Department of Justice

STATEMENT OF

JOSEPH DEMAREST
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

HOMELAND SECURITY COMMITTEE
SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE
AND
SUBCOMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES
U.S. HOUSE OF REPRESENTATIVES

FOR A HEARING ENTITLED

ASSESSING PERSISTENT AND EMERGING CYBER THREATS TO THE U.S. HOMELAND

PRESENTED ON

MAY 21, 2014

Statement of Joseph Demarest
Assistant Director, Cyber Division, Federal Bureau of Investigation
Homeland Security Committee
U.S. House of Representatives
May 21, 2014

Good morning Chairmen's Meehan and King and Ranking Members Clarke and Higgins. I'm pleased to appear before you today to discuss the cyber threats facing our nation and how the FBI and our partners are working together to protect the United States government and private sector networks.

Today's FBI is a threat-focused, intelligence-driven organization. Each employee of the FBI understands the key threats facing our nation and we must constantly strive to be more efficient and more effective. Just as our adversaries continue to evolve, so, too, must the FBI. We live in a time of acute and persistent terrorist, state sponsored, and criminal threats to our national security, our economy, and our communities. These diverse threats facing our nation and our neighborhoods underscore the complexity and breadth of the FBI's mission.

We remain focused on defending the United States against terrorism, foreign intelligence, and cyber threats; upholding and enforcing the criminal laws of the United States; protecting civil rights and civil liberties; and providing leadership and criminal justice services to federal, state, local, and international agencies and partners.

The Cyber Threat & FBI Response

The United States faces cyber threats from state-sponsored hackers, hackers for hire, global cyber syndicates, and terrorists. They seek our state secrets, our trade secrets, our technology, our personal and financial information, and our ideas, all of which are of incredible value to all of us. They may seek to strike our critical infrastructure and our economy.

Given the scope of the cyber threat, agencies across the federal government are making cyber security a top priority. Within the FBI, we are prioritizing high-level intrusions – the biggest and most dangerous botnets, state-sponsored hackers, and global cyber syndicates. We want to predict and prevent attacks, rather than simply react after the fact.

FBI agents, analysts, and computer scientists are using technical capabilities and traditional investigative techniques, such as sources and communication intercepts, as well as forensics, to fight cyber crime. We are working side-by-side with our federal, state, and local partners on Cyber Task Forces in each of our 56 field offices and through the National Cyber Investigative Joint Task Force (NCIJTF). Through our 24/7 cyber command center, CyWatch, we combine the resources of the FBI and NCIJTF, allowing us to provide connectivity to federal cyber centers, government agencies, FBI field offices and legal attachés, and the private sector in the event of a cyber intrusion.

We also work with the private sector through partnerships such as the Domestic Security Alliance Council, InfraGard, and the National Cyber Forensics and Training Alliance. The FBI is

training our state and local counterparts to triage local cyber matters, so that we can focus on the most pressing issues with national impact.

In addition, our Legal Attaché offices overseas work to coordinate cyber investigations and address jurisdictional hurdles and differences in the law from country to country. We are supporting partners at Interpol and The Hague as they work to establish international cyber crime centers. We continue to assess other locations to ensure that our cyber personnel are in the most appropriate locations across the globe.

We know that to be successful in the fight against cyber crime, we must continue to recruit, develop, and retain a highly skilled workforce. To that end, we have developed a number of creative staffing programs and collaborative partnerships with private industry to ensure that over the long term we remain focused on our most vital resource, our people.

As the Committee is well aware, the frequency and impact of cyber attacks on our nation's private sector and government networks have increased dramatically in the past decade and are expected to continue to grow.

Recent Successes

While the FBI and our partners have had multiple recent investigative successes against the threat, we are continuing to push ourselves to respond more rapidly and prevent attacks before they occur.

One area in which we recently have had great success with our overseas partners is in targeting infrastructure we believe has been used in Distributed Denial of Service (DDOS) attacks, and preventing that infrastructure from being used for future attacks. A DDOS attack is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network. Since October 2012, the FBI and the Department of Homeland Security (DHS) have released nearly 168,000 Internet Protocol addresses of computers that were believed to be infected with DDOS malware. We have released this information through Joint Indicator Bulletins (JIBs) to more than 130 countries via DHS's National Cybersecurity and Communications Integration Center (NCCIC), where our liaison officers provide expert and technical advice for increased coordination and collaboration, as well as our Legal Attachés overseas.

