ATLANTIC COUNCIL
IDEAS. INFLUENCE. IMPACT.

ISSUEBRIEF

Barbara Slavin
Jason Healey

BRENT SCOWCROFT CENTER ON INTERNATIONAL SECURITY
SOUTH ASIA CENTER

Iran: How a Third Tier Cyber Power Can Still Threaten the United States

When most people think of the “military option” against Iran, they imagine a US attack that takes out Iran’s most important known nuclear facilities at Natanz, Fordow, Arak, and Isfahan. They expect Iran to retaliate by closing the Strait of Hormuz, sending missiles into Israel, and/or supporting terrorist attacks on US personnel in Iraq and Afghanistan.

But what if the response came in the form of an anonymous cyber attack that shut down the New York Stock Exchange for a few hours? Or an assault that cut off electrical power in a major US city, froze civilian air traffic, or interfered with further military strikes on Iran by conveying incorrect information to American military commanders?

Atlantic Council Iran Task Force

The Iran Task Force, launched in 2010 and chaired by Ambassador Stuart Eizenstat, seeks to perform a comprehensive analysis of Iran’s internal political landscape, as well as its role in the region and globally, to answer the question of whether there are elements within the country and region that can build the basis for an improved relationship with the West and how these elements, if they exist, could be utilized by US policymakers. The Iran Task Force is a project of the Atlantic Council’s South Asia Center, and is supported generously by a grant from the Ploughshares Fund.

Atlantic Council Cyber Statecraft Initiative

The Atlantic Council’s Cyber Statecraft Initiative helps foster international cooperation and understanding of new forms of competition and conflict in cyberspace through global engagement and thought leadership. This report is sponsored by Saab North America, Inc.

Many US officials and experts on cyberspace say Iran is probably not yet in a position to mount such a damaging assault against the United States. Iran, they say, is a “third tier” cyber power compared to the United States, its Western allies, or Russia and China. Yet this overlooks an important factor. In the history of cyber conflict, few attacks have themselves been devastating. For example, the Russian-encouraged attacks which hit Estonia in 2007—overwhelming government web sites, Estonia’s largest bank, and several newspapers[1]—were neither technically significant nor very effective. They were disruptive, but for only short periods and with little or no long-term impact to Estonia’s GDP. The primary impact was political, not military, serving as a wake-up call on cyber vulnerabilities and leading to NATO establishing a Cyber Center of Excellence in the capital, Tallinn. In this way, a significant Iranian cyber attack against the United States would take on outsized importance regardless of its technical sophistication.

Moreover, technological edges in warfare tend to be ephemeral. There is no assurance that Iran’s growing

[1] Mark Landler and John Markoff, “Digital Fears Emerge After Data Seige in Estonia,” *The New York Times*, May 29, 2007, http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all.

Jason Healey is director of the Atlantic Council’s Cyber Statecraft Initiative.

Barbara Slavin is a senior fellow at the Atlantic Council’s South Asia Center, a journalist, and author of a 2007 book on Iran entitled *Bitter Friends, Bosom Enemies: Iran, the U.S. and the Twisted Path to Confrontation* (St. Martin’s Press, 2007).

cyber forces—or a skilled foreign or nonstate actor hired by Iran—will not be capable of significantly disruptive activities in the next few years, especially as the United States continues to extend its already deep dependence on a very vulnerable cyberspace.

In fact, there has already been an ongoing tit-for-tat of clandestine cyber conflict between Iran and the United States (and probably also Israel), though so far it has not passed into open cyber warfare. Concerns about Iran's cyber abilities rose in 2012 in connection with so-called distributed denial of service (DDoS) attacks on American financial institutions that briefly cut off access to online accounts and required expensive countermeasures.[2] The attacks appear to have come in retaliation for US-led banking sanctions on Iranian financial institutions and the Stuxnet worm that set back Iran's nuclear program in 2010. Iran is also believed to have been behind an even more destructive assault in August 2012 on the Saudi Aramco oil company that wiped out data on more than 30,000 computers.

