Department of Justice

**STATEMENT OF**

**LESLIE R. CALDWELL**
**ASSISTANT ATTORNEY GENERAL**
**CRIMINAL DIVISION**

**BEFORE THE**

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

**AT A HEARING ENTITLED**

**"TAKING DOWN BOTNETS: PUBLIC AND PRIVATE EFFORTS TO DISRUPT AND DISMANTLE CYBERCRIMINAL NETWORKS"**

**PRESENTED**
**JULY 15, 2014**

**Statement of**
**Leslie R. Caldwell**
**Assistant Attorney General**
**Criminal Division**
**Department of Justice**

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

**At a Hearing Entitled**
**"Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks"**

**Presented**
**July 15, 2014**

Good afternoon, Chairman Whitehouse, Ranking Member Graham, and Members of the Subcommittee. Thank you for the opportunity to appear before the Subcommittee today to discuss the Department of Justice's fight against botnets. I also particularly want to thank the Chair for holding this hearing and for his continued leadership on this important issue.

The threat from botnets—networks of victim computers surreptitiously infected with malicious software, or "malware," that are controlled by an individual criminal or an organized criminal group—has increased dramatically over the past several years. The computers of American citizens and businesses are, as we speak, under attack by individual hackers and organized criminal groups using state-of-the-art techniques seemingly drawn straight from a science fiction movie. Unfortunately, this cybercrime wave is all too real. Botnet attacks are intended to undermine Americans' privacy and steal from unsuspecting victims. If left unchecked, they will succeed.

The Department of Justice, working through highly trained prosecutors and Federal Bureau of Investigation (FBI) agents, recognizes this threat, and is working day and night to protect our citizens, our national security interests, and our businesses. We

responsibly employ the investigative and remedial tools Congress has given us, and we leverage our strengths by teaming up with partners across the federal government and, where appropriate, in the private sector and foreign law enforcement. As in the recent disruption of the Gameover Zeus botnet, which I will discuss more later, we find ourselves matched against increasingly sophisticated cyber criminals, and must evolve our tools and tactics minute-by-minute to prevent further harm to innocent victims.

Our successful effort to suppress the Gameover Zeus botnet should remind us that those who use botnets to cause harm are increasing in number and sophistication, and we cannot expect continued success if we merely rest on our laurels. The Department is armed with the laws and resources that we have been granted, but those tools must be updated and enhanced. If we want to remain effective in protecting our citizens and businesses, our laws and our resources must keep pace with the tactics and numbers of our adversaries. Our adversaries are always adapting. So must we. In my testimony, I will outline several legislative proposals that will assist the Department in its efforts to counter the threat posed by botnets. Finally, I will outline our resource needs—in particular the need for additional specialized criminal prosecutors.

**Current DOJ Anti-Botnet Activities**

Cybercrime overall has increased dramatically over the last decade, and caused enormous financial damage and innumerable invasions of Americans' privacy. The advances in computing technology that have powered our economy have also empowered those who seek to do us harm. Today, cyber criminals can steal personal and financial information from tens of millions of citizens in a single breach. To be sure, thefts of such information were committed long before the digital revolution. But stealing ten million credit card numbers previously would have required burglarizing thousands of stores, whereas now it can be done from a basement with a laptop. And some crimes have been uniquely adapted in the digital age. For example, in a new, disturbing twist on extortion, hackers have secretly activated the cameras on victims' laptop computers, taken compromising pictures or videos, and demanded payments not to expose those pictures or videos to the public. All the while, technological advances, including advances designed to protect privacy, such as anonymizing software and encryption, are being used to

frustrate criminal or civil investigations and, perversely, protect the wrongdoers. Our cyber crimefighters must be equipped with the tools and expertise to compete with and overcome our adversaries.

