# Ranking Member Yvette D. Clarke (D-NY)

## Committee on Homeland Security's Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

## "Cyber Threats from China, Russia, and Iran: Protecting American Critical Infrastructure"

March 20, 2013 – 2 P.M.

I think that the topic at hand is an appropriate one for our subcommittee's first hearing this Congress.

I do not have to tell you, Mr. Chairman, that the cyber threats to our critical infrastructure are growing and serious, and cybersecurity is perhaps the most prominent national security issue we will face this Congress.

Last week, in the Intelligence Community's Annual Worldwide Threat Assessment report to Congress, Director of National Intelligence James Clapper named cyber as the leading threat to our national security, ahead of terrorism, transnational crime, and WMD proliferation.

To set the stage for the important actions that our Committee must take to enhance our nation's cybersecurity, it is important that we first examine the evolving nature of the threat we are facing.

Each month seems to bring a new wrinkle in our understanding of the threat to our government, to our businesses, and to individuals.

Malicious cyber actors have destroyed 30,000 computers on an oil company's network in the blink of an eye.

They have bombarded dozens of our banks with denial of service attacks on a weekly basis in a concerted campaign dragging on for months.

They have infiltrated the manufacturer of smart grid industrial control systems which are currently installed all across the country in our critical infrastructure.

And these are just reports that have been made public in the last nine months.

We have long since passed the time when our biggest challenge in cyberspace was dealing with the stereotypical teenager in his parents' basement.

A small group of nation states are taking advantage of the internet's openness to conduct cyber espionage, not only against traditional government targets such as defense and intelligence agencies, but against all variety of economic targets and critical infrastructure.

But though I think we have recognized this for some time, what has been missing is a public discussion of this bad behavior.

That’s why I think the events of the last few weeks have been a real tipping point in the way our Nation responds to cyber threats.

Foreign actors can no longer be permitted to commit industrial-strength espionage against our government and businesses without being brought to account, and I have been heartened to see that the Obama Administration has recently made great strides in this area.

Two weeks ago, National Security Advisor Tom Donilon went on the record about China’s aggressive behavior in cyberspace, outlining key areas where the US will require China’s engagement moving forward.

Then, last week, President Obama himself expanded upon the threat posed by the Chinese and other state actors and the strong messages that we are beginning to send.

I applaud the Administration’s willingness to raise this issue to the Presidential level, and I hope that it leads to substantive engagement with foreign governments on proper conduct in cyberspace.

Finally, I am pleased that we are joined today by this distinguished panel of witnesses, and I look forward to learning more about the cyber threats to our critical infrastructure and further informing the public debate on cybersecurity.