The Government's Four Cyber Silences

Testimony of

Jason Healey

Director, Cyber Statecraft Initiative, Atlantic Council to the

US-China Economic and Security Review Commission on

"Developments in China's Cyber and Nuclear Capabilities"

Monday, March 26, 2012
George Mason University, Manassas, Virginia

Thank you for the opportunity to be here.

I am going to speak very plainly today. The government is finally becoming more clear-minded about the risks of Chinese cyber espionage and is rushing towards solutions. And while there is no doubting the hard work and patriotism of those behind these efforts, it is not clear we are heading in the right direction.

The threat of Chinese espionage is so critical that the commander of our military cyber defenses has called it the "the biggest transfer of wealth through theft and piracy in the history of mankind." It is so bad, in fact, the United States may need to regulate the private sector and our companies need to submit to government monitoring.

But the threat has *not* bad enough to interest the government in the history of how we got here, or enough to go on the record about the threat, to take risks to share needed information or be willing to tell the Chinese to back off.

I call these the government's Four Silences. Added together I fear they are driving us to defeat.

First: **Silence about how we got here**.   This silence is more of ignorance than inaction.   When I meet with them, too many of America's cyber warriors and policy makers feel the battle only started sometime between 2003 and 2008 – that is, roughly when they personally got involved. We have been breathlessly rushing into the future, rarely looking back to learn what has happened before. No wonder we keep having new wake-up calls.

Our understanding of the basic issues is as old as I am. The Defense Science Board report that discussed hardware and software leakages, intrusions, supply chain attacks, and risk levels was researched *in 1969*. And yet we're still struggling.

We know we face adversaries that have "extensive resources in money, personnel, and technology;" and are "adept in circumventing physical and procedural safeguards," "patient and motivated," and "capable of exploiting a successful attack for maximum long-term gain." However, those exact phrases come, not from any recent NCIX report, but the 1991 "Computers at Risk" report from the National Research Council.

For more than 20 years, then the Executive branch has understood the advanced persistent threat … and yet we're still struggling.

America had its first state-sponsored cyber espionage case not in 2003, but in the mid-1980s. Our first Title 10 combat unit conducting offense and defense stood up in 1995, not 2005. We had a joint warfighting cyber commander in 1998 not 2008.

We treat cyber as forever novel and so we can't learn any lessons. No wonder we're forever struggling.

Looking back should teach us important lessons, perhaps the most important of which is we're stuck in a cycle of suffering.

If we’re going to learn from this history we need to collect it and teach it. The Atlantic Council has started a history series, starting with “Lessons from the First Cyber Commanders” to help and I am principal investigator with the Cyber Conflict Studies Association on the first cyber conflict history book. The US government should begin their own efforts, to collect key documents, conduct oral histories with the first generations of cyber warriors and start codifying the lessons learned.

And just as today’s military officers learn the lessons of Cannae, Trafalgar, the Chosin Reservoir, and MIG Alley, so must DoD’s new cyber cadre study *yesterday’s* cyber operations to understand those of *tomorrow*. This history should be part of the professional military training of our new military officers and a core part of the curriculum in courses to build military cyber warriors. DHS should likewise include this in their own coursework as part of their education projects to ensure it reaches the civilian workforce.

Second: **Silence about the threat we face**.

Government officials seem keen to *leak* information on how bad Chinese espionage is, but unwilling to actually *tell* the American people or our companies in critical infrastructure. If espionage is such a problem, how come we have to hear about it from the press or from experts like those sharing this panel with me today? Thank goodness for the Commission's reports.

When I poke government officials about this, they get giddy about trifles, a few sentences in an NCIX report or pat themselves on the back because a few members of industry in critical sectors have received security clearances and get periodic briefings. These are worthy achievements, but pale before the problem.

