CyberPro

April 2010

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: JAMES LEWIS

NSCI's Lindsay Trimble recently had the opportunity to interview James Lewis, senior fellow and program director at the Center for Strategic and International Studies. In this role, Lewis writes on technology, national security and the international economy. He has authored numerous CSIS publications with the theme of how government policies adjust to technological innovation. Most recently, Lewis was the project director for CSIS's Commission on Cybersecurity for the 44th President, whose report has been downloaded more than 40,000 times.

NSCI: During your time at CSIS, you have authored more than 40 publications on a range of cyber and defense topics. How are we doing in adopting or implementing recommendations in the CSIS Cybersecurity Commission's "Securing Cyberspace for the 44th Presidency" report?

LEWIS: Some parts are going better than others, but overall, almost everything that we wanted has started. The biggest changes were adding the cyber coordinator; merging the National Security Council and the Homeland Security Council, which other people also recommended; and making cybersecurity a central focus for U.S. policy. All of these are great.

Some of the other issues, such as rebuilding public-private partnerships, are getting a slower start. Overall, the big picture has been taken care of, but some of the details have been slow in getting started.

NSCI: What positive steps have you seen the current administration take to secure cyberspace?

LEWIS: They're just starting an effort on securing online transactions, which was one of our recommendations and was also a recommendation in the 60-day cyber review. They're figuring out a way for people to identify themselves better online. They're also taking a look at different public-private partnership models, whether that's bringing the NSTAC back to the White House or creating this new group called the Enduring Security Framework. They put a lot of effort, particularly in the DoD, into thinking about a national strategy and a national response. Howard Schmidt is starting to pull things together, in terms of coordinating. The State Department is coming up with an international strategy. There are a lot of things you can point to that show that things are better than they were five years ago.

NSCI: There has been much discussion since the beginning of the Obama administration over U.S. cyber leadership. Shortly after naming Howard Schmidt as the first Cybersecurity Coordinator, he appeared to dismiss much of the cyberwar threat[1]. How do you think this will impact the urgency of this administration in improving our cybersecurity?

[1] http://www.govinfosecurity.com/articles.php?art_id=2267&rf=030810eg

LEWIS: I don't think there's a cyber war either. We're not in a cyber war and I'm actually kind of bored with people saying it's a cyber war. There are two ways to look at it. First, do foreign militaries have the capability to strike the U.S. using cyber weapons? Absolutely! So is it a risk we should think about? Yes, indeed. But does that mean it's going to happen tomorrow? No way! They also have missiles on airplanes, but we're not going to watch them just for fun. I don't think we're in a cyber war.

What we do have a big problem with is on the espionage side and the constant headlines about Google, other companies and the Dalai Lama – you name it. Espionage is the name of the game here. So are we in a cyber war? No. Do we have a big national security problem? Yes.

NSCI: Lt. Gen. Keith Alexander had his Senate confirmation hearing last week to become Commander of U.S. Cyber Command. How do you think a U.S. Cyber Command led by the Intelligence Community will impact cyber security for .mil, and perhaps .gov and .com, during times of crisis?

LEWIS: For .mil, it's pretty straightforward. I think Cyber Command will bring greater coordination to train all the elements in DoD that are all involved in this – the Services, DISA, NSA. They're all going to be co-located in many cases; they're going to have a common management structure. For .mil, we'll see significant improvement.

For .gov, we don't know what it's going to mean because we haven't figured out how to connect Cyber Command to the rest of .gov. It will probably be something working in partnership with DHS, but the details aren't clear at the moment. If you look at the thrashing around about Einstein 3, it's a good example of how we know the things we could be doing better, but we haven't figured out the organization or the policies we need to do them.

Cyber Command really doesn't have a role in .com. Nobody has a role in .com; we still have kind of a faith-based policy when it comes to securing .com – we pray every night that something bad won't happen.

NSCI: There seems to be a growing stack of cyberspace studies. How do we move from studying the problem to actually doing something about it, such as tackling the issues of authorities, standards, processes and procedures?

