups is included in the graphic as a reference. In addition to the names the groups themselves use, the table also includes names assigned by cyber security firms when identifying campaigns, malware, and infrastructure. Different firms may ascribe different names to the same actors.[66] Some of these groups appear to have ceased operations over time, while some individual operatives may have shifted affiliation to other groups. Some hackers claim affiliation with the "Iranian Cyber Army,"[67] although the name implies more official backing from Tehran than the group receives.

59. U.S. Department of the Treasury, "Fact Sheet: Sanctions on Iranian Government and Affiliates," November 8, 2012. (https://www.treasury.gov/press-center/press-releases/Documents/Fact%20Sheet%20-%20Sanctions%20on%20Iranian%20Govt%20and%20Affiliates%20-%20November%208,%202012.pdf)
60. "Iran's supreme leader tells students to prepare for cyber war," *RT* (Russia), February 23, 2014. (https://www.rt.com/news/iran-israel-cyber-war-899/)
61. Frederick W. Kagan and Tommy Stiansen, "The growing cyberthreat from Iran: The initial report of Project Pistachio Harvest," *American Enterprise Institute and Norse Corporation*, April 2015, page 10. (https://www.aei.org/publication/growing-cyberthreat-from-iran/)
62. Collin Anderson, "Flying Kitten to Rocket Kitten, A Case of Ambiguity and Shared Code," *Iran Threats*, December 5, 2017. (https://iranthreats.github.io/resources/attribution-flying-rocket-kitten/)
63. Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," *Carnegie Endowment for International Peace*, January 2018, page 18. (https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf)
64. Ibid.
65. Jaqueline O'Leary, Josiah Kimble, Kelli Vanderlee, and Nalani Fraser, "Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware," *FireEye*, September 20, 2017. (https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html)
66. For an explanation of naming, see: Florian Roth, "The Newcomer's Guide to Cyber Threat Actor Naming," *Florian Roth Blog*, March 25, 2018. (https://medium.com/@cyb3rops/the-newcomers-guide-to-cyber-threat-actor-naming-7428e18ee263)
67. Ilan Berman, "The Future of Iranian Terror and Its Threat to the U.S. Homeland," *Statement before the House Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence*, February 11, 2016. (https://docs.house.gov/meetings/HM/HM05/20160211/104455/HHRG-114-HM05-Wstate-BermanI-20160211.pdf)

Names of Prominent APT Groups Linked to Iran



See Appendix for citations with additional information

While the Islamic Republic relies primarily on quasi-independent cyber operators to conduct its cyber attacks, experts have concluded that there is "consistent evidence" that Iranian cyber campaigns are "government-sponsored."[68] The U.S. government has also consistently connected Iran's malicious cyber activities to the regime and, more specifically, to the IRGC. DNI Clapper attributed the 2014 cyber attack on Las Vegas Sands to the Iranian government.[69] In March 2016, the Department of Justice unsealed an indictment against seven individuals responsible for the distributed denial of service (DDoS) attacks on U.S. financial institutions between 2011 and 2013. The Justice Department also charged one of the hackers with infiltration of the control systems of a dam in New York in August and September of 2013. According to the Justice Department's press statement, the companies employing the hackers were "sponsored by" the IRGC. Then-U.S. Attorney Preet Bharara called the incidents "calculated attacks by groups with ties to Iran's Islamic Revolutionary Guard and designed specifically to harm America and its people."[70]

Two years later, in 2018, the Department of Justice similarly stated that the individuals responsible for the infiltration of computers at hundreds of U.S. and foreign universities and dozens of U.S. companies, and the exfiltration of 30 terabytes of data, had "conducted many of the intrusions on behalf of" the IRGC.[71] Even the 2017 indictment for unauthorized access to HBO's computer systems and attempted extortion of the company noted that the accused "previously worked on behalf of the Iranian military to conduct computer network attacks that targeted military systems, nuclear software systems, and Israeli infrastructure."[72]

The Impact of Stuxnet, Sanctions, and the Nuclear Agreement

Three key incidents have significantly shaped the evolution of Iran's cyber capabilities: (1) the revelations of the Stuxnet virus in 2010; (2) escalating U.S. sanctions culminating with the "de-SWIFTing" of Iranian banks in 2012; and (3) the regime's decision in 2013 to negotiate a nuclear agreement with the P5+1 group, led by the United States.

Stuxnet: Cyber Domain as a Nation-State Weapon

The summer of 2010 marked a step-change in Tehran's – and the world's – understanding about the power of cyber tools. Researchers assess that a nation-state actor created the malware of then-unprecedented complexity to target Iran's core nuclear infrastructure.[73] Press reporting has since attributed the attack to a joint

68. Levi Gundert, Sanil Chohan, and Greg Lesnewich, "Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations," *Recorded Future*, May 9, 2018, page 7. (https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf)

69. James Clapper, "Hearing to Receive Testimony on Worldwide Threats," *Hearing before the Senate Armed Services Committee*, February 26, 2015, page 11. (https://www.armed-services.senate.gov/imo/media/doc/15-18%20-%202-26-15.pdf)

70. U.S. Department of Justice, Press Release, "Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities," March 24,2016. (https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated)

71. U.S. Department of Justice, Press Release, "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign On Behalf Of The Islamic Revolutionary Guard Corps," March 23, 2018. (https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic)

72. U.S. Department of Justice, Press Release, "Acting Manhattan U.S. Attorney Announces Charges Against Iranian National For Conducting Cyber Attack And $6 Million Extortion Scheme Against HBO," November 21, 2017. (https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-charges-against-iranian-national-conducting)

73. "W32.Stuxnet," *Symantec*, accessed September 14, 2018. (https://www.symantec.com/security-center/writeup/2010-071400-3123-99); Paul Szoldra, "A new film gives a frightening look at how the US used cyberwarfare to destroy nukes," *Business Insider*, July 7, 2016. (https://www.businessinsider.com/zero-days-stuxnet-cyber-weapon-2016-7)

U.S.-Israeli operation, but neither government has claimed responsibility.[74]

The virus first infiltrated Iranian systems in 2008, making its way to Iran's nuclear enrichment plant at Natanz[75] where it began slowly and meticulously to destroy centrifuges,[76] the precision machines that enrich uranium for both civilian nuclear fuel and atomic weapons. At the time, the Islamic Republic was pursuing a nuclear program in defiance of multiple UN Security Council resolutions.[77]

At Natanz, the Stuxnet virus quietly sabotage the Iranian nuclear program.[78] The virus sped up and slowed down the speed of the centrifuges, causing them to self-destruct.[79] Even more disorienting for Iran's nuclear scientists, the infected computer systems would report only normal activity. The scientists thus assumed there was an equipment or engineering problem and often shut down entire centrifuge cascades after one machine failed.[80]

Early iterations of the virus disabled a few centrifuges at a time, but then in the summer of 2010, a new variant knocked out about 1,000 machines, or roughly 10 percent of Iran's equipment.[81] After the virus was inadvertently discovered,[82] Iran had to briefly shut down the entire Natanz facility to contain the virus.[83] It confirmed that the virus had infected 30,000 computers.[84]

Investment and Restructuring

In the years following Stuxnet, the Islamic Republic dramatically improved its cyber capabilities.[85] Prior

74. Ellen Nakashima and Joby Warrick, "Stuxnet was work of U.S. and Israeli experts, officials say," *The Washington Post*, June 2, 2012. (https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.c6a19f64c443)
75. David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012. (https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html)
76. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014. (https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/)
77. Four times between December 2006 and March 2008, the United Nations Security Council demanded that Iran cease uranium enrichment and comply with International Atomic Energy Agency verification requirements, culminating with UN Security Council Resolution 1803. United Nations Security Council, Resolution 1803, March 3, 2008. (http://www.un.org/ga/search/view_doc.asp?symbol=S/RES/1803%282008%29)
78. For a detailed, technical study of Stuxnet, see: Ralph Langner, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," *The Langner Group*, November 2013. (https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf)
79. Karl Kruszelnicki, "Stuxnet the world's dirtiest digital bomb," *ABC* (Australia), November 1, 2011. (http://www.abc.net.au/science/articles/2011/11/01/3353334.htm)
80. David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012. (https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html)
81. Ibid; Ellen Nakashima and Joby Warrick, "Stuxnet was work of U.S. and Israeli experts, officials say," *The Washington Post*, June 2, 2012. (https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.c6a19f64c443)
82. Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, July 11, 2011. (https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/)
83. Ellen Nakashima and Joby Warrick, "Stuxnet was work of U.S. and Israeli experts, officials say," *The Washington Post*, June 2, 2012. (https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.c6a19f64c443)
84. Thomas Erdbrink and Ellen Nakashima, "Iran struggling to contain 'foreign-made' 'Stuxnet' computer virus," *The Washington Post*, September 27, 2010. (http://www.washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092706229.html)
85. 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/); Natasha Bertrand, "Iran is building a non-nuclear threat faster than experts 'would have ever imagined,'" *Business Insider*, March 27, 2015. (https://www.businessinsider.com/irans-cyber-army-2015-3); Eric Auchard, "Once 'kittens' in cyber spy world, Iran gaining hacking prowess -security experts," *Reuters*, September 20, 2017. (https://www.reuters.com/article/iran-cyber/once-kittens-in-cyber-spy-world-iran-gaining-hacking-prowess-security-experts-idUSL5N1M12OJ)

to 2011, Iran's entire cyber budget was believed to be about $76 million.[86] By 2016, Tehran was claiming to spend $1 billion per year on cyber programs,[87] although some experts have raised doubts about this figure.[88] Examining the Ministry of Information and Communications Technology's budget may provide a sense of Iran's cyber security investment: between 2013/14 and 2015/16, the ministry's cyber security budget increased more than tenfold.[89] Following the nuclear deal, Iran's budget for information technology infrastructure increased another 20 percent.[90]

> **"The summer of 2010 marked a step-change in Tehran's – and the world's – understanding about the power of cyber tools."**

To consolidate government bodies responsible for cyber space and internet policy,[91] Khamenei created the Supreme Cyberspace Council in March 2012 to oversee the full range of Iran's cyber activities.[92] Members of the council include the president, cabinet ministers, the head of the Islamic Republic of Iran Broadcasting, the commander of the IRGC, and other high-ranking officials from its intelligence and security agencies. In 2015, Khamenei reshuffled the membership, and as a result, the number of President Hassan Rouhani's cabinet ministers on the council increased.[93] The Supreme Cyberspace Council is not answerable to the Iranian parliament but rather reports to the supreme leader.[94] Seven months after creating the council, Iran reportedly held its first nation-wide cyber defense exercise.[95]

Proliferation of Government-Linked Hacker Groups

In the early 2000s, Iranian hackers defaced tens of thousands of websites in the United States, Israel, the UK, and France with crude attacks.[96] Stuxnet and the widespread domestic protests, in response to the fraudulent presidential election in 2009 (now known as the Green Movement), changed the Islamic Republic's relationship with these hackers.