Over the same time period, botnets have emerged as a major threat. Sometimes called "botmasters" or "botherders," cyber criminals who control botnets can use advances in communications technology to take control of thousands, or even hundreds of thousands, of victim computers, or "bots." They can then command the computers they control to, for example, deluge an internet site with junk data, overwhelming it and knocking it offline. They may conduct such distributed denial-of-service (DDOS) attacks out of malice, as ideological attacks on those with whom they disagree, or even as a paid service to other criminals. They can also use the infected bots to steal banking credentials, credit card numbers, and other financial information. They can use them to send spam—email messages that range from advertising for illegal and dangerous pharmaceutical products, to fraud schemes aimed at artificially inflating the price of stocks, to "phishing" messages that gather sensitive information. Moreover, cybercriminals can use botnets to engage in other online crime by using their networks of infected computers as "proxies." This activity allows such criminals to conceal their identity and location while they commit crimes that range from fraud and theft of data to drug dealing and the sexual exploitation of children.

Botnets pose a threat to the United States, our citizens, and our businesses that must not be underestimated. By hijacking numerous victims' identities, credit cards, and bank accounts, criminal groups already have stolen hundreds of millions of dollars. And every day cyber criminals violate the privacy of Americans on a staggering scale, by stealing financial information, personally identifiable information, login credentials, and other information from victims who often do not even realize their computers have been compromised. Because botnets can be so lucrative, their designers use sophisticated code, locate their servers in countries around the world, and employ the latest in encryption methods—all designed to frustrate personal and corporate cybersecurity efforts, and to prevent law enforcement from responding effectively. Indeed, recent cases and ongoing investigations reveal that botnets are used by criminals halfway around the

world to commit crimes of a scope and sophistication that was difficult to imagine only a few years ago.

To counter this significant and complex threat, the Justice Department is vigorously responding to botnets and other cybercrimes through the tenacious work of the Criminal Division's Computer Crime and Intellectual Property Section, also known as CCIPS, and the Computer Hacking and Intellectual Property Coordinators and National Security Cyber Specialists in U.S. Attorneys' Offices across the country. These prosecutors, along with colleagues in the National Security Division (NSD), form a network of almost 300 Justice Department cybercrime prosecutors. In addition, the FBI has made combating cyber threats one of its top national priorities, working through Cyber Task Forces in each of its 56 field offices and continuing to strengthen the National Cyber Investigative Joint Task Force. The FBI has also moved aggressively to counter the botnet threat through Operation Clean Slate, a major FBI initiative designed to identify and eliminate the most significant criminal botnets. The United States Secret Service also focuses on cyber threats to financial networks and the personal financial information of Americans. Through a network of 35 Electronic Crimes Task Forces across the country and in key foreign countries, Secret Service investigations have resulted in the arrest and successful prosecution of the criminals responsible for some of the largest data breaches. U.S. Immigration and Customs Enforcement, Homeland Security Investigations (HSI), through the HSI Cyber Crimes Center (C3), has also dedicated significant resources to equip its Special Agents with the tools and knowledge necessary to combat transnational cybercrime.

The Department's response to botnets takes two tracks, often at the same time. First, whenever possible, we seek to arrest, prosecute, and incarcerate the criminals who use botnets to victimize Americans. For example, in January 2014, Aleksandr Andreevich Panin, a Russian national, pled guilty in federal court in Atlanta, Georgia to conspiracy to commit wire and bank fraud for his role as the primary developer and distributor of the malicious software known as "SpyEye." According to industry estimates, SpyEye has infected over 1.4 million computers in the United States and abroad. SpyEye secretly infected victims' computers and enabled cyber criminals to remotely control them through command and control servers. Designed to automate the

theft of confidential personal and financial information, such as online banking credentials, credit card information, usernames, passwords, PINs, and other personally identifying information, SpyEye was the preeminent malware toolkit used from approximately 2009 to 2011. Panin sold versions of the SpyEye virus to other criminals for prices ranging from $1,000 to $8,500. Panin is believed to have sold the SpyEye virus to at least 150 "clients" who, in turn, used it to set up their own botnets. One of Panin's clients alone was reported to have stolen over $3.2 million in a six-month period using SpyEye. Panin is awaiting sentencing, and four of his clients and associates were arrested by foreign law enforcement agencies.

