The Evolution of Iranian Cyber Warfare

Jonathan Disegi

jrd2194

27th October 2016

Developing into a first tier cyber power:

In the last five years Iran has been rapidly developing into a "a first-tier cyber power.[1]" While early attacks were somewhat crude, Iran's offensive cyber capabilities have evolved from DDoS attacks and data destruction to sophisticated and specifically targeted social engineering campaigns for cyber espionage and ICS infrastructure probes. Iran's learning curve advanced quickly after wake up calls of the Green Revolution showed Iran the coercive power of social media, and Stuxnet demonstrated the kinetic power of ICS attacks[2]. Since 2011, Iran has invested heavily in the structures and capabilities for cyber warfare and has taken a relentless "test and learn" approach to cyber attacks. Iran is now a maturing cyber adversary that poses a formidable threat to the national security of the United States.

Cyber conflict and Iran's strategic context:

The importance of cyber to Iran's foreign policy goals and strategic context are paramount, and thus Iran's embrace of cyberwarfare goes all the way up to Supreme Leader Ayatollah Khamenei. In many ways the cyber domain is an ideal means for Iran to project power and sees cyberattack as another tool of its broader asymmetric warfare strategy against more powerful opponents[3], as well strengthening regional influence:

---

[1] Harris, Shane, "Forget China: Iran's Hackers are America's Newest Cyber Threat," *Foreign Policy*, http://foreignpolicy.com/2014/02/18/forget-china-irans-hackers-are-americas-newest-cyber-threat/.

[2] Siboni, Gabi, and Kronenfeld, "Developments in Iranian Cyber Warfare 2013-2014," *Military and Strategic Affairs*, August 2014, http://www.inss.org.il/uploadImages/systemFiles/SiboniKronenfeld.pdf

[3] Lewis, James Andrew, "Cybersecurity and Stability in the Gulf," CSIS Gulf Analysis Paper, January 2014,https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/140106_Lewis_GulfCybersecurity_Web_0.pdf

- The asymmetric and covert nature of cyber is a perfect tool for "going grey" - antagonizing the United States below the response threshold, and allowing Iran to act outside of its geographical and regional confines. With cyber, Iran can now engage the "Great Satan" on US home territory.

- Regime survival is crucial for the Islamic Republic. Internally, cyber defensive measures are utilized to monitor, limit and coerce political opposition and as a tool for repression[4] - including building a second or "Halal Internet."

- Iran uses cyber attacks to inflict damage and project power on key regional Sunni rivals such as Saudi Arabia.

- Funding and support for regional cyber -proxies such as the Syrian Electronic Army, the Houthis in Yemen, and Shia militias in Iraq advance Iran's regional goals as instigator and hegemon.[5]

- As the foremost sponsor of international terrorism, cyber intelligence, espionage and social media attacks are new pillars of support Iran can provide Hamas, Hezbollah, Shi'a militias Palestinian Islamic Jihad to further promote their agendas.[6]

- Iran's increasing alignment with Russia and China will allow for cyber knowledge transfer to Iran as well as opportunity for co-conspiring.[7]

---

[4] Shafa, Eric K, "Iran's Emergence as a Cyber Power, " *Strategic Studies Institute*, August 20, 2014, http://www.strategicstudiesinstitute.army.mil/index.cfm/articles/Irans-emergence-as-cyber-power/2014/08/20

[5] Brunner, Jordan, "Iran Has Built an Army of Cyber-Proxies", *The Tower*, August 2015, http://www.thetower.org/article/iran-has-built-an-army-of-cyber-proxies/

[6] Berman, Ilan, "The Future of Iranian Terror and Its Threat to the U.S. Homeland," *Statement before the House of Representatives Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence*, February 11, 2016, http://docs.house.gov/meetings/HM/HM05/20160211/104455/HHRG-114-HM05-Wstate-BermanI-20160211.pdf.

[7] Shafa

- With the July 2015 JCPOA agreement reached on limiting Iran's nuclear ambitions, Iran may replace the "nuclear threat" with the "cyber threat" - especially now that Iran has access to previously frozen funds.

Establishing the structures and capabilities:

The opaque nature of the Islamic Republic makes it difficult to classify the precise structure of Iran's defensive and offensive cyber capabilities, but the following are key institutions – all created soon after the Green Revolution and Stuxnet:

Supreme Council of Cyberspace:
In 2011 Iran's Supreme Leader Ayatollah Khamenei authorized the establishment of the "Supreme Council of Cyberspace" to coordinate efforts for both offense and defense - overseeing all cyber domain activities for Iran. The council includes heads of intelligence, militia, security, media chiefs, and the IRGC (Iran Republican Guard Corps - Iranian elite Special Forces.) By late 2011 Iran had invested at least $1 billion in cyber technology, infrastructure, and expertise[8].

