The Iranian Cyber Threat, Revisited

Statement before the
U.S. House of Representatives Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

Ilan Berman
Vice President
American Foreign Policy Council

March 20, 2013

Chairman Meehan, distinguished members of the Subcommittee:

Thank you for the invitation to appear before you again today. Let me begin by commending the House Homeland Security Committee for its continued leadership on the issue of Iran and cyberwarfare. It is a topic that is of the utmost importance to the safety and security of the United States.

A year ago, I had the privilege of testifying before this committee regarding the Islamic Republic's cyber warfare capabilities, and the threat that they could potentially pose to the American homeland. Today, the questions that were posed at that time are more relevant than ever.

The past year has seen the Iranian regime evolve significantly in its exploitation of cyberspace as a tool of internal repression, with significant consequences for country's overall political direction. During the same period, Iran also has demonstrated a growing ability to hold Western targets at risk in cyberspace, amplifying a new dimension in the asymmetric conflict that is now taking place over the Iranian regime's nuclear program.

IRAN VERSUS THE WORLD-WIDE WEB

A little over three-and-a-half years ago, the fraudulent reelection of Mahmoud Ahmadinejad to the Iranian presidency galvanized the largest outpouring of opposition to the Iranian government since the 1979 Islamic Revolution. That protest wave, colloquially known as the Green Movement, made extensive use of the Internet and social media in its

anti-regime activities. Iranian authorities responded with a similar focus—one that has both persisted and expanded in the wake of their successful suppression of the Green Movement during the 2009/2010 timeframe.

Most conspicuously, the Iranian government is moving ahead with the construction of a new national Internet system. As of October 2012, some 10,000 computers—from both private users and government offices—were found to be connected to this "halal" or "second" Internet, which is aimed at isolating the Iranian population from the World Wide Web.[1] The eventual goal of the Iranian regime is to force all Iranian citizens to use this system. Iranian officials thus have announced plans to reduce Internet speeds within the Islamic Republic, as well as increase costs of subscriptions to Internet Service Providers (ISPs) within the country.[2]

Along the same lines, Iran in December 2012 launched *Mehr*, a home-grown alternative to YouTube that features government-approved video content designed specifically for domestic audiences.[3] Iranian authorities also reportedly are working on new software suites designed to better control social-networking sites (a hub of activity during the 2009 protests and after).[4]

The Iranian regime likewise has expanded control of domestic phone, mobile and Internet communications. In the months after the summer 2009 protests, Iranian authorities installed a sophisticated Chinese-origin surveillance system to track and monitor phone, mobile and Internet communications.[5] They have since supplemented such tracking with methods intended to limit access to such media. Just this month, for example, Iranian authorities blocked most of the virtual private networks (VPNs) used by Iranians to circumvent the government's Internet filters.[6]

The Iranian regime has stepped up its detention and intimidation of reporters and activists who utilize the World-Wide Web as well. Its tool of choice to do so has been the Cyber Police, a dedicated division of the country's national police that was established in January 2011.[7] Earlier this year, the European Union added the Cyber Police to its sanctions list for the unit's role in the November 2012 torture and death of blogger Sattar Beheshti while in police custody.[8] In all, some 58 journalists and "netizens" are currently imprisoned by Iranian authorities, according to the journalism watchdog group Reporters Without Borders.[9]

The Iranian regime also has established a new government agency to monitor cyberspace. The Supreme Council on Cyberspace was formally inaugurated by Iranian Supreme Leader Ali Khamenei in April of 2012, and serves as a coordinating body for the Islamic Republic's domestic and international cyber policies.[10]

All of these activities have been propelled by a sense of urgency on the part of the Iranian leadership. This June, Iranians will go to the polls to elect a new president. That political contest, although sure to be stage-managed by clerical authorities, will nonetheless serve to

some degree as a referendum on the Iranian regime's stewardship of the nation amid deepening Western sanctions. It could also see renewed activity by Iran's opposition forces, which have been politically sidelined in recent years. Iran consequently has made what the U.S. intelligence community terms "cyber influence" a major governmental focus, clamping down on Internet activity "that might contribute to political instability and regime change."[11]

FROM DEFENSE TO OFFENSE

Iran's offensive cyber capabilities likewise continue to evolve and mature. Over the past three years, repeated cyber attacks have targeted the Iranian nuclear program, with considerable effect. In response, Iranian officials have focused on cyberspace as a primary flashpoint in their regime's unfolding confrontation with the West. Officials in Tehran now believe cyber war to be "more dangerous than a physical war," in the words of one top leader of Iran's Revolutionary Guard Corps (IRGC).[12]

