The Iranian Cyber Threat to the U.S. Homeland

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

and

Subcommittee on Counterterrorism and Intelligence

Ilan Berman
Vice President
American Foreign Policy Council

April 26, 2012

Congressman Lundgren, Congressman Meehan, distinguished members of the Subcommittees:

Thank you for the opportunity to appear before you today to address the cyber warfare capabilities of the Islamic Republic of Iran, and the threat that they pose to the U.S. homeland.

Conventional wisdom suggests that the Iranian regime, now being squeezed significantly by sanctions from the United States and Europe and grappling with significant domestic socio-economic malaise, is far from an imminent threat to the American homeland (even if it does present a vexing foreign policy challenge for the U.S. and its allies). Yet, over the past three years, the Iranian regime has invested heavily in both defensive and offensive capabilities in cyberspace. Equally significant, its leaders now increasingly appear to view cyber warfare as a potential avenue of action against the United States.

IRANIAN CAPABILITIES IN GEOPOLITICAL CONTEXT

Iran's expanding exploitation of cyberspace can be attributed to two principal geopolitical drivers.

The first are the Iranian regime's efforts to counter Western influence and prevent the emergence of a "soft revolution" within its borders. In his March 2012 Nowruz message to the Iranian people, President Obama alluded to the growing efforts of the Iranian regime to isolate its population from the outside world when he noted that an "electronic curtain has

fallen around Iran."[1] That digital barrier has grown exponentially over the past three years, as Iran's leadership has sought to quell domestic dissent and curtail the ability of its opponents to organize.

The proximate cause of this effort was the fraudulent June 2009 reelection of Mahmoud Ahmadinejad to the Iranian presidency, which catalyzed a groundswell of domestic opposition that became known colloquially as the "Green Movement." In the months that followed, Iran's various opposition elements relied extensively on the Internet and social networking tools to organize their efforts, communicate their messages to the outside world, and rally public opinion to their side. In turn, the Iranian regime utilized information and communication technologies extensively in its suppression of the protests—and thereafter has invested heavily in capabilities aimed at controlling the Internet and restricting the ability of Iranians to access the World-Wide Web.[2]

This focus has only been reinforced by recent revolutionary fervor throughout the Middle East and North Africa. For while Iranian authorities have sought to depict the so-called "Arab Spring" as both the start of an Islamic awakening and an affirmation of their regime's worldview[3], the anti-regime sentiment prevalent in the region actually represents a mortal threat to their corrupt, unrepresentative regime. As a result, the past year has seen a quickening of the regime's long-running campaign against "Western influence" within the Islamic Republic. These efforts include:

- The construction of a new, "halal" national internet. This "second Internet," which will effectively sever Iran's connection to the World-Wide Web by routing web users to pre-approved, Iranian-origin sites, is currently expected to come online by late summer 2012.[4]
- Installation of a sophisticated Chinese-origin surveillance system for monitoring phone, mobile and Internet communications.[5]
- The passage of new, restrictive governmental "guidelines" forcing Internet cafes to record the personal information of customers—including vital data such as names, national identification numbers, and phone numbers—as well the installation of closed-circuit cameras to keep video logs of all customers accessing the World-Wide Web.[6]
- Movement toward the formation of a new government agency to monitor cyberspace. Once operational, this "Supreme Council of Cyberspace," which will be headed by top officials from both Iran's intelligence apparatus and the Revolutionary Guards, will be tasked with "constant and comprehensive monitoring over the domestic and international cyberspace," and be able to issue sweeping decrees concerning the Internet that would have the full strength of law.[7]

The second geopolitical driver of Iran's interest in cyberspace relates to the expanding conflict with the West over its nuclear ambitions. Since the Fall of 2009, Iran has suffered a series of sustained cyber attacks on its nuclear program. The most well-known of these is Stuxnet, the malicious computer worm that attacked the industrial control systems at several Iranian nuclear installations, including the uranium enrichment facility at Natanz, between late 2009 and late 2010. At the height of its effectiveness, Stuxnet is estimated to have taken ten percent or more of Iran's 9,000 then-operational centrifuges offline.[8]

Stuxnet has been followed by at least two other cyber attacks aimed at derailing Iran's nuclear development. "Stars," a software script targeting execution files, was uncovered by the Iranian regime in April 2011.[9] Subsequently, "Duqu," a malware similar to Stuxnet and aimed at gaining remote access to Iran's nuclear systems, was identified in October/November 2011.[10]