These actions have enabled our foreign partners to take action and reduced the effectiveness of the botnets and the DDOS attacks. We are continuing to target botnets through this strategy and others.

In April 2013, the FBI Cyber Division initiated an aggressive approach to disrupt and dismantle the most significant botnets threatening the economy and national security of the United States. This initiative, named Operation Clean Slate, was implemented to appropriately address the threat neutralization actions through collaboration with the private sector, Department of Homeland Security and other United States Government partners, and our foreign partners. This

includes law enforcement action against those responsible for the creation and use of the illegal botnets, mitigation of the botnet itself, assistance to victims, public-service announcements, and long-term efforts to improve awareness of the botnet threat through community outreach. Although each botnet is unique, Operation Clean Slate's strategic approach to this significant threat ensures a comprehensive neutralization strategy, incorporating a unified public/private response and a whole-of-government approach to protect US interests.

The impact of botnets has been significant. Botnets have caused over $113 billion in losses globally, with approximately 378 million computers infected each year, equaling more than one million victims per day, translating to 12 victims per second.

To date, Operation Clean Slate has resulted in several successes. Working with our partners, we disrupted the Citadel Botnet. This botnet was designed to facilitate unauthorized access to computers of individuals and financial institutions to steal online banking credentials, credit card information, and other personally identifiable information. Citadel was responsible for the loss of over a half billion dollars. As a result of our actions, over 1,000 Citadel domains were seized, accounting for more than 11 million victim computers worldwide. In addition, working with foreign law enforcement, we arrested a major user of the malware.

Building on the success of the disruption of Citadel, in December 2013, the FBIand Europol, together with Microsoft and other industry partners, disrupted the ZeroAccess Botnet. ZeroAccess was responsible for infecting more than 2 million computers, specifically targeting search results on Google, Bing, and Yahoo search engines, and is estimated to have cost online advertisers $2.7 million each month.

In January 2014, Aleksandry Andreevich Panin, a Russian national, pled guilty to conspiracy to commit wire and bank fraud for his role as the primary developer and distributer of the malicious software known as "Spyeye" which infected over 1.4 million computers in the United States and abroad. Based on information received from the financial services industry, over 10,000 bank accounts were compromised by Spyeye infections in 2013 alone. Panin's co-conspirator, Hamza Bendelladj, an Algerian national who helped Panin develop and distribute the malware, was also arrested in January 2013 in Bangkok, Thailand.

Next Generation Cyber Initiative

The need to prevent attacks is a key reason the FBI has 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 the FBI Cyber Division on intrusions into computers and networks, as opposed to crimes committed with a computer as a modality. The Cyber Division established Cyber Task Forces in each of our 56 field offices to conduct cyber intrusion investigations and respond to significant cyber incidents. The Cyber Division has also hired additional computer scientists to assist with technical investigations in the field and expanded partnerships to enhance collaboration with the NCIJTF.

The NCIJTF, which serves as a coordination, integration, and information sharing center among

19 U.S. agencies and our Five Eyes partners for cyber threat investigations has resulted in unprecedented coordination. This coordination involves senior personnel at key agencies. NCIJTF, which is led by the FBI, now has deputy directors from the NSA, DHS, the Central Intelligence Agency, U.S. Secret Service, and U.S. Cyber Command. In the past year, we have had our Five Eyes partners join us at the NCIJTF. Australia embedded a liaison officer in May 2013, the UK in July 2013, and Canada in January 2014. By developing partnerships with these and other nations, NCIJTF is working to become the international leader in synchronizing and maximizing investigations of cyber adversaries.

While we are primarily focused with our federal partners on cyber intrusions, we are also working with our state and local law enforcement partners to identify and address gaps in the investigation and prosecution of Internet fraud crimes.

Currently, the FBI's Internet Crime Complaint Center (IC3) collects reports from private industry and citizens about online fraud schemes, identifies emerging trends, and produces reports about them. The FBI investigates fraud schemes that are appropriate for federal prosecution (based on such factors as the amount of loss). Others are packaged together and referred to state and local law enforcement.

The FBI is also working to develop the Wellspring program in collaboration with the International Association of Chiefs of Police, the Major Cities Chiefs Association, and the National Sheriffs' Association to enhance the Internet fraud targeting packages IC3 provides to state and local law enforcement for investigation and potential prosecution. During the first phase of this program's development, IC3 worked with the Utah Department of Public Safety to develop better investigative leads for direct dissemination to state and local agencies.