As a result, the Iranian regime has made major investments in its offensive cyber capabilities. Since late 2011, the Iranian regime reportedly has invested more than $1 billion in the development of national cyber capabilities.[13] As a result, Iranian officials now claim to possess the "fourth largest" cyber force in the world—a broad network of quasi-official elements, as well as regime-aligned "hacktivists," who engage in cyber activities broadly consistent with the Islamic Republic's interests and views.[14] The activities of this "cyber army" are believed to be overseen by the Intelligence Unit of the IRGC.[15]

Increasingly, the Iranian regime has put those capabilities to use against Western and Western-aligned targets. Between September of 2012 and January of 2013, a group of hackers known as the Izz ad-Din al-Qassam Cyber Fighters carried out multiple distributed denial-of-service (DDoS) attacks against a number of U.S. financial institutions, including the Bank of America, JPMorgan Chase and Citigroup. Due to the sophistication of the attacks, U.S. officials have linked them to the Iranian government.[16]

A similar attack attributed to the Iranian regime took place in August 2012, when three-quarters of the computers of Saudi Arabia's Aramco state oil corporation were targeted by a virus called "Shamoon." The malicious software triggered a program that replaced Aramco's corporate data with a picture of a burning American flag at a predetermined time.[17]

The Iranian regime has also begun to proliferate its cyber capabilities to its strategic partners. Iran reportedly has provided the regime of Syrian dictator Bashar al-Assad, now locked in a protracted civil war against his own people, with crucial equipment and technical assistance for carrying out Internet surveillance.[18] This, in turn, has helped the Assad regime to more effectively target and neutralize elements of the Syrian opposition.

A MATURING THREAT

Despite recent advances, Iran's cyber capabilities are still nascent when compared to those of China and Russia. There is broad agreement among technical experts that the cyber threat posed by the Iranian regime is more modest than that posed by either Moscow or Beijing, at least for the moment. Yet Iran's activities in, and exploitation of, cyberspace should be of utmost concern to American policymakers, for several reasons.

The first is opportunity. The capabilities "gap" that currently exists in Iran's ability to carry out sustained and significant cyber attacks against U.S. infrastructure could close rapidly. This is because all of the resources that the Islamic Republic requires, whether human or technological, can be acquired quickly and comparatively cheaply from gray and black market sources. Additionally, recent years have seen the Iranian regime receive significant inputs to its strategic programs from abroad, most prominently from China and North Korea. This assistance is known to have furthered Iran's nuclear and ballistic missile capabilities, perhaps significantly so. Given this history, there is every reason to conclude that cooperation between Iran and its strategic partners is ongoing in the cyber domain as well.

The second is intent. Over the past two years, no fewer than five distinct cyber assaults have targeted the Iranian regime's nuclear effort. (At least one, moreover, has been determined to be domestic in origin, suggesting the Iranian regime faces an internal cyber threat as well). As a result, Iranian officials have come to believe—with considerable justification—that conflict with the West has already begun. The cyber attacks that Iran has carried out in recent months provide a strong indicator that the Iranian regime is both willing and able to retaliate in kind.

Finally, it is worth noting that Iran represents a *qualitatively* different cyber actor from either Russia or China. While both the PRC and the Russian Federation actively engage in cyber espionage against the United States, each has repeatedly avoided mounting a cyber attack so disruptive that it precipitates a breakdown of diplomatic relations with Washington. Iran, by contrast, could well countenance exactly such a course of action in the not too distant future.

In his most recent testimony to the Senate Select Committee on Intelligence, Director of National Intelligence James Clapper noted that "Iran prefers to avoid direct confrontation with the United States because regime preservation is its top priority."[19] This, however, has the potential to change rapidly in the event of a further deterioration of the current, tense standoff between the international community and Iran over its nuclear program. Iranian officials have made clear that they see cyberspace as a distinct warfighting medium in their unfolding confrontation with the West.

Government officials increasingly recognize this fact. A draft National Intelligence Estimate now circulating within the U.S. government reportedly identifies Iran as one country which would benefit substantially from having the capability to target and disable sectors of the U.S. economy.[20] What is not yet visible, however, is a comprehensive approach to understand, address and mitigate Iran's ability to hold American interests and infrastructure at risk via cyberspace.

CYBERSPACE AND THE IRANIAN BOMB

Back in October, then-Secretary of Defense Leon Panetta warned publicly that the United States could soon face a mass disruption event of catastrophic proportions, a "cyber Pearl Harbor" of sorts. "An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches," cautioned the Defense secretary. "They could derail passenger trains, or even more dangerous, derail trains loaded with lethal chemicals. They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country."[21]

Such a scenario is plausible, although the U.S. intelligence community currently judges its likelihood to be "remote," at least in the near term.[22] However, geopolitical events could dramatically alter this assessment, and incentivize threat actors in cyberspace to target both American interests and infrastructure.

