

**Remarks Prepared for Delivery by  
Robert S. Mueller, III  
Director, Federal Bureau of Investigation  
Critical Incident Analysis Group  
University of Virginia  
Charlottesville, Virginia  
March 31, 2008**

Good evening, and thank you, George, for your kind introduction, and congratulations to you, Leonard, on your well-deserved award. I am indeed honored to be here.

I want to express my appreciation for the work of the Critical Incident Analysis Group, and its executive director, Greg Saathoff.

Since its first conference in 1998, CIAG's partnership with the FBI has indeed been a fruitful one. We have confronted some of the critical topics of our time — threats to symbols of democracy, bioterrorism, radicalization — and now, cyber threats.

Throughout, the CIAG has been a tremendous support to, and partner with, the FBI, and we are most grateful to you.

As you may know, fighting cyber crime is among the FBI's highest priorities, just after counterterrorism and counterintelligence. Every day, our cyber agents and analysts investigate computer fraud, child exploitation, theft of intellectual property, and worldwide computer intrusions.

Tonight, I want to talk about cyber threats to our national security, and what the FBI is doing to meet those diverse dangers.

I recently watched a video on YouTube about the impact of the Internet. And for anyone here under the age of 25, I will say yes, those of us over a certain age are allowed to access YouTube.

According to this video, entitled "Did You Know," the average 21-year-old has sent and received more than 250-thousand e-mails and instant messages. More than 70 percent of four-year-olds in the United States have used a computer at least once. And Internet users query Google nearly three billion times every month.

The Internet has become the primary means by which we conduct business, store data, and connect operating systems, from air traffic control to power grids. But that widespread use has also left us vulnerable to attack from hostile foreign powers, hackers, and even terrorists.

The Internet is not only the means by which attacks may be planned and executed; it is also a target in and of itself.

Just imagine a country experiencing a "cyber blockade." Wave after wave of data requests from computers around the world shut down banks and emergency phone lines, gas stations and grocery stores, newspapers and television stations, even the President or Prime Minister's office.

As you may know, this scenario is not the stuff of science fiction. These very events occurred just last April in Estonia.

Although the source of this attack has not been confirmed, the effect was real, and left all of us aware of the potential risk we face.

We see this effect on a smaller scale every day. Computer intrusions are becoming more and more commonplace. And studies show that computers in the United States are attacked at a rate 10 times that of other countries.

Today, botnets are the weapon of choice. Botnets are considered the Swiss Army knives of cyber crime. You name it, they can do it, from attacking networks, sending spam, and collecting data, to infecting computers and injecting spy ware.

Botnets do not require highly technical skills, yet the national security implications are broad. A botnet could shut down a power grid, flood an emergency call center with millions of spam messages, or disable a military command post. The possibilities are endless, and that is what makes it so daunting.

Take, for example, an operation we initiated last June, called “Bot Roast” (I don’t know where we come up with these code names, but it was called “Bot Roast”).

Together with the Department of Justice, the Computer Emergency Response Team (CERT) Coordination Center at Carnegie Mellon, private sector companies such as Microsoft, and Internet service providers, we identified more than one million infected computers and shut down several bot-herders, as they are called.

In a second phase of “Bot Roast,” cleverly-named “Bot Roast II,” completed last November, an individual used botnets to make off with some \$20 million dollars as part of a phishing scam.

It is clear that computer intrusions can also have large-scale implications for our economy and our national security. There is no shortage of countries that seek our information technology, our innovation, and our intelligence – information we have spent years and billions of dollars developing.

The simple truth is we do not protect cyber space to the same degree we protect our physical space. We have in large part left the doors open to our business practices, our sensitive data, and our intellectual property.

The espionage game once pitted spy versus spy, country against country. But today, our adversaries sit on fiber optic cables and wi-fi networks. Hackers are using sophisticated techniques to steal sensitive intelligence, scientific research, and communications data. They are difficult to identify and track because they move in and out of international systems at will, and they leave no visible trail.

A member of our cyber team describes it as having an invisible man in the room, standing over your shoulder, seeing and hearing everything you do, watching every word you type. And you may never know he is there . . . who he represents . . . or how much damage he has done.

We are concerned not only with loss of data, but also with corruption of data. Such manipulation can cause electronic devices to fail and networks to freeze. It can alter critical air temperatures in laboratories, and shut down safety systems in nuclear power stations.

There are also those who seek to block access to our own information, for political, financial, or ideological gain. If we lose the Internet, we do not simply lose the ability to email or to surf the web. We lose access to our data. We lose our connectivity. We lose our intellectual property. We lose our security.

And the threat is not limited to hackers on the outside. Insiders present a significant problem. Contractors may take the appropriate security measures, but what about those with whom they subcontract, and their subs? And what of those who may take advantage of open access to research and development facilities on campuses such as this?