86. Eric Shafa, "Iran's Emergence as a Cyber Power," *Strategic Studies Institute*, August 20, 2014. (http://ssi.armywarcollege.edu/index.cfm/articles/Irans-emergence-as-cyber-power/2014/08/20)
87. Sam Jones, "Cyber warfare: Iran opens a new front," *Financial Times* (UK), April 26, 2016. (https://www.ft.com/content/15e1acf0-0a47-11e6-b0f1-61f222853ff3)
88. For example, Saeed Ghasseminejad and Collin Anderson, both Iran experts and reviewers of this monograph, questioned the accuracy of this number.
89. The Small Media report notes an increase from 42,073 million IRR ($1.7 million) in 2013/2014 to 550,000 million IRR ($19.3 million) by 2015/2016. To convert to dollars, the authors used the budget exchange rates of 24,500 IRR to 1 dollar in 2013/4 and 28,500 IRR to 1 dollar in 2015/6. "Iranian Internet Infrastructure and Policy Report Special Edition: The Rouhani Review (2013-15)," *Small Media*, February 2015, page 7. (https://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb15.pdf)
90. Author interview with Mahmood Enayat, April 19, 2018.
91. "Institutional developments," *Center for Human Rights in Iran*, January 9, 2018. (https://www.iranhumanrights.org/2018/01/ir2017-institutional-developments/)
92. Eric Shafa, "Iran's Emergence as a Cyber Power," *Strategic Studies Institute*, August 20, 2014. (http://ssi.armywarcollege.edu/index.cfm/articles/Irans-emergence-as-cyber-power/2014/08/20)
93. "Rewiring Iran's Supreme Council of Cyberspace," *Small Media*, December 2, 2015. (https://smallmedia.org.uk/news/rewiring-irans-supreme-council-of-cyberspace)
94. Farnaz Fassihi, "Iran's Censors Tighten Grip," *The Wall Street Journal*, March 16, 2012. (https://www.wsj.com/articles/SB10001424052702303717304577279381130395906)
95. James A. Lewis, "Cybersecurity and Stability in the Gulf," *Center for Strategic and International Studies*, January 2014, page 3. (https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/140106_Lewis_GulfCybersecurity_Web_0.pdf)
96. Dorothy Denning, "Following the developing Iranian cyberthreat," *The Conversation*, December 11, 2017. (https://theconversation.com/following-the-developing-iranian-cyberthreat-85162)

The Green Movement: The First Catalyst

One of the most pivotal moments for the Iranian regime was the 2009 Green Movement. Following the June 2009 presidential election, demonstrations rocked the country as Iranian citizens protested what they viewed as a rigged outcome. The regime responded aggressively, deploying volunteer and regular forces to scatter, beat, and arrest thousands of protestors.

While the regime crushed the protests in relatively short order, the Iranian population's use of the internet to mobilize spontaneously and rapidly share information convinced the leadership that the cyber battlefield was a key weakness. The government sought to develop its cyber capabilities for regime security, as well as to protect the ideological purity of the Islamic Republic by surveilling and censoring internal dissent and blocking the infiltration of Western ideas.[97] The regime leverages an elaborate network of private actors to execute these policies.[98] To date, most victims of Iranian cyber operations are Iranians.[99]

New evidence suggests that Iran is expanding the ideological battle beyond its "internal enemies." Facebook, Twitter, and Google announced in August 2018 the dismantling of an Iranian social media influence campaign aimed at U.S., UK, Latin American, and Middle Eastern audiences.[100] The operation is one of the first reported cases of actors from the Islamic Republic exploiting social media to target audiences outside Iran.[101]

In the immediate aftermath of the Green Movement and Stuxnet, the regime wanted to create a formal offensively oriented cyber organization but was unable to build a "politically and religiously reliable workforce."[102] Instead, the government and IRGC employed "an ideologically and politically trusted group of middle managers" to delegate specific tasks to hackers or groups of hackers, at times employing "sub-contractors" to assemble and deploy the tools for a single objective.[103] For example, two different

97. Gabi Siboni and Sami Kronenfeld, "Iran and Cyberspace Warfare," *Military and Strategic Affairs*, December 2012, page 77. (http://www.inss.org.il/wp-content/uploads/systemfiles/MASA4-3Engd_Siboni%20and%20Kronenfeld.pdf); Gabi Siboni and Sam Kronenfeld, "Developments in Iranian Cyber Warfare, 2013-2014," *Institute for National Security Studies*, April 3, 2014. (http://www.inss.org.il/wp-content/uploads/systemfiles/No.%20536%20-%20Gabi%20and%20Sami%20for%20web.pdf)

98. "Freedom on the Net 2017: Iran," *Freedom House*, accessed September 21, 2018. (https://freedomhouse.org/sites/default/files/FOTN%202017_Iran.pdf); "2017 In Review: Filterwatch: An Iranian Internet Infrastructure and Policy Report," *Small Media*, accessed September 21, 2018. (https://www.smallmedia.org.uk/media/projects/files/Filterwatch2017InReview.pdf)

99. Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," *Carnegie Endowment for International Peace*, January 4, 2018, pages 6 and 22-23. (http://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134)

100. Annie Fixler, "Iran's Facebook operation shows that it never restrained its hackers," *The Hill*, August 26, 2018. (http://thehill.com/opinion/cybersecurity/403433-irans-facebook-operation-shows-that-it-never-restrained-its-hackers)

101. Craig Timberg, Elizabeth Dwoskin, Tony Romm, and Ellen Nakashima, "Sprawling Iranian influence operation globalizes tech's war on disinformation," *The Washington Post*, August 21, 2018. (https://www.washingtonpost.com/technology/2018/08/21/russian-iran-created-facebook-pages-groups-accounts-mislead-users-around-world-company-says/?utm_term=.6051b5222fc1); "Suspected Iranian Influence Operation: Leveraging Inauthentic News Sites and Social Media Aimed at U.S., U.K., Other Audiences," *FireEye*, August 2018, page 5. (https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-FireEye-Iranian-IO.pdf)

102. Levi Gundert, Sanil Chohan, and Greg Lesnewich, "Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations," *Recorded Future*, May 9, 2018, page 3. (https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf)

103. Levi Gundert, Sanil Chohan, and Greg Lesnewich, "Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations," *Recorded Future*, May 9, 2018, pages 3 and 6-7. (https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf)

hackers or groups might work on separate components of malware rather than Iran assigning the entire task to one operator.

Initially adopted for expediency, this "contractor" model has endured. Since Stuxnet, Iranian hackers have professionalized. The marketplace has expanded, and there has been a proliferation of Iranian cyber groups.[104] In an in-depth study of the hacker landscape in Iran, experts at the cyber threat intelligence firm Recorded Future concluded that there are as many as 50 contractors "vying for Iranian government-sponsored offensive cyber projects."[105] These actors often work within Iranian corporate entities or for the security services.[106] Iranian private companies and government entities "blur the line between legitimate engineering companies and state-sponsored cyber hacking teams."[107] The same cyber operatives may simultaneously engage in criminal activity, legitimate software development, and regime-sponsored operations.[108] There are also indications that the government adopts successful, independently initiated operations and throws its support behind enterprising hackers.[109]

Iranian cyber actors have since become resourceful and astute students, reportedly learning not only to use existing tools but also to replicate the kinds of attacks Iran has suffered.[110] They combine off-the-shelf malware with custom tools.[111] Whereas the distributed denial of service (DDoS) attacks on U.S. banks between 2011 and 2013 may have relied on "botnets-for-hire,"[112] Operation Saffron Rose in 2013-14, which targeted both internal dissidents and U.S. defense companies, was the first reported case of Iranian operatives using custom malware tools.[113] Tehran has been able to cause significant damage even while relying on mostly

104. For example, see: "Advanced Persistent Threat Groups: Who's who of cyber threat actors," *FireEye*, accessed September 12, 2018. (https://www.fireeye.com/current-threats/apt-groups.html); Matt Dahl, "Cat Scratch Fever: CrowdStrike Tracks Newly Reported Iranian Actor as FLYING KITTEN," *CrowdStrike*, May 13, 2014. (https://www.crowdstrike.com/blog/cat-scratch-fever-crowdstrike-tracks-newly-reported-iranian-actor-flying-kitten/); "Rocket Kitten: A Campaign with 9 Lives," *Check Point*, 2015. (https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf); "2018 Global Threat Report: Blurring the Lines between Statecraft and Tradecraft," *CrowdStrike*, 2018. (https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf); Eduard Kovacs, "Iran-Linked Espionage Group Continues Attacks on Middle East," *Security Week*, September 2, 2015. (https://www.securityweek.com/iran-linked-espionage-group-continues-attacks-middle-east)

105. Levi Gundert, Sanil Chohan, and Greg Lesnewich, "Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations," *Recorded Future*, May 9, 2018, page 3. (https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf)

106. David E. Sanger and Nicole Perlroth, "Iran Is Raising Sophistication and Frequency of Cyberattacks, Study Says," *The New York Times*, April 15, 2015. (https://www.nytimes.com/2015/04/16/world/middleeast/iran-is-raising-sophistication-and-frequency-of-cyberattacks-study-says.html)

107. "Operation Cleaver," *Cylance*, December 2014, page 5. (https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf)

108. Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," *Carnegie Endowment for International Peace*, January 2018, pages 18 and 23-25. (https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf)

109. Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (New York: Cambridge University Press, 2018) pages 83-88.

110. Kim Zetter, "The NSA Acknowledges What We All Feared: Iran Learns From Us Cyberattacks," *Wired*, February 10, 2015. (https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/); "Operation Cleaver," *Cylance*, December 2014, page 63. (https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf)

111. "OilRig is Back with Next-Generation Tools and Techniques," *Nyotron*, March 2018, page 3. (https://www.nyotron.com/wp-content/uploads/2018/03/Nyotron-OilRig-Malware-Report-March-2018C.pdf)

112. Eduard Kovacs, "The Jester: Anonymous Hackers Helped Izz ad-Din al Qassam DDOS US Banks," *Softpedia News* (Romania), September 27, 2012. (https://news.softpedia.com/news/The-Jester-Anonymous-Hackers-Helped-Izz-ad-Din-al-Qassam-DDOS-US-Banks-295009.shtml); Lucian Constantin, "Botnets for hire likely used in attacks against US banks, security firm says," *CSO*, January 9, 2013. (https://www.csoonline.com/article/2132747/data-protection/botnets-for-hire-likely-used-in-attacks-against-us-banks--security-firm-says.html)

113. Nart Villeneuve, Mike Scott, Thoufique Haq, and Ned Moran, "Operation Saffron Rose," *FireEye*, May 2014. (https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf)

rudimentary cyber tools – DDoS techniques, spear phishing, and wiper malware.

Escalating Sanctions and Cyber Retaliation

As the Islamic Republic was dealing with the aftershocks of Stuxnet and expanding its own cyber capabilities, it became the target of a second campaign that shaped its thinking on cyber. By 2012, the regime began to feel the full power of U.S. economic warfare capabilities. Beginning in 2006, when the U.S. Treasury initiated a campaign to convince banks around the world to cease doing business with Iran, hundreds of Iranian companies and individuals found themselves cut off from the global banking system and their assets frozen, as the United States systematically sanctioned Iranian nuclear and weapons proliferators, terrorist supporters, human rights violators, and their financial enablers.[114] By 2010, U.S. sanctions were having a significant effect on the Iranian economy. In the latter half of that year, Iran lost between $50 and $60 billion in potential energy investments.[115] Over the next two years, additional U.S. and EU measures[116] jointly reduced Iran's crude oil exports – which accounted for approximately 80 percent of the country's export earnings – from 2.5 million barrels per day to approximately 1 million.[117]

"Iranian cyber actors have since become resourceful and astute students. … Tehran has been able to cause significant damage even while relying on mostly rudimentary cyber tools."

