Contact Us
- Your Local FBI Office
- Overseas Offices
- Submit a Crime Tip
- Report Internet Crime
- More Contacts

Learn About Us
- Quick Facts
- What We Investigate
- Natl. Security Branch
- Information Technology
- Fingerprints & Training
- Laboratory Services
- Reports & Publications
- History
- More About Us

Get Our News
- Press Room
- E-mail Updates
- News Feeds

Be Crime Smart
- Wanted by the FBI
- More Protections

Use Our Resources
- For Law Enforcement
- For Communities
- For Researchers
- More Services

Visit Our Kids' Page

Apply for a Job

Major Executive Speeches

Robert S. Mueller, III
Director
Federal Bureau of Investigation

International Conference on Cyber Security 2010
New York, New York

August 5, 2010

Good morning. It is a pleasure to be here. My thanks to Fordham University for hosting this conference and for co-sponsoring it with the FBI.

It is perhaps a little unusual to start a speech by pausing for five seconds, but that is what I would like to do.

What just happened? In those five seconds, computer users conducted some 170,000 Google searches. An estimated 22 million e-mails were sent—and about 80 percent of those were spam. Users posted at least 3,500 status updates on Facebook and 3,000 “tweets” on Twitter.

Meanwhile, the Automated Clearinghouse—the network that connects all U.S. financial institutions—processed almost 3,000 electronic payments. All of that happened in just five seconds.

We live in a wired world. Our networks help us to stay in touch with family and friends, collaborate with colleagues worldwide, and shop for everything from books to houses. They help us manage our finances and make businesses and government more efficient.

But our reliance on these networks also makes us vulnerable. Criminals can 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 to steal our secrets, attack our critical infrastructure, and threaten our national security. And because the web offers near-total anonymity, it is difficult to discern the identity, the motives, and the location of an intruder.

Yet for too many individuals and businesses, cyber crime remains a nebulous concept. So today, I want to talk about the evolving nature of cyber threats, what the FBI is doing to combat them, and how we can work together to keep them at bay.

Cyber Terrorism

Let me begin with cyber threats to our national security. As you well know, a cyber attack could have the same impact as a well-placed bomb.

To date, terrorists have not used the Internet to launch a full-scale cyber attack. But they have executed numerous denial-of-service attacks and defaced numerous websites.

In the past decade, al Qaeda’s online presence has become almost as potent as its physical presence. Extremists are not limiting their use of the Internet to recruitment or radicalization; they are using it to incite terrorism.

Of course, the Internet is not only used to plan and execute attacks; it is also a target itself. Usama bin Laden long ago identified cyberspace as a means to damage both our economy and our morale—and countless extremists have taken this to heart.

We in the FBI, with our partners in the intelligence community, believe the cyber terrorism threat is real, and is rapidly expanding. Terrorists have shown a clear interest in pursuing hacking skills. And they will either train their own recruits or hire outsiders, with an eye toward coupling physical attacks with cyber attacks.

Apart from the terrorist threat, nation-states may use the Internet as a means of attack for political ends. Consider what took place in Estonia in 2007 and in the Republic of Georgia in 2008. Wave after wave of data requests shut down banks and emergency phone lines, gas stations and grocery stores, even parts of each country's government. The impact of these attacks left all of us aware of our vulnerabilities.

Counterintelligence and Economic Espionage

Let me turn for a moment to counterintelligence intrusions and economic espionage.

Espionage once pitted spy versus spy and country against country—as we have recently seen. Today, our adversaries sit on fiber optic cables and wi-fi networks, often unknown and undetected. They may be nation-state actors or mercenaries for hire, rogue hackers or transnational criminal syndicates.

These hackers actively target our government and corporate networks. They seek our technology, our intelligence, and our intellectual property, even our military weapons and strategies. In short, they have everything to gain, and we have a great deal to lose.

We are concerned not only about the loss of data, but corruption of that data as well. If hackers made subtle, undetected changes to your company's source code, they would have a permanent window into everything you do.

Some in the industry have likened this to "death by a thousand cuts." We are bleeding data, intellectual property, information, and source code—bit by bit, and in some cases, terabyte by terabyte.

The solution does not rest solely with better ways to detect and block intrusion attempts. We are playing the cyber equivalent of cat and mouse, and, unfortunately, the mouse seems to be one step ahead.

We must work to find those responsible. And we must make the cost of doing business more than they are willing to bear.

The FBI: Protecting Our Infrastructure

The FBI pursues cyber threats from start to finish. We have cyber squads in each of our 56 field offices around the country, with more than 1,000 specially trained agents, analysts, and digital forensic examiners.