In such an environment, while cyber attacks should be one of the options the United States continues to maintain in trying to stop Iran from developing nuclear weapons, it may be advisable to exercise caution about mounting new attacks on the order of Stuxnet, recognizing the costs of likely retaliation. At the same time, the United States should fully engage in cyber surveillance of Iran's nuclear program while continuing to improve both US cyber offense and defense. The Obama administration should also continue efforts to assist private companies and US allies improve their defenses while building support for international agreements regulating behavior in cyberspace.

Stuxnet: The Worm that Escaped

It would be no surprise if there were prior digital exchanges, but the earliest that has become public is Stuxnet, which US officials have described as a delaying tactic devised to set back the Iranian uranium enrichment program at Natanz. It also helped convince Israel that there was no imminent need to bomb Iran and pull the United States into a third regional war.[3] The cyber worm is said to have been developed by the National Security Agency starting in 2005,[4] then embellished by the Central Intelligence Agency and Israel's Unit 8200,[5] the counterpart to the NSA. It went through several iterations as it was tested on Pakistani centrifuges obtained from Libya. Inserted into Siemens-made logic controllers via an infected thumb drive, the worm absorbed and sent back information about the operation of the centrifuges. This enabled cyber warriors to devise code to destroy the centrifuges—causing them to speed up and slow down erratically—while monitoring systems at Natanz gave no indication that anything was wrong.

The worm was so targeted and ingenious that the Iranians initially thought the problems were the result of faulty materials or design flaws in their antiquated P-1 machines. But in early summer 2010, the bug "escaped" onto the Internet when an Iranian scientist connected an infected laptop to the Internet, ultimately spreading to other computers in Iran as well as Germany, Indonesia, India, Pakistan, and even the United States.[6] Apparently-related cyber programs, including Duqu and Flame, also made headlines which made it clear that Stuxnet was not an isolated attack.

The attendant publicity did not stop the program—dubbed "Olympic Games"—and it eventually scored a major blow by disabling nearly 1000 centrifuges at Natanz. Even so, while Stuxnet may have caused a year or two of delay and unsettled Iranian nuclear engineers, it did not stop Iran's nuclear program. Eventually, the Iranians figured out the problem and moved forward with installing both P-1

[2] Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *The New York Times*, January 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?hp&_r=1&.

[3] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York, Crown Publishing Group, 2012).

[4] Ellen Nakashima, "Stuxnet worm targeting Iran in works as early as 2005, Symantec finds," *The Washington Post*, February 26, 2013, http://articles.washingtonpost.com/2013-02-26/world/37306995_1_stuxnet-worm-centrifuges-nuclear-program.

[5] Sanger, *Confront and Conceal*.

[6] Symantec report on W32.Stuxnet, 13 July 2010, http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

and more advanced centrifuges, and they have steadily increased their stockpiles of low and medium-enriched uranium.[7] As journalist and author David Sanger has noted, "Stuxnet was a setback but not a crippling one." The United States, he said, also "lost a bit of the moral high ground when it comes to warning the world of the dangers of cyber attacks."[8]

The Iranian government has sought to earn propaganda points by accusing the United States and Israel of starting a cyber conflict. In response to assertions that it was behind the DDoS attacks on American banks, the spokesman for the Iranian mission to the United Nations, Alireza Miryousefi, stated, "Unlike the United States, which has per reports in the media given itself the license to engage in illegal cyber warfare against Iran, Iran respects the international law and refrains from targeting other nations' economic or financial institutions."[9]

Michael Hayden, the former CIA chief, told Sanger that Stuxnet "crossed the Rubicon" by attacking another country's critical infrastructure. Hayden compared the event to the dropping of the first nuclear weapon on Hiroshima by the United States in 1945.[10] As the Atlantic Council Cyber Statecraft Initiative has pointed out, there is a need for caution before the US government mounts further attacks that may "destroy or degrade an adversary's critical infrastructure, cripple its economy and seriously compromise its ability to defend itself" or even cause deaths.[11] The United States must anticipate that targeted countries will retaliate against US facilities if it attacks their infrastructure first.

Iran's Place in the Cyber Arms Race

How advanced is Iran and how much should we worry about its cyber capabilities? According to Dmitri Alperovich, cofounder and chief technical officer of the cyber-security firm CrowdStrike and a senior fellow at the Atlantic Council, the most effective cyber warriors—what he terms the "tier one actors"—are the United States, Russia, and US allies such as Great Britain. Alperovitch puts China a step behind at tier two and says that Iran is tier three.[12]

But this categorization should not give the United States false confidence that it can defeat any Iranian cyber threat. Iran does not need the equivalent of a Ferrari to inflict damage on US infrastructure: a Fiat may do.

