Department of Justice

STATEMENT OF
JOSEPH M. DEMAREST, JR.
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
SUBCOMMITTEE ON CRIME AND TERRORISM
COMMITTEE ON JUDICIARY
UNITED STATES SENATE

ENTITLED:
"CYBER THREATS: LAW ENFORCEMENT AND PRIVATE SECTOR RESPONSES"

PRESENTED
MAY 8, 2013

Statement of
Joseph M. Demarest, Jr.
Assistant Director
Cyber Division
Federal Bureau of Investigation

Before the
Subcommittee on Crime and Terrorism
Committee on the Judiciary
United States Senate

At a Hearing entitled
"Law Enforcement and Private Sector Responses"

May 8, 2013

Chairman Whitehouse, Senator Graham, and distinguished members of the Committee, I am pleased to appear before you today to discuss 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

The 21st century brings with it entirely new challenges, in which criminal and national security threats strike from afar through computer networks, with potentially devastating consequences. These intrusions into our corporate networks, personal computers, and government systems are occurring every single day by the thousands. Such attacks pose an urgent threat to the nation's security and economy. The threat has reached the point that given enough time, motivation, and funding, a determined adversary will likely be able to penetrate any system accessible from the Internet.

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

Dozens of countries have sophisticated cyber espionage 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. Although most such groups currently lack the capability to conduct sabotage operations over the Internet themselves, the tools and expertise to perpetrate a cyber attack with physical effects are readily available for purchase or hire.

Organized criminal groups, meanwhile, are increasingly migrating their traditional criminal activity from the physical world to the online world. 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 are pioneering their own forms of digital anarchy, posing novel cybersecurity threats by repeatedly, illegally accessing computers or networks for a variety of reasons including politically or socially motivated goals.

With these diverse actors, we face significant challenges in our efforts to address and investigate cyber threats. While the FBI has already made great strides in developing its capability to address the cyber threat, we are currently prioritizing our immediate and long-term areas for strategic development in order to best position ourselves for the future.

FBI Response

The FBI recognized the significance of the cyber threat more than a decade ago and created the Cyber Division in 2002 to combat cyber-based terrorism, hostile foreign intelligence operations conducted over the Internet, and cyber crime, by applying the highest level of technical capability and investigative expertise. Since then, the FBI elevated the cyber threat to its number three national priority – after only counterterrorism and counterintelligence – and significantly increased the hiring of technically trained agents, analysts, and forensic specialists.

The FBI has also seen the value of its trusted partnerships and worked tirelessly to support and improve them. Securing our networks demands cooperation, and cyber vulnerabilities are magnified when you consider the ever-connected, interdependent ecosystem of the cyber world.

To that end, we have 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.

The FBI has made significant progress in recent years. 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.

Since then, the FBI has placed cyber specialists in key European locations to effectively facilitate the investigation of cyber crimes affecting the United States. This, along with improvements in our ability to track IP addresses back to their source, has 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 more than four million computers in more than 100 countries with malware. 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 specified 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 were located in Estonia and one was 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 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 pleased to report on our progress against the threat, we recognize that we must be pro-active in order to respond more rapidly and prevent attacks.

Next Generation Cyber

The need to prevent attacks 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, is an FBI-wide initiative to enhance our ability to address the full range of cybersecurity threats to the nation. In just the last year, this initiative has enhanced the FBI's ability to collect, coordinate, integrate, share, and act on information related to cyber intrusion investigations at headquarters, throughout its 56 domestic field offices, and with its partners overseas.

Implementation of this initiative is focused in four areas: strengthening the National Cyber Investigative Joint Task Force (NCIJTF); expanding the Cyber Task Forces focused on intrusions in each of our 56 Field Offices; advancing the capability of the cyber workforce and supporting enterprise infrastructure; and enhancing information sharing and operational collaboration with the private sector.

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 federal agencies. The FBI aims to strengthen and solidify the NCIJTF as the cybersecurity center for coordinating cyber threat investigations and disruption options. In the last year, the NCIJTF has made significant progress in developing its supporting capabilities and operational coordination, as well as expanding its interagency leadership. The NCIJTF now involves senior personnel from key agencies, including Deputy Directors from the National Security Agency, the Department of Homeland Security, the Central Intelligence Agency, the U.S. Secret Service, and U.S. Cyber Command.