In March 2012, the global financial messaging system SWIFT removed sanctioned Iranian banks from its network, while permitting some to remain on the network to facilitate permitted humanitarian trade.[118] Without this access, Iranian banks and businesses reportedly resorted to conducting business using suitcases of cash.[119] Then, Congress passed legislation requiring purchasers of Iranian crude oil to deposit payments to Iran in escrow accounts, significantly restricting Iran's access and use of its foreign currency.[120] By the end of 2013, Tehran was facing a balance of payments crisis with as little as $20 billion in fully accessible foreign currency reserves.[121]

114. For a history of U.S. sanctions on Iran, see: Mark Dubowitz and Annie Fixler, "'SWIFT' Warfare: Power, Blowback, and Hardening American Defenses," *Foundation for Defense of Democracies*, July 2015. (https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/publications/Cyber_Enabled_Swift.pdf)
115. William Burns, "Implementing Tougher Sanctions on Iran: A Progress Report," *Testimony before the House Foreign Affairs Committee*, December 1, 2010. (https://2009-2017.state.gov/p/us/rm/2010/152222.htm)
116. Farnaz Fassihi and John M. Biers, "EU Bans Imports of Iran's Oil, Raising Pressure on Tehran," *The Wall Street Journal*, January 24, 2012. (https://www.wsj.com/articles/SB10001424052970203718504577178231285985826)
117. U.S. Energy Information Administration, "Sanctions reduced Iran's oil exports and revenues in 2012," April 26, 2013. (http://www.eia.gov/todayinenergy/detail.cfm?id=11011)
118. "Payments system SWIFT to expel Iranian banks Saturday," *Reuters*, March 15, 2012. (http://www.reuters.com/article/2012/03/15/us-nuclear-iran-idUSBRE82E15M20120315); Society for Worldwide Interbank Financial Telecommunication (SWIFT), Press Release, "SWIFT Instructed to Disconnect Sanctioned Iranian Banks Following EU Council Decision," March 15, 2012. (https://www.swift.com/insights/press-releases/swift-instructed-to-disconnect-sanctioned-iranian-banks-following-eu-council-decision); "Swift Sanctions on Iran," *The Wall Street Journal*, February 1, 2012. (https://www.wsj.com/articles/SB10001424052970203718504577178902535754464)
119. Christopher Harress, "Iran's Rouhani Faces Music as Sanctions Bite Harder, Is There a SWIFT Solution in the Works?" *International Business Times*, October 8, 2013. (https://www.ibtimes.com/irans-rouhani-faces-music-sanctions-bite-harder-there-swift-solution-works-1417768)
120. Iran Threat Reduction and Syria Human Rights Act of 2012, Pub. L. 112-158, 126 Stat. 1214, codified as amended at 112 U.S.C. (https://www.congress.gov/112/plaws/publ158/PLAW-112publ158.pdf)
121. Mark Dubowitz and Rachel Ziemba, "When Will Iran Run Out of Money?" *Foundation for Defense of Democracies and Roubini Global Economics*, October 2, 2013. (https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/Iran_Report_Final_2.pdf)

Targeting the U.S. Financial System

Facing an economic crisis, Iran responded aggressively – and directly – against the United States by launching widespread distributed denial of service (DDoS) attacks against U.S. banks. Iran sought to show the world that it, too, could cause economic damage to its adversaries. Given the size of the American economy and the role of the dollar in global commerce, it would have been pointless for Iran to respond using conventional economic or financial tools. Rather, to engage in its own form of economic warfare, Iran turned to cyber.

The offensive began in December 2011 and continued into mid-2013, comprising a series of DDoS attacks known as Operation Ababil.[122] The attacks occurred only intermittently for the first ten months and then escalated to a near-weekly basis starting in September 2012,[123] six months after the "de-SWIFTing" of Iranian banks. The attacks targeted 46 banks and financial systems including Bank of America, Wells Fargo, JPMorgan Chase, and the New York Stock Exchange, according to a U.S. Department of Justice indictment. Using infected internet servers around the world to flood the banks' websites with an overwhelming volume of traffic, the attackers paralyzed the websites of banks and other financial institutions,[124] preventing hundreds of thousands of individuals and businesses from accessing their online accounts, and costing these financial firms tens of millions of dollars to remediate.[125] At the time, the Obama administration appealed to 120 countries to intercept the malignant traffic and debug the internet servers located in their territory. While many countries assisted, the response was not fully effective, and some attacks continued.[126]

A group calling itself Izz ad-Din al-Qassam claimed responsibility for the DDoS attacks[127] and denied state sponsorship. The Islamic Republic likewise denied official involvement.[128] Press reporting concurrent with the attacks, however, confirmed that U.S. officials believed the Iranian government was responsible.[129] In March 2016, the U.S. Department of Justice formally accused Tehran of sponsoring the attack, unsealing an indictment against seven Iranian hackers and alleging that their employers, ITSec Team and Mersad, "performed work on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps."[130]

122. Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *The New York Times*, January 8, 2013. (https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html)
123. U.S. Department of Justice, Press Release, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," March 26, 2016. (https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged)
124. Joseph Menn, "Cyber attacks against banks more severe than most realize," *Reuters*, May 17, 2013. (https://www.reuters.com/article/us-cyber-summit-banks/cyber-attacks-against-banks-more-severe-than-most-realize-idUSBRE94G0ZP20130518)
125. U.S. Department of Justice, Press Release, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," March 26, 2016. (https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged)
126. Ellen Nakashima, "U.S. rallied multinational response to 2012 cyberattack on American banks," *The Washington Post*, April 11, 2014. (https://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html?utm_term=.0a2194e5bef4)
127. Rym Momtaz and Lee Ferran, "US Bank Cyber Attackers Deny Iran Connection." *ABC News*, November 12, 2012. (http://abcnews.go.com/Blotter/us-bank-cyber-attackers-deny-iran-connection/story?id=17620096)
128. Eduard Kovacs, "The Jester: Anonymous Hackers Helped Izz ad-Din al Qassam DDOS US Banks," *Softpedia News* (Romania), September 27, 2012. (https://news.softpedia.com/news/The-Jester-Anonymous-Hackers-Helped-Izz-ad-Din-al-Qassam-DDOS-US-Banks-295009.shtml)
129. Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *The New York Times*, January 8, 2013. (https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html)
130. Indictment, *United States of America v. Ahmad Fathi et al*, 16 Cr. (S.D.N.Y filed March 16, 2016). (https://www.justice.gov/opa/file/834996/download)

In the same indictment, the Justice Department charged Hamid Firoozi of ITSec with hacking into New York's Bowman Avenue Dam between August and September 2013.[131] While the dam itself is small and inconsequential to national critical infrastructure, experts and officials speculated that the hacker had either confused the dam for a much larger one with a similar name, or was conducting a dry run for a future, more destructive attack.[132]

"On August 15, 2012, the Shamoon malware wiped the data on 35,000 network computers at Saudi Arabia's Aramco, the world's largest oil producer. … Overnight, the company had to revert to faxes, interoffice mail, and typewriters."

Saudi Aramco Hack

Iran also turned its attention to its primary regional rival (and American ally): Saudi Arabia. Iran sought to damage Riyadh by undermining its oil industry, on which the U.S. would increasingly rely to stabilize oil markets as U.S. sanctions began cutting Iranian oil exports and production. On August 15, 2012, the Shamoon malware wiped the data on 35,000 network computers at Saudi Arabia's Aramco, the world's largest oil producer.[133] The virus erased the data on three-quarters of Aramco's corporate computers and replaced the files with an image of a burning American flag.[134] While Shamoon did not affect Aramco's oil production, the virus disrupted a majority of Aramco's business processes, including its supply management, shipping, and contract management.[135]

Overnight, the company had to revert to faxes, inter-office mail, and typewriters. Aramco professionals physically unplugged the firm's computers to stop the virus from spreading, and representatives purchased 50,000 new hard drives, temporarily causing a spike in global hard drive prices. It took approximately five months to get the entire organization back online.[136]

The Iranian hacker group Cutting Sword of Justice claimed responsibility, stating that the attack was in retaliation for Saudi Arabia's oppression and regional crimes.[137] After investigating the virus, FireEye concluded it showed the characteristics and sophistication of a state actor.[138] U.S. officials later confirmed Iran's involvement.[139]

---

131. Ibid.

132. Joseph Berger, "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case," *The New York Times*, March 25, 2016. (https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html)

133. Jose Pagliery, "The inside story of the biggest hack in history," *CNN Money*, August 5, 2015. (http://money.cnn.com/2015/08/05/technology/aramco-hack/); A variant of the Shamoon virus also hit joint ExxonMobil-Qatar Petroleum operation RasGas a few weeks after the Aramco attack. "Computer virus hits second energy firm," *BBC* (UK), August 31, 2012. (https://www.bbc.com/news/technology-19434920); Camilla Hall and Javier Blas, "Qatar group falls victim to virus attack," *Financial Times* (UK), August 30, 2012. (https://www.ft.com/content/17b9b016-f2bf-11e1-8577-00144feabdc0); "Virus attack takes down RasGas," *Doha News* (Qatar), August 30, 2012. (https://dohanews.co/virus-attack-takes-down-rasgas-computer-systems/#axzz252TZUzKO)

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

135. Jose Pagliery, "The inside story of the biggest hack in history," *CNN Money*, August 5, 2015. (http://money.cnn.com/2015/08/05/technology/aramco-hack/)

136. Ibid.

137. The Iranian hacker group Cutting Sword of Justice claimed responsibility for the Aramco hack on this message board: "Untitled," *Pastebin*, August 15, 2012. (https://pastebin.com/HqAgaQRj)

138. Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, and Christopher Glyer, "Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure," *Fire Eye*, December 14, 2017. (https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html)

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

The attack was part of a longstanding rivalry between Saudi Arabia and Iran and likely had multiple intended outcomes. At the time, Iran's oil exports were dropping rapidly as the EU imposed its ban on imports of Iranian crude. It is possible that Tehran hoped an attack on a major oil producer would drive up prices so that Iran's limited exports would bring in more revenue. If that was the goal, the operation failed. Global prices did not experience a sustained spike following the attack.[140]

"Iran likely targeted Saudi economic assets to undermine Saudi energy power and its related geopolitical power because the Islamic Republic understands the connection between economic and geopolitical power."

The campaign may also have been retaliation for a suspected cyber attack on Tehran's Oil Ministry and various Iranian energy companies in April 2012.[141] The Shamoon malware reportedly mimicked the wiper malware used against the Iranian Oil Ministry and the National Iranian Oil Company.[142]

While each of these motivations may have been a factor, Iran likely targeted Saudi economic assets to undermine Saudi energy power and its related geopolitical power because the Islamic Republic understands the connection between economic and geopolitical power. From its founding, the Islamic Republic conceptualized its own economy as providing the means to fortify the revolution at home and export it abroad. The Iranian constitution states that the economy "is a means that is not expected to do anything except better facilitate reaching the goal [of advancing the Islamic revolution]."[143] This is also why the IRGC – created to consolidate, defend, and export the ideology of the revolution[144] – plays a dominant role in the Iranian economy.[145] Supreme Leader Ayatollah Ali Khamenei has called the U.S. Department of the Treasury "America's war chamber," and noted that the "method of the US is to confront the freedom-seeking and independent system of the Islamic Republic by pursuing this economic war."[146] The Saudi Aramco hack applied this logic to weaken the House of Saud and undermine an energy superpower on which the U.S. and global economy depends.

