

Threat.com – Part One: Vulnerabilities of the Cyber Age

Computers have made our lives easier. Instant communication. Encyclopedic knowledge at our fingertips. Paperless financial transactions. Social and professional networking. Online media. Yet, the information age has proven to be a double-edged sword. In addition to the benefits, there are nefarious applications of the same tools and information available to anyone with internet access. Add the intentional and strategic use of cyber attacks by individuals and organizations – even governments, and the scale and scope of the cyber threat seems overwhelming.

The nature of vulnerabilities posed by cyber threats are reviewed here in three broad categories: Targets, Tools, and Transparency.

Targets – Governments will likely always be prime targets of cyber attacks. However, past boundaries between military & civilian entities have been blurred. Today, anyone with a network connection is a potential target, making the damage easier to inflict and with greater consequences. Companies and financial markets are targeted by those who seek to steal information as well as undermine corporate credibility and investor confidence. Attacks on supply chains can have wide-ranging crippling effects. Attacks on individuals, previously focused on phishing schemes and identity theft, have evolved to include the undermining and persecution of political and human rights. “[I]n cyberattacks, the damage can range from the minor to the catastrophic, from slowing computer searches to bringing down a country’s cellular networks, neutralizing its spy satellites, or crashing its electrical grid or its air traffic control systems. It is difficult to know if small attacks could escalate into bigger ones,” according to a recent *New York Times* article. There are many recent disturbing examples:

- Although Marathon Oil, ExxonMobil, and ConocoPhillips systems were breached in 2008, the companies were not aware of the full extent of the attacks until 2009 when the FBI informed them that proprietary information, including e-mail passwords, messages, and other information on exploration and discovery, had been stolen. The attacks are suspected to have originated in China, where the flow of some of the data was detected to be going.
- The Russian government has been strongly suspected to have been behind cyberattacks against Estonia and Georgia. A cyber attack on Estonia in spring 2007 paralyzed the country's entire Internet infrastructure, affecting the websites of Estonian banks, ministries, newspapers, broadcasters, and Parliament. At the worst point, bank cards and mobile-phone networks were temporarily frozen. Estonia was embroiled in a dispute with Russia at the time over the relocation of Soviet-era war memorials in Tallinn. In July 2008, weeks before Russia’s invasion, Georgian websites, including the pages of the president, the parliament, the foreign ministry, news agencies and banks, were attacked by Russian viruses as a supplement to Russia's military operations in South Ossetia.
- In July 2009, the White House, the Defense Department, the New York Stock Exchange, the National Security Agency, NASDAQ, and the Washington Post were all targeted by attackers. The same attackers were responsible for problems with equivalent institutions in South Korea, where several South Korean government websites were either slowed or shut down. South Korean officials suspected North Korea to be behind the attacks.

Tools – The same tools many use for networking, entertainment, and education are also being used as tools for increasing terrorist capabilities. While YouTube is known for entertainment purposes, terror groups post videos glamorizing violent attacks and track who has viewed them. Social networking sites, like Facebook, have helped terrorist organizations recruit new members and disseminate their propaganda. Information on how to build bombs and carry out individual attacks is also readily available online. On the disabling side, oppressive regimes routinely hack into email accounts of individuals and engage in online censorship. The evidence is daunting.

- As early as 2006, about 90 percent of terrorist activity on the Internet consisted of using social networking tools.
- A Hamas-launched interactive website called “Military Academy” offers courses in the production and assembly of explosives, rockets and light aircraft, as well as methods to identify targets. While students can correspond with bomb instructors, courses have strict attendance rules and tests must be taken after each stage.

- In January 2010, Google announced that it and as many as 30 other companies had been targeted or attacked, focusing on the Gmail accounts of Chinese human rights activists.

