REMARKS AS PREPARED FOR DELIVERY

BY SPECIAL ASSISTANT TO THE PRESIDENT AND WHITE HOUSE CYBERSECURITY COORDINATOR MICHAEL DANIEL

RSA Conference USA 2013
San Francisco, CA

"007 or DDoS: What is Real World Cyber?"

February 28, 2013

OPENING COMMENTS

Good morning everyone. Thank you for the kind introduction**.** It's a pleasure to be here with you today and speak to the 2013 RSA Conference USA.

One of the great learning experiences of this job is to engage and listen to a diverse range of representatives from across government and the private sector.

My name is Michael Daniel, and I currently serve as Special Assistant to the President and Cybersecurity Coordinator at the White House.

In my role, I lead the federal government's development of national cybersecurity strategy and policy and oversee the implementation of those policies on behalf of President Obama. That makes me the chief cat herder for government cybersecurity.

007 VS. REAL WORLD CYBER

All too often, when people like me come to talk to people like you, the conversation sounds like the pitch for a new Hollywood blockbuster. You know the kind – it's the one involving a vaguely Keifer Sutherland look-alike and depicting a dark cyber future where intruders easily blow past all defenses in nanoseconds.

We toss around worst-case scenarios with major repercussions for U.S. national security, including massive physical destruction or loss of life. It's a great way to grab attention, and we must prepare for those scenarios, but I'm sure those of you living in the real world and dealing with the daily barrage of cyber threats wonder: "What's up with that?!"

So I'm not here to talk to you about 007-like exploits or "cybergeddon." I'm here to talk to you about real world, day-to-day cybersecurity. Not as exciting as a movie plot, but arguably more productive.

THE NEW NORMAL

I'm here to talk about the "new normal" cyber environment – where cybersecurity threats are increasingly broader, sophisticated, and dangerous – just not in the way Hollywood likes to portray it. In this context, I want to focus on a conversation, a question really, that's being asked right now: what is government's role in helping you manage this "new normal"?

Now don't get me wrong… as a government, our job is to prepare for the worst. But movie plot scenarios represent extreme situations – high impact, but low probability events. What about the far more likely problems – the every day, "real world" cybersecurity situations that make up this new normal?

The new normal is not massive power outages or train traffic grinding to a halt nationwide – those kinds of things are not "normal." Rather, the new normal is less flashy but still troubling: persistent intrusions, violations of privacy, thefts of business information, and degradation and denial of service to legitimate entities trying to do business or getting their message out on the Internet.

DDOS AS A TOOL

More powerful, sophisticated, and persistent distributed denial of service attacks (DDoS-es) are a good example of this "new normal." They have gotten quite big – with some pushing 100 gigabits per second – and sophisticated – with some designed to overwhelm servers with active requests instead of junk bits.

But for all of their sophistication and power, so far DDoS-es have been of limited – not catastrophic – impact.

- I'll readily admit that if you're an institution on the receiving end of one of these DDoS attacks, it probably doesn't feel that way. Your IT staff is probably working late hours, spending more money than planned, and scrambling to keep ahead of the disruptions.

- But looked at systemically, DDoS-es are annoying and result in limited delays and brief outages for those trying to access websites. It doesn't exactly scream "Die Hard" does it?

WHAT IS THE GOVERNMENT'S ROLE?

So that's what the new normal looks like. But what about the government's role here? Even if it's "just a DDoS," a significant amount of malicious online activity emanates from overseas; isn't it the government's responsibility to defend the U.S. from foreign attacks?

The short answer is: "yes, but…"

Consider the physical realm. There, we accept that security involves a spectrum of responsibilities from the individual – for example, putting locks on doors – to the community – for example, local police – to the national – for example, the military.

For cyberspace, we're trying to figure out that spectrum of responsibilities entails right now. So what follows the "but"?

GOVERNMENT'S ROLE IN PREVENTION

One governmental role is clear and uncontroversial: the government should help you – private sector companies – help yourself, particularly in the area of prevention. We're doing that now and we want to do more of it.

That means we will share actionable information with you. For example, we have shared hundreds of thousands of signatures and indicators with the private sector and over a hundred nations just in the past six months. In the Executive Order that the President announced at the State of the Union, we committed to redoubling this effort.

We also committed to expanding the Enhanced Cybersecurity Services for critical infrastructure beyond the U.S. defense industrial base. As called for in the new Executive Order, this capability provides classified signatures to firms or their ISPs to help counter known malicious cyber activity. OK, so maybe that's a little bit 007.

Additionally, we want to work with you to create a framework of baseline standards for cybersecurity. This is the baseline stuff that many firms here in this room already do. Sadly, though, that's not true for every firm in critical infrastructure.

GOVERNMENT'S ROLE IN PREPARATION AND RESPONSE

But information sharing for prevention is the easy answer from a policy standpoint, even though we still have work to do in this area. It gets much more complicated when it comes to responding to cyber incidents.

We know that geography and sovereignty still matter in cyberspace; the computers and wires that make up cyberspace all exist in someone's country. But the rules of geography are different in cyberspace. "Near" and "far"; "fast" and "slow"; and "big" and "small" have different meanings. These different rules mean that spectrum of security in cyberspace might not follow the same format as in the physical realm.

So the entire burden of network defense, regardless of where the threat originates, cannot fall solely on the government.

