

Cyber Attacks: Missing in Action April 2003

The first warnings of an “electronic Pearl Harbor” appeared in 1995.¹ They have appeared regularly since then. Before the conflict with Iraq that began in March 2003, there was speculation that the U.S. would experience cyber attacks in retaliation. Since the onset of the war, however, there have been no reported attacks that damaged U.S. infrastructure or affected U.S. military operations in Iraq. Nor have there been any reports of cyber attacks that damaged U.S. infrastructure or affected U.S. military operations since 1996.

This is not the result of inactivity by terrorist groups. The State Department reports there were 1,813 international terrorists attack between the start of 1996 and end of 2001.² While many of these attacks did not involve U.S. citizens or targets, some of the most damaging terrorist attacks against the United States took place in this period. They include the Khobar Tower bombings (June 1996), the U.S. Embassy Bombings in East Africa (August 1998), the attack on U.S.S. Cole, (October 2000). Three hundred and twenty seven people died in these attacks, which were followed by the horrific attacks on the World Trade Center and the Pentagon in 2001, which cost more than three thousand lives and caused billions of dollars in damage.

Since September 11, the United States discovered a number of terrorist cells operating within its borders and in other countries. Other nations (the United Kingdom, Germany, Spain and others) also discovered active terrorist cells. These terrorist cells reportedly planned attacks using bio-toxins, chemical weapons and radiological weapons, in addition to attacks using conventional explosives and firearms. None, however, are reported to have planned attacks using cyber weapons. One fundamentalist cleric who lives in London and who frequently acts as a spokesperson for Al Qaeda did, in November 2002, threaten attacks against the U.S. economic infrastructure using all types of technologies, including the Internet.³

Nor is the absence of cyber terror the result of inactivity by hackers. Carnegie Mellon’s Computer Emergency Response Team has collected statistics showing that since 1996, there have been 217, 394 computer security incidents reported.⁴ This number is probably an underestimate. None of these security incidents damaged U.S. infrastructure or degraded U.S. military capabilities. Terrorism requires overt, public acts of violence that create widespread shock and horror in the minds of opponents. None of the 217,394 attacks had this effect or can be regarded as terrorist actions.

A large number of cyber-events did occur during the conflict in Iraq. Arab news sites

¹ A summary examination finds that one of the first widespread public uses of the term was in an August 1995 *Time Magazine* article by Douglas Waller: <http://www.csm.ornl.gov/~dunigan/timemag.html>, or http://www.time.com/time/archive/preview/from_redirect/0,10987,1101950821-134566,00.html

² <http://www.state.gov/s/ct/rls/pgtrpt/2000/>; <http://usinfo.state.gov/topical/pol/terror/01103131.htm>;
<http://library.nps.navy.mil/home/tgp/chrono2001.htm>, <http://www.state.gov/s/ct/rls/pgtrpt/2000/2452.htm>

³ <http://www.computerworld.com/securitytopics/security/story/0,10801,76000,00.html>

⁴ http://www.cert.org/stats/cert_stats.html#incidents

reported hundreds of hacking incidents and a leading Arab news site found its English-language website replaced with a large American flag.⁵ Large numbers of anti-war or pro-Saddam hackers also defaced a number of U.S. and British websites. Some unclassified U.S. military networks reported “slower download times” because of the attacks. A small number of computer viruses were released as anti-war gestures, but there have not been any reports of significant disruption as a result (one security firm noted that the virus ‘Ganda,’ thought to be Iraq-related, “seems to be a protest against the Swedish school system rather than an anti-war protest.”).⁶

Nor are there reports of cyber attacks by U.S. forces against Iraq. This could simply be an absence of reporting on the use of secret cyber weapons, or it may reflect the fact that Iraq had practically no computer network infrastructure. Iraq was an uninviting target for cyber attack, but it is not alone in this regard. One dilemma for the U.S. is that the countries where it has deployed military forces – Iraq, Serbia, Somalia, Haiti – are not advanced economies and do not use computer networks for critical functions, making cyber weapons of limited utility.

The contrast between the thousands of terrorist attacks, tens of thousands of computer hacking incidents and an absence of cyber terror or cyber attacks on infrastructure, is striking and suggestive. It suggests that, as so many commentators have noted, that cyber terror or cyber attacks on infrastructure are an unlikely threat to the security of the United States.