Transparency - The ubiquity of the internet is only matched by its anonymity. Identifying the source of cyber attacks and, hence, the “enemy” is one of the greatest challenges in cybersecurity. VADM Dennis Blair, U.S. Director of National Intelligence, noted. “We often find persistent, unauthorized, and at times, unattributable presences on exploited networks, the hallmark of an unknown adversary intending to do far more than merely demonstrate skill or mock a vulnerability.” Another cybersecurity challenge is the lack of cyber accountability and standards. Within the U.S., the cyber security infrastructure is strong, yet still evolving. Both domestically and internationally, the development of a common cyber glossary and protocols is still in the early stages and will require significant cooperation. Also, without knowing from where the attacks come or having standard operating procedures, the costs of prevention and protection from cyber attacks will be difficult to ascertain.

The extent of vulnerabilities is even more evident in the numbers. In 2007, there were an estimated 37,000 reported breaches of government and private systems in the United States. There were also nearly 13,000 direct attacks on federal agencies and 80,000 attempted network attacks on Department of Defense systems. As of October 2009, cyber attacks on the federal government are up 300 percent since 2005. A study by the Congressional Research Service estimated the economic impact of cyber attacks on businesses at over \$226 billion a year. The U.S. government spent \$7.9 billion on vendor furnished information security products and services in 2009, an amount expected to increase to \$11.7 billion by 2014.

In a recent speech on internet freedom, Secretary of State Hillary Clinton remarked that, “the spread of information networks is forming a new nervous system for our planet.” As a result, it seems that the greatest challenge of cybersecurity is the prevention of paralysis. The U.S. government and its national security organizations are becoming more focused upon these threats. However, there is much to be done in developing a comprehensive response to these awesome threats and the potentially catastrophic consequences being posed by such deeply penetrating network and cyber attacks.

Sources

- Coalson, Robert, “Behind the Estonia Cyber Attacks”, *Radio Free Europe*, March 6, 2009, http://www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html.
- Coleman, Kevin, “The Cyber Attack Danger” *DefenseTech.org*, October 20, 2008, <http://defensetech.org/2008/10/20/the-cyber-attack-danger/>.
- Clayton, Mark, “US oil industry hit by cyberattacks: Was China involved?” *Christian Science Monitor*, January 25, 2010, <http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved>.
- “Governments hit by cyber attacks,” *BBC News*, July 8, 2009, <http://news.bbc.co.uk/2/hi/technology/8139821.stm>.
- Markoff, John, David E. Sanger, and Thom Shanker, “In Digital Combat, U.S. Finds No Easy Deterrent,” *New York Times*, January 26, 2010, <http://www.nytimes.com/2010/01/26/world/26cyber.html?hp>.
- “Remarks on Internet Freedom by Secretary of State Hillary Rodham Clinton,” January 21, 2010, <http://www.state.gov/secretary/rm/2010/01/135519.htm>.
- Sachoff, Mike, “Federal Spending On Cyber Security to Reach \$11 Billion,” *SecurityProNews.com*, October 26, 2009, <http://www.securitypronews.com/insiderreports/insider/spn-49-20091026FederalSpendingOnCyberSecurityToReach11Billion.html>.
- Sophos, “Security Threat Report: 2010,” <http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf>.
- “US intel chief warns of dire cybersecurity threats,” *Sydney Morning Herald*, February 3, 2010, <http://news.smh.com.au/breaking-news-technology/us-intel-chief-warns-of-dire-cybersecurity-threats-20100203-nbgz.html>.
- Weimann, Gabriel, “Online Training Camps for Terrorists,” *InSite*, Vol. 2 No. 9, November 2009, http://sitemultimedia.org/docs/inSITE_Nov_2009.pdf.
- Weimann, Gabriel, “Terrorism’s New Avatars—Part II; Al Qaeda recruits terrorists on-line, turning the democratic space on its head,” *Epoch Times*, January 18, 2010, <http://www.theepochtimes.com/n2/content/view/28200/>.
- Wentworth, Travis, “You’ve Got Malice; Russian nationalists waged a cyber war against Georgia. Fighting back is virtually impossible,” *Newsweek*, August 23, 2008, <http://www.newsweek.com/id/154965>.