CSIS COMMENTARY
Center for Strategic and International Studies ■ Washington D.C.

Cyber Attacks Explained

By James A. Lewis, Director, Technology and Public Policy Program

June 15, 2007

The small Baltic country of Estonia was the target of a series of cyber attacks in May 2007. These were “denial of service” attacks, where an attacker floods the target network with bogus messages, causing its servers (computers that serve as a hub in a network) to slow or shut down.

The attacks caused grave concern among NATO officials, in large part because, at first, Russia was blamed. This attribution was wrong, in the sense that the attacks were not launched from Russian government computers. Like many things in cyberspace, it was difficult to tell who was at the other end of the Internet. Attribution in the Estonia case was made even harder by the use of “botnets.” Botnets—short for robot networks—are the big new thing in cyber crime. A cyber criminal takes remote control of a computer by surreptitiously loading software on it. Most consumers don’t know that their computers have been compromised. Some botnets are huge, using tens of thousands of computers around the world. Having these gigantic criminal networks simultaneously send thousands of messages every minute overburdened Estonian servers and caused them to crash.

Attacks, crashes, robots—sounds like a war—and many commentators saw this as the first “cyber war.” This was, of course, completely erroneous. Botnets are used all the time—they are the source of most spam—and are nothing special for cyber crime. This was not the first time that a government had seen foreign protestors attack servers and Web sites with botnets, hacks, and graffiti. China, Israel, India, Pakistan, and the United States have seen similar attacks, albeit on a smaller scale.

Nor was the Russian government inept enough to leave a trail of e-mails leading back to the Kremlin. Though one Russian government computer was used in the attacks, that was because it had been captured and controlled in a botnet. This does not prove that the Russian government is innocent. Russian government agents could have used chat rooms and e-mail to incite patriotic Russian hackers and cyber criminals to batter Estonian networks as punishment for daring to move a statue of a Soviet soldier. Estonian police arrested one such hacker, an ethnic Russian and Estonian citizen. Again, this is standard stuff—intelligence agents inciting a protest or riot. The attacks on Estonia are better seen as cyber protests than as war, like demonstrators lying down in a capital’s streets to block traffic (only without the risk of being run over).

On the Estonian end, there was turmoil, but not collapse or terror. Since independence, Estonia has been a leader in “e-government,” or service using the Internet. This made them more vulnerable, but it also made them prepared to work in cyberspace. The Estonians responded calmly and were able to restore key services to minimal levels within a few days. Parliament, the president’s office, the police, and the foreign ministry were the primary targets, along with Estonia’s largest bank. Some took the simple response of blocking messages coming from other countries—this reduced the attacks, although it kept Estonians on travel from accessing their bank accounts.

Denial of service is not the most dangerous form of attack. A serious attack would not have been as noisy but would have penetrated Estonian computers and databases and scrambled or erased the data. Making health records and bank accounts disappear would have been far more disruptive. The United States faces this kind of attack, and it is vulnerable—U.S. government networks are routinely penetrated. We have many more networks than Estonia. Many are secure. Others are not. Unfortunately, we do not know which is which. All will be made clear when it is our turn to be attacked, but it might be better to find and fix our vulnerable systems before this occurs.

Center for Strategic and International Studies
1800 K Street N.W. ■ Washington D.C. 20006 ■ Tel: (202) 887-0200 ■ Fax: (202) 775-3199 ■ Web: www.csis.org