LEWIS: That turns out to be really hard. I know that, just in talking with different groups, we all agree it's a problem but we have to decide what we want to do about it. People don't usually think that way, but we have a few folks in the government that are working on it: Howard Schmidt and his deputy, Chris Painter; General James Cartwright at the Joint Chiefs of Staff; DoD Deputy Secretary William Lynn; Randy Beers and Phil Reitinger at DHS; General Keith Alexander. They are all thinking about how to operationalize a response. You've got a very select group of people trying to figure this out. It's a good team that has literally just started working on this and they'll face a lot of obstacles because people are wedded to the old way of doing things and authorities are kind of out of date. We need to rethink a lot

of our policies to get real action. I think we'll see it in the next couple of years, but it's just been a hard start.

NSCI: Should a more definitive cyber policy precede the passing of significant cyber legislation?

LEWIS: I think we need a real national strategy. We have a couple national strategies, but they're largely ornamental; they say things like "cybersecurity is good." That's a great first step, but it's time to actually say what we want to do about this. I think a new national strategy is an essential part of this.

NSCI: What major cybersecurity legislation do you think is needed?

LEWIS: I think that the Rockefeller-Snowe Bill has a lot of potential. Some others are the Kerry Bill and the Gillebrand-Hatch Bill, both on international strategy; the Lieberman-Collins Bill (if it ever sees the light of day, it has some really good stuff in it); Carper and the FISMA Rewrite and the NERC/FERC Authorities Bill that's coming out of the House Homeland Security Committee. All of these paint a really good picture for things we might want to do. They each address separate issues and pulling them into some kind of comprehensive package would be helpful. The Rockefeller-Snowe Bill is especially critical because it talks about standards, workforce and authorities and really fills a crucial need.

NSCI: How do we ensure flexibility in our legislation to accommodate the ever-changing cyber security landscape?

LEWIS: I think a lot depends on how you write it. If you want to write very specific, technical and prescriptive legislation, it will fail. I saw this during the Clinton administration with the 1990s digital signatures legislation, which were designed for specific technology. It's just not a technology that people use anymore.

People want to set goals, standards, processes for coming up with standards and processes for coming up with compliance. But then they want to let the private sector come up with how to actually populate these things, while working with the government. So we need to stay away from prescription in our goals.

NSCI: How do you recommend we balance effective security with privacy concerns, such as getting beyond the general discomfort with discussing Internet regulation? How are we doing with getting beyond secrecy issues and improving public-private information sharing and collaboration?

LEWIS: You will need to do two things. First, we need to reassure the public. The NSA's Warrantless Surveillance Program actually damaged some of these opportunities for cybersecurity because we had government agencies spying on American citizens without the approval of the court. The program itself was probably essential. I'm not opposed to the program; I'm opposed to the way they did it. Part of the reason I'm opposed is because it scared a lot of people. We need to think of some way to reassure folks that we can do this stuff without violating their civil liberties.

The second thing we need to do is think about what the protections are that private companies need in order to share information –the liability protections, consumer protections, etc. Our laws were designed for companies acting on their own, without coordinating with anyone else. They were created for a pre-network era. A company may have good data on a breach, but they can't share it because it violates laws. How do we change the laws so they can share this information without hurting themselves and without hurting their customers?

NSCI: How do you think the United States should proceed in the area of international collaboration and/or possible treaties related to cybersecurity?

LEWIS: We're very far from a treaty, but we should start thinking about what we want other countries to do when it comes to cybersecurity and what responsible behavior would look like for another country. Starting those discussions and engaging other countries in how we want cyberspace to look is crucial. People have very different views about how these things should work. The Internet and cyberspace are going to look very different 5 to 10 years from now. I think we need to get out there and engage people, talking about the things we can improve right now, the important values for cybersecurity and what it will eventually look like. This wasn't done in the last administration; they believed that talking to foreigners was bad. That's the main thing we need to change.

We need to think carefully about a treaty. A treaty that bans technology doesn't make any sense and a treaty that's unenforceable doesn't make any sense, but there are still things we can do.

NSCI: Is there anything else you'd like to add?

LEWIS: There's this larger issue of the way the Internet is designed: Can the way it's designed now ever be secure? That's another hard one. People built the Internet 40 years ago, but they didn't think about security. So one of the big questions is do we need to go back and revisit some of those fundamental design issues and fundamental technologies? Only the federal government can do that because only the federal government could create the Internet in the first place. As a nation, we will need to decide if we have the will to invest the money it might take to make this infrastructure more secure. I don't know if we still have the ability to pull these things off and that worries me. We could do things in the '60s, '70s and '80s that we couldn't do now. Back then we could do big projects, but now there's this reluctance and it could mean a more dangerous world for the United States.