

## US Law Enforcement Holds Meeting on Cyber Security

---

06 August 2010

Adam Phillips | New York

---

As the world becomes increasingly dependent on the Internet and computer technology to conduct its business, its social and international relationships and its wars, the threat to those networks from terrorists and criminals becomes more dire. A three day FBI-sponsored conference on cyber-security was attended by leaders in law enforcement, industry, government, and the military and reports on some of the issues involved and strategies proposed.

In the 20 seconds it will take to listen to this paragraph, the world will conduct 680,000 Google searches and send 88 million emails. The world's half billion Facebook users will post 140,000 status updates, and the "Automated Clearing House" computer network that connects all American financial institutions will process 12,000 electronic payments.

Indeed, the near-boundless scope of Internet use underscores the global threat of cyber crime and terrorism, said FBI Director Robert Mueller during his speech at the 2010 International Conference on Cyber Security at New York's Fordham University. "We live in a wired world. And our networks help us to stay in touch with family and with friends, collaborate with colleagues worldwide and shop for everything from books to houses. And they help us manage our finances, and make businesses and government more efficient," he said.

But he adds our reliance on these networks also makes us vulnerable. "Criminals use the Internet to commit fraud and theft on a grand scale and to prey upon our children. Spies and terrorists can exploit our networks by attacking our critical infrastructure and threatening our national security," he said.

What makes Internet-based terrorism particularly challenging, says Austin Berglas, who oversees over 1000 special agents in the FBI's New York Cyber Branch, is the way the Internet makes their identities and physical locations extremely difficult to trace. "They don't have to park a car on 42nd street and blow it up. They could disable financial institutions networks and not allow people to access to their funds. They can bring down electrical grids and power grids. They could create a power blackout in New York City. That's an act of terrorism," he said.

The Internet's ability to transmit information instantly across international borders is a strength when done for legitimate purposes, but a huge vulnerability when the intent is malicious or criminal. The threat is even more dangerous when military computer networks are involved.

U.S. Navy Captain Daryl Hancock is the intelligence officer assigned to Cyber Command for the United States 10th Fleet. He says that much like the business and government sectors, much of the navy's business is conducted over the World Wide Web.

"We have some closed networks but much of what we rely on is the World Wide Web, the Internet as you know it. That's how we move our supplies; that's how we communicate through those mechanisms. Our biggest concern right now is espionage. People don't do espionage nowadays so much cloak and dagger. They do it through cyberspace. They can do it with a thumb drive. They can do it through hacking into your secure networks and they can exfiltrate [take out] the data that way. So we're focused on defending those networks and keeping them secure," he said.

Hancock says that some Navy weapons systems remain connected to the World Wide Web, and that this makes it possible, at least in theory, for outsiders to hack into those systems, and launch weapons remotely. That's one reason why a huge part of his job is educating Navy personnel to be the first line of defense against cyber-threats.

"We've got to change the culture of our sailors in order to make them aware of the threats and vulnerabilities so that they can't just introduce things or charge their iPod on a computer that's hooked into our network, or use a thumb drive that's not been cleared and is safe. It's difficult nowadays when everybody has a cell phone, everybody has a Facebook page. And a lot of that is education - just helping them understand the importance that they play," he said.

As our dependence on the Internet skyrockets, so do the sophistication and number of cyber-security threats, and therefore the number of business dedicated to creating new products and approaches to counter those threats. Traditionally, that has meant firewalls, password codes and the like to prevent criminal from entering one's computer network.

However, according to Gary Gagnon who directs Cyber Security for the MITRE Corporation, the real challenge is how to minimize damage once a hacker or criminal has actually made it past those first-line defenses.

"Once the guy is in what happened in your network? What did he do in your network, what has been taken, has been compromised. How do I figure out all the places that he is. So that when I do pull him out I know I've got him out completely and he doesn't have one more toehold in my network that I didn't see. And I think I'm all set and I'm running my business or I'm running my federal government organization again he comes back into that little toehold and begins his operation again. It's a game. He's trying to get in and we're trying to get him out. Industry is starting to see that there is a market for products like that It's a game," he said.

Because the world that gets even more tightly interconnected every day, the stakes of that game could not be higher. Finding the right balance between the freedom of access to information on which the Internet depends, and the need for cyber security and safeguards to privacy on which both prosperity and peace largely depend will remain a challenge far into the future.