Cybersecurity and Cross-Sector Coordination

A Conversation with Keith Alexander

FLETCHER FORUM: *General, you have extensive government experience; how has this informed your transition to the private sector, and specifically your approach to securing systems at IronNet?*

KEITH ALEXANDER: Think about how the military teaches you to look at assessing a problem. If you were to think about taking over a piece of terrain, and you had no military training, you would think one way. But if you had military training, you would think about all these different things you would need to put together at many levels. What you learn in the military and in our government is that, in defending a network, you need to take a much broader view and you need to account for more things; so I think from that learning you get a more comprehensive solution. Knowing the depths of the threat helps you understand how bad it could be. For example, in November I had a [Ukrainian] group saying, "We haven't heard about any attacks on our power grid!"—but, you see, Ukraine got hit. Threats like that are coming, and will get worse: I think that's part of what you learn in government.

Keith Alexander *is the founder and CEO of IronNet Cybersecurity. General Alexander was previously the highest-ranked military official of U.S. Cyber Command, the National Security Agency and the Central Security Service. At U.S. Cyber Command, he was charged with defending the nation's security in cyberspace against sophisticated cyber threats to businesses and government operations in an increasingly interconnected world. General Alexander holds a B.S. from the U.S. Military Academy, an M.S. in Business Administration from Boston University, and M.S. degrees in Systems Technology, Physics, and National Security Strategy.*

FLETCHER FORUM: *You've mentioned the need for a new strategy as threats become more severe and credible. What does this strategy look like, and how do you see it evolving?*

ALEXANDER: The tech community has got to come up with more comprehensive solutions—an approach to security as not just singular pieces of equipment that go into networks, but pieces that actually work together in a collaborative way. Otherwise, the approach can sound like, "I'm going to prioritize this, this, and this, and then your IT people have to put all those pieces together." That approach is analogous to buying a car by having someone give you all the pieces and saying, "You put these together; hope you can drive." We don't buy cars like that, so why do we buy cybersecurity like that?

The tech community has got to come up with more comprehensive solutions—an approach to security as not just singular pieces of equipment that go into networks, but pieces that actually work together in a collaborative way.

What we need is a comprehensive solution, and companies in the cybersecurity business need to work together to help develop just such a solution. That's what we at IronNet are trying to do.

FLETCHER FORUM: *Given the need for that solution, where do you see an opening for coordination between private companies and the U.S. government?*

ALEXANDER: When companies get attacked, how do they inform the government? Today, they don't. With the introduction of the Cybersecurity Information Sharing Act, we've now got to come up with technical means for sectors to share information with the government about attacks that doesn't include personally identifiable information, but does include information about the attack itself. For example, if I'm being attacked by someone at a given site in Foreign Country A, that technical means should allow me to pass that information to the government, and then let the government take it from there. That's the kind of coordination we need for cybersecurity, just like you would have in knocking down a missile for traditional security. When you think about it, the only real difference between a missile and cyber is that cyber moves a lot faster: it takes 133-134 milliseconds to do a lap around the earth. That's your new decision space.

FLETCHER FORUM: *Given that speed, how should we address incidents such as the the recent Office of Personnel Management (OPM) hack, which was unprecedented in the U.S. system? Should we be prepared to see more of these?*

ALEXANDER: We should be concerned about those incidents and create the solution to stop them—that's the comprehensive solution. Not creating that solution would be like saying, "We're all going to sink, so what we've got to do is learn how to die gracefully." I'd say that doesn't make sense. Rather than accepting that everyone is going to lose all their intellectual property, get hammered, and get sued—which is not right—can't we come up with a solution? We can and should. Let's find the solution and help drive that, with government and industry working together to come up with a solution from our nation and coordinate that with other countries around the world.

FLETCHER FORUM: *What role do cyber weapons play in that solution?*

ALEXANDER: With cyber weapons, first and foremost, before you throw anything at anybody, you have to think about your position. I liken the United States' position to a huge glass tower: we're not ready to deploy anything into cyberspace; if we do that, we will have all this broken glass. Let's first fix our defense issues and talk about our strategy for defense coordination with other countries; let's discuss the rules of the road, the rules of engagement, and what we'll do.