140. U.S. Energy Information Administration, "2012 Brief: Average 2012 crude oil prices remain near 2011 levels," January 10, 2013. (https://www.eia.gov/todayinenergy/detail.php?id=9530)

141. Thomas Erdbrink, "Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals From Internet," *The New York Times*, April 23, 2012. (http://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html); Jen Alic, "Attack on Iran's Oil Industry Ups Cyber Warfare Stakes," *Oilprice.com*, May 1, 2012. (http://oilprice.com/Energy/Crude-Oil/Attack-on-IransOil-Industry-Ups-Cyber-Warfare-Stakes.html); "Suspected cyber attack hits Iran oil industry," *Reuters*, April 23, 2012. (https://www.reuters.com/article/net-us-iran-oil-cyber-idUSBRE83M0P120120423)

142. Kim Zetter, "The NSA Acknowledges What We All Feared: Iran Learns from US Cyberattacks," *Wired*, February 10, 2015. (https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/)

143. Constitution of the Islamic Republic of Iran 1979 (as last amended on July 28, 1989), Preamble. (http://www.wipo.int/edocs/lexdocs/laws/en/ir/ir001en.pdf)

144. Afshon Ostovar, *Vanguard of the Imam: Religion, Politics, and Iran's Revolutionary Guards* (New York: Oxford University Press, 2016), pages 121-140; Karim Sadjadpour, *Reading Khamenei: The Worldview of Iran's Most Powerful Leader* (Washington, DC: Carnegie Endowment for International Peace, 2009), pages 14-27. (http://carnegieendowment.org/files/sadjadpour_iran_final2.pdf); Mehdi Khallaji, *Tightening the Reins: How Khamenei Makes Decisions* (Washington, DC: The Washington Institute for Near East Policy, 2014), pages 1-15. (http://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyFocus126_Khalaji.pdf)

145. Emanuele Ottolenghi, Saeed Ghasseminejad, Annie Fixler, and Amir Toumaj, "How the Nuclear Deal Enriches Iran's Revolutionary Guard Corps," *Foundation for Defense of Democracies*, October 2016, page 7. (https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/IRGC_Report.pdf)

146. Iranian Supreme Leader Ali Khamenei, "The best way to confront the enemy's economic war is to support Iranian products," *Remarks on Labor Day*, April 30, 2018. (http://english.khamenei.ir/news/5642/The-best-way-to-confront-the-enemy-s-economic-war-is-to-support)

The Nuclear Deal

While Operation Ababil and the Saudi Aramco hack showed that Iran could retaliate in the cyber domain, neither offensive relieved the economic pressure imposed by Western sanctions. Tehran realized that it could not financially sustain its quest for nuclear capabilities and therefore sought to negotiate a reprieve from economic sanctions.[147] In the middle of 2013, Supreme Leader Ali Khamenei empowered President Rouhani to pursue a nuclear deal using the same strategy Rouhani, a regime loyalist,[148] had used a decade earlier in negotiations with the Europeans: In exchange for sanctions relief, Iran would suspend nuclear work in areas where it had completed its research while preserving the ability to continue work on other components of the nuclear cycle that its scientists had not yet perfected.[149]

From the beginning of nuclear negotiations in 2013 through the implementation of the deal in January 2016, the clerical regime did not curtail its support for violent militias and terrorist groups throughout the region.[150] It continued to advance its ballistic missile program, take Western hostages, and threaten U.S. and Western shipping in the Gulf.[151] Similarly, Tehran did not cease its malicious cyber activity. Israeli Prime Minister Benjamin Netanyahu said in June 2013 that Israel had seen a "significant increase in the scope" of cyber attacks on its "vital national systems" by hackers backed by Iran and its terrorist proxies Hezbollah and Hamas.[152]

Iranian cyber operatives targeted nearly every country in the region, with its most aggressive actions aimed at Saudi Arabia.[153] It does appear, however, that the regime made a decision, starting in 2013, to refrain from conducting destructive cyber operations against

147. Behnam Ben Taleblu, "Misreading Khamenei's Nuclear Role," *War on the Rocks*, June 25, 2015. (https://warontherocks.com/2015/06/misreading-khameneis-nuclear-role/)

148. Sohrab Ahmari, "Behind Iran's 'Moderate' New Leader," *The Wall Street Journal*, June 16, 2013. (http://www.wsj.com/articles/SB10001424127887323566804578549262039104552); Hassan Rouhani, "Remarks before the Iranian Majlis," *Translation provided by BBC*, July 14, 1999. (http://news.bbc.co.uk/2/hi/world/monitoring/394731.stm); Reuel Marc Gerecht and Ali Alfoneh, "The Man and The Myth," *The Weekly Standard*, July 5, 2014. (https://www.weeklystandard.com/reuel-marc-gerecht-and-ali-alfoneh/the-man-and-the-myth); Ray Takeyh, "Iran's President Isn't a Reformer. He's an Enabler," *Politico*, May 22, 2017. (https://www.politico.com/magazine/story/2017/05/22/irans-president-isnt-a-reformer-hes-an-enabler-215171)

149. Iranian Supreme National Security Council Secretary Hasan Rouhani, "Beyond the Challenges Facing Iran and the IAEA Concerning the Nuclear Dossier," *Remarks to Iran's Supreme Cultural Revolution Council*, translated by Arms Control Wonk, September 30, 2005. (http://www.armscontrolwonk.com/files/2012/08/Rahbord.pdf); Behnam Ben Taleblu, "Why the US should be wary about Rouhani's reelection in Iran," *The Hill*, May 24, 2017. (https://thehill.com/blogs/pundits-blog/international-affairs/334916-why-the-us-should-be-wary-about-rouhanis-reelection)

150. Aaron David Miller, "One Year After Nuclear Deal, Iran's Rights Violations and Regional Aggression Continue," *The Wall Street Journal*, July 14, 2016. (https://blogs.wsj.com/washwire/2016/07/14/one-year-after-nuclear-deal-irans-rights-violations-and-regional-aggression-continue/)

151. Melissa Etehad and Carol Morello, "Another American has been detained in Iran, the fourth dual national in five months to be arrested," *The Washington Post*, July 27, 2016. (https://www.washingtonpost.com/world/national-security/another-american-has-been-detained-in-iran-the-fourth-dual-national-in-five-months-to-be-arrested/2016/07/26/84ab02fa-52a7-11e6-88eb-7dda4e2f2aec_story.html?utm_term=.20c42d9d0c37); Idrees Ali, "Iran tested medium-range ballistic missile: U.S. official," *Reuters*, January 30, 2017. (https://www.reuters.com/article/us-usa-iran-missiles/iran-tested-medium-range-ballistic-missile-u-s-official-idUSKBN15E2EZ); Alex Lockie, "Why Iran is 'playing with fire' in the Persian Gulf against US Navy ships," *Business Insider*, September 6, 2016. (https://www.businessinsider.com/iran-playing-with-fire-in-persian-gulf-2016-9)

152. "Iran ups cyber attacks on Israeli computers: Netanyahu," *Reuters*, June 9, 2013. (https://uk.reuters.com/article/us-israel-iran-cyber/iran-ups-cyber-attacks-on-israeli-computers-netanyahu-idUKBRE95808H20130609)

153. Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," *Carnegie Endowment for International Peace*, January 2018, pages 34-35. (https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf)

U.S. targets, with the exception of the February 2014 Las Vegas Sands casino attack.[154] Tehran may have reasoned that its hackers could better hone their skills by practicing on the Gulf Arab states – targets with weaker cyber defenses. That said, Iran occasionally sought to challenge Israel in the cyber domain. During the summer 2014 conflict between Israel and Hamas, Israeli experts noted an increase in website defacements and DDoS attacks by Iranian and proxy hackers.[155]

"During the nuclear negotiations and after the nuclear agreement was reached, Iran also engaged in a global campaign of cyber espionage and infiltration."

By limiting the majority of its destructive attacks to the region, Iran exploited the rift that formed between the United States and its regional allies during the nuclear negotiations.[156] The clerical regime likely calculated (correctly) that just as the Obama administration was not going to scuttle the nuclear negotiations over Iranian-backed violence in Syria, Gaza, or Yemen, its hackers could continue to attack America's regional allies without provoking a response from Washington.

Expanding Global Cyber Infiltration

During the nuclear negotiations and after the nuclear agreement was reached, Iran also engaged in a global campaign of cyber espionage and infiltration. Between 2013 and 2017, at the direction of the IRGC, Iranian hackers infiltrated hundreds of universities, private companies, and government agencies in the U.S. and around the world, stealing more than 30 terabytes of academic data and intellectual property.[157] The affected universities had spent $3.4 billion on subscription services alone to access the data in question. Iranian hackers simply stole it. The intellectual property was the result of thousands of hours of academic research. Data stolen from 11 technology companies, an industrial machinery company, and a biotechnology company may have helped Iran circumvent increasingly strict U.S. export controls as a means to improve its military capabilities.

In December 2014, cyber security firm Cylance published an in-depth study of another two-year global Iranian cyber operation named Operation Cleaver. The firm assessed the motivation of the attackers was to establish a "beachhead for cyber sabotage."[158] Another goal was to strategically pre-position assets for exploitation. The principal difference between computer network exploitation (CNE) and computer network attack (CNA) is the intent of the perpetrator. Exploitation and intelligence collection can create a persistent access route. If the intent of an attacker changes, that access route can easily be utilized to deliver a cyber weapon.

---

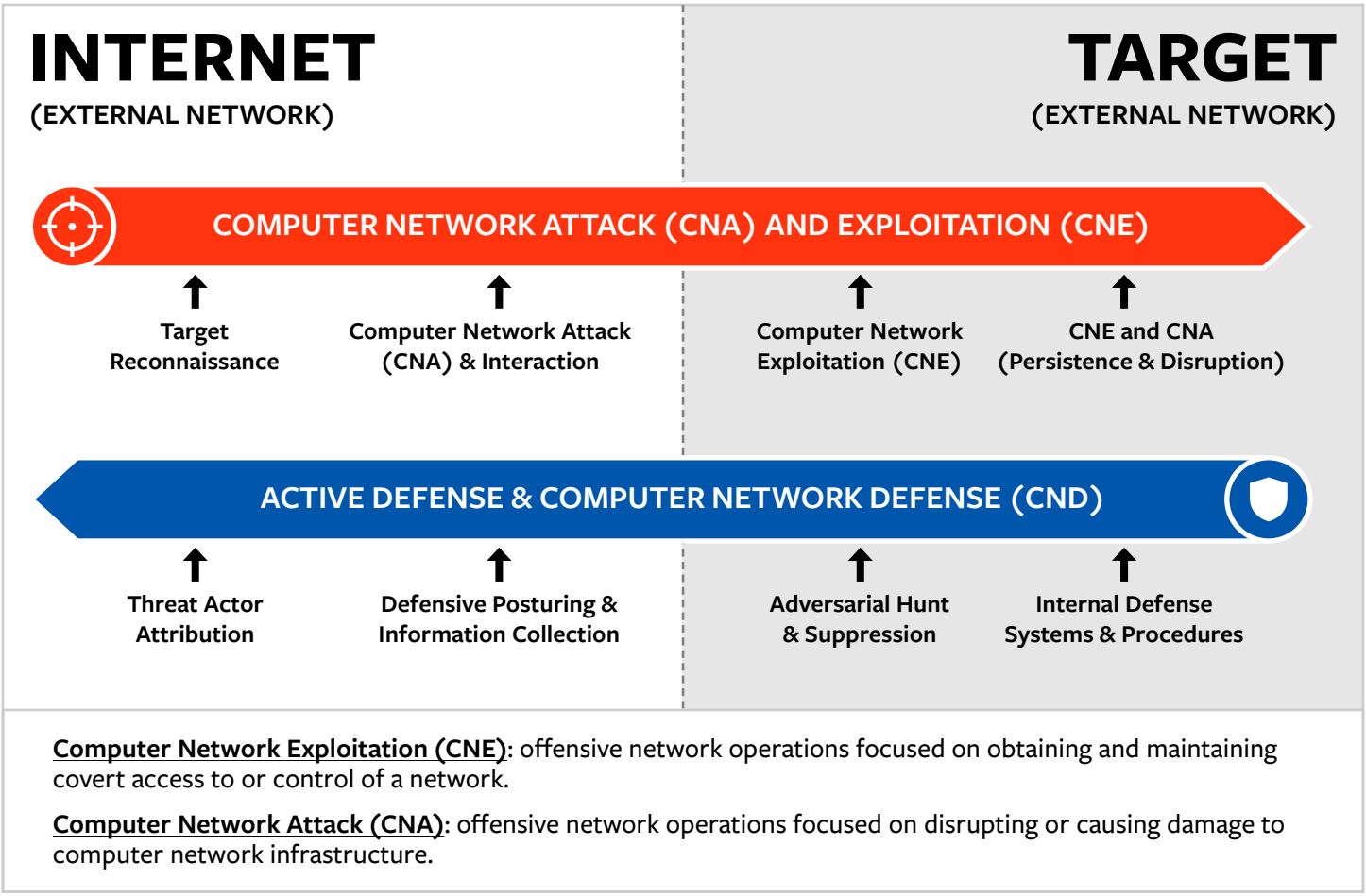
154. Kate Brannen, "Abandoning Iranian Nuclear Deal Could Lead to New Wave of Cyberattacks," *Just Security*, October 2, 2017. (https://www.justsecurity.org/45549/abandoning-iranian-nuclear-deal-lead-wave-cyberattacks/)