One case especially underscores this insider threat. In November 2001, a man named Li Sun (Lee Sunh) told FBI agents in Palo Alto that he believed his business partner had stolen trade secrets from his employers.

One week later, Fei Ye (Fay Yeh) and Ming Zhong (Jong) were arrested at the San Francisco airport, just moments before boarding a flight bound for Shanghai. FBI agents and Customs officials seized several hard drives, and thousands of proprietary documents and electronic media from two major semiconductor companies.

They found these two men had planned to start a semiconductor company in China, using this proprietary information. They had requested funding from a Chinese government program dedicated to acquiring and developing science and technology. They had received more than two million dollars in start-up funds, from city and provincial Chinese government agencies.

In December 2006, these two pled guilty to economic espionage to benefit a foreign country. Each faces up to thirty years in prison.

The intersection between cyber crime and terrorism is also becoming increasingly evident. We know terrorist organizations have the interest and intent, to attack American cyber networks. And there are thousands of extremist websites, comprising everything from propaganda to blogs.

In the past six years, al Qaeda's online presence has become pervasive. For terrorists, the Internet has become a marketing tool, a moneymaker, a training ground, and a virtual town square, all in one.

In July of 2007, three men in Britain were the first to be sentenced to prison for using the Internet to incite terrorism. One of these men, Younis Tsouli, went by the moniker "Irhabi Double Oh Seven" – which translates in Arabic to "Terrorist Double Oh Seven." He was a loner living in a London basement apartment, with no previous connection to al Qaeda, yet he became a key part of its propaganda campaign.

Tsouli posted thousands of files online, from videos of beheadings to detailed instructions for building car bombs. He hacked into servers around the world to gain additional bandwidth.

But he did more than merely act as an al Qaeda webmaster. He was a hub of communication between terrorist plotters in Canada, Denmark, Bosnia, and the United States.

He and his colleagues stole thousands of credit card accounts through phishing schemes. They ran up charges of more than \$3 million dollars for items they thought fellow extremists might need, from night vision goggles to GPS devices. And they laundered money through more than a dozen Internet gambling sites.

At the time of his arrest, Tsouli was just a 22-year-old student. Today, he is a guest of Belmarsh Prison in the U.K. But he is hardly the end of the line; many more cyber-savvy extremists hope to carry on where he left off.

The FBI has the authority to handle these varied threats from start to finish. We have cyber squads in each of our 56 field offices across the country. These agents, intelligence analysts, and computer experts mesh technological expertise with investigative experience. They run complex undercover operations to catch computer hackers and child predators the world over.

They also investigate threats to both companies and consumers. And they teach their law enforcement counterparts – at home and abroad – how to work cyber investigations.

Our capabilities are strong, but they rely on key partnerships with other federal agencies, law enforcement, private industry, and academia – indeed, many of you here tonight.

But we do not limit our operations to the United States. Increasingly, cyber threats originate outside of our borders. And as more people around the world gain access to computer technology, new dangers will surface. For this reason, global cooperation is vital.

To that end, we have 61 Legal Attaché offices around the world. We are working with our partners in Romania, Russia, Poland, Hungary, Italy, and Estonia, amongst others, to investigate international cyber threats.

Just last month, cyber agents arrested more than one hundred individuals across the globe who had been trading and distributing roughly 400,000 files of child pornographic material over a period of some 15 years.

These individuals used sophisticated encryption technology to elude detection.

We worked with our counterparts in Australia, Germany, and the United Kingdom to bring these individuals to justice.

We also understand that we must continue to work closely with all of you – members of the private sector and the academic community.

Through the FBI's InfraGard program, members from a host of industries, from computer security to the chemical sector, share information about threats to their own companies, to their own communities, through a secure computer server.

To date, there are nearly 24-thousand members of InfraGard — individuals from Fortune 500 companies to small businesses.

We are also reaching out to academia by way of the National Security Higher Education Advisory Board.

The Board provides a forum to discuss issues that affect not just the academic culture, but the country, from campus security and counterterrorism, to espionage and cyber crime. University presidents and chancellors from across the country share their concerns and their collective expertise.

There is an old saying that all roads lead to Rome. In the days of the Roman Empire, roads radiated out from the capital city, spanning more than 52-thousand miles.

The Romans built these roads to access the vast areas they had conquered. But, in the end, it was these same roads led to Rome's downfall, for they allowed the invaders to march right up to the city gates.

The Internet has opened up thousands of new roads for each of us – new ideas and information, new sights and sounds, new people and places. But the invaders – those whose intent is not enlightenment, but exploitation and extremism – are marching right down those same roads, to attack us in multiple ways.

We stand a much greater chance of staying safe if we stand together. We must continue to safeguard our systems and our data. We must continue to share intelligence. Most importantly, we must continue to stay connected.

The enemies, as they say, are at the gates, and we must rely on our agility, our resourcefulness, and our resolve to stop them, together.

Thank you again for having me here tonight and God bless. I would be happy to take some questions.