Cyber Defense Command:
Established by Khamenei in November 2010 , Iranian Cyber Defense Command is supervised by the Passive Civil Defense Committee, and is an internal unit responsible for Iran's cyber defense - overall state cybersecurity, protection of critical infrastructure, spying on dissidents, and spreading of defensive propaganda[9].

Iranian Cyber Army:

[8] Shafa
[9] Bastani, Hossein, "Structure of Iran's Cyber Warfare," December 13, 2012, *IFAS*, http://www.strato-analyse.org/fr/spip.php?article223

The Iranian Cyber Army is an "unofficial" group of highly skilled specialists and professional hackers thought to be controlled by the IRGC[10].

Basij Cyber Council:

The Basij are paramilitary volunteers that came to prominence during the Iran-Iraq war. Basij activities have extended into the cyber realm with the Basij Cyber Council a relatively unskilled and loosely organized group of volunteer hacktivists recruited from universities and religious schools. 120,000 volunteers are claimed but certainly an exaggeration[11].

Iranian Cyber Police- FATA :

Founded in 2011, under control of the Iranian Police, the Iranian Cyber Police or FATA aggressively enforce censorship restrictions and prevent subversive activity in cyberspace. FATA activities include identifying and detaining bloggers, journalists, opposition members, and closing Internet cafes[12]. In November 2012 FATA received worldwide condemnation when Iranian blogger Sattar Beheschi died in custody.

Defensive measures - Building the Halal Internet:

The 2009 "Green Revolution" protests against the rigged re-election of President Ahmadinejad alerted Iranian leaders to the destabilizing potential of social media and inaugurated a major program of defensive internal cyber security for the Islamic Republic. Stuxnet was a further wakeup call that showed the vulnerability of critical infrastructure. Iranian defensive measures as dictated by the Supreme Council of Cyberspace have 3 goals: 1. Create a protective envelope against attacks on critical infrastructure and information. 2. Neutralize cyber activities by

[10] Bastani
[11] Lewis
[12] Siboni, Gabi, and Kronenfeld

opposition groups and opponents of the regime, and 3. Prevent harmful western content from infiltrating Iran's internal cyberspace[13].

The Networks Isolation Project, or "Halal Internet" is one of Iran's key defensive strategies in cyberspace. The project began in 2009 in the wake of the Green Revolution, its objective was to transfer cyber activity from the World Wide Web to an isolated internal state communications network. The Halal Internet was designed to adhere to Shiite Muslim norms regarding content, and is under total control of the government. The wholesale separation of Iranian cyberspace from global cyberspace is seen as a key measure in strengthening Iran's defenses against western attacks, and of course, controlling and censoring content and monitoring citizens[14].

Iran is also investing in developing home-grown cyber technologies and defense tools that reduce dependence on foreign products that could have trojan horses - this includes cellular telephones, operating systems, GPS devices, and a national cyber protection system called "Shahpad.[15]" The FATA or Iranian Cyber Police are also heavily involved in monitoring and the physical enforcement of Iranian cyber defenses.

A steep learning curve - Key Iranian cyber attacks on US interests:

Since the 2012 founding of the Supreme Council of Cyberspace, Iran has conducted multiple prominent attacks on US interests at home and abroad. The first attacks in late 2012 - Shamoon and the US Banking attack - were wakeup calls that Iran was building an aggressive offensive force in cyberwarfare, initially relatively crude, but very destructive. Over time the attacks have become far more complex and nuanced, moving from away from disruption and recently focusing more on espionage.

[13] Ibid
[14] Ibid.
[15] Ibid.

Shamoon virus/ Saudi Aramco attack: In August 2012 malware called Shamoon destroyed the hard drives of 35,000 computers at Saudi Aramco, the state-owned national oil company of Saudi Arabia. Aramco IT immediately disconnected their IT infrastructure and reverted to faxes and typewriters to to ensure business continuity[16]. Shamoon infected the Aramco network through a spear-phishing email that spread all over the network, overwriting the Master Boot Record on hard drives, wiping out data and displaying an image of a burning American flag. Aramco had to completely rebuild their security operations center from scratch and crucial data was beyond recovery. A group called the "Cutting Sword of Justice" claimed responsibility. Leaked NSA documents indicate the US attributes the attack to Iran, while some private cybersecurity firms believe non-state hacktavists were the culprit. Shamoon appears to be a copy of the Wiper malware that attacked and wiped out Iranian Oil Ministry computers in April 2012[17].

