Cyberwar:

MAD 2.0

From the earliest of days, humans have warred against each other, with the tools of warfare evolving over time from sticks and stones, to arrows and spears, to artillery and bombs. Physical warfare and weaponry are familiar and readily recognizable. But today, there is also another type of warfare that is becoming increasingly common, a type that is conducted by a hidden army of hackers wielding weaponry that consists of algorithms and computer code. Cyberspace has become a new battlefield, one that often involves other targets, such as financial systems and communications networks, as collateral objectives.

© Rafal Olechowski / Fotolia

The phrase "shot heard round the world" is sometimes used to identify the start of a chain of events of historic import, such as the Revolutionary War and World War I. Although certainly not "heard" in the traditional sense, the release of the Stuxnet worm can be viewed as the first shot in a cyberwar between the United States and Iran that is still ongoing today. Thought to have been created by a secret joint U.S./Israeli task force that began while President George W. Bush was in office, Stuxnet was first discovered in June 2010. Stuxnet was designed to disable the software and computers that controlled the centrifuges in Iran's uranium enrichment process, and reportedly delayed Iran's ability to make nuclear arms for as many as five years. Stuxnet is the first cyberweapon believed to have caused significant physical damage to its target.

Another piece of malware, the Duqu worm, emerged in September 2011. Believed to have been created by Stuxnet's developers, Duqu was designed to collect passwords, take desktop screenshots to monitor users' actions, and pilfer various kinds of documents. It is believed that Duqu was intended to further gauge the status of Iran's nuclear program. In another strike against Iran, in April 2012, a Trojan named Flame hit computers in the Iranian Oil Ministry and the National Iranian Oil Company. Flame used a fraudulent digital certificate and spread via USB flash drives and other methods. It could sniff network traffic and record audio, screenshots, Skype conversations, and keystrokes, as well as download information from other devices via Bluetooth. Flame was suspected of pursuing multiple Iranian objectives including key oil export hubs. It shared some key characteristics with both Stuxnet and Duqu.

In August 2012, security experts Kaspersky Labs announced the detection of another cyberwarfare tool. Called Gauss, it was likely used to "follow the money" in Middle

Eastern banking transactions. With an online banking module, and laden with encrypted malicious code, the Trojan was designed to collect the banking credentials of patrons of multiple Lebanon-based banks, Citibank, and PayPal. Gauss was built on the same platform as Flame and appears closely related to, and probably built in the same laboratory as, Stuxnet. Added together, the evidence suggests a possible effort by the U.S. government to root out terrorist group funding networks.

Around the same time, a virus named Shamoon appeared. It wiped out the data on 75% (30,000) of the computers on the main computer network of Saudi Arabia's Aramco, in what was termed one of the most destructive private sector attacks to that date. U.S. and Israeli officials felt that this strike at an American ally likely originated from Iran. Not long after, in September 2012, another wave of cyberattacks began, this time focusing on U.S. financial institutions. Thought to be another Iranian effort in response to the U.S.'s previous cyberattacks, the Web sites of a number of banks were knocked offline by distributed denial of service (DDoS) attacks. The severity of the attacks was unprecedented: although no account information was stolen, nor financial gain sought, the financial institutions spent millions dealing with the attacks, which continued through March 2013.

North Korea is another budding cyberwarfare adversary. In March 2013, it was accused of launching its most damaging attack to date on South Korean and American commercial, educational, governmental, and military institutions. Over 30,000 computers at three major South Korean banks and the two largest television broadcasters were affected. Internet banking sites were temporarily blocked, computer screens went blank, ATM machines failed, and commerce was disrupted. The attackers used the Chinese-written Gondad exploit kit to infect PCs with a Trojan that provides an entryway for an attacker to take control of the machine, creating a bot or zombie computer. Once the digital backdoor is created, the controller can deposit a malware payload, in this case, a wiper agent named Dark Seoul. Like Shamoon, Dark Seoul overwrites the master boot record (MBR). U.S. and South Korean security experts at South Korea's newly formed cyber security command center believe North Korea has been assembling and training a cyberwarrior team of thousands. For North Korea, the threat of cyber-retaliation is negligible. Internet access is only now extending beyond a privileged few, businesses are just beginning to adopt online banking, and worthwhile targets are virtually nonexistent.

Although cyberattacks tend to be reported as discrete incidents, they are in fact ongoing activities punctuated by major events. In July 2010, after 10 years of debate, 15 nations including the United States and Russia agreed on a set of recommendations that it was hoped would lead to an international treaty banning computer warfare. It never materialized. Kaspersky Labs founder, Eugene Kaspersky, has continued to advocate for its passage. As Kaspersky points out, cyberweapons are both cheap and potent, and today more than 100 nations have cyberwarfare capabilities and programs. Digital security companies can discover only a fraction of the existing malware. And because telecommunications security necessarily requires inspecting content, democratic nations' attempts to pass cybersecurity legislation usually meets opposition from privacy groups. An international treaty seems the best hope of avoiding MAD 2.0, the modern version of the Cold War era "mutually assured destruction," in which cyber-offensive actions are