1996-2003	
Computer Security Incidents	217,394
Terrorist Attacks	1,813
Cyber Terror Incidents	0

Part of the explanation of this disparity lies with the goals and motives of terrorists. The people who are attracted to terrorism seek to do violence against their opponents. Cyber attacks are unsatisfactory in this regard. Terrorists’ plans call for actions that have a political and psychological effect produced by the shock and horror of physical destruction and casualties. Cyber attacks do not produce these. Terrorists have a keen sense of operational risk and will avoid untested weapons whose effect is unclear or unknown. Some experts go so far as to say that terrorists may avoid cyber weapons because of the potential risk it could pose to their own operations and communications.⁷

There is also the separate issue of how vulnerable nations are to the effects of computer network attacks should a cyber attack ever actually occur. A careful review suggests that if there were cyber attacks, their effect on national security would be limited. The hypothetical vulnerability of various infrastructures - water systems, air traffic control, electrical grids – is routinely overstated in cyber attack scenarios. These infrastructures are not dependent on computer networks for their operation. A closer examination suggests that: (a) computer networks and critical infrastructure are not equally

⁵ http://abcnews.go.com/wire/Business/ap20030417_163.html

⁶ <http://www.f-secure.com/virus-info/iraq.shtml>

⁷ Vincent Cannistraro, a former CIA counter terrorism chief, quoted in Computer World in November 2002, <http://www.computerworld.com/securitytopics/security/story/0,10801,76000,00.html>

vulnerable; (b) nations are robust and resilient in responding to attacks, thus the potential for damage is limited, and (c) critical infrastructures in the U.S. have considerable redundancy, are accustomed to system failure, know how to repair these failures, and still require human intervention for many control mechanisms. This makes it difficult for remote computer attacks to disrupt critical functions.⁸

Although unrelated to Iraq, the recent “Slammer” worm shows some of the problems associated with analyses of cyber attacks. Several reports said that Slammer ‘shut down Wall Street,’ or led elections to be cancelled. Closer examination showed these reports to be exaggerations or errors. Some credit card companies and banks were affected for a few hours; others were not. Other reports said that Slammer degraded 911 emergency response systems in Washington State. In fact, Slammer’s effect was to slow the computers dispatchers use to log calls. Dispatchers are trained to use paper logs in the event of a power failure or other problem, and did so in response to Slammer. Response time by emergency services was not affected,⁹ and there was no degradation of 911 service. Examinations of other alleged cyber attacks uniformly show similar errors or exaggeration.

The network problems caused by Slammer for banks, credit card companies and police computers, while troubling and annoying, were not a threat to U.S. national security, but the incident shows the tendency to declare that network failures translate automatically into national security risks. A more realistic assessment is that cyber weapons do not now pose a risk to U.S. security and will never offer potential opponents an ‘Achilles heel’ where a few hack attacks could paralyze the nation.

The Federal government, although usually criticized for exaggerations, seems to have adopted a more measured tone in some of its public pronouncements. A February advisory from the National Infrastructure Protection Center issued as tensions over Iraq increased offers a good model for thinking about cyber security.¹⁰ Instead of warning of catastrophic surprise attacks, infrastructure failures or terrorism, it offered a risk scenario that emphasized “spamming, web defacements, denial of service attacks” and, potentially, computer viruses and called on network operators to monitor their systems and use ‘best practices.’ The absence of cyber attacks in the last eight years suggests that it makes sense to call for reasonable measures to safeguard information rather than to warn of potential calamity.

Along these lines, it may be useful to think about how to refocus analyses of cyber security. First, analyses of cyber security would improve if they focused on the issues for business practices and law enforcement created by networks, instead of emphasizing military attacks and terrorism. National security is the responsibility of governments;

⁸ An earlier essay examines the relationship between national security and cyber attacks in more detail: http://www.csis.org/tech/0211_lewis.pdf

⁹ Wells, Robert Marshall, *Seattle Times* “Dispatchers go low-tech as bug bites computers” <http://archives.seattletimes.nwsource.com/cgi-bin/texis.cgi/web/vortex/display?slug=webworm27m&date=20030127>

¹⁰ <http://www.nipc.gov/warnings/advisories/2003/03-002.htm>

protecting one's business from crime is a responsibility shared between governments and citizens. An overemphasis on terror may actually be a disincentive for private sector effort to improve security. People might take cyber security more seriously if it was presented as an issue for business and law enforcement.

Second, cyber security analyses would improve if they remembered that the most valuable part of Information Technology is information. Many of the existing analyses that predict 'electronic Pearl Harbors' assume that there is a close connection between the physical and the cyber. In most instances, however, this connection seldom exists. Hackers, for example, cannot cause aircraft to fly into each other because there are still pilots and air traffic controllers that do not depend on computers. The real risk of cyber attack lies in the potential to manipulate or gain access to valuable information, e.g. espionage, theft of intellectual property or financial data, and vandalism. This is the area of greatest risk for users of computer networks, not infrastructure attacks, and it is the area cyber security should emphasize.