As a result, that means when you talk about incident response, emergency management might be a better model than an action movie.

For example, the government provides weather reports on approaching storms so that you have time to prepare. We will often recommend steps you can take to protect yourself in a storm. In cyberspace, that is the information sharing effort we discussed earlier.

But not every storm results in a federal government-led response. Only if a disaster exceeds state and local capabilities does the federal government jump in for support. And the federal government works to make state and local capabilities as robust as possible.

So what's the digital analogue to individual and local preparedness? You know what they are better than I do:

- It's that no CIO or CISO should be caught off guard if their public websites come under a DDoS attack.
- It's that senior management needs to understand the risk and business impact of various cyber events.
- It's that firms should participate in an information sharing organization, such as an ISAC.
- It's that nearly everyone should test their cybersecurity incident response plans – and have contingencies in place with service providers should those plans fail.
- It's that companies should use modern network defense best practices and technologies.
- It's that companies should have robust cybersecurity policies and training programs and continuously monitor their networks under the assumption that they have been breached.

Since individual firms can't address every cyber threat on their own, we must also develop strong community-based response capabilities, such as the cyber equivalents of mutual assistance agreements.

RESPONDING TO SIGNIFICANT CYBER INCIDENTS

Okay, but some disasters do prompt a federal response. What's the digital analogue for that? That's precisely the question we are trying to answer – when does a cyber incident warrant a federal response?

Now, I don't have the answer to that question just yet.

But what I can say is that once we decide that a federal response is warranted, there's still a broad spectrum of action of actions we could potentially take:

- DHS with the support of FBI, NSA, and other agencies might intensify information sharing efforts and provide technical assistance to companies that are the target of an attack;
- The State Department might use diplomatic channels to call upon countries to stop this activity. For example, we are now regularly raising these kinds of issues with countries such as China;
- Using other tools, federal law enforcement may investigate, attribute, arrest, and prosecute perpetrators;

- The FBI, as they did in CoreFlood, or the Secret Service, as they did with Mcolo, could work through the courts and companies to stop U.S. infrastructure from being used in the attack;

- U.S. CERT might coordinate with other CERTs to get foreign infrastructure participating in the attack shutdown;

- The Executive Branch might issue financial sanctions or visa restrictions against foreign hackers involved in efforts to target and disrupt our networks and critical infrastructure;

- And if warranted by a cyber incident's effects, the President might call on the U.S. military to take action.

I would note that many of these tools are not "cyber." And we want to continue to expand the tools and responses available to the President.

As a matter of policy, the government's responses will be cautious and incremental, and more robust federal responses have a higher threshold to cross for two main reasons:

- First, governments are not resourced or authorized to defend every network. Even if we were, we couldn't do it as well as local network owners, who are in the best position to protect their networks.

- Second, the risk of misattribution, miscalculation, and escalation in cyberspace are very real. As a government, any action we take in cyberspace must be considered against its possible foreign policy implications and our desire to establish international norms of acceptable behavior in cyberspace.

We don't want our response to something annoying to harm our relationships with other nations or worse, result in physical conflict.

We don't want to create a truly unstable "new normal" that would tell other countries it's OK to intervene on U.S. networks. Advocates of "hacking back" often don't stop to think how they would react if a foreign country did the same thing on our networks.

So the federal government will not ride in on a white horse like the Lone Ranger to respond to every incident. Oh wait, that movie's not out yet, but you get the picture.

Rather than responding reflexively, we believe that a better strategy is to encourage mutual responsibility. We need to move to an environment where we routinely and quickly respond to requests to prevent our infrastructure from being used in malicious cyber activities.

OUR AGENDA

So, what's left to do? Well, the answer is "a lot," of course.

First, we want to work with the private sector to implement the President's Executive Order. In particular, we need you to work with NIST to get the Framework done on time and done right.

However, the EO is a down payment. That's why we will continue to support congressional action in this area that:

- Incorporates privacy and civil liberties safeguards into all aspects of cybersecurity;
- Strengthens our critical infrastructure's cybersecurity by further increasing information sharing and by promoting the adoption of standards;
- Updates laws guiding federal agency network security;
- Gives law enforcement the tools to fight crime in the digital age; and
- Harmonizes data breach notification requirements.

We will support continuing preparation and response for cyber incidents to ensure that the government's national incident response capabilities are in shape and tested.

We're also pushing to improve the security of all federal networks; we have to get our own house in order.

We will continue to engage our Allies and partners worldwide to solidify norms of cyber behavior, and to ensure the Internet remains open, interoperable, secure, reliable, and stable. We will maintain a meaningful dialogue with the world's largest cyber actors, such a China, and work together to develop an understanding of acceptable behavior in cyberspace.

Finally, we will continue collaborating with the private sector to make the future Internet more resilient and less favorable to the attacker. And we will continue to support market innovations, such as those underway in the National Strategy for Trusted Identities in Cyberspace.

CONCLUSION

Adjusting to the "new normal" will be hard work. And while I can't promise exciting movie plots, I can work with all of you to tackle something much more practical for the long-run. Together, we can ensure that the role for the government in cyberspace is appropriate, balanced, and effective. As I said, we won't answer that question here, today. But we can keep the conversation going that will ultimately get us to an answer. We can develop a truly wide set of tools to tackle the cyber threat. Working together, we can finally build network defenses worthy of the name.

Thank you.

###