RANKING MEMBER YVETTE D. CLARKE (D-NY) OPENING STATEMENT

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES
COMMITTEE ON HOMELAND SECURITY

JOINT HEARING: **"THE IRANIAN CYBER THREAT TO THE U.S. HOMELAND"**

THURSDAY, APRIL 26, 2012

State-sponsored cyber threats from Iran, and actual attacks from other countries directed at the U.S. have been a hot topic over the past few years. As you know, we have had a number of classified briefings concerning these state-sponsored attacks.

Our ability to detect, prevent, preempt, and deter terrorist and malicious state-sponsored cyber attacks reflects on our capability, and our political will, to protect our vital national critical infrastructure from devastating consequences.

I am glad my colleague and fellow New Yorker, Mr. Higgins, has brought some legislation to bear on the issue we are discussing today. His bill would amplify the State Department's reports to Congress on the proficiencies of Iran's cyber and technological capabilities. This will help us assess Iran's threat in greater detail.

There is quite a story to be told about Iran and cyber threats, and I will be interested in hearing the testimony today.

I have seen the report put out by ***Reporters Without Borders*** that places Iran on a list of "enemies of the internet", describing the various censoring techniques that Iran uses to control the flow of information among its own people. The report refers to the government-sponsored cyber police function that uses a combination of content-filtering and access controls. The report also mentions the use of distributed denial-of-service cyber attack techniques used as a form of political oppression, which it says may or may not be official state-sponsored activity.[1]

Reports of an "Iranian Cyber Army" have raised questions about the regime's cyber attack capabilities and the extent to which these attacks are coordinated by the government. Some have said 'The Iranian Cyber Army' may be a loose confederation of hackers and cyber activists similar to other hacking clusters, and may include cyber-crime networks and other groups.

One such group, known as the Ashiyaneh Digital Security Team, has claimed responsibility for hacking into and defacing thousands of websites.[2] Both the Iranian Cyber Army and Ashiyaneh are alleged to have ties with the Iranian government's Revolutionary Guards, but who can tell?

Given the Iranian regime's control over the Internet and attempts to crack down on citizen Internet activity, it would appear to be an sweeping promotion of hacking, without any legal or public recourse, and suggests a tacit governmental approval of these activities.

Some have said the Iranian Cyber Army resembles a collective of regime-backing hackers acting of their own volition, yet it may be that the regime has actively leveraged and employed the talents of a young population adept with computing tools.[3]

In the wake of Iran's presidential election in June of 2009, protesters had used Twitter to skirt government filters to report events and to organize opposition rallies, prompting the U.S. Department of State to request that Twitter reschedule its planned maintenance activities in order to ensure access to pro-democracy users.

---

[1] Reporters Without Borders, "Enemies of the Internet Report", March 13, 2012, accessed at http://en.rsf.org/beset-by-online-surveillance-and-12-03-2012,42061.html.

[2] FARS News, "Iran's Cyber Army Hacks 1000 US, British, French Gov't Websites", August 30, 2010, accessed at http://english.farsnews.com/newstext.php?nn=8906081424.

[3] Kellogg, Amy. "Iran is Recruiting Hacker Warriors for Its Army to Fight Enemies", Fox New, March 14, 2011.

But the Iranian regime's brutal crackdown on the protests has seemingly succeeded; demonstrations are now few and far between, and many of the web-based citizen journalists who documented the uprising have been killed, imprisoned, or gone underground, their voices silenced.

The most well known cyber event in Iran occurred later in 2009, when a Central European security firm reported the discovery of a software worm called Stuxnet that had infected computers controlling centrifuges of several Iranian nuclear enrichment plants. However, these computers were not connected to the Internet, and the worm was said to have been injected into those computers using an external device such as a thumb drive.

Stuxnet may be proof of Iran's vulnerability and the effectiveness of other nation-states cyber arsenals. However, it would also be possible for Iran to gain some knowledge of creating a Stuxnet-like virus from analyzing its network effects. This leads to fears of reverse-engineering leading to a capability of the types of cyber attacks on U.S. critical infrastructure that could rise to the level of a national security crisis.

We must be prepared for such rogue actions, and be prepared on a national defense level, as well as protecting our critical business operations, vital infrastructure functions, and frankly our daily lives.

The rapid technological advances in cyber security threats over the last several years have outpaced our ability as lawmakers to keep our laws up to date. The needed coordination of the many governmental agencies and private institutions, and the implementation of the procedures that will protect our infrastructure are huge undertakings, and will continue to have huge challenges. We are seeing some of those challenges being played out on the House floor this week, and my ranking Member, Mr. Thompson, is talking about some of the most constructive alternatives to the cyber legislation we are considering.

Our Intelligence Community and law enforcement agencies face many challenges to anticipate, investigate, and respond to cyber threats. Simply, all these challenges must be overcome, and protection of our infrastructure accomplished without violating our fundamental rights of individual privacy that are enshrined in our Constitution.