As the Atlantic Council has pointed out, the blowback for US government-approved attacks has come largely against the US private sector.[13] Already, DDoS attacks attributed to Iran have cost the US financial industry millions of dollars. The attacks, starting in 2012, hit more than a dozen major institutions including SunTrust, JPMorgan Chase, CitiGroup, Wells Fargo, U.S. Bancorp, Capital One, PNC, HSBC, and BB&T; at least five websites crashed in the face of traffic 10 times higher than any previously recorded assaults.[14] Just one bank estimated spending least $10 million mitigating the attacks.[15] Another hacking episode in April 2013 claimed by a group that may have ties to Iran—the so-called Syrian Electronic Army—caused the Dow Jones Industrial average to drop 150 points, briefly wiping out $136 billion in value. The damage was done by hacking the Twitter account of the Associated Press to report bogus explosions at the White House that were said to have injured President Barack Obama.[16] In May 2013, there were allegations that Iran was behind new attacks on US energy firms.[17]

[7] "Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolutions in the Islamic Republic of Iran," IAEA Board of Governors, May 22, 2013, http://isis-online.org/uploads/isis-reports/documents/IAEA_Iran_Safeguards_report_--_22May2013.pdf.

[8] Sanger, *Confront and Conceal.*

[9] Email to the author, January 10, 2013.

[10] Sanger, *Confront and Conceal.*

[11] Jason Healey and A.J. Wilson, "Cyber Conflict and the War Powers Resolution: Congressional Oversight of Hostilities in the Fifth Domain," Atlantic Council, February 2013, http://www.acus.org/files/publication_pdfs/403/bsc130221cyberwprpub.pdf.

[12] Telephone interview with the author, February 20, 2013.

[13] Healey and Wilson, "Cyber Conflict and the War Powers Resolution: Congressional Oversight of Hostilities in the Fifth Domain."

[14] Michael Joseph Gross, "Silent War," *Vanity Fair*, July 2013, http://www.vanityfair.com/culture/2013/07/new-cyberwar-victims-american-business.

[15] Comment by the co-author at the Atlantic Council on February 13, 2013, http://www.acus.org/event/role-congress-cyber-conflict.

[16] Gross, "Silent War."

[17] Nicole Perlroth and David E. Sanger, "New Computer Attacks Traced to Iran, Officials Say," *The New York Times*, May 24, 2013, http://www.nytimes.com/2013/05/25/world/middleeast/new-computer-attacks-come-from-iran-officials-say.html.

US allies have also been targeted. An individual with access to employees' desktop computers at Saudi Aramco infected them last year with a virus that destroyed data on three quarters of the machines and displayed a picture of a burning US flag. These computers became paperweights, entirely useless with all their data destroyed—a significant escalation from attacks that entail only stealing information or causing short-term disruption.[18]

Beyond the private sector, there have been reports of Iranian targeting of US government facilities. Diplomats from Iran and Venezuela were secretly filmed discussing plans for cyber attacks against US targets including nuclear facilities.[19] Given Iranian terrorist attacks in Europe, the Middle East and Europe—and a foiled plot in 2011 to kill the Saudi ambassador in Washington—it is fair to draw a straight line to some potentially very bad scenarios.

Indeed, given Iran's conventional weakness, cyber is an attractive alternative—the ultimate asymmetric weapon. Attacks can be mounted from outside the country—say by hackers in Russia or Lebanon—and difficult to trace. An assault in March 2013 on South Korea that paralyzed ATMs and three television networks has been blamed on North Korea.[20] There is no reason to believe that Iran's growing cyber army is any less capable than that of an isolated Asian rogue state with few IT graduates, limited Internet access, and a paucity of computers.