In the future, the FBI must continue to strengthen the NCIJTF, which will include expediting analysis of interagency holdings and perfecting the coordination model on incident response and threat disruption operations.

Another critical element of the FBI's success is the restructuring and expansions of the FBI's network of field office Cyber Task Forces (CTFs), which emulate the successful Joint Terrorism Task Force (JTTF) model, such that each office has a robust multi-disciplinary, cross-program, and multi-agency domestic ground team to conduct cyber threat investigations and respond to significant cyber incidents.

In just the last year, the FBI has formally established a CTF in each field office, staffed by cyber-specialized agents, analysts, and other agency participants. The CTF is now established as a national brand, under which all field office efforts addressing cyber intrusion matters are addressed. The FBI offers a robust curriculum of FBI-developed and industry certification courses to its CTF members. In the future, each CTF will continue to grow its capabilities, leveraging nationally developed systems and investigative efforts. The FBI will also increase the participation of state and local law enforcement officers and expand the cadre of agents, analysts, and computer scientists on each CTF to ensure a high baseline capability.

The FBI is committed to advancing the capability of its cyber workforce and the supporting enterprise infrastructure. We have leveraged and developed our human capital by establishing core cyber competencies and further supported the workforce by extending enterprise capabilities. The FBI established its High-Technology Environment Training (HiTET) initiative to enhance the technical proficiency of Special Agents, Intelligence Analysts, Professional Staff,

and Task Force Officers (TFOs) who are directly involved in operations. HiTET training consists of numerous web-based courses, case studies and/or practical demonstrations, job-aids, legal fact sheets, technology articles and other related reference materials. HiTET training is developed in bundles to provide context and applicability to law enforcement and domestic intelligence missions requiring technical skills.

The current results of this effort are increased efficiencies and improved information analysis. Since the roll-out of the Next Generation Cyber initiative, the FBI has expanded visibility into the source of cyber threat activities and dramatically increased its cyber intelligence reporting. While we have seen success, the threat continues to grow and advance; in the future, the FBI must continue to expand the capability of its cyber workforce and its supporting technical infrastructure.

Last but not least, the FBI is working to strengthen both local and national information sharing and collaboration to support success in network defense, intelligence operations, and disruption operations. The private sector is an essential partner if we are to succeed in defeating the cyber threat. A critical piece of the relationship with private industry and individuals is assisting them in protecting themselves and their systems from the threat posed by terrorists, nation-states, and criminal groups conducting computer network operations against the U.S. To support this, the FBI has created an organizational unit focused on leveraging FBI operational information and intelligence to provide victims of cyber attacks more timely and valuable information regarding cyber attacks targeting them.

To maximize our efficiency, we adopted and enhanced the successful Counterterrorism Division Guardian terrorist threat tracking and collaboration system called eGuardian and enhanced it to accept cyber incidents from the fusion centers and state and local law enforcement. Further, we are deploying a platform called iGuardian to enable trusted private industry partners to also report cyber incidents in a secure and efficient manner to the FBI, and we are leveraging intelligence from the NCIJTF to effectively identify and notify cyber attack victims. We coordinate these efforts closely with the cybersecurity centers and our cybersecurity partners.

Conclusion

In conclusion, Mr. Chairman, in order to counter the growing cyber threats, we are focusing our resources, expanding our presence both at the local and national levels, and engaging in an unprecedented level of intergovernmental collaboration and cooperation with the private sector.

As the Committee knows, we face significant challenges in our efforts to combat cyber crime. We are optimistic that by identifying and prioritizing strategic areas for change, the FBI will continue to succeed in identifying and neutralizing cyber criminals, thereby protecting U.S. businesses and critical infrastructure from harm.

We look forward to working with the Committee and Congress as a whole to determine a successful course forward to ensure our defense. Thank you again for the opportunity to appear before you today. I would be happy to answer any questions you may have.