SOURCES: "Budget Documents Detail Extent of U.S. Cyberoperations," by David E. Sanger, *New York Times*, August 31, 2013; "Silent War," by Michael Joseph Gross, *Vanity Fair*, July 2013; "U.S. Helps Allies Trying to Battle Iranian Hackers," by Thom Shanker and David E. Sanger, *New York Times*, June 8, 2013; "Cyberattacks Against U.S. Corporations Are on the Rise," by David E. Sanger and Nicole Perlroth, *New York Times*, May 12, 2013; "Cyberattacks Seem Meant to Destroy, Not Just Disrupt," by Nicole Perlroth and David E. Sanger, *New York Times*, March 28, 2013; "Experts: NKorea training teams of 'cyber warriors'," by Rachael King and Youkyung Lee, Associated Press, March 24, 2013; "Why China Is Reading Your Email," by David Feith, *Wall Street Journal*, March 19, 2013; "New Clue in South Korea Cyberattack Reveals Link to Chinese Criminals," by Mark Clayton, *Christian Science Monitor*, March 21, 2013; "Computer Networks in South Korea Are Paralyzed in Cyberattacks," by Choe Sang-Hun, *New York Times*, March 20, 2013; "U.S. Steps Up Alarm Over Cyberattacks," by Siobhan Gorman and Siobhan Hughes, *Wall Street Journal*, March 12, 2013; "As Hacking Against U.S. Rises, Experts Try to Pin Down Motive," by Nicole Perlroth, David E. Sanger, and Michael S. Schmidt, *New York Times*, March 3, 2013; "U.S., China Ties Tested in Cyberspace," by Julian E. Barnes, Siobhan Gorman, and Jeremy Page, *Wall Street Journal*, February 19, 2013; "Obama Order Gives Firms Cyberthreat Information," by Michael S. Schmidt and Nicole Perlroth, *New York Times*, February 12, 2013; "Bank Hacking Was the Work of Iranians, Officials Say," by Nicole Perlroth and Quentin Hardy, *New York Times*, January 8, 2013; "Iran Blamed for Cyberattacks: U.S. Officials Say Iranian Hackers Behind Electronic Assaults on U.S. Banks, Foreign Energy Firms," by Siobhan Gorman and Julian E. Barnes, *Wall Street Journal*, October 12, 2012; "Wiper Malware Could Be Connected to Stuxnet and Duqu, Researchers Say," by Lucian Constantin, *Computerworld*, August 30, 2012; "Analysis Shows Traces of Wiper Malware,

engaged in to destroy aggressors' Internet and other critical infrastructure. In the absence of a treaty, individual nations are building up their arsenals and offensive capabilities. In the United States, that includes the U.S. CyberCommand, commanded by General Keith B. Alexander, the director of the National Security Association. Alexander has spoken publicly of having 40 cyberteams, including 13 focused on offensive operations.

Industrial cyberespionage is closely related to cyberwarfare. Google has been battling Chinese cyberespionage for some time. In January 2010, it was the victim of a phishing attack that enabled China to steal some of its proprietary code. In March 2011, Google blamed the Chinese government for manipulating and disrupting Gmail and Google Talk. In June 2012, Google detected a possible Chinese-sponsored cyberattack against its users' Gmail accounts. Google is not the only company that has been targeted. At least 17 cyberespionage rings based in China have been identified. Their modus operandi is to insert spyware through phishing e-mails. Evidence suggests that it is a well-financed, centralized effort. The seven economic objectives in China's 12th Five-Year Plan (2011–2015) parallel the corporate and research targets. For example, in the biotechnology sector, drug manufacturers Wyeth and Abbott Laboratories and medical device maker Boston Scientific were hit. The computing center for the Food and Drug Administration, where sensitive information including chemical formulas and drug trial documents are stored, also was infiltrated. In the manufacturing sector, the networks of Cypress Semiconductor Corp, Aerospace Corp, and Environmental Systems Research Institute were compromised, possibly yielding China data regarding the manufacture of telecommunication chips, semiconductors, mapping software, and documents pertaining to national security space programs. Small strategic targets such as iBahn, the company that provides Internet access to business travelers at the Marriott and other large hotel chains, have exposed access points into numerous corporate networks as well as access to millions of confidential, and possibly encrypted, e-mail messages.

According to 2012 congressional testimony, over the past 12 years, China has penetrated the networks of at least 760 ISPs, corporations, research universities, and government agencies. Cyberespionage is a far quicker and cheaper path to economic dominance than independent research and development. Representative Mike Rogers estimated that China had garnered $500 billion worth of U.S. corporate assets. The magnitude of this wealth transfer is difficult to quantify because there are so many unknown variables. How quickly can source code, blueprints, chemical formulas, and other data be translated into products that can outcompete?

In response to these revelations, the Obama administration has publicly castigated the Chinese government, naming it the top cyberthreat to U.S. firms. Efforts to pass the Cyber Intelligence Sharing and Protection Act (CISPA), which would allow ISPs and other Internet companies to collect, analyze, and share with the National Security Agency (NSA) and other agencies activities perceived as possible threats, have thus far failed, in part because of concerns about privacy. With CISPA stalled in Congress, President Obama signed an executive order in February 2013 that allows companies associated with the supervision of electrical grids, dams, and financial institutions to voluntarily join a program to receive classified and other cybersecurity threat information previously available only to government contractors, and to develop and implement a cybersecurity framework.

But No Links to Flame," by Dennis Fisher, ThreatPost.com, August 29, 2012; "Nation-backed Surveillance Malware Monitors Middle East Bank Accounts," by Gregg Keizer, *Computerworld*, August 9, 2012; "Google to Warn Users of Possible State-Sponsored Cyber Attacks," by Jason Ryan, ABCNews.com, June, 5, 2012; "Attacks on Iranian Oil industry Led to Flame Malware Find," by Gregg Keizer, *Computerworld*, May 29, 2012; "Virus Linked to State-Sponsored Cyber Espionage," by Doug Isenberg, GigaLaw.com, May 28, 2012; "Iran Probes Cyberattack on Oil Ministry," by Doug Isenberg, GigaLaw.com, April 23, 2012; "How China Steals Our Secrets," by Richard A. Clarke, *New York Times*, April 2, 2012;"China-Based Hacking of 760 Companies Shows Cyber Cold War," by Michael Riley and John Walcott, Bloomberg.com, December 14, 2011.