Department of Justice

STATEMENT OF

JOHN BOLES
DEPUTY ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

ENTITLED

"INVESTIGATING AND PROSECUTING 21ST CENTURY CYBER THREATS"

PRESENTED

MARCH 13, 2013

Statement of
John Boles
Deputy Assistant Director
Cyber Division
Federal Bureau of Investigation

Before the
Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
United States House of Representatives

At a Hearing Entitled
"Investigating and Prosecuting 21st Century Cyber Threats"

March 13, 2013

Chairman Sensenbrenner, Ranking Member Scott, and Members of the Subcommittee, I am pleased to appear before you today to discuss the nature of the cyber threat, how the FBI has responded to it, and how we are marshaling our resources and strengthening our partnerships to more effectively combat the increasingly sophisticated adversaries we face in cyberspace.

The Cyber Threat

Some of the most critical threats facing our nation today emanate from the cyber realm. Intrusions into our corporate networks, personal computers, and government systems are occurring every single day by the thousands.

We see four malicious primary actors in the cyber world: foreign intelligence services, terrorist groups, organized crime enterprises, and hacktivists.

Dozens of countries have offensive cyber capabilities, and these foreign cyber spies have become increasingly adept at exploiting weaknesses in our computer networks. Once inside, they can exfiltrate government and military secrets, as well as valuable intellectual property—information that can improve the competitive advantage of state-owned entities and foreign companies.

Terrorist groups would like nothing better than to digitally sabotage our power grid or water supply. Some say they do not currently have the capability to do it themselves. But the reality is that the capability is readily available on the open market.

Organized crime groups, meanwhile, are increasingly migrating their traditional criminal activity from the physical world to computer networks. They no longer need guns to rob a bank; they use a computer to breach corporate and financial institution networks to steal credentials, account numbers, and personal information they can use to make money.

These criminal syndicates, often made up of individuals living in disparate places around the world, have stolen billions of dollars from the financial services sector and its customers. Their crimes increase the cost of doing business, put companies at a competitive disadvantage, and create a significant drain on our economy.

Hacktivist groups such as Anonymous and LulzSec are pioneering their own forms of digital anarchy by illegally accessing computers or networks for a variety of reasons including politically or socially motivated goals.

With these diverse threats, we anticipate that cyber security may well become our highest priority in the years to come. Computer intrusions and network attacks are the greatest cyber threat to our national security. That is why we are strengthening our cyber capabilities, in the same way we enhanced our intelligence and national security capabilities in the wake of the September 11th attacks.

FBI Response 2002-2012

The FBI recognized the significance of the cyber threat more than a decade ago and, in response, created the Cyber Division in 2002; elevated the cyber threat as our number three national priority (only after counterterrorism and counterintelligence); significantly increased our hiring of technically trained agents, analysts, and forensic specialists; and expanded our partnerships with law enforcement, private industry, and academia, through initiatives like InfraGard—a public-private coalition of 55,000 members to protect critical infrastructure—and the National Cyber-Forensics and Training Alliance, a proven model for sharing private sector intelligence in collaboration with law enforcement.

We have made great progress in the interim. Ten years ago, if you were an agent conducting a cyber investigation and the Internet Protocol (IP) address tracked back to a foreign country, that was effectively the end of your investigation. Although you could send a lead to one of the FBI's overseas Legal Attaché Offices, the likelihood that you would discover who was behind the keyboard was small.

Since then, we have embedded cyber agents with law enforcement in several key countries: Estonia, Ukraine, the Netherlands, and Romania. Some countries in cyber hot spots also enhanced their domestic laws and agreed to allow extraditions to the United States.

Those changes, along with improvements in our ability to track IP addresses back to their source, have led to a recognition in the underground economy that there are fewer safe hiding places around the globe. Building on the success of our international outreach, we are currently expanding our Cyber Assistant Legal Attaché program to additional countries.

A prime example of how our investigations have progressed in the 10 years since the Cyber Division was created is the 2011 takedown of Rove Digital, a company founded by a ring of Estonian and Russian hackers to commit a massive Internet fraud scheme.

The scheme infected with malware more than four million computers located in more than 100 countries. The malware secretly altered the settings on infected computers, enabling the hackers

to digitally hijack Internet searches using rogue servers for Domain Name System (DNS) routers and re-routing computers to certain websites and ads. The company received fees each time these web sites or ads were clicked on or viewed by users. This scheme generated $14 million in illegitimate income for the operators of Rove Digital.

Because Estonia has improved its domestic laws, we were able to work with our law enforcement counterparts and our private industry partners to execute a takedown of this criminal organization. Following the arrest of several co-conspirators in Estonia, teams of FBI agents, linguists, and forensic examiners assisted Estonian authorities in retrieving and analyzing data that linked the co-conspirators to the Internet fraud scheme. At the same time, we obtained a court order in the United States to replace the rogue DNS servers with court-ordered clean servers.

In this case, we not only took down the criminal organization, but worked with our partners in DHS and other agencies to mitigate the damage. Seven individuals have been indicted in the Southern District of New York in this case: six in Estonia and one in Russia. The United States has sought extradition of all six Estonian subjects. To date, two of them have been remanded to U.S. custody. One pleaded guilty on February 1, 2013.

We are also employing novel ways of combating the threat. In Operation Coreflood, the FBI worked with our private sector and law enforcement partners to disable a botnet that had infected an estimated two million computers with malicious software.

