SESSION 5: CYBERSECURITY

Admiral Dennis C. Blair, Chair

We switch now to the topic of cybersecurity, about which, in general, those who do the talking don't know the technology, and those who know the technology don't do much of the talking, and we're going to try to change that dynamic with our panel this afternoon.

When I was director of national intelligence, I delivered two annual threat assessments. The first in January of 2009 identified the global economic recession as the greatest threat to American and world security interests. As the global economy recovered in the following months, some said I had overplayed the threat or that I had been mistaken in my analysis. "On the contrary," I replied. "My warning caused the action that averted the disaster, and so it worked."

So, emboldened by that success in 2009, when I gave my annual threat assessment in January of 2010, I identified the vulnerabilities of the global information network as my top security concern. I'm still waiting for the same effect that I had with the global recession, because, unfortunately, the cybersecurity threat is still with us. If anything, the situation has become worse.

We read about it all the time, penetrations of Google, WikiLeaks, RSA, the people who provide network security, NASDAQ, the Australian prime minister's personal email account. Every week brings us a new disclosure of cyber attacks on very experienced, very savvy, cyber-capable organizations.

I think that both government and private leaders have a very difficult time coming to grips with this subject, and one of the reasons is a lack of a common understanding or even a common vocabulary in the necessary discussions between the executives responsible for resources and operations on the one hand and the technical chief information officers responsible for the technical side of it.

Executives know that the benefits of modern networks are enormous. What they don't know is the risks that accompany these very tangible benefits—a malcontent employee, a competitor gathering information or damaging a proprietary network, the ability of a criminal syndicate or an outraged cyber freedom group to shut down a company's online orders.

Now, in other areas of business, risk-versus-reward decisions are made all the time, but they're better understood. Business leaders have both an instinctive feel for the risks and benefits involved, and they have tremendous fine-grained analysis supporting their decisions. But this level of understanding and communication does not underlie the investments that are made in protecting cyber networks in most major organizations. The decisions are treated more as, say, overhead expenses in which perhaps you benchmark a competitor's expenditure and make yours.

Just taking a government example, Wikileaks, and without prejudging the guilt or evidence of Sergeant Manning, let's assume that it was a sergeant on a classified computer terminal in Iraq who downloaded 1.5 gigabytes of data onto a Lady Gaga CD and sent it to Wikileaks. How did that happen? How did that happen?

It happened because the commanders and the network operators in Iraq had decided to spend their network resources on more network capability to share, to be able to pass information around using simple password-security-protected procedures rather than to allocate a greater portion of those network resources to a stronger network security system that would have identified unusual downloads.

Those military commanders were driven by the imperatives of information sharing, and they did not have nor were they presented, based on my experience, a well-developed understanding and presentation of the risk they were running, the mitigation alternatives that were available to them with the attached costs.

Yet these same reward and risk calculations are made by the organizations of every single one of you in this room, whether you're in business, in government, or in university academic departments, and I doubt, really, that any of you feels completely confident of the decisions that you have made or that have been made in your organizations. They've been made based on gut instincts, the trust that you had in your chief information officer, the cost of the security alternatives that were presented to you, whether or not you have been burned in the past.

Our panel this afternoon has thought about these issues. They've experienced both success and failure in the technological and the resource decisions involved, and they are going to tell us about their experiences.

President Ilves of Estonia, a former Trilateral member returning home, I should say, was a witness to a massive cyber attack on his country a couple of years ago, and, as we were talking ahead of time, things have progressed tremendously since that time.

David DeWalt, chief executive officer of McAfee, earns his living by helping both individuals and organizations protect their information they keep and exchange on their networks.

Ian Dudgeon has extensive government and private experience in Australia in cyber security and, in fact, was the author of Australia's first information operations policy.

Finally, General Keith Alexander commands the largest single collection of cyber talent in the world, and he is responsible both for the offensive and defensive cyber operations conducted by the American Department of Defense and the intelligence community. We'll begin with President Ilves talking about his observations.

Admiral Dennis C. Blair is former U.S. director of national intelligence.