Together, they run complex undercover operations and examine digital evidence. They share information with our law enforcement and intelligence partners. And they teach their counterparts —both at home and abroad—how best to investigate cyber threats.

But the FBI cannot do it alone. The National Cyber Investigative Joint Task Force includes 18 law enforcement and intelligence agencies, working side by side to identify key players and schemes. The goal is to predict and prevent that which is on the horizon, and to pursue the enterprises behind these attacks.

The task force operates through Threat Focus Cells—smaller groups of agents, officers, and analysts from different agencies, focused on particular threats.

For example, the Botnet Focus Cell investigates high-priority botnets. We are reverse-engineering those botnets, with an eye toward disrupting them. And we are following the money wherever it leads, to find and stop the botmasters.

The recent takedown of the Mariposa botnet is but one example of that collaboration. As you may know, Mariposa was an information-stealing botnet—one that infected millions of computers worldwide, from Fortune 500 companies to major banks.

During a two-year investigation, the FBI worked closely with our overseas counterparts to track down and arrest the main operators of the Mariposa botnet and the original creator of the malicious software that helped to build and control it.

In February, the Spanish police arrested three individuals who used Mariposa to hack into online bank accounts. And just two weeks ago, the Slovenian police identified and arrested the botnet's creator. This individual had sold the original virus to hundreds of criminals worldwide, and developed customized versions to meet their needs.

The Mariposa takedown sends a clear message to cyber criminals: We are going after both the cyber equivalent of the house burglar—and the person who gives him the crowbar, the map, and the locations of the best houses in the neighborhood.

The skill, dedication, and unprecedented cooperation provided by our partners in Spain and Slovenia were crucial to the success of this effort. In international cases such as this, global cooperation is absolutely essential.

To that end, the FBI has 61 legal attaché offices around the world, sharing information and coordinating investigations with our host countries. We have embedded agents with police forces in Romania, Estonia, Ukraine, and the Netherlands, to mention just a few.

Together, we are making progress. But law enforcement agencies alone cannot defeat our cyber adversaries. In the Mariposa case, our private sector partners also provided valuable help. The Mariposa Working Group, an informal band of security researchers and volunteers, gave us intelligence to track down the subjects, and worked to dismantle the botnet after we made our arrests.

Importance of Private Sector Partnerships

But to stem the rising tide of cyber crime and terrorism, we also need *your* help.

We in the FBI understand that those of you in the private sector have practical concerns about reporting breaches of your network security. You may believe that notifying the authorities will harm your competitive position. You may have privacy concerns. Or you may think that the information flows just one way—and that is to us.

We do not want you to feel victimized a second time by an investigation. We will minimize the disruption to your business, and safeguard your privacy and your data. Where necessary, we will seek protective orders to preserve trade secrets and business confidentiality. And we will share with you what we can, as quickly as we can, about the means and the methods of attack.

Remember that for every investigation in the news, there are hundreds that will never make the headlines. Disclosure is the exception, and not the rule. That said, we cannot act if we are not aware of the problem. Maintaining a code of silence will not benefit you or your clients in the long run.

It calls to mind the old joke about two hikers in the forest who run into a bear. The first hiker says to the other, "We just need to outrun him." And the second replies, "I don't need to outrun him. I just need to outrun you."

You may well outrun one attack, but you aren't likely to avoid the second, or the third. Our safety lies in protecting not just our own interests, but our critical infrastructure as a whole.

Conclusion

Following World War I, France built a line of concrete fortifications and machine gun nests along its borders. It was designed to give the French army time to mobilize in the event of an attack by Germany. The secondary motivation was to entice Germany to attack Belgium as the easier target.

As we all know, the Maginot Line held strong for a brief time. However, in the long run, it failed. The Germans invaded Belgium, outflanked the line, and stormed France. In the end, neither fortresses nor fortifications stopped Nazi Germany.

Our success in defeating Germany was built on a united front. We stopped playing defense, and we pushed back, day by day. No one country, standing alone, could have ended that war.

The same is true today, in this new context. No one country, no one company, and no one agency can stop cyber crime. A “bar the windows and bolt the doors” mentality will not ensure our collective safety. Fortresses will not hold forever; walls will one day fall down. We must start at the source; we must find those responsible.

The only way to do that is by standing together. For ultimately, we all face the same threat. Together, we can and we will find better ways to safeguard our systems, minimize these attacks, and stop those who would do us harm.

Thank you all for attending this conference, and God bless.

Executive Speeches | Press Room Home