THE TRILATERAL COMMISSION PLENARY MEETING
WASHINGTON, APRIL 8-10, 2011

SESSION 5: CYBERSECURITY

David DeWalt

What I'll try to do here in just a couple of minutes, if I can, is give you, at least from a private sector point of view, a bit of the state of the union in cyberspace.

At McAfee, I'm fortunate to get a chance to see an operation in 110 countries around the world. We have more than 300 million users of our products, both on the consumer, as well in corporate, as well as governments around the world, so we have a pretty interesting, at least, private sector view on what's going on.

So I'll probably start out by giving a little bit of bad news, but I'll also try to end it a bit on what we can do about it and perhaps some good news, as well. There is a lot that's happening and a lot of positive progress as well, much like the positive white hat example President Ilves used there.

But first the bad news. What I would tell you is we're almost in a perfect storm. I've written about this and talked at the World Economic Forum about this as well, and I see four major forces that are coming together to almost create a scenario that is very, very dangerous, to say the least. I'll give you a couple examples.

The first is what I just call the rise of malware, and for those of you not in the technical world, malware is a bit of an amalgamated word to mean malicious software, but it's viruses, it's trojans. It's all types of denial-of-service type attacks that you start to see, and it's just amazing to watch how much malware we're starting to see in the world. It is literally an epidemic.

I've now run McAfee for just over four years, and in my four years of being at McAfee I've seen more than an exponential increase in the amount of malware that we get into our labs on a daily and yearly basis. When I first started in late 2006-2007, we averaged about three million bad pieces of malware every year, and this past year we got more than 48 million bad pieces of malware.

Just to give you an example of how much that's grown: every day right now we're getting somewhere in the neighborhood of 55,000 net new pieces of malware every day, so that means 55,000 content pieces, files, and attacks that are being submitted to my labs every single day.

To give you a couple other examples, we're seeing about two million bad websites, malicious websites being created every single month. So to see two million websites being created every single month, 48 million bad pieces of content being created a year, literally 200,000 what we call zombies, which is, as the president referred, like robotic networks on your machines or what we call bot nets that are being deployed where it can take over your computer, we're seeing 200,000 of those every day.

So this has become an epidemic just in terms of the amount of bad things we're seeing around the world, and, of course, what's happening to compound that is what we call the speed of infection. So now a bad piece of content can spread around the world in milliseconds, so now a piece of content that we may receive on our email, on our Blackberry or our iPhone can be spread around and infect millions and millions of computers within minutes. This is a very, very dangerous scenario, just watching what's happening.

Compounding that is what I call the amount of devices that we're seeing. We're just seeing an explosion of net new devices entering the internet, and for those of you who are reasonably technical, we've moved from what we call IPV4 to IPV6, which is a network protocol backbone for the internet, globally around the world, and this now offers us trillions of devices that can connect to the internet.

So you start to look at the amount of malware, the amount of websites that are bad, the amount of devices that are being connected to the network, you start to see an interesting picture, and these aren't your normal computing devices like your desktops and your laptops and your servers that corporations and consumers use. This is all your mobile phones. These are now ATM machines that run your banking industries. These are your car, your automobiles. Nearly every automobile that's being generated in the world today has an on-board computer, and those computers are connected to the internet while those cars are operating. Your television now is completely internet-enabled. At home, if you're watching television, you can watch and browse the internet directly through websites. Televisions can be infected.

Nearly everything that's electronic is being connected to the internet, so we're seeing this almost perfect environment for criminals and for bad actors to perpetrate crime and other types of terrorism and warfare on the internet.

On top of that, we've seen what I call just a lack of governance of the internet around the world, which is a real problem, and we have to fix that. I'll give you a couple examples.

When you look at these two million websites that are created every day, these are domains or brand new websites that get created. Well, there's absolutely no governing model as to who can create a website, so bad actors can go and register domains, sometimes in thousands if not tens of thousands of them at a time, and perpetrate attacks on a network, what's called phishing attacks against the network.

They can do so by paying $5 for a website and just doing it 10,000 times and changing those domains very quickly and perpetrating attacks like the denial-of-service attack that the president had seen.

So you've got a lack of governing model coupled with devices and malware, and now you get this complexity issue that's hitting all our infrastructure, so the stakes are getting a little higher.