Publicly, the origins of these intrusions are still an open question. Israel has steadfastly denied any role in the authorship of Stuxnet or other cyber attacks, despite widespread speculation to the contrary. The United States, too, has remained silent on the subject, although suspicions abound that the CIA played at least some part in putting together and deploying Stuxnet (and perhaps other malware as well).[11]

For the Iranian regime, however, the conclusion is clear. War with the West, at least on the cyber front, has been joined, and the Iranian regime is mobilizing in response. In recent months, it reportedly has launched an ambitious $1 billion governmental program to boost national cyber capabilities—an effort that involves acquisition of new technologies, investments in cyber defense, and the creation of a new cadre of cyber experts.[12] It has also activated a "cyber army" of activists which, while nominally independent, has carried out a series of attacks on sites and entities out of favor with the Iranian regime, including social networking site Twitter, Chinese search engine Baidu, and the websites of Iranian reformist elements.[13]

CYBERWAR AND IRANIAN STRATEGY

In his testimony to the Senate Select Committee on Intelligence this past January, General James Clapper, the Director of National Intelligence, alluded to what amounts to a seismic shift in Iranian strategy. In response to growing economic sanctions and mounting pressure from the United States and its allies, he noted, "Iranian officials—probably including Supreme Leader Ali Khamenei—have changed their calculus and are now willing to conduct an attack in the United States."[14]

Gen. Clapper was referring, most directly, to the foiled October 2011 plot by Iran's Revolutionary Guards to assassinate Saudi Arabia's envoy to the U.S. in Washington, DC. But, as the international crisis over Iran's nuclear ambitions continues to deepen, Iran's cyber capabilities should be a matter of significant concern as well. Experts have warned that, should the standoff over Iran's nuclear program precipitate a military conflict, Iran "might try to retaliate by attacking U.S infrastructure such as the power grid, trains, airlines, refineries."[15]

The Iranian regime appears to be contemplating just such an asymmetric course of action. In late July 2011, for example, *Kayhan*, a hardline newspaper affiliated with Iran's Revolutionary Guards, issued a thinly-veiled warning to the United States when it wrote in an editorial that America, which once saw cyberwarfare as its "exclusive capability," had severely underestimated the resilience of the Islamic Republic. The United States, the paper

suggested, now needs to worry about "an unknown player somewhere in the world" attacking "a section of its critical infrastructure."[16]

In keeping with this warning, over the past year infrastructure professionals in the United States have noted that Iran's "chatter is increasing, the targeting more explicit, and more publicly disseminated."[17] The Islamic Republic, in other words, increasingly has begun to seriously contemplate cyberwarfare as a potential avenue of action against the West.

Iran has significant capacity in this sphere. A 2008 assessment by the policy institute Defense Tech identified the Islamic Republic as one of five countries with significant nation-state cyberwarfare potential.[18] Similarly, in his 2010 book *Cyber War*, former National Security Council official Richard Clarke ranks Iran close behind the People's Republic of China in terms of its potential for "cyber-offense."[19] These capabilities, moreover, are growing. In his January 2012 Senate testimony, General Clapper alluded to the fact that Iran's cyber capabilities "have dramatically increased in recent years in depth and complexity."[20]

PREPARING FOR CYBERWAR WITH IRAN

Where does the United States stand with regard to a response? The Obama administration has made cybersecurity a major area of policy focus since taking office in 2009, and the past year in particular has seen a dramatic expansion of governmental awareness of cyberspace as a new domain of conflict. But this attention remains uneven, focused largely on network protection and resiliency (particularly in the military arena), and on the threat capabilities of the People's Republic of China and, to a lesser extent, of the Russian Federation. Serious institutional awareness of, and response to, Iran's cyberwarfare potential has lagged behind the times.

Indeed, personal conversations with a range of experts inside and outside of government reveal a troubling lack of clarity about the Iranian cyber threat—and the absence of serious planning to counter it. While some parts of the federal bureaucracy (namely U.S. Strategic Command and the State Department's Nonpoliferation Bureau) have begun to pay attention to Iran's threat potential in the cyber realm, as yet there exists no individual or office tasked with comprehensively addressing the Iranian cyberwarfare threat. The U.S. government, in other words, has not yet even begun to get ready for cyberwar with Iran.