Similarly, in federal court in New York in May 2014, Michael Hogue pled guilty, and an indictment was unsealed against Alex Yucel, in connection with their development of a particularly insidious piece of computer malware known as Blackshades. This malware was sold and distributed to thousands of people in more than 100 countries and was used to infect more than half a million computers worldwide. Once installed on a computer, the malware could collect the user's financial information and even turn on the computer's camera to spy on the unsuspecting user. An individual who helped market and sell the malware and two Blackshades users who bought the malware and then unleashed it upon unsuspecting computer users were also charged and arrested in the U.S. The charges and guilty plea were part of a law enforcement operation involving 18 other countries. More than 90 arrests have been made so far, and more than 300 searches have been conducted worldwide.

Arresting and convicting key players can disrupt criminal enterprises, but such actions are not always sufficient to counter the threat, particularly given the transnational nature of cybercrime. They also will not always remedy the harm caused by a botnet. Accordingly, the Department has pursued a second approach to botnets: the use of seizures, forfeitures, restraining orders, and other civil and criminal legal process to dismantle criminal infrastructure. In cases such as Gameover Zeus, Blackshades, and a 2011 case involving the Coreflood botnet, the Department used these legal authorities, with judicial authorization and oversight, to wrest domains and servers from cyber criminals' control, prevent infected computers from communicating with the criminals' command and control infrastructure, and liberate hundreds of thousands of computers.

In May of this year, CCIPS, the United States Attorney for the Western District of Pennsylvania, and the FBI, in partnership with other federal and private-sector organizations, disrupted a botnet that illustrates the magnitude of the threat. Before it was disrupted, the Gameover Zeus botnet was widely regarded as the most sophisticated criminal botnet in existence. One common and sinister method used by Gameover Zeus was a "man-in-the-middle" attack, in which victims trying to access websites for purposes such as online banking were tricked into entering login credentials, passwords, and other personal information that communicated that information to criminals at the same time they were passed onto their destination. With the click of a mouse, the botmasters then used this stolen information to rob small businesses, hospitals, and other victims, transferring funds from victim accounts to their own accounts. From September 2011 through May 2014, Gameover Zeus infected between 500,000 and 1 million computers and caused more than $100 million in financial losses. In one case alone, nearly $7 million was fraudulently transferred from a regional bank. Other victims included an Indian tribe, a corporation operating assisted living facilities, and a composite materials company.

Gameover Zeus was also used to install Cryptolocker—a type of malware known as "ransomware"—on infected computers. Cryptolocker enabled cyber criminals to encrypt key files on the infected computers. Victims then saw a splash screen on their computer monitors, telling them that their files were encrypted and that they had three days to pay a ransom, usually between about $300 and $750, if they wanted to receive the decryption key. The victims found themselves confronted with the loss of critical data, such as family photographs or essential business records. In the short period between its emergence in mid-to-late 2013 and the disruption action in May 2014, the Cryptolocker malware infected more than 260,000 computers worldwide. Many victims simply paid the ransom that was demanded of them. These victims included the police department of Swansea, Massachusetts, which paid approximately $750 to recover its investigative files and arrest photographs. Others refused to pay the ransom and tried to defeat the malware. A Pittsburgh insurance company was eventually able to restore data from a backup, but only after incurring an estimated $70,000 in losses and sending employees home during remediation. A Florida company lost critical files, which resulted in an

estimated $30,000 in loss. And a North Carolina business, whose main files and backup were both encrypted, lost its critical files despite engaging a computer forensics firm to try to restore its access. That company has lost about $80,000, and the owner told the FBI that he may have to lay off employees as a result.