Through IC3, Operation Wellspring provided Utah police 22 referral packages involving over 800 victims, from which the FBI opened 14 investigations. Additionally, another nine investigations were opened and developed from the information provided.

The following are reported loss totals:

- IC3-referred investigations = $2,135,264
- Cyber Task Force initiated investigations = $ 385,630
- Operation Wellspring/Utah Total = $2,520,894

The FBI is also partnering closely with DOJ's Bureau of Justice Assistance to support efforts of the International Association of Chiefs of Police to develop a national Cyber Center designed specifically to identify and share resources from across government to assist local, state, and Tribal law enforcement agencies better address their cybercrime needs.

The FBI's newly established Guardian for Cyber application, being developed for Cyber use by the Guardian Victim Analysis Unit (GVAU), provides a comprehensive platform that tracks U.S. government coordination and efforts to notify victims or targets of malicious cyber activity.

The FBI is working toward the full utilization of Guardian for Cyber across FBI, other government agencies, state, local, tribal and territorial (SLTT) governments, as well as industry

partners, in order to provide forward understanding of cyber related threats, increase awareness of victim actions to mitigate those threats, and facilitate a coordinated overall cyber incident response by the U.S. government.

Private Sector Outreach

In addition to strengthening our partnerships in government and law enforcement, we recognize that to effectively combat the cyber threat, we must significantly enhance our collaboration with the private sector. Our nation's companies are the primary victims of cyber intrusions and their networks contain the evidence of countless attacks. In the past, industry has provided us information about attacks that have occurred, and we have investigated the attacks, but we have not always provided information back.

The FBI's newly established Key Partnership Engagement Unit (KPEU) manages a targeted outreach program focused on building relationships with senior executives of key private sector corporations. Through a tiered approach the FBI is able to prioritize our efforts to better correlate potential national security threat levels with specific critical infrastructure sectors.

The KPEU team promotes the FBI's government and industry collaborative approach to cyber security and investigations by developing a robust information exchange platform with its corporate partners.

Through the FBI's InfraGard program, the FBI develops partnerships and working relationships with private sector, academic, and other public/private entity subject matter experts. Primarily geared toward the protection of critical, national infrastructure, InfraGard promotes ongoing dialogue and timely communication between a current active membership base of 25,863 (as of April 2014).

InfraGard members are encouraged to share information with government that better allows government to prevent and address criminal and national security issues. One of the resources available to members is the Guardian for Cyber program, which facilitates real time incident reports to the FBI. InfraGard members also benefit from access to robust on and offline learning resources, connectivity with other members and special interest groups, and relevant government intelligence and information updates that enable them to broaden threat awareness and protect their assets.

The FBI's Cyber Initiative & Resource Fusion Unit (CIRFU) maximizes and develops intelligence and analytical resources received from law enforcement, academia, international, and critical corporate private sector subject matter experts to identify and combat significant actors involved in current and emerging cyber-related criminal and national security threats. CIRFU's core capabilities include a partnership with the National Cyber Forensics and Training Alliance (NCFTA) in Pittsburgh, Pennsylvania, where the unit is collocated. NCFTA acts as a neutral platform through which the unit develops and maintains liaison with hundreds of formal and informal working partners who share real-time threat information and best practices, and who collaborate on initiatives to target and mitigate cyber threats domestically and abroad. In addition, the FBI, Small Business Administration and the National Institute of Standards and

Technology (NIST) partner together to provide cybersecurity training and awareness to small business as well as citizens leveraging the FBI InfraGard program.

The FBI recognizes that understanding the cyber threat is critical to effectively combating it. As part of our enhanced private sector outreach, we have begun to provide industry partners with classified threat briefings and other information and tools to better help them repel intruders. Earlier this year, in coordination with the Treasury Department, we provided a classified briefing on threats to the financial services industry to executives of more than 40 banks who participated via secure video teleconference in FBI field offices. We provided another classified briefing on threats to the financial services industry in April 2014, with 100 banks participating. Another illustration of the FBI's commitment to private sector outreach is our increase in production of our external use products such as the FBI Liaison Alert System (FLASH) reports and Private Industry Notifications (PINs).

Conclusion

In conclusion, to counter the threats we face, we are engaging in an unprecedented level of collaboration within the U.S. government, with the private sector, and with international law enforcement.

We are grateful for the Committee's continued support and look forward to working with you and expanding our partnerships as we determine a successful course forward for the nation to defeat our cyber adversaries.