This doesn't mean we shouldn't be prepared to respond; it just means that we ought to put more effort into fixing this defense first before we respond with any types of weapons. Throwing weapons is easy: you can come up with arrows, you can come up with rocks, you can come up with machine guns, you can come up with all these weapons in cyberspace. What we have to do is assess our glass building and understand which weapons will hurt us worse than others. If we solve that problem, then we will have the ability and capacity to withstand just such an attack and counter with whatever means, cyber or otherwise, the President or Secretary [of Defense] dictates.

FLETCHER FORUM: *As far as rising threats go, we're seeing an unprecedented level of digital recruiting from groups such as ISIL, and may continue to see that trend regardless of ISIL's existence. With the internet as a largely unpoliced area, how should the United States respond to the rise of extremism online?*

ALEXANDER: I think we should take away extremists' Internet access to the maximum extent possible. There is a big debate around this in the intelligence and law enforcement community: do we watch extremist recruiters to try to get intel or do we stop them from doing it? My assessment of the situation is they are getting more recruits than we are getting intel. Stop them from getting recruits. They are recruiting and radicalizing people online: this is crazy. Take that capacity away from them.

Do we watch extremist recruiters to try to get intel or do we stop them from doing it? My assessment of the situation is they are getting more recruits than we are getting intel. Stop them from getting recruits.

People say this is too hard to do, but we haven't actually tried. And if all the countries of the world united then we could do it, and we should. We don't allow other crimes on the network, so why do we allow terrorism? Extremists want their own website? Good. They can have a rock. Paint it on there.

FLETCHER FORUM: *How might the government coordinate with private corporations to remove that capacity?*

ALEXANDER: You send those people with that capacity a notice to delete their recruiting materials. Actually, some public companies already do that. Take Twitter, for example: if they see extremist recruiting, they take it down. That's a way of self-policing that we all need to do on a very serious scale. If we all work together, we could do it. There are more of us than there are terrorists.

FLETCHER FORUM: *The concept of self-policing is connected to the balance between security and privacy that you've discussed before. The Obama administration has made an effort to reform that legislation that you talked about. Do you think that the Freedom Act and other measures that have been taken since the review group have gone far enough?*

ALEXANDER: You have to strike a balance, and the balance really comes down to asking, "How do I maintain sufficient levels of privacy and security to ensure that we don't have people dying needlessly?" I actually wrote an op-ed to push the Freedom Act because I think those changes are

acceptable. In fact, we pushed for them a few years before. I don't have a problem with it, and that's what I told [American Civil Liberties Union board member] Geoffrey Stone.

Is there more? I don't know. What I'm concerned about is that when we talk about this, we frame it as a choice between security *or* privacy. That's the Apple debate, and I'm not there. I think we haven't yet exhausted the opportunity to find a better middle ground. Arguing about security versus privacy turns the debate into a zero-sum choice, like two kids saying "Tommy stole my football." We inflame that choice in the media. The real question becomes how we can get the media to responsibly portray the debate to the nation, getting us where we need to be, versus acting in their own self-interests to sell stories and get more airtime. That's the big issue.

Arguing about security versus privacy turns the debate into a zero-sum choice.

FLETCHER FORUM: *Where do you see that middle ground in the Apple debate?*

ALEXANDER: I think that middle ground involves telling the tech companies and the government, "Go sit down and see if you can come up with a better solution." I don't want to hear "I'm all A" or "I'm all B." Now I don't know that the courts can enforce that, but the companies and the government can do it, and that's the kind of action our nation would expect.

Here's what I'm concerned about: what happens if you have a sequence of big attacks, and the attackers are using encryption methods that the government can't access or respond to? The 2012 attack attempt on the New York City subway system involved an email that wasn't encrypted well enough to prevent the government from getting it. What would have happened if that email had been better-encrypted and we couldn't have seen that attack coming? We would have killed hundreds of people. Would that have been worth it? Some would argue that a few hundred people dying was okay, but how about a thousand? How about ten thousand? Tell me when you get to that point, because threats are going to get there. If you can't stop these attacks, they are going to grow. That's what worries me.

People say, "Well, you're exaggerating terrorism." I've worked on terrorism issues since the 1998 East Africa Embassy bombings. At that time, I was the new intelligence officer at Central Command and I saw

firsthand what Osama bin Laden and his folks were up to. They mean to kill us, and our people, and our way of life. The issue is how do you protect both security and privacy? It's not one or the other.

I think that's where you all can help, and that's where we've got to have—in these kinds of academic forum—people seeking the truth so they know the facts and can get our nation to a better answer. We're not doing that, and the presidential debates highlight how childish we really can be. ***f***