When I ask *why* the Executive branch cannot say more, I get a range of overlapping but contradictory responses:

1. We *are* sharing, didn't you see those sentences in the NCIX report?
2. I have no opinion and can't discuss this: it is classified way above my pay grade.
3. We would like to but it is caught up in the interagency.
4. We can't prove it's really China.
5. If we say China is doing it, they may get angry and stop lending us money.
6. There's nothing illegal about spying; after all, we do it!
7. If we declassified what we knew of the threat, people would panic.
8. The private sector isn't sharing with us, so why should we share with them? (Somehow, my response of, "government for the people" wins that argument less than you'd imagine.)
9. If we discussed this, it wouldn't matter since the Chinese would not change their behavior.
10. It's a wilderness of mirrors. If we discussed this, then the Chinese would know that we know.
11. If we talk, then our intelligence take won't be as good.

None of these reasons given, singly or in combination, are sufficient given how badly we're losing. If the private sector is truly critical, we have to change our mindset to be able to discuss the problem.

Intelligence officers love to collect, more and more, and if they act it on that collection it might disrupt the flow. But by treating this problem as a state secret, even from those under attack, the government is creating our own wilderness of mirrors, built entirely around itself. Worse, this familiar counterintelligence game is one our adversaries do not even know. We are not facing a single, monolithic KGB but a splash of non-state hacker groups loosely affiliated with many different official organs of the Chinese state.

What must be done? The government must follow the example of the Commission and be clear about the depth of the problem and name the country involved: China. If it is time for action we need to take this out of intelligence and counterintelligence channels and declassify significant portions, something that can only be done from the top.

We will never make progress if everyone looks for their classification stamps when the words "China," "cyber" and "espionage" are used together. ***The spy-versus-spy mentality is driving us into defeat.***

Given that it has said so little, no wonder there are so many skeptics of the government's motives. If the administration wants America to take it seriously, it must be clear: repeated speeches from senior officials, not just occasional sound bites; not just one NCIX report, but a slew of them; not just leaks to media, but interviews. The frequency and seriousness of their statements need to match the crisis at hand and this should start from the White House.

Third: **Silence about practical information which could help the private sector**.

A related point to the one I just made is that the government has been far too cautious giving needed practical information to the private sector. The reasons are usually the same, but the impact affects their day-to-day defenses. When the private sector does not share, then they are either not patriots or too fixated on their shareholders. When the government does not share, it is okay, because it is classified, stuck in the interagency, someone else's job, or we had a Deputies Committee say it was permissible to not share it for intel gain/loss.

In cyber conflict, the offense already begins with a head start. To beat them, the defenders need to significantly increase the bad guys' work factor more than their own. While the government has started projects, most notably the DIB cyber pilot to share NSA's signatures of malicious software, these typically don't easily scale, requiring security clearances and secure facilities. They likely increase our work factor probably more than our adversaries.

Indeed, a recent study found that only 1% of NSA's signatures shared with the Defense Industrial Base were novel. How many hours were spent in interagency meetings for that one percent? Some in Congress and the military seem to want constitutionally troubling government monitoring of private sector companies, but does this make sense for marginal gains?

The fix is to shift the government's mindset: in cyber conflict, the private sector is usually the "supported command" not the "supporting command." They are the targets, the ones fighting in the trenches every day, and if we want to win they need more help. Think about past cyber crises: in how many did the solution depend primarily on government solutions? In most cases, the critical solutions instead came from McAfee, or Microsoft, not from any a department or agency. The exceptions tend to be attacks that predominantly only affected the government to begin with. Yet too many of the government's plans put the government at the center, and look to the private sector to give support.

This is the reverse of what is needed: it is the private sector that will fix the problem and the government should be supporting them.

To put it another way, we are finishing two major wars. When American soldiers have been in harm's way, intelligence agencies will take significant risks to declassify the right information to keep them safe. Though it is a different kind of fight, the US government should be willing to take similarly bold risks to support our embattled companies on the front lines against Chinese espionage.