155. Armin Rosen, "Israel Faced A Huge Wave Of Cyber Attacks During Its War With Hamas — And Iran Could Be The Reason Why," *Business Insider*, August 18, 2014. (https://www.businessinsider.com/israel-faced-a-wave-of-cyber-attacks-2014-8)

156. For example, see: Frida Ghitis, "Obama, Arab nations dance to different tunes," *CNN*, May 15, 2015. (https://www.cnn.com/2015/05/15/opinions/ghitis-arab-leaders-summit/index.html); "Why Arab allies are worried over the Iran nuclear deal," *CBS News*, July 15, 2015. (https://www.cbsnews.com/news/iran-nuclear-deal-saudi-arabia-arab-allies-israel-middle-east-sunni-shiite/); Adam Entous, "Spy vs. Spy: Inside the Fraying U.S.-Israel Ties," *The Wall Street Journal*, October 22, 2015. (https://www.wsj.com/articles/spy-vs-spy-inside-the-fraying-u-s-israel-ties-1445562074)

157. U.S. Department of Justice, Press Release, "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign On Behalf Of The Islamic Revolutionary Guard Corps," March 23, 2018. (https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic)

158. "Operation Cleaver," *Cylance*, December 2014, page 6. (https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf)



Cylance assessed that Operation Cleaver was "too significant to be a lone individual or a small group." Leveraging publicly available hacking tools and custom malware, the group infiltrated companies worldwide in the energy, utility, and aviation sectors; military intelligence; and even hospitals and universities. Comparing the operation to those conducted by Chinese cyber operators, Cylance warned, "Iran is no longer content to retaliate against the US and Israel alone," but rather seeks to "position [itself] to impact critical infrastructure globally."[159]

In another case, Israeli cyber security firm Clearsky uncovered an Iranian cyber campaign they called Thamar Reservoir, dating back to at least mid-2014, whose purpose seemed to be neither stealing money nor conducting destructive cyber attacks. Instead, the attackers engaged in espionage, stole information, and potentially used their infiltration to enable future attacks. Clearsky did not identify the specific types of information the hackers stole, but noted that the majority of targets were academics, researchers, and practitioners in social sciences, as well as journalists and human rights activists.[160]

Interestingly, there may have also been a cyber-enabled economic warfare component to the operation identified by Clearsky. Some of the targets were physicists, security companies, and defense firms, and Clearsky noted that the hackers engaged

159. Ibid, page 7.
160. "Thamar Reservoir: An Iranian cyber-attack campaign against targets in the Middle East," *Clearsky*, June 2015, page 12. (https://www.clearskysec.com/wp-content/uploads/2015/06/Thamar-Reservoir-public1.pdf)

in intellectual property theft.[161] Again, the cyber security firm does not specify what kind of intellectual property the hackers stole so it is unclear if this refers to the research of social scientists or corporate secrets of defense firms.

Another Iranian group, "Leafminer," has attempted to infiltrate government organizations and private businesses across the Middle East since at least early 2017. The group's techniques "followed the recent trend among targeted attack groups for 'living off the land'—using a mixture of publicly available tools alongside its own custom malware." In addition to government targets – which made up 17 percent of affected entities – 37 percent of all Leafminer targets were in the financial and petrochemical sectors. The analysis, performed by Symantec, did not attempt to determine the group's motivation but noted that the toolkits used indicate that the hackers were seeking "email data, files, and database servers."[162]

In January 2017, the Iranian hacker group known as OilRig targeted an American technology firm, its first known U.S. target. The hackers stole the company's security certificates to disguise their malware when targeting additional victims. OilRig is considered one of the most active Iranian government-sponsored cyber groups.[163]

APT33

Another group, APT33, began carrying out cyber espionage operations as early as 2013 and conducted its most significant infiltrations between mid-2016 and early 2017. APT33 gathered intelligence and stole trade secrets from a U.S. aerospace organization, Saudi business conglomerates in the aviation sector, and a South Korean petrochemical and oil-refining firm.[164]

Examining the forensic details of the malware and open-source reporting, FireEye concluded that APT33 is an Iranian government-supported group.[165] Specifically, FireEye determined that an individual hacker developed the malware based on the inclusion of his handle in samples of the virus – a handle that open-source reporting tied to the Nasr Institute, an Iranian government-controlled entity. These facts, combined with the presence of "Farsi language artifacts" in the malware and the timing and tempo of APT33's operations, consistent with the Iranian workday, led FireEye to name Iran as the entity behind APT33.

FireEye also concluded that APT33 was state-backed because its targets aligned with the interests of the Islamic Republic. According to FireEye:

> APT33's focus on aviation may indicate the group's desire to gain insight into regional military aviation capabilities to enhance Iran's aviation capabilities or to support Iran's military and strategic decision making. Their targeting of multiple holding companies and organizations in the energy sectors aligns with Iranian national priorities for growth, especially as they relate to increasing petrochemical production.[166]

161. Ibid, pages 12 and 14.
162. "Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions," *Symantec*, July 25, 2018. (https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east)
163. Thomas Brewster, "Inside OilRig -- Tracking Iran's Busiest Hacker Crew On Its Global Rampage," *Forbes*, February 15, 2017. (https://www.forbes.com/sites/thomasbrewster/2017/02/15/oilrig-iran-hackers-cyberespionage-us-turkey-saudi-arabia/#245f072c468a)
164. Jaqueline O'Leary, Josiah Kimble, Kelli Vanderlee, and Nalani Fraser, "Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware," *FireEye*, September 20, 2017. (https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html); Chris Bing, "Newly uncovered Iranian hacking group targeted energy, aerospace firms to steal secrets," *CyberScoop*, September 20, 2017. (https://www.cyberscoop.com/apt33-iranian-hackers-fireeye/)
165. Jaqueline O'Leary, Josiah Kimble, Kelli Vanderlee, and Nalani Fraser, "Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware," *FireEye*, September 20, 2017. (https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html)
166. Ibid.

Both FireEye and the infrastructure security firm Dragos raised concerns that APT33 might be pre-positioning for a more destructive attack. FireEye Director of Intelligence Analysis John Hultquist noted, "[w]e've seen them deploy destructive tools they haven't used. We're looking at a team whose mission could change to disruption and destruction overnight." Similarly, Dragos founder Robert M. Lee observed, "This is economic espionage with the added ability to be destructive, but we have no reason to think they've gone destructive yet."[167]

Shamoon 2

Even as Iranian operations expanded around the globe, Saudi Arabia has borne the brunt of the Islamic Republic's malicious cyber activities.[168] While Operation Cleaver, Thamar Reservoir (likely conducted by threat actor Rocket Kitten[169]), and Leafminer targeted a broad range of victims, the plurality of targets in each case were Saudi institutions and companies. OilRig likewise has focused its campaigns largely on the Saudi private sector, in particular financial institutions, technology companies, and the defense sector, dating back to at least autumn 2015.[170]

The reason that Riyadh is Iran's primary target is two-fold. Obviously, Iran and Saudi Arabia are bitter regional rivals. Secondly, Saudi cyber defenses are perceived as being significantly less capable than those of Israel and the United States. Collin Anderson and Karim Sadjadpour explain:

> Weak Saudi cyber defenses have not only made the country vulnerable to Iranian coercion but also made Riyadh a soft target for Tehran's retaliation against destructive cyber operations performed by third countries. If Iran cannot cause significant damage to the United States during times of conflict, then damaging the economic institutions of American allies will suffice.[171]

Despite its partnerships with leading technology firms, Saudi Arabia remains vulnerable to Iranian cyber attacks.[172] Riyadh is known to purchase expensive defense equipment but not invest in the human capital necessary to effectively deploy the hardware.[173]

---

167. Andy Greenberg, "New Group of Iranian Hackers Linked to Destructive Malware," *Wired*, September 20, 2017. (https://www.wired.com/story/iran-hackers-apt33/)
168. Gili, "The Iranian-Saudi Conflict and Its Cyber Outlet," *Recorded Future*, June 26, 2015. (https://www.recordedfuture.com/iranian-saudi-cyber-conflict/)
169. "Rocket Kitten: A Campaign with 9 Lives," *Check Point*, 2015. (https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf)
170. Robert Falcone and Bryan Lee, "The OilRig Campaign: Attacks on Saudi Arabian Organizations Deliver Helminth Backdoor," *Palo Alto*, May 26, 2016. (https://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/)
171. Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," *Carnegie Endowment for International Peace*, January 2018, page 34. (https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf)
172. "Enhancing Saudi Arabia's cybersecurity readiness," *Oxford Business Group*, accessed October 15, 2018. (https://oxfordbusinessgroup.com/analysis/front-lines-enhancing-kingdom%E2%80%99s-cybersecurity-readiness); Melissa Hathaway, Francesca Spidalieri, and Fahad Alsowailm, "Kingdom of Saudi Arabia Cyber Readiness at a Glance," *Potomac Institute For Policy Studies*, September 2017, page 5. (https://www.belfercenter.org/sites/default/files/files/publication/cri-2.0-ksa.pdf); "Saudi Arabia to overhaul its cybersecurity preparedness: Potomac assessment," *CISO Magazine*, September 26, 2017. (https://www.cisomag.com/saudi-arabia-to-overhaul-its-cybersecurity-preparedness-potomac-assessment/)
173. Anthony H. Cordesman, "Military Spending: The Other Side of Saudi Security," *Center for Strategic and International Studies*, March 13, 2018. (https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180311_Saudi_Military_Spending.pdf?ZiU0dawl1CwU76RaQH_sAygDb_xL3FjB); Ben Brimelow, "Saudi Arabia has the best military equipment money can buy — but it's still not a threat to Iran," *Business Insider*, December 16, 2017. (https://www.businessinsider.com/saudi-arabia-iran-yemen-military-proxy-war-2017-12)

In late 2016 and early 2017, a virus called "Shamoon 2" struck key Saudi companies and government ministries.[174] Shamoon 2 rapidly spread to 15 government agencies and businesses within the Saudi civil and defense sectors.[175] In testimony before Congress in March 2018, Director of National Intelligence Dan Coats publicly attributed the attack to Iran.[176]

While the Shamoon code itself was "largely unchanged," the attackers used a different delivery system and devoted "a significant amount of preparatory work" to the operation.[177] McAfee concluded the attack was "an intentional attempt to disrupt key organizations and the country of Saudi Arabia."[178] While in the 2012 attack on Aramco, hackers inflicted damage and then quickly disappeared, this time, "the actors penetrated networks and established remote control to gather intelligence for future planned wiping attacks."[179] Additionally, the virus infected a wide range of targets throughout the Middle East, Symantec noted, but "[o]nly specific organizations affiliated with Saudi Arabia appear to have been earmarked for destructive wiping attacks."[180]

The Saudis retained Junaid Islam, a cyber security researcher with decades of experience, to provide an independent assessment of the attack. He and the Saudi security team discovered that the malware was able to spread so effectively because it used Microsoft Active Directory (AD) credentials to propagate throughout the network.[181] The local Saudi security team thus changed the AD credentials within 48 hours of the initial outbreak. It worked only briefly, however, and a new wave of the attack using the new AD credentials followed. The attackers likely had established a clandestine presence in the network and had knowledge of the systems in place and how to bypass them.

Shamoon 2 spread and installed itself without human interaction or enablement – without a user "click." The malware autonomously scanned the network for other Windows devices and repeated the process while deleting data.[182] There was no exfiltration of data or ransom demanded, and thus the attack seems to have been aimed at disrupting systems.