Disrupting and mitigating these threats requires determination, technical skill, and creativity. In response to previous efforts to disable botnets, the creators of the Gameover Zeus botnet designed a novel and resilient structure, including three distinct layers of command and control infrastructure that rendered the botnet particularly difficult to overcome. The Department's successful disruption began with a complex international investigation conducted in close partnership with the private sector. It continued through the Department's use of an inventive combination of criminal and civil legal process to obtain authorization to stop infected computers from communicating with each other and with other servers around the world. The operation simultaneously targeted all three command and control layers of Gameover Zeus, and stopped Cryptolocker from encrypting additional computers. The investigation and court-authorized operation ultimately permitted the team not only to identify and charge one of the leading perpetrators, but also to stop the botnet and ransomware from functioning. Moreover, the FBI was able to identify victims and, working with the Department of Homeland Security, foreign governments, and private-sector partners, facilitate the removal of malware from many victim computers. Disclosure to, and engagement with, the public was critical to this remediation effort. DOJ and DHS released a technical alert to raise awareness of the botnet and lay out resources available to help affected entities minimize the damage.

I cannot emphasize enough the importance to our anti-botnet efforts of the cooperation of foreign governments and our U.S. government and private-sector partners. In every case I have mentioned, foreign law enforcement services took carefully coordinated steps worldwide to disrupt the scheme and investigate the offenders, by seizing servers, interviewing subjects, making arrests, and providing evidence to U.S. investigators. The Department has devoted substantial resources to building the relationships with foreign law enforcement partners that made these coordinated efforts possible. The FBI, for example, maintains more than 60 legal attachés in embassies

around the world. The Criminal Division's Office of International Affairs provides immeasurable legal support to evidence collection and extradition. CCIPS conducts training programs to help our allies develop cyber laws, and our federal law enforcement partners work to improve investigative capacities. Due in large part to our extensive engagement with, and training of, foreign criminal prosecutors and law enforcement officers, we have developed highly productive international relationships that are critical to the success of our investigations and prosecutions.

One factor has harmed our relationships with foreign law enforcement agencies, however: our inability to rapidly respond to foreign requests for electronic evidence located in the United States. Our capacity to do so simply has not kept up with the demand. The President's budget for fiscal year 2015 requests additional prosecutors, together with support personnel, to be assigned to the Criminal Division and to United States Attorneys' Offices to streamline and facilitate the process of handling Mutual Legal Assistance Treaty (MLAT) requests between the United States and its law enforcement partners around the world. The FY 2015 request, if granted, will enable the Department to meet the Administration's commitment to cut MLAT response times in half by the end of 2015 and reduce the amount of time to comply with legally sufficient requests to a matter of weeks, as well as to strengthen the Department's relationships with our foreign law enforcement partners, particularly in regard to cyber investigations.

Like the value of our relationships with foreign law enforcement, the expertise, dedication, and cooperation of private-sector entities have been crucial to our success. For example, security researchers develop highly specialized expertise in particular botnets and help develop countermeasures that match the botnets in sophistication. Their technical contributions are truly astounding. Private-sector companies also serve a critical function when they notify victims that their computers have been compromised and supply the tools needed to clean up those computers. Because the vast majority of the internet is owned and operated by the private sector, we simply could not conduct anti-botnet operations without the firm commitment of network service providers to protecting their customers.

**Proposals to Enhance Anti-Botnet and other Cyber Capabilities**

The Department is dedicated to using innovative means to target increasingly complex botnet threats as they emerge. But there is a lot more work to be done, and we ask that Congress continue its support of these critical efforts. I would like to highlight some of the Department's legislative and budgetary proposals that would enhance our ability to identify botnet perpetrators, bring them to justice, disrupt their criminal enterprises, and protect the security, privacy, and property of Americans.

Department prosecutors rely on criminal statutes to bring cyber criminals to justice and to halt their criminal activity. One of the most important of these laws is the Computer Fraud and Abuse Act, also called the "CFAA." The CFAA is the primary Federal law against hacking. It protects the public against criminals who hack into computers to steal information, install malware, and delete files. The CFAA, in short, reflects our shared baseline expectation that people are entitled to have control over their own computers and are entitled to trust that the information they store in their computers remains safe.

