ligence, stated that if even a single large American bank were successfully attacked, it would have an order-of-magnitude greater impact on the global economy than the World Trade Center attacks, and that the ability to threaten the U.S. money supply is the financial equivalent of a nuclear weapon.

Many security experts believe that U.S. cybersecurity is not well-organized. Several different agencies, including the Pentagon and the National Security Agency (NSA), have their sights on being the leading agency in the ongoing efforts to combat cyberwarfare. The first headquarters designed to coordinate government cybersecurity efforts, called Cybercom, was activated in May 2010 in the hope of resolving this organizational tangle. In May 2011 President Barack Obama signed executive orders weaving cyber capabilities into U.S. military strategy, but these capabilities are still evolving. Will the United States and other nations be ready when the next Stuxnet appears?

Sources: Brian Royer, "Stuxnet, The Nation's Power Grid, And The Law Of Unintended Consequences, *Dark Reading*, March 12, 2012; Thomas Erdbrink, "Iran Confirms Attack by Virus That Collects Information," *The New York Times*, May 29, 2012; Nicole Perlroth, "Virus Infects Computers Across Middle East," *The New York Times*, May 28, 2012; Thom Shanker and Elisabeth Bumiller, "After Suffering Damaging Cyberattack, the Pentagon Takes Defensive Action," *The New York Times*, July 15, 2011; Robert Lcos, "Secure Best Practices No Proof Against Stuxnet," CSO, March 3, 2011; Lolita C. Baldor, "Pentagon Gets Cyberwar Guidelines," Associated Press, June 22, 2011; William J. Broad, John Markoff, and David E. Sanger, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay," *The New York Times*, January 15, 2011; George V. Hulme, "SCADA Insecurity" and Michael S. Mimoso, "Cyberspace Has Gone Offensive," *Information Security's Essential Guide to Threat Management* (June 14, 2011); and Sibhan Gorman and Julian A. Barnes, "Cyber Combat: Act of War," *The Wall Street Journal*, May 31, 2011.

CASE STUDY QUESTIONS

1. Is cyberwarfare a serious problem? Why or why not?
2. Assess the management, organization, and technology factors that have created this problem.
3. What makes Stuxnet different from other cyberwarfare attacks? How serious a threat is this technology?
4. What solutions for have been proposed for this problem? Do you think they will be effective? Why or why not?

millions of paths would require thousands of years. Even with rigorous testing, you would not know for sure that a piece of software was dependable until the product proved itself after much operational use.

Flaws in commercial software not only impede performance but also create security vulnerabilities that open networks to intruders. Each year security firms identify thousands of software vulnerabilities in Internet and PC software. For instance, in 2011, Symantec identified 351 browser vulnerabilities: 70 in Chrome, about 50 in Safari and Firefox, and 50 in Internet Explorer. Some of these vulnerabilities were critical (Symantec, 2012).

To correct software flaws once they are identified, the software vendor creates small pieces of software called **patches** to repair the flaws without disturbing the proper operation of the software. An example is Microsoft's Windows 7 Service Pack 1, which features security, performance, and stability updates for Windows 7. It is up to users of the software to track these vulnerabilities, test, and apply all patches. This process is called *patch management*.

Because a company's IT infrastructure is typically laden with multiple business applications, operating system installations, and other system services, maintaining patches on all devices and services used by a company is often time-consuming and costly. Malware is being created so rapidly that companies have very