The malware on this Coreflood botnet allowed infected computers to be controlled remotely by criminals to steal private personal and financial information from unsuspecting users. In an unprecedented move, the FBI obtained a court order to seize domain names, re-route the botnet to FBI-controlled servers, and respond to commands sent from infected computers in the United States, telling the zombies to stop the Coreflood software from running. The success of this innovative operation will help pave the way for future cyber mitigation efforts and the development of new "outside the box" techniques.

While we're proud of these investigative successes and our progress against the threat, we are continuing to push ourselves to respond more rapidly and prevent attacks before they occur.

Last month, President Obama released the Administration's Strategy on Mitigating the Theft of U.S. Trade Secrets. As part of the Strategy, the FBI is expanding its efforts to fight computer intrusions that involve the theft of trade secrets by individuals, foreign corporations, and nation-state cyber hackers.

Over the past year, under our legal authorities and in conjunction with our government partners, we have successfully warned some potential victims ahead of time that Computer Network Exploitation (CNE) or Computer Network Attacks (CNA) were about to happen. They were able to use that information to shore up their defenses.

Another area in which we've had success recently is in targeting infrastructure we believe has been used in Distributed Denial of Service (DDOS) attacks, and preventing it from being used for future attacks.

Since October, the FBI and the Department of Homeland Security (DHS) have released nearly 130,000 IP addresses that were believed to be infected with DDOS malware. We have released this information through Joint Intelligence Bulletins (JIBs) to 129 countries. These JIBs are released by both the DHS' Computer Emergency Readiness Team (CERT) mechanisms as well as by our Legal Attachés to our foreign partners.

These actions have enabled our foreign partners to take action and reduced the effectiveness of the botnets and the DDOS attacks.

Next Generation Cyber

The need to prevent attacks before they occur is a key reason we have redoubled our efforts to strengthen our cyber capabilities while protecting privacy, confidentiality, and civil liberties. The FBI's Next Generation Cyber Initiative, which we launched in 2012, entails a wide range of measures, including focusing our Cyber Division on intrusions; hiring additional computer scientists; creating Cyber Task Forces focused on intrusions in each of our 56 Field Offices; and expanding partnerships and collaboration at the National Cyber Investigative Joint Task Force (NCIJTF).

The nature and severity of the cyber threat have led the government agencies with a role in cyber security to recognize that we must work together more efficiently than ever to keep pace with and surpass our adversaries in this realm.

To that end, FBI Director Robert Mueller, DHS Secretary Janet Napolitano, and National Security Agency (NSA) Director Keith Alexander recently held a series of meetings to clarify the lanes in the road in cyber jurisdiction. The group mutually agreed on their respective roles and responsibilities related to a cyber incident. The FBI's role is to investigate, attribute, and disrupt cybercrimes affecting the United States. DHS' role is to protect our critical infrastructure and our networks, coordinate mitigation and recovery from cyber incidents, and to disseminate threat information across various sectors. NSA's role is to gather intelligence on foreign cyber threats and to protect national security systems.

We are coordinating at an unprecedented level, including rapid, real-time exchanges from FBI investigative activities to DHS, allowing the Department to push out information to help safeguard other networks from similar attacks.

A key part of the intergovernmental effort is the FBI-operated National Cyber Investigative Joint Task Force (NCIJTF), which serves as the deconfliction center on cyber investigations among 19 agencies. The NCIJTF involves senior personnel from key agencies, including Deputy Directors from NSA, DHS, the Central Intelligence Agency, and U.S. Secret Service. A fifth deputy will soon be appointed by U.S. Cyber Command. NCIJTF brings together a partnership of agencies focused on addressing cyber threats through investigations and intelligence sharing.

Not only have we recognized that the cyber threat warrants considerably strengthening our intergovernmental partnerships, but it also warrants significantly enhancing our collaboration with the private sector.

Today, the private sector is the essential partner if we are to succeed in defeating the cyber threat. The private sector is a primary victim of cyber intrusions—and its networks contain the evidence of countless such attacks. Our nation's companies and businesses possess the information, the expertise, and the knowledge we need to combat the threat. They also build the components of cyber security—the hardware, the software, and the networks—and drive future technology.

In the past, industry has provided us information about attacks that have occurred, and we've investigated the attacks. Our adversaries have taken advantage of the fact that we have been limited in the kind of information we exchange with the private sector. We now realize this can no longer be a one-way flow of information.

As part of our enhanced private sector outreach efforts, we're providing industry with tools, including information, to help repel intruders. In fact, in line with a strategic government-wide shift, we have recently begun to provide classified threat briefings to key industry partners and work with them to exchange information. InfraGard, NCFTA, and our other partnerships are a step in the right direction. But we must build on these initiatives, in conjunction with our federal partners, to expand the channels of information sharing and collaboration. We recognize that there are many considerations to take into account when considering the level of public-private collaboration we believe is necessary, including industry concerns about the protection of their proprietary information and questions about how best to share classified information. We are committed, however, to engaging in this collaboration in a way that fully protects privacy, confidentiality, and civil liberties.

Conclusion

In conclusion, Mr. Chairman, to counter the cyber threats we face, we are engaging in an unprecedented level of intergovernmental collaboration and cooperation with the private sector.

We look forward to continuing to expand on those partnerships and working with the Committee and Congress as a whole to determine a successful course forward for the nation to combat the cyber threat while protecting privacy, confidentiality, and civil liberties.

Thank you again for the opportunity to appear before you today. I would be happy to answer any questions you may have.