The CFAA was first enacted in 1986, at a time when the problem of cybercrime was still in its infancy. Over the years, a series of measured, modest changes have been made to the CFAA to reflect new technologies and means of committing crimes and to equip law enforcement with tools to respond to changing threats. But the CFAA has not been amended since 2008, and the intervening years have again created the need for the enactment of modest, incremental changes. The Administration's May 2011 legislative proposal proposed revisions to keep Federal criminal law up to date. We continue to support changes like these that will keep up with rapidly evolving technologies and uses.

In addition, our investigations of those responsible for creating and using botnets and our efforts to disrupt botnets rely substantially on the availability of legal investigative process pursuant to the Electronic Communications Privacy Act ("ECPA"). ECPA governs the Department's access to much of the electronic evidence necessary to investigate botnets, hold perpetrators accountable, and develop methods to free unsuspecting victims. It is essential to the success of our anti-botnet initiatives, and to

our efforts against cybercrime as a whole, that the government maintain the ability to obtain relevant electronic evidence in a responsible, timely and effective manner.

***Selling Access to Botnets***

In the years since 2011, experience has revealed additional shortcomings in the criminal law. For example, while botnets can be used for various nefarious purposes, including theft of personal or financial information, the dissemination of spam, and DDOS attacks, the creators and operators of botnets do not always commit those crimes themselves. Frequently they sell, or even rent, access to the infected computers to others. The CFAA does not clearly cover such trafficking in access to botnets, even though trafficking in infected computers is clearly illegitimate, and can be essential to furthering other criminal activity. We thus propose that section 1030(a)(6) of the CFAA be amended to cover trafficking in access to botnets.

In addition, section 1030(a)(6) presently requires proof of an intent to commit a financial fraud. Such intent is often difficult—if not impossible—to prove because the traffickers of unauthorized access to computers often have a wrongful purpose other than the commission of fraud. Indeed, sometimes they may not know or care why their customers are seeking unauthorized access to other people's computers. This reality has made it more challenging in many cases for our prosecutors to identify a provable offense, even when we can establish beyond a reasonable doubt that individuals are selling access to thousands of infected computers. We therefore recommend that Congress amend section 1030(a)(6) of the CFAA to address this shortcoming. .

***Enhancing Judicial Authority to Disrupt Botnets and other Malware***

Under current law, two federal statutes, 18 U.S.C. §§ 1345 & 2521, give the Attorney General the authority to bring civil suits against defendants who are engaged in or "about to" engage in wiretapping or the violation of specified fraud crimes.[1] *See* 18

[1] The specified fraud crimes include those listed in Title 18, Chapter 65 (mail fraud, wire fraud, bank fraud, and health care fraud), section 287 (fraudulent claims), section 1001

U.S.C. §§ 1345(a), 2521. The court is then empowered to enjoin the violation, "or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought." 18 U.S.C. § 1345(b); *see also* 18 U.S.C. § 2521. Due process is ensured by the balancing test applied by the court to determine whether an injunction is appropriate and by the applicable Federal Rules of Civil Procedure.

These authorities played a prominent role in the Department's successful disruptions of the Coreflood botnet in 2011 and the Gameover Zeus botnet in 2014. These botnets collected online financial account information as it was transmitted from infected computers, thus violating the Wiretap Act, and the criminals used their access to steal from victims' bank accounts, which constitutes wire and bank fraud. Because these botnets violated statutes against fraud and wiretapping, courts were authorized to issue orders under sections 1345 and 2521 that permitted the United States to take corrective action necessary to disrupt them.

No analogous statutory authority exists, however, for violations of the CFAA that do not involve fraud or the interception of communications. As a result, the law does not provide a clear statutory remedy for the government to use against botnets or other types of malware that criminals employ for other purposes, such as DDOS attacks. Similar to frauds and illegal wiretaps, these types of computer hacking—which are prohibited under section 1030—present serious threats that can cause severe and continuing damage as long as they persist. We would welcome the opportunity to work with the Committee to ensure that the law appropriately addresses this challenge.