It should. After all, it is not out of the question that the Iranian regime could attempt an unprovoked cyber attack on the United States. As the foiled October 2011 plot against Saudi Arabia's ambassador to the United States indicates, Iran has grown significantly bolder in its foreign policy, and no longer can be relied upon to refrain from direct action in or against the U.S. homeland. Far more likely, however, is a cyberwarfare incident related to Iran's nuclear program. In coming months, a range of scenarios—from a renewed diplomatic impasse to a further strengthening of economic sanctions to the use of military force against Iranian nuclear facilities—hold the potential to trigger an asymmetric

retaliation from the Iranian regime aimed at vital U.S. infrastructure, with potentially devastating effects.

At the very least, it is clear that policymakers in Tehran are actively contemplating such an eventuality. Prudence dictates that their counterparts in Washington should be doing so as well.

---

[1] White House, Office of the Press Secretary, "Remarks of President Obama Marking Nowruz," March 20, 2012, http://www.whitehouse.gov/the-press-office/2012/03/20/remarks-president-obama-marking-nowruz.

[2] See, for example, Saeid Golkar, "Liberation or Suppression Technologies? The Internet, the Green Movement and the Regime in Iran," *International Journal of Emerging Technologies and Society* 9, no. 1 (2011), 50-70, http://www.swinburne.edu.au/hosting/ijets/journal/V9N1/pdf/Article%204%20Golkar.pdf.

[3] "Khamenei Credits Iranian Revolution With Fuelling Egyptian Revolt," Reuters, February 4, 2011, http://www.thenational.ae/news/world/middle-east/khamenei-credits-iranian-revolution-with-fuelling-egyptian-revolt; Robert F. Worth, "Efforts To Rebrand Arab Spring Backfires In Iran," *New York Times*, February 2, 2012, http://www.nytimes.com/2012/02/03/world/middleeast/effort-to-rebrand-arab-spring-backfires-in-iran.html?pagewanted=all.

[4] See Steven Musil, "Iran Expected To Permanently Cut Off Internet By August," CNET, April 9, 2012, http://news.cnet.com/8301-1023_3-57411577-93/iran-expected-to-permanently-cut-off-internet-by-august/

[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] *Radio Free Europe*, January 4, 2012

[7] Ramin Mostaghim and Emily Alpert, "Iran's Supreme Leader Calls for New Internet Oversight Council," *Los Angeles Times*, March 7, 2012, http://latimesblogs.latimes.com/world_now/2012/03/iran-internet-council-khamenei.html.

[8] David Albright, Paul Brannan, and Christina Walrond, "Stuxnet Malware and Natanz: Update of ISIS December 2, 2010 Report," Institute for Science and International Security *ISIS Reports*, February 15, 2011, http://www.isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/.

[9] "After Stuxnet: Iran Says It's Discovered 2nd Cyber Attack," Reuters, April 25, 2011, http://www.jpost.com/IranianThreat/News/Article.aspx?id=217795.

[10] "Iran Says Has Detected Duqu Computer Virus," Reuters, November 13, 2011, http://www.reuters.com/article/2011/11/13/us-iran-computer-duqu-idUSTRE7AC0YP20111113.

[11] Ralph Langner, "Cracking Stuxnet, a 21st Century Cyber Weapon," TED Talks, March 2011, http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html.

[12] 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.

[13] Farvartish Rezvaniyeh, "Pulling the Strings of the Net: Iran's Cyber Army," PBS *Frontline*, February 26, 2010, http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/02/pulling-

the-strings-of-the-net-irans-cyber-army.html; Alex Lukich, "The Iranian Cyber Army," Center for Strategic & International Studies, July 12, 2011, http://csis.org/blog/iranian-cyber-army.

[14] James Clapper, testimony before the Senate Select Committee on Intelligence, January 31, 2012.

[15] Brian Ross, "What Will Happen to the US if Israel Attacks Iran?" ABC News, March 5, 2012, http://abcnews.go.com/Blotter/israel-attacks-iran-gas-prices-cyberwar-terror-threat/story?id=15848522#.T4g5tqvY9Ll.

[16] "STUXNET has Returned Home," *Kayhan* (Iran), July 27, 2011. (Author's collection).

[17] Author's personal communication, August 17, 2011.

[18] Kevin Coleman, "Iranian Cyber Warfare Threat Assessment," Defense Tech, September 23, 2008, http://defensetech.org/2008/09/23/iranian-cyber-warfare-threat-assessment/.

[19] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It* (New York: Harper Collins, 2010), 148.

[20] Clapper, testimony before the Senate Select Committee on Intelligence.