Operation Ababil - US Bank DDoS attack: Beginning in September 2012 approximately 4 dozen US bank web sites were hit with DDoS attacks, causing them to crash. Bank of America, Wells Fargo, Capital One, Citigroup, HSBC and many more suffered outages that that disrupted the availability and functionality of their web sites - even though no money was taken, the attacks caused millions of dollars in lost business. This was viewed as the most sophisticated and coordinated DDoS attack to date, with botnets of thousands of computers and whole data centers directed to attack. Attacks continued through 2013. Attributed to Cyber Fighters of the Izz ad-Din-al Qassam Brigades, suspected by US intelligence to be a front for IRGC cyber operations[18]. The attack was viewed as a retaliation for Stuxnet and a signal that

---

[16] Rashid, Fahmida, "Inside the Aftermath of the Saudi Aramco Breach," *InformationWeek Dark Reading*, August 8, 2015, http://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676

[17] Zetter, Kim, "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/

[18] Harris, Shane. *@War.* New York: Harcourt, 2014. 194-196.

Iran's cyberwarfare capabilities were a force to be reckoned with. As the attacks continued US banking executives pressed the NSA and Homeland Security to take action, but they refused as the attacks didn't disrupt or threaten the transactional infrastructure of the banking sector. In this attack Iran used classic "Grey Zone" tactics by causing a provocation that was damaging yet below the threshold of retaliation by the US. Finally, in March 2016 the US DOJ brought charges against seven Iranians alleged to be responsible for the attacks; all worked for Iranian companies that were fronts for the IRGC[19].

Rye Brook Dam ICS attack – Iranian hacker Hamid Firoozi (believed to be a member of the IRGC) broke into the command and control system of a small dam in upstate New York in 2013, apparently through a cellular modem. While Firoozi had remote access to the dam, he could not release water as the sluice gate of the dam had been manually disconnected for maintenance at the time of the intrusion[20]. The Rye Brook Dam incident was the first publicised compromise of a US ICS system by a foreign state actor and was interpreted as Iran sending a signal that they were now capable of damaging US infrastructure. Firoozi was named and shamed by the DoJ in May 2014 for the attack[21].

Sands Casino attack: In February 2014, the Sands Corporation, owned by pro-Israel businessman Sheldon Adelson, experienced a computer attack that shut down PCs and servers and wiped hard drives clean. The attack is thought to be an Iranian retaliation to comments that Adelson made in October 2013, suggesting that the US detonate a nuclear weapon in the Iranian desert. 2 weeks later Ayatollah Khamenei denounced Adelson's remarks and by January/February 2014 Iranian hackers has

---

[19] Sanger, David, "U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam," *New York Times*, March 24, 2016, http://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-banks-and-a-dam.html?_r=0

[20] Thompson, Mark, Iranian Cyber Attack on New York Dam Shows Future of War, *Time*, March 24, 2016, http://time.com/4270728/iran-cyber-attack-dam-fbi/

[21] Sanger

used brute force password cracking techniques to enter the Sands network through a small outpost in Bethlehem PA, eventually gaining login credentials to the corporate network in Las Vegas[22]. In Feb 2015 DNI James Clapper told the Senate Armed Services Committee that the US intelligence community had determined the hack had been carried out by Iran.

US Navy Marine Corps Intranet attack: In Fall 2013 Iranian hackers infiltrated and conducted surveillance on the US Navy Marine Corps unclassified Intranet. While no classified networks or data were breached, it was a significant penetration into US Military networks, exposing vulnerabilities in the system and the increasing effectiveness of Iranian cyber espionage efforts. Adm Mike Rogers, future NSA director and then Navy chief of cybersecurity, initiated Operation Rolling Tide to purge the hackers from the network, the operation took about four months to complete, indicating how deeply entrenched and hidden the Iranians had become[23].

Operation Cleaver: Identified in December 2014 by US cybersecurity firm Cylance. Operation Cleaver was a 2-year Iranian cyber intelligence operation to probe ICS globally. Cleaver intrusions targeted military, oil and gas, energy and utilities, transportation, airline, airports, hospitals and aerospace – over 50 entities across 15 industries, 10 in the US. Tools used included custom malware, SQL injection, spear phishing, and waterholing attacks[24]. Cleaver was attributed to the same Tehran-based group behind the 2013 US Navy cyberattack. Cleaver was so concerning in

---

[22] Elgin, Benjamin and Riley, Michael, "Nuke Remark Stirred Hack on Sands Casinos that Foreshadowed Sony," *Bloomberg*, December 11, 2014, https://www.bloomberg.com/news/articles/2014-12-11/nuke-remark-stirred-hack-on-sands-casinos-that-foreshadowed-sony

[23] Gorman, Siobhan and Barnes, Julien E, "Iranian Hacking to Test NSA Nominee Michael Rogers," *Wall Street Journal*, February 18, 2014, http://www.wsj.com/news/articles/SB10001424052702304899704579389402826681452

[24] Cylance, "Operation Cleaver," December 2, 2014, https://www.cylance.com/operation-cleaver-cylance

the context of Stuxnet as it represented a higher level of sophistication and move from disruptive attacks to intelligence gathering for possible future ICS disruption.