***Criminalizing the Overseas Sale of Stolen U.S. Financial Information***

To ensure that we can take action when cyber criminals acting overseas steal data from U.S. financial institutions, we also recommend a modification to what is known as the access device fraud statute, 18 U.S.C. § 1029. One of the most common motivations for criminal hacking is to obtain financial information. The access device fraud statute

---

(false statements to government officers), and conspiracies to commit these offenses. *See* 18 U.S.C. § 1345(a)(1).

proscribes the unlawful possession and use of "access devices," such as credit card numbers and devices such as credit card embossing machines. Not only do lone individuals commit this crime, but, more and more, organized criminal enterprises have formed to commit such intrusions and to exploit the stolen data through fraud.

The Department of Justice recommends that the statute be expanded to enable prosecution of offenders based in foreign countries who directly and significantly harm United States financial institutions and citizens. Currently, a criminal who trades in credit card information issued by a U.S. financial institution, but who otherwise does not take one of certain enumerated actions within the jurisdiction of the United States, cannot be prosecuted under section 1029(a)(3). Such scenarios are not merely hypothetical. United States law enforcement agencies have identified foreign-based individuals selling vast quantities of credit card numbers issued by U.S. financial institutions where there is no evidence that those criminals took a specific step within the United States to traffic in the data. The United States has a compelling interest in prosecuting such individuals given the harm to U.S. financial institutions and American citizens, and the statute should be revised to cover this sort of criminal conduct.

***Enhancing Resources to Combat Botnets and other Cyber Threats***

This last May, the Department submitted to Congress a multiyear cyber threat strategic plan. The report identified six strategic initiatives:

- Ensure that all of DOJ's investigators and attorneys receive training on cybercrime and digital evidence.
- Increase the number of digital forensic experts and the capacity of available digital forensic hardware.
- Enhance DOJ's expertise in addressing complex cyber threats.
- Improve information sharing efforts with the private sector.
- Expand and strengthen relationships with international law enforcement and criminal justice partners on cybercrime to enhance the sharing of electronic evidence.

- Enhance capacity in the area of cyber policy development and associated legislative work.

The plan repeatedly highlighted the disruption of botnets as a key priority. In order to properly address the threat of botnets and other cybercrimes, components across the Department, such as CCIPS, NSD, and the United States Attorneys' Offices, need additional resources.

The Department confronts an increasing demand for its anti-cybercrime expertise. CCIPS, for example, conducts its own prosecutions, receives requests for consultation of its attorneys or digital investigative analysts, provides advice to law enforcement agencies, engages with the private sector regarding the implementation of investigative authorities, and delivers domesic and international training. This escalation in activity is due in part to the ever-expanding nature of the cyber threat. Prosecutorial needs have also resulted from the expansion of investigative efforts, as the FBI has increased its resources in support of the Next Generation Cyber Initiative to enhance the technical capabilities of investigative personnel, increase cyber investigations, and improve cyber collection and analysis

The Department would like to thank the Senate for its continued support of our national security-related cyber efforts, including fiscal year 2014 funding increases that are allowing the Department to hire more than a dozen additional national security cyber professionals, including attorneys, in furtherance of our efforts to combat cyber-based terrorism and nation state-sponsored cyber intrusions. Just this summer, thanks in part to your support, those efforts yielded historic results, with the indictment of five members of the Chinese military on charges of cyber-based economic espionage. Cyber threats to the national security continue to evolve, and to outpace our growth, but the Department is committed to following the facts and evidence where they lead to detect, deter, and disrupt them. We look forward to continuing to work with you on this front.

**Conclusion**

I very much appreciate the opportunity to discuss with you the Department's efforts to combat botnets. We are committed to using all available tools to disrupt these

networks and bring perpetrators to justice, as we seek to protect Americans' security, privacy, and property.

Thank you for the opportunity to discuss the Department's work in this area, and I look forward to answering any questions you might have.