



## Defining and Debating Cyber Warfare

By Mike Lennon on Apr 16, 2010

Cyber warfare is a hot topic in the security industry, but what does this term actually mean? At what point does a cyber conflict become a cyber war? Are cyber threats, cyber attacks and cyber espionage acts of cyber war? Many of these questions need to be discussed – and that discussion is about to take place.

Intelligence Squared U.S. announced this week that it will conduct a live debate from Washington D.C. on the motion, *The Cyber War Threat Has Been Grossly Exaggerated*.

This is sure to be an interesting debate, mainly due to the fact that “cyber warfare” is a term that isn’t clearly defined and agreed upon. Security and policy experts and high ranking government officials have mixed thoughts and opinions on its status, and for that matter, its very existence.



Mike McConnell, a Booz Allen Hamilton executive who served as Director of the NSA 1992-96 and Director of National Intelligence 2007-2009, claimed in a Washington Post article that cyber war is real and the stakes are high. “The United States is fighting a cyber war today, and we are losing. It’s that simple. As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking.”

Booz Allen Hamilton was recently awarded a \$14.4 million contract to help build a new command center for the U.S. Cyber Command, the arm of the U.S. Strategic Command responsible for coordinating computer network defense and directing cyber attack operations.

White House Cybersecurity Coordinator Howard Schmidt took a contrary position in his speech at the 2010 RSA Conference, insisting that the U.S. was not presently involved in a cyber war.

Robert Rosenkranz, the founder of debate host Intelligence Squared U.S., said, “It’s the great strategic irony of the last twenty years. Our commitment to and mastery of digital technologies has in certain respects played into the hands of our enemies. Our cyber

sophistication has made us vulnerable to those who look to exploit the Internet to plan for and attack America. Might we need to sacrifice openness to protect America? This and other critical questions will be considered during our debate in Washington."

"It is heartening to see that the challenges and threats in the cyber security arena are now in everyday discussion and that a public debate can garner such wide interest," said Jeff Ganek, CEO of Neustar, which has provided underwriting support for the event.



Debating for the motion will be Marc Rotenberg, Executive Director of the Electronic Privacy Information Center (EPIC) and Adjunct Professor of Information Privacy Law at Georgetown University Law Center. Bruce Schneier, well known security technologist, author, and Chief Security Technology Officer of BT will join Rotenberg on the "for" team.

Debating against the motion will be Mike McConnell and Jonathan Zittrain, Professor of Law at Harvard Law School and co-founder of the Berkman Center for Internet & Society.

Earlier this year, The Bipartisan Policy Center created, "Cyber ShockWave," a simulated cyber attack on the United States, providing a look at how the government would develop a real-time response to a large-scale cyber attack. The results of the simulation showed that the United States is not well prepared. The simulation moved through a series of technology breakdowns, from mobile phone networks to internet traffic and communication between financial institutions. More details about Cyber Shockwave are available [here](#).

The Cyber war debate takes place on **Tuesday, June 8, 2010**. We should all hope that, at minimum, a clearer definition of cyber war emerges. It's hard to debate a term appropriately before it has been defined but this should be an interesting discussion nonetheless.

Full details can be found at the Intelligence Squared US Website:

<http://intelligencesquaredus.org/index.php/debates/cyber-war-threat-has-been-grossly-exaggerated/>