174. "Saudi Arabia warns on cyber defense as Shamoon resurfaces," *Reuters*, January 23, 2017. (https://www.reuters.com/article/us-saudi-cyber/saudi-arabia-warns-on-cyber-defense-as-shamoon-resurfaces-idUSKBN1571ZR); Zahraa Alkhalisi, "Saudi Arabia warns of new crippling cyberattack," *CNN*, January 26, 2017. (https://money.cnn.com/2017/01/25/technology/saudi-arabia-cyberattack-warning/)
175. Ms. Smith, "Saudi Arabia again hit with disk-wiping malware Shamoon 2," *CSO*, January 24, 2017. (https://www.csoonline.com/article/3161146/security/saudi-arabia-again-hit-with-disk-wiping-malware-shamoon-2.html)
176. Courtney Kube, Carol E. Lee, Dan De Luce, and Ken Dilanian, "Iran has laid groundwork for extensive cyberattacks on U.S., say officials," *NBC News*, July 20, 2018. (https://www.nbcnews.com/news/us-news/iran-has-laid-groundwork-extensive-cyberattacks-u-s-say-officials-n893081)
177. "Shamoon: Back from the dead and destructive as ever," *Symantec*, November 30, 2016. (https://www.symantec.com/connect/blogs/shamoon-back-dead-and-destructive-ever); "Threat Brief: Credential Theft – The Keystone of the Shamoon 2 Attacks," *Symantec*, March 27, 2017. (https://researchcenter.paloaltonetworks.com/2017/03/unit42-threat-brief-credential-theft-keystone-shamoon-2-attacks/)
178. Raj Samani and Christiaan Beek, "Shamoon Returns, Bigger and Badder," *McAfee*, April 25, 2017. (https://securingtomorrow.mcafee.com/business/shamoon-returns-bigger-badder/); "Shamoon: Back from the dead and destructive as ever," *Symantec*, November 30, 2016. (https://www.symantec.com/connect/blogs/shamoon-back-dead-and-destructive-ever); "Threat Brief: Credential Theft – The Keystone of the Shamoon 2 Attacks," *Palo Alto*, March 27, 2017. (https://researchcenter.paloaltonetworks.com/2017/03/unit42-threat-brief-credential-theft-keystone-shamoon-2-attacks/); Raphael Satter, "Security firm: Cyberattacks against Saudi Arabia continue," *Associated Press*, April 26, 2017. (https://apnews.com/192ceca6163f4f1ca5a9dea8c43b5312)
179. Raj Samani and Christiaan Beek, "Shamoon Returns, Bigger and Badder," *McAfee*, April 25, 2017. (https://securingtomorrow.mcafee.com/business/shamoon-returns-bigger-badder/)
180. "Shamoon: Multi-staged destructive attacks limited to specific targets," *Symantec*, February 27, 2017. (https://www.symantec.com/connect/blogs/shamoon-multi-staged-destructive-attacks-limited-specific-targets)
181. Author interview with Junaid Islam, May 18, 2018.
182. Ibid.

A New Inflection Point? Withdrawal from the Nuclear Deal

Following the 2015 nuclear deal, Iran's GDP growth rebounded from negative 6 percent in 2012/2013 to a positive 4.3 percent in 2017/2018, after spiking to 12 percent in 2016/2017.[183] The Islamic Republic used the economic breathing room provided by sanctions relief[184] to expand its military budget, including its spending on cyber.[185]

The U.S. withdrawal from the nuclear deal in May 2018 may upset the regime's plans. Even before the reinstatement of U.S. sanctions, the Islamic Republic experienced a rapid depreciation of its currency.[186] Between May and September of this year, the value of the Iranian rial dropped 160 percent.[187] By September 2018, three months before the full re-imposition of sanctions, Iran's oil exports had already fallen by 35 percent.[188] Scores of foreign investors are leaving the Iranian market.[189] The International Monetary Fund and the World Bank both predict that Iran's economy will shrink modestly before the end of 2018 and more than 3.5 percent in 2019.[190]

Experts warn that Iran may respond to the withdrawal and re-imposition of sanctions by lashing out with new destructive cyber attacks.[191] Secretary of Homeland Security Kirstjen Nielsen testified before Congress that Washington is "anticipating" the "possibility" of

183. Mark Dubowitz, Annie Fixler, and Rachel Ziemba, "Don't Buy the Spin: Iran is Getting Economic Relief," *Foundation for Defense of Democracies and Roubini Global Economics*, June 2016. (https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/Dont_Buy_The_Spin.pdf); International Monetary Fund, Press Release, "IMF Executive Board Concludes 2018 Article IV Consultation with the Islamic Republic of Iran," March 29, 2018. (https://www.imf.org/en/News/Articles/2018/03/29/pr18114-iran-imf-executive-board-concludes-2018-article-iv-consultation)

184. Jennifer Hsieh, Rachel Ziemba, and Mark Dubowitz, "Iran's Economy Will Slow but Continue to Grow Under Cheaper Oil and Current Sanctions," *Foundation for Defense of Democracies and Roubini Global Economics*, February 2015. (https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/publications/RoubiniFDDReport_FEB15.pdf)

185. Saeed Ghasseminejad, "Iran Doubles Down on its Military Budget," *Foundation for Defense of Democracies*, June 3, 2016. (https://www.fdd.org/analysis/2016/06/03/iran-doubles-down-on-its-military-budget/); Bozorgmehr Sharafedin, "Iran to expand military spending, develop missiles," *Reuters*, January 9, 2017. (https://www.reuters.com/article/us-iran-military-plan/iran-to-expand-military-spending-develop-missiles-idUSKBN14T15L); Ahmad Majidyar, "Rouhani Says Iran's Military Budget Increased by 145 Percent During His Term," *The Middle East Institute*, April 18, 2017. (http://www.mei.edu/content/io/rouhani-says-iran-s-military-budget-increased-145-percent-during-his-term)

186. Ladane Nasseri, "Iran's Rial Tumbles Ahead of U.S. Sanctions, Dozens Arrested," *Bloomberg*, July 30, 2018. (https://www.bloomberg.com/news/articles/2018-07-30/iran-rial-tumbles-ahead-of-u-s-sanctions-dozens-arrested)

187. @mdubowitz, "Rial has dropped from 70,000 (day after US exited nuke deal) to 183,000 today. 160% drop in under 5 months. https://www.bonbast.com/archive," *Twitter*, September 26, 2018. (https://twitter.com/mdubowitz/status/1044921622430396416?s=19); Michael Lipin, "Iran's Currency Hits Another Record Low, With Six Weeks to US Sanctions," *Voice of America*, September 24, 2018. (https://www.voanews.com/a/iran-currency-hits-another-record-low-with-six-weeks-to-us-sanctions/4585869.html)

188. Javier Blas, "In Big Win for Trump, U.S. Sanctions Cripple Iranian Oil Exports," *Bloomberg*, September 17, 2018. (https://www.bloomberg.com/news/articles/2018-09-18/in-big-win-for-trump-u-s-sanctions-cripple-iranian-oil-exports); Clifford Krauss, "Trump Hit Iran With Oil Sanctions. So Far, They're Working," *The New York Times*, September 19, 2018. (https://www.nytimes.com/2018/09/19/business/energy-environment/iran-oil-sanctions.html)

189. David Adesnik and Saeed Ghasseminejad, "Foreign Investment in Iran: Multinational Firms' Compliance with U.S. sanctions," *Foundation for Defense of Democracies*, September 10, 2018. (https://www.fdd.org/wp-content/uploads/2018/09/MEMO_CompaniesinIran.pdf)

190. Saeed Ghasseminejad, "IMF and World Bank Predict Economic Slowdown in Iran," *Foundation for Defense of Democracy*, October 12, 2018. (https://www.fdd.org/analysis/2018/10/12/imf-and-world-bank-predict-economic-slowdown-in-iran/)

191. For example, see: Deb Riechmann, "US braces for possible cyberattacks after Iran sanctions," *Associated Press*, August 8, 2018. (https://www.apnews.com/d910275db6c0465ca27da40c4331b949)

increased Iranian cyber attacks.[192] Analysts at Recorded Future warn that as economic sanctions pressure escalates, "the IRGC may forgo careful contractor selection and planning in an attempt to deliver a destructive attack within a short period of time."[193]

Even before the U.S. withdrew from the nuclear deal, Iranian hackers appear to have gotten bolder. By March 2018, cyber security experts were noting that OilRig's campaigns had evolved, using more sophisticated malware and "new data exfiltration methods,"[194] and assessed that the group's operations "are likely to accelerate even further in the near future."[195]

FireEye also reported at least a ten-fold increase in the number of phishing emails APT33 sent in the month of July 2018 to Middle Eastern, North American, and Japanese companies in the oil and gas, utilities, and other industries.[196] The firm warned that this spear phishing campaign might be part of a larger effort to engage in disruptive attacks or to pre-position assets for later disruptive or destructive attacks.

As Iran begins to feel the full effects of renewed sanctions pressure, the regime may instruct OilRig, APT33, and others to respond by hitting the American economy like its hackers did during the previous escalation of sanctions. Days before Washington re-implemented sanctions, Khamenei urged Iranian officials responsible for civil defense and cyber operations to "confront" the United States with "scientific, accurate, and up-to-date … action."[197] Having honed its cyber capabilities against U.S. allies, the Islamic Republic may turn to cyber-enabled economic warfare attacks against American private companies. Washington must implement strategies now to prevent such campaigns.

Policy Recommendations

U.S. policy to counter Iran's malicious cyber activity must be built on three pillars: understanding the threat, strengthening defense, and imposing costs on Tehran including through cyber and kinetic capabilities. This report offers 10 recommendations to that end.

Understand the Iranian Cyber Threat Landscape

1. Analyze Tehran's cyber escalatory ladder.

Policymakers need to understand Iranian strategies and escalatory ladder so that the United States can implement policies that convince Tehran to de-escalate. Put simply: "A better understanding of the history and strategic rationale of Iran's cyber activities is critical to assessing Washington's broader cyberwarfare posture against adversaries, and prudent U.S. responses to

192. Courtney Kube, Carol E. Lee, Dan De Luce, and Ken Dilanian, "Iran has laid groundwork for extensive cyberattacks on U.S., say officials," *NBC News*, July 20, 2018. (https://www.nbcnews.com/news/us-news/iran-has-laid-groundwork-extensive-cyberattacks-u-s-say-officials-n893081)
193. Levi Gundert, Sanil Chohan, and Greg Lesnewich, "Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations," *Recorded Future*, May 9, 2018, page 15. (https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf)
194. "OilRig is Back with Next-Generation Tools and Techniques," *Nyotron*, March 2018. (https://nyotron.com/wp-content/uploads/2018/03/Nyotron-OilRig-Malware-Report-March-2018b.pdf); Tara Seals, "OilRig APT Significantly Evolves in Latest Critical Infrastructure Attacks," *InfoSecurity Magazine*, March 21, 2018. (https://www.infosecurity-magazine.com/news/oilrig-apt-significantly-evolves/)
195. Bryan Lee and Robert Falcone, "OilRig Targets Technology Service Provider and Government Agency with QUADAGENT," *Palo Alto*, July 25, 2018. (https://researchcenter.paloaltonetworks.com/2018/07/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/)
196. Jon Gambrell, "Cybersecurity firm: More Iran hacks as US sanctions loomed," *Associated Press*, September 18, 2018. (https://www.apnews.com/88ab2debee36432d8d0498991e9f5768)
197. "Iran's Khamenei calls for fight against enemy 'infiltration,'" *Reuters*, October 28, 2018. (https://www.reuters.com/article/us-iran-khamenei/irans-khamenei-calls-for-fight-against-enemy-infiltration-idUSKCN1N20CN)

future cyber threats from Iran and elsewhere."[198] The U.S. government should task the intelligence community (if it has not already) to produce an assessment of how Iran's cyber capabilities are (or are not) affecting Tehran's national strategies and when and how the Islamic Republic is most likely to deploy cyber capabilities.