Operation Newscaster : Uncovered by iSight in May 2014 and attributed to Iran, Operation Newscaster targeted current and former senior US & Israeli military officials, using spear phishing techniques and social engineering, luring them through social networks to a fake news site called NewsOnAir.org[25]. The Iranian group created more than a dozen fake personas or identities that appeared as reporters or employees; using these personas the hackers established online relationships with target's social media graph on Linkedin and Facebook, then sought to "friend" or connect with their targets. Once connected with targets they would send a link to content and then attempt to steal passwords through re-directed fake e-mail login pages. Called "the most elaborate social engineering scheme associated with cyber.[26]" Newscaster demonstrated a further evolution of Iranian cyberattacks - leveraging nuanced social engineering for cyber espionage, an operation far more sophisticated and subtle than earlier destructive hacks.

State Department diplomatic attacks: Iran's spear phishing attacks and critical infrastructure probes suddenly stopped during the during the negotiating period of the JCPOA nuclear accord in June and July 2015. Four months after the accord was signed, however, Iran resumed attacks by identifying individual State Department officials who focused on Iran and the Middle East and breaking into their email and social media accounts. The State Department only became aware of the attacks after Facebook had alerted the victims that state-sponsored hackers had breached their

---

[25] Higgins, Kelly Jackson, "Iranian Cyberspies Pose As Journalists to Ensnare Their Targets," *InformationWeek Dark Reading*, May 5th 2014, http://www.darkreading.com/attacks-breaches/iranian-cyberspies-pose-as-journalists-online-to-ensnare-their-targets/d/d-id/1269270

[26] Nakashima, Ellen, "Iranian Hackers are Targeting U.S. Officials Through Social Networks, Report Says," *Washington Post*, May 29th, 2014, https://www.washingtonpost.com/world/national-security/iranian-hackers-are-targeting-us-officials-through-social-networks-report-says/2014/05/28/7cb86672-e6ad-11e3-8f90-73e071f3d637_story.html

accounts[27]. This attack demonstrated Iran's cyber espionage capabilities had further evolved to target and compromise specific individuals. The attack is also significant as it marked an uptick in Iran cyber activities after the JCPOA accord.

Conclusion: An alarming, fast-evolving cyber threat to US security and the stability of the greater Middle East

While not yet at the level of China, Russia, or the US, Iran is dramatically upping their defensive and offensive game in the cyber domain. Cyber is now a key instrument in achieving the Islamic Republic's many foreign policy goals. Iran has shown a great sense of timing with regards to synchronizing cyber attacks with its bigger strategic agenda - witness the dropoff and resumption of Iranian cyberattacks against the US before and after the signing of the JCPOA nuclear accord. Ironically the JCPOA may embolden Iran - with hundreds of billions in released funds, and the inability to use the "nuclear card" expect Iran to become even more aggressive and sophisticated with using the "cyber card."

It would be naive to assume that the JCPOA heralds a new era of US-Iranian cooperation - America has been the "Great Satan" since 1979 and Iranian contempt for the US goes back to the ousting of Mossadegh in 1953. With hardliner Khamenei at the helm of the Supreme Council of Cyberspace, expect cyber provocations against the US to continue, with even greater complexity and effect.

We should also expect Iran to continue to utilize cyber to destabilize the greater Middle East through cyber-proxies, cyber support of terrorism, and provocations with Saudi Arabia. As Syria, Iraq and Yemen continue to be unravel, expect Iran to leverage its ever improving offensive cyber capabilities to try and gain further regional power and influence. Growing alliances with Iran and Russia may also

---

[27] Sanger, David, and Perlroth, Nicole, "Iran Hackers Attack State Dept. via Social Media Accounts," *New York Times*, November 24th, 2015, http://www.nytimes.com/2015/11/25/world/middleeast/iran-hackers-cyberespionage-state-department-social-media.html

accelerate the security threat to the US and greater Middle East, and complicate attribution by creating hybrid Iran/Russian attacks. The US should not underestimate Iran's growing cyber capability, and even more crucially, Iran's willingness to act.