We're starting to see a lot of accidents occurring, and we just produced this report that about 90 percent of all data loss that occurs in the world is actually an accident. We find employees and consumers who will leave their mobile device in the taxicab or the airplane, and it's got critical information on it, or they'll leave behind a CD, or even little thumb drives or little USB sticks now contain a tremendous amount of storage on them, or the example of the Wikileaks, where you could find just a malicious insider, in addition to just accidents, bringing out a lot of data from the networks.

So you've got a very interesting set of problems occurring with the complexity of the technology. This creates an atmosphere where now almost all our critical infrastructure is online. Our airplanes, our auto industries, our nuclear industries, our energy industries are all connected online, and, of course, they can all be accessed online by both the good and the bad.

This has kept me up at night as I've watched this change happening around the world, and we've seen some examples. President Ilves mentioned just a couple of those, you know, the Stuxnets of the world. Just a little bit more than a year ago, McAfee was engaged in what I had seen as probably the most hellacious attack that we had ever seen before. We had called it Aurora. Some of you might have seen it as the Google attack that occurred, and here was a very sophisticated, high-tech company that was penetrated by what's called an advanced persistent threat or an APT, which is a new style of attack that's occurring. This type of attack was targeting intellectual property, and it used a very unsophisticated model to penetrate Google, what's called spear-fishing.

In spear-fishing, for example, I could send somebody in this room an email, and it has an attachment or a website that you could click on, and the website is a bad website or the attachment is a bad attachment, and it can actually load a key logger or some type of malware onto your device and steal your credentials. Then the attacker can log back into the network as if they were a developer or a QA personnel or somebody who could access high intellectual property in the network and basically steal the source code or steal important information. A year ago, we saw more than 100 companies in the high-tech sector get penetrated by this type of attack.

So we're moving way beyond sort of the hacker in the basement now. We're moving into an era where devices are accessible. The cost of offense is very low versus the cost of defense, and as a supplier for security, we're watching the ability to buy vulnerabilities online on services like eBay. You can literally buy for about $25 a vulnerability kit to essentially exploit a network, so we've seen a tremendous set of capitalism enter into the world of crime and the world of terrorism that's pretty scary.

We're watching scenarios right now where you basically can just buy something online, and a pretty unsophisticated group can penetrate into a network, steal source codes, steal money, and we're finding the need for an uplifting of our security postures in the world.

Here's the good news. I think the good news is that we have a lot of positive progress that's been occurring here, particularly in response to a lot of what's been going on.

I'm here on the panel because we've developed some partnerships as a private company with not just the U.S. government but also governments around the world. Public-private partnership is just essential to solving some of these problems, but also, as the president of Estonia mentioned, we also have private-to-private partnerships that are needed.

As a large supplier of security, we speak regularly with other companies in the industry including Symantec, Trend Micro, Kaspersky, and others to exchange malware and solutions to the problems that are happening around the world.

So we've actually elevated cooperation, not only amongst competitors but across governments, but we've got to take it to another level, and I think it's especially important that we continue that progress in an effort to create teaming, not just from governments to governments but corporations to governments and corporations to corporations to come together.

For example, we've developed a technology, much like some of our competitors have, where we have a cloud architecture that's collecting information all the time around the world. In our case, it's called Global Threat Intelligence. We launched it about two years ago, and this Global Threat Intelligence collects encrypted hashes or intelligence about bad pieces of content or bad websites or bad applications that can download onto your networks. Well, when we first launched it, we got about a million queries a day to this back-end architecture.

Today, we're averaging in excess of six billion queries every day, and that's making our system smarter and smarter. So now we can see a bad actor that's doing something in the Asian marketplace and fix it in milliseconds as it hits the North American marketplace.

So the speed of technology, the smarts of the intelligence, and the ability to cooperate and educate is coming together in ways that a year ago or two years ago I never could have imagined as a supplier of security products like we are today.

My last comment I would make is education is probably—you know, one of the reasons I'm sitting here, we find ourselves constantly as a supplier needing to educate. There are so many generations and so many leaders that just don't understand the threat landscape, the issues that are really happening. In some cases, they just myopically go along with, "Okay, I should just spend an X amount of my resources on security. That shouldn't change." Admiral Blair mentioned that in his opening comment.

Corporations sometimes don't adequately defend themselves in a way that they can, so training and education becomes critical again for us to solve this problem as a community and cooperate effectively to solve this.

David DeWalt was chief executive officer of McAfee, Inc., Santa Clara, CA from 2007 to 2011.