Notes from the Cyber Trenches
A Security Intelligence Blog

Posted by Rick Howard, Director of iDefense Operations, VeriSign
June 17, 2010

Intelligence Squared, Cyber Warfare and Entertainment Extravaganzas

Mike McConnell   Johnathan Zittrain   Mark Rotenberg   Bruce Schneier

I attended the Intelligence Squared debate on Cyber Warfare on June 8, in Washington, DC.

Those of you who read my blogs regularly know that I am an avid podcast listener (I have a one-hour commute each way to work). One of the podcasts in my regular rotation is the Intelligence Squared debates. The organizers use an Oxford-style format where two sides debate an issue and the audience decides the winner. Before the debate, the organizers ask the audience to vote on the motion. After the debate, the organizers ask the audience to vote again. The winner is the team that changed the most votes. Intelligence Squared has debated many interesting issues during the last year: "Organic Food is Marketing Hype," "America cannot and will not succeed in Afghanistan," and "Blame Washington more than Wall Street for the Financial Crisis," just to name three.

The debate itself was a hoot. It was a beautiful night in the capital and the debate was well attended even though it was competing with several high-end entertainment extravaganzas at the same time including the Washington National's debut of their phenom pitcher Stephen Strasberg and a family concert by Carly Simon and her son Ben Taylor.

This was the motion: The Cyber War Threat has been grossly exaggerated.

On the left side of the stage (for the motion) was Marc Rotenberg, executive director of the Electronic Privacy Information Center (EPIC) and Bruce Schneier, my former boss and general pundit for the security community.

On the right side of the stage (against the motion) was Jonathan Zittrain, co-founder of the Berkman Center for Internet & Society and Mike McConnell, executive vice president for Booz Allen Hamilton and a former US Director of National Intelligence (DNI).

Let me just say that the Zittrain/McConnell team spanked the Rotenberg/Schneier team and the star of the show was Zittrain. He was funny and articulate and every time the Rotternberg/Schneier team tried to make a point, Zittrain bumped them right back into their corner. Here are the results:

Before the Debate:

For the Motion (Rotternberg/Schneier): 24 percent
Against the Motion (Zittrain/McConnell): 54 percent
Undecided: 22 percent

After the Debate:

For the Motion (Rotternberg/Schneier): 23 percent
Against the Motion (Zittrain/McConnell): 71 percent
Undecided: 6 percent

Like I said, this was a spanking. Throughout the debate, the Rotternberg/Schneier team never debated the issue. They were more concerned about what the US Intelligence apparatus might do to US citizens' privacy rights if the US government ever considered the threat of Cyber War to be real. Rottenberg repeatedly came back to the point that the NSA has been trying to take control of the Internet since the early 1970s and this is just the latest salvo in that effort. The Zittrain/McConnell team challenged this argument by agreeing that it was a concern, but it does not really address the question at hand.

Schneier pointed out that Cyber War is a theatrical metaphor similar to other metaphors we use to add emphasis to important issues; like the war on drugs or the war on terrorism. The Zittrain/McConnell team countered with the idea that this is not a metaphor; that it is possible to disrupt and destroy in cyber space just like it is in the real world and that we should prepare to defend against those contingencies. McConnell explained that the US economy is annually valued at $14 trillion. In just one day, two high-end US banks

transfer more than $8 trillion alone. If a nation state made it impossible for bankers to track that dollar flow, the result would ruin the country. From my point of view, we can all come up with our pet "Doomsday" scenarios that a nation state might use against our respective countries. If we went to war with another country, do we really think that the other side would not use cyber space as a vector? The Rotternberg/Schneier team said yes; they did not think that another nation state would use Cyber War as a vector.

The Rotternberg/Schneier team also denied the two examples that everybody trots out, including me, to prove the point that cyber war is real: Estonia and Georgia. They said they were done by kids and therefore not an act of war and they failed to see how denying access to government websites qualifies as a war. The Zittrain/McConnell team countered with the fact that, at least in the Georgia incident, the attacks were deliberate, rehearsed and executed with impeccable timing. For my part, I would make the argument that anything that adds to your adversary's "Fog of War" only helps your cause. If you can't communicate with your staff electronically just before the tanks roll across your border, I'd say your pucker factor would rise exponentially. Moreover, just as an aside, kids conduct many of the conflicts going on today; it does not make them any less lethal.

In the end, both sides agreed that the policies the US adopts around cyber warfare should be open to everyone; that there should be no secret planks hidden in the bowels of the Pentagon. McConnell suggested that we need to get the law right before there is a crisis. Everybody agreed.

From my perspective, this is a no-brainer. Of course there will be a cyber warfare component in any future war. It is the great leveler. For relatively little cost, a small country could easily compete with a big country in terms of affect in cyber space. Compare that to trying to outspend the US in building an aircraft carrier fleet that can travel unopposed in five oceans. Does the press over hype the phrase "cyber warfare" sometimes? Absolutely. Does that make the threat of cyber warfare grossly exaggerated? I don't think so. I am not the only one who thinks that either. The debate audience definitely thought that at the end of the festivities, but so do a lot of governments around the world. In iDefense's 2010 Trends Paper, published in December 2009, we talked about a shift in the center of gravity away from enterprise IT departments and toward governments in terms of cyber security policy, money spent on cyber security programs and the cyber security personnel that governments hire. Part of that shift concerns itself with cyber warfare.

In the end, I had a great time. I got to see some cyber security super stars square off on a very important issue and witnessed the crowd shift their viewpoint from one side to the other. I'll admit, it was a little geeky, but hey, the geeks of the world need entertainment extravaganzas too.