In this regard, no scenario is more urgent or potentially dangerous than the unfolding crisis over Iran's nuclear program. Despite a massive expansion of Western economic pressure over the past year, the Iranian regime still shows no signs of slowing its drive toward atomic capability. To the contrary, Iranian officials have taken a defiant stance, laying out the need for an "economy of resistance" with which they will be able to weather economic pressure from the United States and Europe until such time as they cross the nuclear Rubicon.[23] As such, the near future could see a further escalation of the crisis, perhaps including the use of force against Iran by one or more nations.

Should that happen, cyber war with Iran could become a distinct possibility. So, too, could Iranian targeting of American forces, interests and infrastructure, with potentially devastating effects on the security of the U.S. homeland.

---

[1] Sara Reardon, "First Evidence for Iran's Parallel Halal Internet," *New Scientist* no. 2886, October 10, 2012, http://www.newscientist.com/article/mg21628865.700-first-evidence-for-irans-parallel-halal-internet.html.

[2] Reporters Without Borders, "The Enemies of Internet: Iran," March 12, 2013, http://surveillance.rsf.org/en/iran/.

[3] David Murphy, "Iran Launches 'Mehr,' Its Own YouTube-Like Video Hub," *PCMag*, December 9, 2012, http://www.pcmag.com/article2/0,2817,2413014,00.asp.
[4] Golnaz Esfandiari, "Iran Developing 'Smart Control' Software for Social-Networking Sites," *Radio Free Europe/Radio Liberty*, January 5, 2013, http://www.rferl.org/content/iran-developing-smart-control-software-for-social-networking-sites/24816054.html.
[5] Steve Stecklow, "Special Report: Chinese Firm Helps Iran Spy on Citizens," Reuters, March 22, 2012, http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B820120322.
[6] "Iran Blocks Use of Tool to Get around Internet Filter," Reuters, March 10, 2013, http://www.reuters.com/article/2013/03/10/us-iran-internet-idUSBRE9290CV20130310.
[7] University of Pennsylvania, Annenberg School of Communications, Iran Media Program, "Internet Censorship in Iran," n.d., http://iranmediaresearch.org/sites/default/files/research/pdf/1363180689/1385/internet_censorship_in_iran.pdf.
[8] "EU Sanctions Iran Judges, Cyber Police for Rights Abuse," Agence France-Presse, March 12, 2013, http://www.france24.com/en/20130312-eu-sanctions-iran-judges-cyber-police-rights-abuse.
[9] Reporters Without Borders, "Intelligence Ministry Admits Arresting News Providers, Blames Foreign Media," February 20, 2013, http://en.rsf.org/iran-intelligence-ministry-admits-20-02-2013,44099.html.
[10] University of Pennsylvania Iran Media Program, "Internet Censorship in Iran."
[11] James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community," Statement for the Record before the Senate Select Committee on Intelligence, March 12, 2013, 2, http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf.
[12] "Iran Sees Cyber Attacks as Greater Threat than Actual War," Reuters, September 25, 2012, http://www.reuters.com/article/2012/09/25/net-us-iran-military-idUSBRE88O0MY20120925.
[13] Yaakov Katz, "Iran Embarks on $1b. Cyber-Warfare Program," *Jerusalem Post*, December 18, 2011, http://www.jpost.com/Defense/Article.aspx?id=249864http://www.jpost.com/Defense/Article.aspx?id=249864.
[14] "Iran Enjoys 4th Biggest Cyber Army in World," FARS (Tehran), February 2, 2013, http://abna.ir/data.asp?lang=3&Id=387239.
[15] University of Pennsylvania Iran Media Program, "Internet Censorship in Iran."
[16] Nicole Perlroth and Quentin Hardy, "Bank Hacking was the Work of Iranians, Officials Say," *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?pagewanted=1&_r=0.
[17] Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing back," *New York Times*, October 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all.
[18] Ellen Nakashima, "Iran aids Syria in Tracking Opposition via Electronic Surveillance, U.S. Officials Say," *Washington Post*, October 9, 2012, http://articles.washingtonpost.com/2012-10-09/world/35500619_1_surveillance-software-syrians-president-bashar.
[19] Clapper, Statement for the Record, 5.
[20] Nicole Perlroth, David E. Sanger and Michael S. Schmidt, "As Hacking against U.S. Rises, Experts Try to Pin Down Motive," *New York Times*, March 4, 2013, http://mobile.nytimes.com/2013/03/04/us/us-weighs-risks-and-motives-of-hacking-by-china-or-iran.xml;jsessionid=8304B2493AF15262FDA4F217DDF0CAFE?f=19.

[21] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, October 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0.
[22] Clapper, Statement for the Record, 5.
[23] "Iran Leader Calls for 'Economy of Resistance,'" Agence France-Presse, August 23, 2012, http://news.yahoo.com/iran-leader-calls-economy-resistance-134523014.html.