



NATIONAL SECURITY COUNCIL

Cyberwarfare

By Chris Ballesteros

Cyberwarfare, a large-scale, politically-motivated iteration of cyberterrorism, has become a serious threat to America's national security. Politicians have taken legislative action to preempt potential cyberwarfare, while the media and watchdog groups have repeatedly warned of shortcomings in America's cybersecurity efforts. Internet hacking, which is traditionally associated with petty scams and white-collar crime, has become a pressing national security concern over the last few years. A series of difficult dilemmas – differentiating between cyberterrorism and acts of war, balancing political relations with security efforts, and coordinating cybersecurity amongst different agencies— require action on the part of the United States government.

Introduction

Perhaps the most dangerous aspect of cyberwarfare is that it can be instigated by anyone with an advanced knowledge of hacking and access to the Internet. The victimized nation or individual often struggle to determine whether a rogue hacker or another nation was responsible for an attack. At the most basic level, cyberwarfare and cyberterrorism can be reduced to three basic categories: vandalism, espionage, and sabotage. Simply put, vandalism is the defacement of web pages. Vandalism can be as simple as leaving a trademark on the targeted site or serve as a form of political propaganda. Vandalism is generally the least troubling type of cyberattack. It can be reversed with relative ease and does little more than aesthetic damage. Unfortunately, it often invites espionage, which poses a legitimate national security threat. Espionage is the act of illegal information gathering, and affects both private entities and government organizations. The United States is often the target of espionage attempts that aim to garner information on weapons, aircraft, and intelligence. Of the three types of cyberwarfare, sabotage has the most tangible real-world repercussions. A properly placed '**logic bomb**,' a virus downloaded into a server, or compromised orders all have the potential to place American lives, infrastructure, and military efforts in jeopardy.

logic bomb—a piece of computer code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

Explanation of the Problem

Ironically, the first known instance of cyberwarfare was perpetrated by the Central Intelligence Agency (CIA) against the Soviet Union. In response to an attempted Soviet espionage attempt, CIA hackers uploaded a logic bomb into the computer code for an oil pipeline, caus-



ing it to explode. The United States remained at the forefront of cyberwarfare efforts until at least the turn of the century, using hacks to disable Serbian Air Defense systems during the Balkans conflict in the early 1990s. During the 21st century, however, cyberattacks have increasingly focused on NATO-bloc countries and US allies. The most glaring instance of cyberwarfare in the past five years was in 2007, when an unknown hacker—likely a foreign agent—infiltrated highly classified government databases and stole **terabytes** of data. Numerous financial institutions, government agencies, and media organizations were compromised in 2009, again from an unknown source. Examples of international cyberwars include the disruption of Estonian infrastructure following the Bronze Soldier controversy involving the relocation of a Soviet-era war memorial in 2007, Lebanese espionage efforts during the Hezbollah-Israel War in 2006, and the Chinese “Operation Aurora” against Google in 2009. Prominent Internet groups that have been implicated in cyberwarfare include GhostNet, Titan Rain, and Moonlight Maze. The proliferation of cyber attacks and cyberwarfare has led to a series of reactionary measures from the United States and its NATO allies, which seek to curb internet espionage and sabotage. Thus far, the only reactions to cyberwarfare have been electronic—increased security, revamped codes, improved software, etc. However, as states become more involved in concerted cyberwarfare attacks, the responses of victimized nations may become more determined. Russia, China, North Korea, and Iran— all perennial US adversaries—boast robust cyberwarfare forces and have demonstrated a willingness to mobilize them against regional rivals.

terabyte—one trillion bytes of digital information.

Focus of the Debate

The Cyber Defense Center (CDC) is one of the so-called “Centres of Excellence,” which seeks to provide specialized training for particular aspects of NATO operations. The CDC was founded in 2008 as a response to cyberattacks against Estonia stemming from the **Bronze Night** controversy. The Cyber Defense Center focuses on improving information security, encouraging cooperation between NATO allies, developing cyber defenses, and modernizing cyberwarfare policies. The Cyber Defense Center currently includes eight countries—Estonia, Germany, Italy, Latvia, Slovakia, Spain, and the United States. In the case of a cyberwar, the CDC would likely take the lead in coordinating NATO response efforts, similar to how NATO’s military forces would be marshaled in a physical war.