2. Analyze the Islamic Republic's cyber investments, industrial base, and partnerships with other rogue actors in order to target these assets as needed.

The U.S. government should task the intelligence community (if it has not already) to develop a deeper understanding of Iran's cyber investment, capabilities, industrial base, and actors (including linkages between and among them). The intelligence community should study the regime's annual spending on cyber and information technology infrastructure and its technology imports and domestic production capacity. This analysis will paint a fuller picture of the Iranian cyber threat and better enable the U.S. and its allies to prevent Iran from importing military and dual-use technology relevant to its cyber warfare capabilities.

A technical analysis of how the release and leak of nation-state toolkits has affected the evolution of Iranian cyber operatives would also shed additional light on whether Iranian cyber capabilities are maturing more substantially due to this leaked information or because of relationships with other cyber actors.

The intelligence community should also be tasked with understanding the full extent of the cyber cooperation between Iran, North Korea, Syria, and other rogue actors, possibly including Russia. This area in particular is where Congress can play an important role by including in legislation reporting requirements and assessments of the Iranian cyber cooperation with Russia, North Korea, and Syria.

Iran has already collaborated with such partners on various military enterprises.[199] In particular, in 2012, the Islamic Republic and North Korea signed a technology cooperation agreement,[200] and Tehran and Moscow have cyber security cooperation agreements.[201] Improved intelligence would allow the United States to better understand and disrupt these efforts, as well as to exploit any potential divisions between Iran and its collaborators.

Strengthen Defense

1. Bolster information sharing with U.S. allies to improve allied defenses.

Coinciding with the White House's release of the National Cyber Strategy, the U.S. Department of Defense also issued a new cyber strategy of its own.

198. Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," *Carnegie Endowment for International Peace*, January 2018, page 3. (https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf)
199. Paul K. Kerr, Steven A. Hildreth, and Mary Beth D. Nikitin, "Iran-North Korea-Syria Ballistic Missile and Nuclear Cooperation," *Congressional Research Service*, February 26, 2016. (https://fas.org/sgp/crs/nuke/R43480.pdf); Jay Solomon, "High-Level Contacts Between North Korea and Iran Hint at Deeper Military Cooperation," *The Washington Institute for Near East Policy*, November 27, 2017. (https://www.washingtoninstitute.org/policy-analysis/view/high-level-contacts-between-north-korea-and-iran-hint-at-deeper-military-co); Raphael Ofek and Dany Shoham, "Iran Is Progressing Towards Nuclear Weapons Via North Korea," *The Begin-Sadat Center for Strategic Studies*, February 28, 2017. (https://besacenter.org/perspectives-papers/iran-progressing-nuclear-weapons-via-north-korea/); Matthew RJ Brodsky, "The North Korean Axis of Middle East Proliferation," *The National Review*, August 31, 2017. (https://www.nationalreview.com/2017/08/un-report-north-korea-syria-iran-relationship-extensive-long-standing/); "Iran & North Korea - Nuclear Proliferation Partners," *United Against a Nuclear Iran*, accessed September 20, 2018. (https://www.unitedagainstnucleariran.com/north-korea-iran)
200. "Iran, North Korea agree to cooperate in science, technology," *Reuters*, September 1, 2012. (https://www.reuters.com/article/us-korea-north-iran-idUSBRE88005H20120901)
201. "Iran and Russia announce plans for cyber security cooperation," *PressTV* (Iran), March 14, 2017. (https://www.presstv.com/Detail/2017/03/14/514354/Iran-Russia-cyber-security-cooperation); Dorothy Denning, "Iran's Cyber Warfare Program is Now a Major Threat to the United States," *Newsweek*, December 12, 2017. (https://www.newsweek.com/irans-cyber-warfare-program-now-major-threat-united-states-745427)

The summary notes that the Pentagon will "work with U.S. allies and partners to strengthen cyber capacity, expand combined cyberspace operations, and increase bi-directional information sharing in order to advance our mutual interests."[202] This is particularly important in the case of the cyber threats from the Islamic Republic. Iran is almost certainly using the Middle East as a testing ground to evaluate cyber tactics, tools, and capabilities that will later be unleashed against U.S. targets. Thus, greater cooperation with allies not only defends U.S. national interests and the security of its allies, but protects the U.S. homeland as well.

Information sharing in real time with regional partners can provide a better understanding of the Iranian cyber threat and facilitate collective defense. As the Defense Department underscored, "[i]nformation-sharing relationships with allies and partners will increase the effectiveness of combined cyberspace operations and enhance our collective cybersecurity posture."[203]

2. Develop a joint R&D agenda with U.S. allies to address common threats from Iran and other malicious cyber actors.

Both the National Cyber Strategy and the Pentagon's cyber strategy note that our allies have capabilities that "complement our own."[204] Washington should work with its allies to develop a joint research and development agenda to leverage such comparative advantages to develop, pilot, and scale solutions to shared problems.

Joint U.S.-Japan research on ballistic missile defense can serve as a potential model of how allies can utilize their comparative scientific advantages. In the late 1990s, the two governments reached an agreement to conduct joint research on lightweight nose cones, stage-two rocket engines, advanced kinetic warheads, and two-color infrared sensors.[205] They chose these areas (at least in part) because they were priorities of the U.S. Navy's risk reduction initiatives[206] and were areas where Japan possessed a comparative advantage.[207]

A joint R&D agenda could also provide a trusted forum for evaluating and testing sensitive, best-of-breed technologies. The research agenda could be informed by small groups of stakeholders who would gather to discuss R&D requirements and goals.

3. Conduct joint cyber wargames with allies in the Middle East to demonstrate our resolve to defend our allies.

True interoperability and collective defense can only occur if the United States and its allies demonstrate their commitment to work together. The United States should establish working groups with its allies to resolve legal, jurisdictional, and other constraints that the nations will face in the event of a "hot" cyber conflict and to identify what effective interoperability entails.

Working groups, however, will be insufficient if their assessments are not tested and the parties do not resolve to work together. Therefore, U.S. regional allies should conduct joint war games with one another under the auspices of the United States. In recent years, the press has reported quiet cooperation and intelligence sharing between Israel and Arab

202. U.S. Department of Defense, "Summary of Department of Defense Cyber Strategy," September 2018, page 2. (https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF)
203. Ibid, page 5.
204. Ibid; The White House, "National Cyber Strategy of the United States of America," September 2018, page 26. (https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf)
205. "Japan-U.S. Cooperation on Ballistic Missile Defense: Issues and Prospects," *Congressional Research Service*, March 19, 2002, page 14. (https://www.everycrsreport.com/files/20020319_RL31337_822a160b7c1a7e8f47606dfa4611eea6c8f7e268.pdf)
206. Ibid.
207. Michael D. Swaine, Rachel M. Swanger, and Takashi Kawakami, "Japan and Ballistic Missile Defense Chapter 3: Domestic Factors Determining Future Decisions," *RAND Corporation*, 2001, page 61. (https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1374/MR1374.ch3.pdf)

states.[208] Washington should explore whether it can leverage these relationships into additional cooperation in the form of regional cyber exercises to respond to the common Iranian cyber threat.

The cyber exercises should bring together decision makers, analysts, operators, technologists, and other relevant parties to discern the capability gaps, recommend ways to prioritize new research and analysis, and determine where legal authorities, command-and-control structures, and decision-making processes succeed or fail in battlefield situations. Joint wargames would help prevent disconnects between technical operators and strategic decision makers that could lead to mission failure. The wargames can also reveal where the United States and its allies have weaknesses and ought to make additional investments.

4. Announce that the U.S. will defend its key allies from significant Iranian cyber attacks.

If Tehran believes that it can attack U.S. allies in cyber space with impunity, Washington must disabuse Iran of this notion. Specifically, Washington should have a declarative policy that the United States will respond to, and defend its allies against, significant Iranian malicious cyber activity. Washington and its allies will need to determine in classified settings the precise details of this arrangement according to the unique needs of each country – for example, whether the U.S. pre-positions assets, has certain types of visibility into allied networks, or deploys cyber operators in crisis scenarios.

5. Share actionable information with the private sector, provide incentives for the private sector to implement better cyber defenses, and establish interoperability to allow the private sector to better defend itself.

Washington should identify mechanisms and technologies that would address both government and private sector vulnerabilities and develop specific strategies to encourage their widespread adoption.

Beyond identifying technological solutions, the U.S. government must provide specific, actionable information to the private sector. As former NSA Director Keith Alexander and Jamil Jaffer vividly describe, "In no other context do we rely on private sector actors to defend themselves against national-level threats. After all, we don't expect Walmart or Tesco to put surface-to-air missiles on top of their warehouses to defend against Russian bombers. Yet when it comes to cyber attacks, we demand exactly that from JPMorgan and Barclays."[209] Instead, the U.S. government needs to distribute broadly operational, usable, and classified information with cleared private sector entities so that they can take defensive measures to protect themselves. The pilot project known as "Project Indigo"[210] between U.S. Cyber Command and major American financial institutions may provide a useful model that can be replicated across other critical industries, including oil and gas, electricity, and transportation.

The new Pentagon cyber strategy announced that the Defense Department must "be prepared to defend, when directed, those networks and systems operated by non-DoD Defense Critical Infrastructure (DCI)

208. Shai Feldman and Tamara Cofman Wittes, "Everyone Loves Israel Now," *Foreign Policy*, March 26, 2018. (https://foreignpolicy.com/2018/03/26/why-everyone-loves-israel-now/); Raphael Ahren, "Israel and UAE have maintained close covert ties since 1990s, magazine claims," *The Times of Israel*, June 11, 2018. (https://www.timesofisrael.com/israel-and-uae-have-maintained-close-covert-ties-since-1990s-magazine-claims/); Jeffrey Heller and Stephen Kalin, "Israeli minister reveals covert contacts with Saudi Arabia," *Reuters*, November 19, 2017. (https://www.reuters.com/article/us-israel-saudi/israeli-minister-reveals-covert-contacts-with-saudi-arabia-idUSKBN1DJ0S1); Neri Zilber, "Israel's Secret Arab Allies," *The New York Times*, July 14, 2017. (https://www.nytimes.com/2017/07/14/opinion/israels-secret-arab-allies.html)

209. Keith Alexander and Jamil Jaffer, "A transatlantic alliance is crucial in an era of cyberwarfare," *Financial Times* (UK), September 4, 2018. (https://www.ft.com/content/c01a7f94-af81-11e8-87e0-d84e0d934341)

210. Chris Bing, "Inside 'Project Indigo,' the quiet info-sharing program between banks and U.S. Cyber Command," *CyberScoop*, May 21, 2018. (https://www.cyberscoop.com/project-indigo-fs-isac-cyber-command-information-sharing-dhs/)

and Defense Industrial Base (DIB) entities."[211] To implement this, the U.S. government must work with its own private sector, partner governments, and foreign companies to develop rules and clear lines of responsibility and, most importantly, to engage in joint training and exercises to develop interoperability between the government and private sector.[212] These trainings and exercises will also reveal when and how the U.S. government should deploy public-private teams of operators to engage in joint defensive operations.

Impose Costs on Tehran

1. Sanction key Iranian leaders for authorizing cyber attacks.

U.S. law enforcement has concluded that the IRGC is responsible for Iranian cyber attacks. The Treasury Department should thus sanction the IRGC under its existing cyber authorities. Sanctions can quarantine funds used to support illicit activities from the international banking system and deny the Islamic Republic financial resources to fund its cyber aggression. Designating the IRGC, however, is likely to have limited practical implications because the organization is already under extensive U.S. sanctions for weapons proliferation, terrorism, and human rights abuses.

It may therefore be effective to sanction Supreme Leader Ali Khamenei. He is the ultimate decision-maker in Iran and it is doubtful that any malicious Iranian cyber activity would occur without his approval. He also sits atop a multi-billion-dollar empire.[213] Taking action against these assets and specifically designating Khamenei would send a strong message that the United States plans to escalate the economic pressure.