Iran's Efforts to Control Domestic Access to the Internet

Iran has used cyber tools to great effect domestically especially since 2009, when it used the Internet to crack down on those protesting fraud-tainted presidential elections. Iran is increasingly adept at blocking access to web sites carrying political and social content deemed threatening to the Islamic regime. The government has defended this censorship as necessary to protect the "peace of mind" of society and especially "children and youth." According to one government website, "Organized and regulated filtering, to purify the cyberspace environment and protect the society's peace of mind, is not just an option but a necessity."[21]

Iran also controls the speed of access to the Internet, slowing it down during sensitive periods so that photos and videos are particularly difficult to send or download. Foreign email services such as Google and Hotmail are also periodically blocked, as is access to virtual private networks.[22] In the run-up to the June 14 presidential elections, there was also an outbreak of phishing that lured tens of thousands of Iranians to a fake Google sign-in page.[23]

However, the Iranian government, which has talked for years about creating a closed or so-called "halal" Internet, has not yet put this national Internet in place. Iranians experienced in circumventing government controls managed to communicate in the last days of the presidential election campaign, contributing to a large turnout and the victory of the least hard-line candidate permitted to run, former nuclear negotiator Hassan Rouhani.[24]

Cyber also figures in many aspects of Iranian strategic planning. Supreme Leader Ayatollah Ali Khamenei in March 2012 announced the creation of a Supreme Council on Cyberspace that includes the country's president, the speaker of the parliament, the head of the judiciary, the commander of the Islamic Revolutionary Guard Corps, the head of the national police, Khamenei's representative on the country's Supreme National Security Council,

[18] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all.

[19] S. Smithson, "U.S. authorities probing alleged cyberattack plot by Venezuela, Iran," *The Washington Times*, December 13, 2011, http://www.washingtontimes.com/news/2011/dec/13/us-probing-alleged-cyberattack-plot-iran-venezuela/?page=all.

[20] "Cyberattack focuses attention on potential for North Korea's 'cyber warriors' to attack South," Associated Press, March 24, 2013, http://bigstory.ap.org/article/experts-nkorea-training-teams-cyber-warriors.

[21] "Filtering and Monitoring of the Internet in Countries around the World," [in Farsi] *Peyvandha*, http://peyvandha.ir/0-5.htm.

[22] After the Green Movement: Internet Controls in Iran 2009-2012," Open Net Initiative, February 2013, https://opennet.net/sites/opennet.net/files/iranreport.pdf.

[23] Nicole Perlroth, "Google Says It has Uncovered Iranian Spy Campaign," *The New York Times*, June 12, 2013, http://bits.blogs.nytimes.com/2013/06/12/google-says-it-has-uncovered-iranian-spy-campaign/.

[24] Mohammad Davari, "Social media abuzz as Iran heads to the polls," Agence-France Press, June 13, 2013, http://www.google.com/hostednews/afp/article/ALeqM5jkr0AvV3GdwljPIuE_QesK3xXTVA?docId=CNG.f3cb848c4cc24c812915350900d10705.9e1.

and officials in charge of state broadcasting, information technology, and science.[25]

The Revolutionary Guards have their own Cyber Defense Command which is said to recruit and train thousands of people to spy on dissidents on the Internet and spread Iranian government views.[26] The so-called Iranian Cyber Army hacks into opposition websites and foreign media such as the Persian Service of the BBC and Voice of America. Another organization, the Passive Defense Organization (PDO), was established by Khamenei a decade ago to combat Internet-based threats. According to a report by the Open Net Initiative, the head of the PDO, Brigadier General Gholamreza Jalali, "defines the organization's activities as aiming to decrease national vulnerabilities, while increasing stability against foreign threats without the use of arms."[27]

These Iranian capabilities are likely to be dangerous but not lethal. Indeed, as of mid-2013, no one is known to have died from a cyber attack anywhere in the world from any source.

Cyber incidents have so far tended to have effects that are either widespread but fleeting, or persistent but narrowly focused. No attacks, thus far, have been both widespread and persistent. Moreover, as with conflict in other domains, cyber attacks can take down many targets. But keeping them down over time in the face of determined defenses has thus far been beyond the capabilities of all but the Tier 1 cyber powers.