Bronze Night—the controversy and riots in Estonia surrounding the 2007 relocation of the Bronze Soldier of Tallinn, the Soviet World War II memorial in Tallinn.

Recent Developments

The so-called ‘kill switch’ is essentially a congressional proposal

that would allow the President of the United States to control and shut down parts of the Internet. It is actually part of a larger legislative act called the Protecting Cyberspace as a National Asset Act of 2010. This law, introduced by Senators Joe Lieberman (I-CT), Tom Carper (D-DE), and Susan Collins (R-ME), seeks to coordinate federal cyberspace policy as well as establish an Office of Cyberspace Policy and expand executive powers over the Internet. The idea of a ‘kill switch’ has proven controversial, forcing the authors of the bill to downplay the scope of powers granted and instead emphasize the public safety ramifications of the act. In essence, the bill seeks to allow the federal government the necessary discretion to react to cyberwarfare. The bill’s authors emphasize that this is particularly important for parts of America’s infrastructure such as financial operations, public utilities, and communications. If passed by Congress and signed by the president, it would allow for the declaration of a “national cyber emergency” in the case of a cyberwar.

The United States has shown in recent years that it is more than willing to engage in preemptive military action to protect its interests. If the perpetrator of a cyberattack was acting on the orders of a foreign government or political entity, the United States could feasibly launch a military strike. A former Director of the National Security Agency (NSA) and **Director of National Intelligence (DNI)**, Michael McConnell, went so far as to propose a policy of massive retaliation for future cyberattacks. Although downplayed by his successor, Howard Schmidt, McConnell’s warning that a coordinated cyberwar could take more lives than the 9/11 attacks remains both poignant and controversial. In the event of a disastrous cyberattack, the US military could be ordered to launch an air strike, tactical insertion, or even invasion of the offending party. Of course, the Obama administration has emphasized that military action remains a last resort as such a response is wrought with serious geopolitical, economic, and strategic consequences. A catastrophic attack, however, could change that policy in a heartbeat.

The United States recently backed a form of cyber arms control, reversing several years of opposition to similar Russian proposals. The current commander of United States Cyber Command, General Keith Alexander, endorsed a dialogue with Russia over limiting malicious software attacks and other forms of cyberwarfare. Although China is conspicuously absent from the talks, the diplomatic proposal seems to be gathering international support. One serious concern with diplomatic limitations on cyberwarfare is that it would not necessarily prevent nations from employing third-party hackers. Such treaties would also be extremely difficult to enforce because of the nature of cyber weapons.

Director of National Intelligence (DNI)—*the US government official responsible for serving as the principal advisor to the President, NSC, and the Homeland Security Council for intelligence matters related to national security and for overseeing and directing the National Intelligence Program.*

Bibliography

- Gorman, Siobhan, "U.S. Backs Talks on Cyber Warfare," *Wall Street Journal*, June 4, 2010
- McCullagh, Declan, "Senators propose granting president emergency Internet power," CNET, June 10, 2010, <http://news.cnet.com/830113578_32000741838.html>.
- North Atlantic Treaty Organization, "NATO opens new centre of excellence on cyber defense," May 14, 2008, <<http://www.nato.int/docu/update/2008/05/may/e0514a.html>>.
- Singel, Ryan, "White House Cyber Czar: 'There is No Cyberwar'," *Wired*, March 4, 2010
- "The Threat from the Internet: Cyberwar," *The Economist*. July 1, 2010
- Wentworth, Travis, "You've Got Malice," *Newsweek*, August 23, 2008, <<http://www.newsweek.com/2008/08/22/you've-gotmalice.html>>