



The Committee on Energy and Commerce

Internal Memorandum

February 6, 2012

To: Members and Staff, Subcommittee on Communications and Technology

From: Majority Committee Staff

Subject: Hearing on “Cybersecurity: Threats to Communications Networks and Private-Sector Responses”

The Subcommittee will hold a hearing Wednesday, February 8, 2012, at 9:30 a.m. in 2322 Rayburn House Office Building entitled “Cybersecurity: Threats to Communications Networks and Private-Sector Responses.” The hearing will examine threats to America’s communications networks, what the private sector is doing to address those threats, what the private sector could be doing better, and what role the federal government should play. One panel of witnesses will testify.

I. Witnesses

Larry Clinton
President and Chief Executive Officer
Internet Security Alliance

Bill Conner
President and Chief Executive Officer
Entrust

Robert Dix
Vice President of Government Affairs
& Critical Infrastructure Protection
Juniper Networks

James A. Lewis
Director and Senior Fellow,
Technology and Public Policy Program
Center for Strategic
and International Studies

Phyllis Schneck
Vice President and Chief Technology
Officer, Global Public Sector
McAfee Inc.

Additional witnesses may be called at the discretion of the Majority.

II. BACKGROUND

Americans are more interconnected today than ever before. Communications networks empower our citizens to share information across the country in the blink of an eye. The Internet

has become an essential component of our economy, and now also supports vital infrastructure such as power distribution and our transportation networks, as well as services such as medicine, finance, and education.

Emerging Vulnerabilities.—Our growing interdependence has also exposed the vulnerabilities of our communications networks, as bad actors exploit the open protocols of the Internet for financial, political, and military gain. While the general public has become aware of Trojan horses, spyware, viruses and other malware that affects computers, the vulnerabilities of communications networks are even more complex and cyberattacks are becoming more prevalent and more sophisticated. When hundreds or thousands of computers are infected by the same malicious software, the bad actors behind that software can transform that collection of computers into a botnet. With a botnet, a hacker has a powerful tool to take down websites through distributed denial-of-service attacks, to hack into protected networks through brute force, and to distribute illegal and unwanted content. With the capability of simultaneously transmitting large amounts of data from thousands of points at one time, botnets possess the capacity to bring down communications networks, at least where those networks are capacity constrained. Even without a botnet, the lightning-fast speeds and global nature of modern networks means that bad actors have more opportunities to exploit weaknesses in network defenses than ever before.

The physical components of communications networks are another potential vulnerability. With trade becoming increasingly global and supply chains increasingly complex, the opportunities for misfeasance and malfeasance within the supply chain network has dramatically increased. Communications network providers purchase networking equipment from manufacturers who in turn outsource the production of chipsets, processors, and other components to others. Weakness can occur at any point in this supply chain, and the costs of overseeing each and every stage of production may be prohibitively expensive. The increasing reliance on wireless communications may create another vulnerability as consumer wireless devices become an additional access point into the network.

The Internet's architecture may itself create vulnerabilities. For example, in 2008, network researcher Dan Kaminsky discovered a flaw in the implementation of the Internet's Domain Name System (DNS), the system that translates human-readable domain names into the machine-readable IP addresses. A bad actor could exploit this flaw to perform a man-in-the-middle attack on a consumer—with such an attack, a consumer thinks his username, password, and financial information are securely transmitted to his bank when in fact the bad actor sits in between the consumer and his bank, able to see all the information transmitted between the two. The discovery of this vulnerability prompted the development of DNS Security Extensions (DNSSEC) as means to prevent such attacks, although DNSSEC's effectiveness depends on its widespread adoption by ISPs and websites. Similarly, the evolution to the next generation of IP addresses, known as IPv6, and the continued expansion of domain names may create new vulnerabilities and obstacles to effective law enforcement.

The Continuing Cyberthreat.—The evidence of the last few years has shown that the threat to communications networks, the threat of persistent cyberattacks for purposes of crime, espionage, agitation, and even warfare is real. Attempted cyberattacks on federal government networks have increased year after year with a double-digit rate of growth. In October 2010, the discovery of the Stuxnet virus demonstrated the ability of a well-placed virus to disable critical

infrastructure—in that case nuclear facilities. According to Symantec’s 2011 State of Security report, 71 percent of companies experienced some form of cyberattack in the past year; and according to a joint study by Verizon and the U.S. Secret Service, there was a comparatively huge increase in the number of external cyberattacks against American business and government.

The sources and motivations behind cyberthreats are numerous. Perhaps the most common are cybercrimes, like identity theft, credit card fraud, and online piracy. Bad actors can exploit malware like the Zeus virus to trick consumers into authorizing fraudulent bank transfers. Online forums foster a black market in stolen credit card and social security numbers, which are often traded in blocks of one thousand or more. The accessibility of private information about individuals online has made companies and individuals more susceptible to social engineering—the practice of tricking individuals into revealing sensitive information using information already known about the individual. Private estimates of the cost of cybercrime range in the billions of dollars each year, a continuing tax on online commerce and innovation.

Cyberagitation is a newer form of cyberthreat. With cyberagitation, the motivation of the cyberattack is often political, not financial, as seen most prominently this past year with the attacks by “Anonymous” on financial organizations in response to the WikiLeaks controversy. Just last month, “Anonymous” launched cyberattacks on the U.S. government, the Motion Picture Association of America, and several other groups in response to anti-digital piracy efforts. Aside from the damage the cyberagitation may do to businesses and our virtual infrastructure, the methods used by cyberagitators could be used to carry out cyberterrorism if done on a massive scale or aimed to incite panic and confusion. What is more, cyberagitation may feed cybercrime—cyberagitators may, for example, purchase access to a botnet or malware in order to carry out their political ends.

Cyberespionage remains a continuing threat to both commercial and national interests. Bad actors, either of their own accord or sponsored by hostile foreign states, may view cyberspace as a new domain to infiltrate American corporations to steal intellectual property and trade secrets. Those same actors may see cyberspace as a cheaper alternative to traditional spycraft. In the 2008 presidential election, for example, bad actors breached the computer networks of both major party candidates. Perhaps even more concerning, classified information at the Department of Defense was breached in 2008 via a virus hidden on a flash drive—it took the Department nearly 14 months to remedy the situation.

Finally, cyberwarfare is most commonly seen in the threats to critical infrastructure that could occur online. A major disruption to a large bank could trigger another financial crisis; a cyberattack on the core components of the communications network could disrupt all Internet-enabled communications including interconnected VoIP service. And such disruptions need not be based online—supply chain vulnerabilities, terrorist attacks, or even a natural disaster could compromise our communications networks. Although the United States has not experienced a catastrophic Internet failure, there have been online and physical incidents that caused localized and regional disruptions.