This means that Iran has the ability to take down important targets—for example, 30,000 computers at Saudi Aramco—but mounting a more strategically significant cyber attack may be well beyond its capabilities. After all, if the goal of the attack was to not just damage desktop computers but to disrupt Saudi oil production, the 2012 attack was a clear failure. To have succeeded, the Iranians would have needed accurate battle damage assessment ("did we achieve the effects we sought?") as well as the capability to continue to restrike their targets. Lacking these, the attack was a one-off and the company was able to rebuild and restore its networks.

Likewise, the DDoS attacks on American banks have been some of the largest and most disruptive, but they did not keep some of the banks said to be affected from easily earning multi-billion dollar profits in 2012. The attacks were unsettling, but came nowhere close to threatening the firms—much less the US financial sector as a whole.

Looking Forward

While the cyber conflict may escalate, it is unlikely that there will be an overt cyber war anytime soon between the United States and Iran. So far, there have been campaigns of relatively limited aims on both sides, and with a new president just elected in Iran who is promising "constructive engagement" with the United States, open and more aggressive campaigns are unlikely in the near future. A continuation of covert irregular conflict, however, with involvement by the Revolutionary Guards and associated militias and proxies, is certainly possible. The Guards report to the hard-line clerical establishment, led by Khamenei, who remains in charge of Iranian defense and foreign policy.

These continuing cyber strikes are not likely to cause any truly significant disruption in the short term. The most likely and most damaging possibility is a campaign of attacks that creates a new political crisis which the American leadership may be loath to escalate.

An Iranian cyber attack on US companies or allies, even if not damaging in itself, could, however, create headlines and renewed demand for cyber or kinetic retaliation. Politicians in the United States and Israel, looking for harsher actions against Iran, could seize the moment to push an escalation far beyond the scale of the actual disruption, especially as there are few—if any—international agreements on international cyber behavior.[28]

[25] "After the Green Movement: Internet Controls in Iran 2009-2012."

[26] Farnaz Fassihi, "Iran's Censors Tighten Grip." *The Wall Street Journal*, 16 March 2012, http://online.wsj.com/article/SB10001424052702303717304577279381130395906.html.

[27] "After the Green Movement: Internet Controls in Iran 2009-2012."

[28] Thom Shanker, "Pentagon is Updating Conflict Rules in CyberSpace," *The New York Times*, June 27, 2013, http://www.nytimes.com/2013/06/28/us/pentagon-is-updating-conflict-rules-in-cyberspace.html?ref=world&_r=0.

Accordingly, the United States should redouble its efforts to augment cyber defenses for both government and private networks and to assist US allies that may present softer targets for Iranian attack—especially when private companies are assaulted because of US national security policy.

Given the likelihood of blowback against the US private sector, it may be advisable for the United States to exercise caution in mounting new attacks on the order of Stuxnet, while continuing to keep them as an option. The United States should also enhance cyber surveillance of Iran's nuclear program while continuing to improve both US cyber offense and defense. Stuxnet was a small step for covert action but a giant leap in cyber conflict, and those with glass infrastructure should not throw stones.

As the nuclear crisis with Iran remains unresolved, the Obama administration should also support developing international agreements regulating behavior in cyberspace—with the understanding that Iran is unlikely to respect such agreements while it is under harsh economic sanctions.

Cyber war, like sanctions, may be preferable to so-called "kinetic" action that puts American forces at risk, but it is not a silver bullet against Iranian centrifuges or any other target. As US intelligence authorities have publicly stated, Iran is already at the point where it could quickly build nuclear weapons if it so chose. The determining factor is the political will of the Iranian leadership.[29] There are other ways to influence Iran—through sanctions and diplomatic outreach—that may have fewer unintended adverse consequences and that could lead to more progress in resolving overall disputes between the international community and Iran,[30] although cyber warfare should remain an option if Iran continues to move toward a nuclear weapon.

JULY 2013

[29] Remarks as delivered by James R. Clapper, Director of National Intelligence, Worldwide Threat Assessment to the Senate Select Committee on Intelligence, March 12, 2013, http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf.

[30] "Time to Move from Tactics to Strategy on Iran," Atlantic Council Iran Task Force, April 4, 2013, http://www.acus.org/files/publication_pdfs/403/itf_report_final.pdf.

Atlantic Council Board of Directors

**Members of the Executive Committee*
List as of April 24, 2013

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

1101 15th Street, NW, Washington, DC 20005
(202) 463-7226, www.acus.org