As just one example of how to do this, we should simply declassify the signatures. After all, by releasing their attacks “in the wild” over the Internet, *the bad guys have themselves already made their malicious software public*. This will be far less expensive in the long run and more effective as it would bolster, not supplant, the security monitoring market.

This leads us to the last silence.

Fourth: **Silence to the Chinese about our increasing fury**.

A recent event at Georgetown University discussed the US experience dealing with China both for WMD non-proliferation and for cyber. The non-proliferation experts explained their long dialog with the Chinese on this sensitive topic, through which they learned some keys to success.

By drawing on a range of discussions, some successful and some not, these negotiators discovered the Chinese government was more willing to limit proliferation to some countries but not others. Sometimes they discovered a discrete word to the Chinese leadership would work, while other times public shaming was needed. They still haven't figured everything out, of course, but they can point to progress in influencing Chinese behavior.

When asked the same question, America's cyber experts answered with a sheepish look, admitting that we have not yet told the Chinese leadership, in any similar fashion, that we are upset with their activities against us. We have mentioned it to them, but rarely more.

How can this be? The first answer I receive is usually that we don't want to upset the Chinese. After all, they own bazillions of US Treasury bonds. But is it true the United States is willing to square off against China on tire imports and rare earths, but not on "the biggest transfer of wealth through theft and piracy in the history of mankind" in General Alexander's words?

We don't need to pick an international fight (or perhaps we do) but at least, let's start the official dialog. We must raise Chinese cyber espionage in every military-to-military dialogue, in ever JCCT meeting, in the Strategic and Economic Dialogue, and with visits from all of their state leaders. How can we say we are trying to stop their espionage by doing anything less? How can we even *consider* government monitoring of private networks before our own government has even told the

Chinese they need to back off? Better yet, we can choose from at least the United Kingdom, Australia, Germany, France and Canada to be a good cop to counter our bad cop routine.

Table 1:
The Spectrum of State Responsibility

1. **State-prohibited**. The national government will help stop the third-party attack
2. **State-prohibited-but-inadequate**. The national government is cooperative but unable to stop the third-party attack
3. **State-ignored**. The national government knows about the third-party attacks but is unwilling to take any official action
4. **State-encouraged.** Third parties control and conduct the attack, but the national government encourages them as a matter of policy
5. **State-shaped**. Third parties control and conduct the attack, but the state provides some support
6. **State-coordinated**. The national government coordinates third-party attackers such as by "suggesting" operational details
7. **State-ordered**. The national government directs third-party proxies to conduct the attack on its behalf
8. **State-rogue-conducted**. Out-of-control elements of cyber forces of the national government conduct the attack
9. **State-executed**. The national government conducts the attack using cyber forces under their direct control
10. **State-integrated**. The national government attacks using integrated third-party proxies and government cyber forces

Better yet, we don't have to prove without doubt that every single espionage case is coming from China or that the Chinese government itself is conducting them. The Atlantic Council just published a ten-point spectrum to help assign responsibility for cyber events (see table 1). This is just one tool that can help us address the forest of Chinese intrusions, rather than the trees of the forensics of each case. As a national security matter, we can simply decide to not care if these are sponsored by the Chinese government or not. If the government (and private sector) releases sufficient evidence showing the incidents are sourced from that country, the administration can just hold them responsible to make it stop. This approach of "national responsibility" is likely to be far more effective than forcing ourselves to jump over the needlessly high bar of proving technical attribution.

Conclusion

The Administration and Congress are taking cyber espionage seriously, more seriously than they have in years. Yet it is far from clear we are doing enough or heading in the right direction.

We must at least tackle these four cyber silences:

1. Silence about how we got here
2. Silence about the threat we face
3. Silence about practical information which could help the private sector
4. Silence to the Chinese about our increasing fury

These will not by themselves solve the problem, but at least we will all understand the scope of the problem and have us towards solutions that may break the cycle of suffering. To win, we must speak. To speak we have to declassify. To declassify we must be bold. And we must do this today.