Introduction to Cyber-Crime and Cyber-Terrorism

Speaker: Michael Bosworth, Special Counsel to the Director of the Federal Bureau of Investigation

What are some of the major types of cyber-crime and cyber-terrorism? How do cyber-criminals and cyber-terrorists inflict harm on others? How is the United States government combating cyber-crime and cyber-terror, and how is it guarding against the risk of a catastrophic cyber-terror attack? These are some of the important issues discussed during Michael Bosworth's lecture.

Mr. Bosworth, a former Assistant United States Attorney for the Southern District of New York ("SDNY"), served as a supervisor for the SDNY's unit investigating and prosecuting cyber-crime before joining the Federal Bureau of Investigation ("FBI"). He used his experiences with the SDNY and the FBI to help the audience understand how cyber-crime works, and how the United States government is fighting it and attempting to strengthen the nation's defenses against cyber-crime and cyber-terrorism.

Mr. Bosworth began his lecture by explaining that, in the words of Director James Comey, cyber-crime is not a "thing," it is a "vector"—a means through which others can harm our businesses, our governments and our personal lives. Criminals and terrorists are using this vector because people are spending increasing amounts of their lives in cyberspace. Mr. Bosworth added that, as Director Comey has stated, the change in the use of vectors "is not something we've seen since the vector change of the early 20th century, when the combination of automobiles and asphalt made it possible for John Dillinger to commit multiple offenses over vast areas in a short period of time."

Mr. Bosworth stated that the cyber-vector takes advantage of the structure of the Internet, which enables computers around the world to communicate with each other via Internet Service Providers ("ISPs"). Computers or computer systems connected to the Internet through ISPs are assigned unique Internet Protocol ("IP") addresses, which may be dynamic (changing over time) or static. Computers communicate over the Internet by contacting other computers, using the IP addresses of those other computers to identify them. Information is then exchanged between computers, identified by their IP addresses, via packets of information that are sent over the Internet between the two devices.

Cyber-criminals and cyber-terrorists differ only in their motives, Mr. Bosworth noted. Both use the open structure of the Internet and similar methods to inflict harm. Mr. Bosworth then described several methods used by both cyber-criminals and cyber-terrorists to harm others. One basic method Mr. Bosworth described is known as "hacking": breaking and entering into a computer system to steal information, spy on the system user or damage the system. The motives of hackers are diverse. Some hackers are fraudsters who are attempting to steal identities or other valuable information for financial gain. Other hackers are state actors who are seeking to gain intelligence on, or to harm, their adversaries. Others are politically-motivated individuals or organizations seeking to make a point.

Mr. Bosworth then discussed another method of cyber-attack: viruses or malware. These are harmful software programs and files that are implanted onto computers, enabling bad actors to damage the infected computers, or to use the infected computers to steal information and harm others. Among other things, explained Mr. Bosworth, infected computers can be employed by bad actors to conduct what is known as Distributed Denial of Service ("DDOS") attacks on intended victims' websites. Mr. Bosworth described how DDOS attackers inflict harm by directing numerous computers under their control to visit a particular website simultaneously, in an attempt to overwhelm the website and force it offline or render it useless. DDOS attacks can be used to make a political point or to mask more harmful hacking occurring at the same time as a DDOS attack.

Other cyber-crime methods summarized by Mr. Bosworth include the publication on the Internet of a victim's private information, a practice known as "doxing," and the use of cyber-tools to generate false reports of emergencies, a practice known as "swatting."

Mr. Bosworth then discussed some of the most serious types of cyber-crimes, including intellectual property theft from governments and businesses, child exploitation and extortion through what is known as "ransomware," which he stated had increased by more than 500 percent over the past year.

Mr. Bosworth cited evidence that cyber-crime targets everyone. He explained that government was a big target because it possesses vast amounts of information, including state secrets and financial information. He cited as an example a recent attack on the South Carolina Department of Revenue in which 3.6 million citizens' Social Security numbers and almost 400,000 debit and credit card numbers were stolen. In addition, businesses of all sizes were targeted.

Mr. Bosworth then addressed efforts by the law enforcement community and the private sector to respond to the growing threat. He described efforts by federal agencies to coordinate efforts and form task forces with state and local authorities to ensure cooperative and effective responses to cyber-crime or cyber-terror incidents. As Mr. Bosworth explained, the FBI and other federal agencies are dedicating significant resources to protecting against and responding to a potential catastrophic cyber-attack by foreign actors, including foreign governments or terrorist groups. He described a 2012 Al-Qaeda video, for example, that "called for electronic jihad against the United States and made a point of equating the vulnerabilities in our nation's cyber-infrastructure with the kind of flaws in aviation security pre-9/11." Mr. Bosworth also highlighted the threat that sophisticated foreign state actors engaged in cyber-attacks posed to the nation. He cited as an example the recent indictment of five members of the Chinese military for hacking and economic espionage offenses that they committed against some of the nation's largest companies over a period of years. He explained that this indictment "was the first time that criminal cyber-charges have been filed against state actors," but "it won't be the last."

Mr. Bosworth informed the audience of significant prosecutions of cyber-crime or cyber-terrorism that were occurring in each of the Second Circuit's judicial districts. He discussed the SDNY's unmasking and prosecution of the creator of the Silk Road online marketplace for illegal drugs and other contraband, which showed cyber-criminals that government has the ability to

track and stop harmful Internet activity that others might have thought was untraceable. The Eastern District of New York, as Mr. Bosworth explained, uncovered and is prosecuting one of the largest coordinated heists of ATM machines in history, enabled by cyber-crime. The District of Connecticut seized and took down servers that controlled a "botnet," a network of infected computers that were used for DDOS attacks and other harmful cyber-activity, representing the first-ever seizure of its kind. The District of Vermont has led the way in prosecutions of individuals who engage in cyber-crime to facilitate child exploitation, while the Northern and Western Districts of New York have prosecuted novel and significant cases in which cyber-criminals stole valuable intellectual property or marketed counterfeit goods over the Internet.

Mr. Bosworth concluded by discussing the challenges ahead as the nation addresses the growing threat. He stated that while government has made good strides, many questions remained, including what role government should play in coordinating responses to cyber-crime and how to balance cyber-security with privacy interests. While there is a way to protect the cyber-sphere and the rights we cherish, Mr. Bosworth noted, "how to do it at all levels with our international partners," some of which "may have different norms and standards," was a challenge that needed to be thought through.

Mr. Bosworth then turned to the role of the private sector and the public in addressing the growing threat. He explained that private sector awareness, coordination and cooperation were critical to combating the cyber-threat, because "all it takes at a company is one bad employee" to compromise network security and enable cyber-criminals to access the company's network. Mr. Bosworth recommended greater outreach and education efforts to raise awareness of the need for businesses and individuals to practice greater cyber-security, citing recent statistics that 30 percent of people who go online do not even think about cyber-security and that 60 percent of the members of corporate boards of directors either do not know about their company's cyber-security policy or say that their company does not have one.

Mr. Bosworth concluded by describing several legal and policy challenges posed by the cyber-threat that have yet to be resolved, including Fourth Amendment issues and challenges associated with the potential use of offensive cyber-weapons.