2. Use cyber-enabled information warfare capabilities to exploit and sharpen divisions between the regime and the Iranian public.

Sanctions alone are unlikely to change the Iranian regime's behavior. "Doxing" Iranian officials could effectively complement financial sanctions. Washington should widely publicize information about how much the regime spends on overseas military and terrorist operations. Some of this information is publicly available and some may require cyber espionage to uncover. In December 2017 and January 2018, protesters in Iran repeatedly chanted slogans demanding the regime focus on economic growth instead of spending blood and treasure in Syria.[214] The United States should exploit this already-sensitive issue and provide the Iranian people with information about how their government is wasting resources abroad.

Washington can further alienate the rulers from the Iranian citizenry by publicizing information about regime officials' corruption, kleptocracy, and embezzlement. Using cyber and financial intelligence capabilities, the intelligence community should locate IRGC and regime funds and investigate whether regime officials and other designated persons are using family members to hide assets. In addition to using this information to impose more sanctions, the United States should publicize its findings using traditional media like the Voice of America Persian service and Radio Farda as well as through social media platforms popular in Iran. A component of this strategy must

211. U.S. Department of Defense, "Summary of Department of Defense Cyber Strategy," September 2018, page 2. (https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF)
212. For a more robust discussion of this concept, see: Keith B. Alexander, Jamil N. Jaffer, and Jennifer S. Brunet, "Clear Thinking About Protecting the Nation in the Cyber Domain," *The Cyber Defense Review*, March 30, 2017. (https://nationalsecurity.gmu.edu/wp-content/uploads/2017/03/CDRV2N1_Clear-Thinking_Alexander_Jaffer_Brunet_032217-1.pdf)
213. Behnam Ben Taleblu and Saeed Ghasseminejad, "Iran's supreme leader has a business empire — the US must sanction it," *The Hill*, November 1, 2017. (https://thehill.com/opinion/national-security/358203-irans-supreme-leader-has-a-business-empire-the-us-must-sanction-it)
214. Asa Fitch, "Iran's Spending on Foreign Conflicts Raises Protesters' Ire," *The Wall Street Journal*, January 2, 2018. (https://www.wsj.com/articles/irans-spending-on-foreign-proxies-raises-protesters-ire-1514920398)

also ensure that the Iranian people have access to secure communications and can evade government censorship so that they can receive and share the information about their own government's behavior.

More broadly, the United States should consider methods for building bridges with the Iranian people directly by providing resources and information that the Iranian people cannot access today. Specifically, these resources may include technical means for disrupting regime censorship and organizing the opposition.

3. Hold at risk Iranian assets using cyber and kinetic means.

To punish Tehran for its malicious cyber attacks, Washington must be willing to deploy the full range of its offensive capabilities – capabilities that far surpass those of its adversaries. When Iran or any adversary threatens American national security, the United States has the ability to – if it chooses – punch back ten times harder. For example, to deter or respond to an Iranian cyber attack on U.S. or allied energy assets, the United States should communicate to the leadership in Tehran that it can hold at risk[215] – using cyber means and/or other military capabilities – Iranian tankers and the infrastructure of its energy sector. If Iran launches cyber attacks on another sector of the U.S. economy, Washington should be prepared to retaliate in the virtual or physical world against the assets that the Islamic Republic most values. Interagency task forces should bring together officials with regional, economic, and cyber expertise to develop offensive options across a range of modalities. Tehran must be made to understand the severe consequences of its malicious cyber activities.

Conclusion

Technological advancements are enabling U.S. adversaries to cause damage disproportionate to the resources deployed in a domain without clearly defined rules of engagement. While Iran does not have the cyber capabilities of China, Russia, or North Korea, Tehran is willing to take greater risks and cause greater destruction. The Islamic Republic cannot match Washington's capabilities on the traditional military battlefield nor in the virtual world, but its hackers can still do serious damage. If U.S. decision makers begin to initiate more robust defensive initiatives with allies and the private sector, and simultaneously prepare cyber and kinetic countermeasures, Washington may well prevent a more devastating cyber battle in the future.

215. For a fuller discussion of the differences between preparing the battlefield, hold at risk, and intelligence gathering in cyber space, see: Robert Chesney, "The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes," *Lawfare Blog*, September 25, 2018. (https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes)

Appendix: List of Names of Prominent APT Groups Linked to Iran

Ajax Security Team[216]
APT33[217]
APT34[218]
APT35[219]
Ashiyane Digital Security Team[220]
Cadelle[221]
Chafer[222]
Charming Kitten[223]
CopyKittens[224]
Cutting Kitten[225]
Cutting Sword of Justice[226]
Flying Kitten[227]
Iranian Cyber Army[228]
Leafminer[229]
Magic Hound[230]
Magic Kitten[231]
Newscaster[232]
OilRig[233]
Rocket Kitten[234]
Sun Army[235]

---

216. Nart Villeneuve, Mike Scott, Thoufique Haq, and Ned Moran, "Operation Saffron Rose," *FireEye*, May 2014. (https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf)
217. Jaqueline O'Leary, Josiah Kimble, Kelli Vanderlee, and Nalani Fraser, "Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware," *FireEye*, September 20, 2017. (https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html)
218. Ly Hay Newman, "Iranian Hackers Have Been Infiltrating Critical Infrastructure Companies," *Wired*, December 7, 2017. (https://www.wired.com/story/apt-34-iranian-hackers-critical-infrastructure-companies/); Manish Sardiwal, Vincent Cannon, Nalani Fraser, Yogesh Londhe, Nick Richard, and Jacqueline O'Leary, "New Targeted Attack in the Middle East by APT34, a Suspected Iranian Threat Group, Using CVE-2017-11882 Exploit," *FireEye*, December 7, 2017. (https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html)
219. "M-Trends 2018," *FireEye*, April 4, 2018, page 16. (https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf)
220. U.S. Department of Justice, Press Release, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," March 26, 2016. (https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged)
221. "Iran-based attackers use back door threats to spy on Middle Eastern targets," *Symantec*, December 7, 2015. (https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets)
222. Ibid.
223. "Charming Kitten: Iranian cyber espionage against human rights activists, academic researchers and media outlets - and the HBO hacker connection," *ClearSky*, December 2017. (https://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf)
224. "Operation Wilted Tulip – Exposing a Cyber Espionage Apparatus," *ClearSky*, July 25, 2017. (https://www.clearskysec.com/tulip/)
225. Nicole Perlroth, "Report Says Cyberattacks Originated Inside Iran," *The New York Times*, December 2, 2014. (https://www.nytimes.com/2014/12/03/world/middleeast/report-says-cyberattacks-originated-inside-iran.html)
226. Jose Pagliery, "The inside story of the biggest hack in history," *CNN Money*, August 5, 2015. (http://money.cnn.com/2015/08/05/technology/aramco-hack/)
227. Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," *Carnegie Endowment for International Peace*, January 4, 2018. (http://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134)
228. Farvartish Rezvaniyeh, "Pulling the Strings of the Net: Iran's Cyber Army," *Frontline Tehran Bureau*, February 26, 2010. (https://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/02/pulling-the-strings-of-the-net-irans-cyber-army.html)
229. "Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions," *Symantec*, July 25, 2018. (https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east)
230. Bryan Lee and Robert Falcone, "Magic Hound Campaign Attacks Saudi Targets," *Palo Alto*, February 15, 2017. (http://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets)
231. Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," *Carnegie Endowment for International Peace*, January 4, 2018, page 20. (http://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134)
232. "Past and Present Iran-linked Cyber-Espionage Operations," *InfoSec Institute*, February 20, 2017. (https://resources.infosecinstitute.com/past-present-iran-linked-cyber-espionage-operations/#gref)
233. "Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford," *ClearSky*, January 5, 2017. (https://www.clearskysec.com/oilrig/); Bryan Lee and Robert Falcone, "OilRig Targets Technology Service Provider and Government Agency with QUADAGENT," *Palo Alto*, July 25, 2018. (https://researchcenter.paloaltonetworks.com/2018/07/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/)
234. "Rocket Kitten: A Campaign with 9 Lives," *Check Point*, 2015. (https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf)
235. U.S. Department of Justice, Press Release, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," March 26, 2016. (https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged)

Acknowledgements

We are grateful to Samantha Ravich for her thought-leadership on the project on cyber-enabled economic warfare and for providing advice and strategic guidance as we worked to refine the research and analysis. We owe a debt of gratitude to Sean Weppner for supporting the early drafts and conceptualizing the CNE/CNA visual. Without his work, and the assistance of Helen Powell and other researchers, this report would not have come to fruition. We also want to thank the many experts who shared their own perspectives and insights, especially Jamil Jaffer, Sharon Cardash, Collin Anderson, Saeed Ghasseminejad, Behnam Ben Taleblu, and Reuel Marc Gerecht, who served as expert reviewers. The final report is stronger as a result of all of their contributions. While these experts helped us to refine the paper, any remaining errors of fact or judgment are exclusively our own. Thank you to David Adesnik, Jonathan Schanzer, Mark Dubowitz, and Richard Brahm for helping us refine the paper and for their expertise and invaluable editing skills. We also wish to thank Nicole Salter, Daniel Ackerman, Erin Blumenthal, and the FDD communications and government relations teams for helping bring the report over the finish line.

This report is part of a series of studies on adversarial strategies from FDD's project on cyber-enabled economic warfare. The project aims to promote a greater understanding within the U.S. government, private sector, and allied countries of the threats and opportunities that this new environment poses and to assist policymakers in developing and implementing a winning strategy for the United States within this domain.

Cover Illustration by Daniel Ackerman

About The Authors

Annie Fixler is a policy analyst at FDD's Center on Sanctions and Illicit Finance (CSIF). She contributes to CSIF's work on offensive and defensive tools of economic coercion. She also serves as the senior project manager of the Cyber-Enabled Economic Warfare project and the deputy director of FDD's Transformative Cyber Innovation Lab working on issues related to the national security implications of cyber attacks on economic targets, adversarial strategies and capabilities, and U.S. cyber resilience.

Prior to joining FDD, Annie worked for the American Israel Public Affairs Committee (AIPAC) in Washington as a senior research analyst and gained expertise in Congressional affairs and Middle East policy. Annie also serves as the director of public affairs at a strategic communications and public affairs firm based in Washington, DC. Annie earned her BA in International Affairs from The George Washington University.

Frank Cilluffo directs the McCrary Institute for Cyber & Critical Infrastructure Security at Auburn University. Prior to joining Auburn, Cilluffo founded and directed the Center for Cyber & Homeland Security at George Washington University where he led a number of national security and cybersecurity policy and research initiatives. He serves on the Homeland Security Advisory Council and is the Vice Chairman of the State, Local, Tribal & Territorial Cybersecurity Task Force. In October 2018, he was appointed to the congressionally-mandated Cyberspace Solarium Commission. Cilluffo previously served as Special Assistant to the President for Homeland Security. He is an advisor to FDD's Cyber-Enabled Economic Warfare project.

About the Foundation for Defense of Democracies' Center on Sanctions and Illicit Finance

The Center on Sanctions and Illicit Finance (CSIF) at the Foundation for Defense of Democracies (FDD) works to expand the understanding of economic warfare in the 21st century to develop further the doctrines and strategies of American financial and economic suasion. Launched in 2014, CSIF builds upon FDD's success as a leading policy institute on the use of financial measures in foreign policy. Our mission is to strengthen and preserve the ability of America and its allies to deploy economic tools to promote national security, develop strategies to isolate rogue actors, and identify and guard against economic threats and vulnerabilities.

For more information, please visit www.fdd.org

FDD
FOUNDATION FOR
DEFENSE OF DEMOCRACIES

P.O. Box 33249
Washington, DC 20033-3249
(202) 207-0190
www.fdd.org