

mind•full: a brainsnack for future leaders with ethical appetites

Volume III • Number 6 • February 2001 • Student Pugwash USA

information warfare

The industrialized world's growing dependence on the electronic infrastructure has made it increasingly vulnerable to attacks by states and other actors. These attacks frequently are categorized under a general term: information warfare. This catch-phrase describes strategic attacks against infrastructure such as telephone systems, banking networks, air traffic control and traffic systems, electricity grids, and the Internet. It also can mean the spreading of false information to confuse both the media and foreign governments. For example, during the 1999 East Timor crisis, programmers believed to be working for the Indonesian government attacked and successfully blocked the domain name used by East Timorese exiles. It is the use of highly skilled professionals, and relatively low-cost technological tools that make information warfare a new battleground.

The United States and other Western governments have taken steps to detect and respond to information warfare attacks, especially those involving computers connected to the Internet. Several centers run by universities and law enforcement agencies act as the front line for detection and defense of viruses and other weaknesses in the information economy's digital defenses. The nature of the response to computer viruses and attacks suggests the difficulty of distinguishing between common criminals, terrorists, and warriors.

Critics of government investment in information warfare believe that concern over a coming "digital Pearl Harbor" is alarmist. They point out that the majority of computer threats—the perceived source of danger—can be covered adequately by cheap virus software provided by private companies without governmental involvement. Civil liberties groups, in particular, warn that defense against "information warfare" is increasingly becoming an excuse by governments to eavesdrop on their citizens' private communications.

The mission of Student Pugwash USA is to promote the socially responsible application of science and technology in the 21st century. As a student organization, Student Pugwash USA encourages young people to examine the ethical, social, and global implications of science and technology, and to make these concerns a guiding focus of their academic and professional endeavors.

The **mind•full** series encourages readers to explore crucial ethical dilemmas associated with the application of science and technology.

STUDENT



PUGWASH

U S A

go figure!

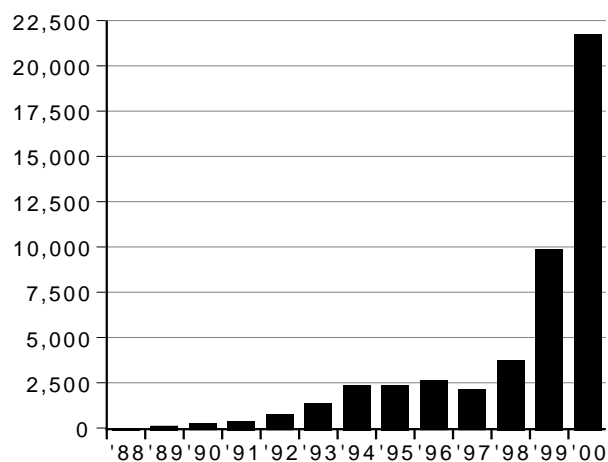
Despite what may appear to be an easily quantifiable technical problem, few experts agree on the extent of the threat to information infrastructures by planned attacks. Even fewer agree on the documented statistics on the cost of computer attacks.

Most incidents that authorities call "computer attacks" are tantamount to trespassing. So, although there may be a large number of attacks, very few are catastrophic or costly. Furthermore, the number of attacks may appear to be growing because more companies and governments are looking for them and trying to attach a price tag to cover costs they consider related to defense against attacks.

Computer viruses may be easier to quantify than other attacks and yet these figures are hard to pin down. For example, according to correspondence with Martin Libicki of RAND, if the recent "I Love You" virus supposedly cost the world economy \$10 billion, then its 12 million victims would have lost on average \$800 per day, an amount far in excess of their average productivity. This is but one example of the difficulty of calculating the social and economic impacts of information attacks. However, the following statistics do indicate increasing importance and awareness of information warfare preparedness.

is the United States at war?

computer security incidents reported to CERT® coordination center, 1988-2000



Source: CERT/CC Statistics, 1988 - 2000, Carnegie Mellon Software Engineering Institute, available January 26, 2001 at www.cert.org/stats/cert_stats.html#incidents.

a defenseless defense department?

Attacks on Department of Defense computers in 1995: 250,000

Infiltrations per day in 1995: 455

Percentage of attacks on DoD computers detected: 4

Percentage of detected attacks actually reported: 27

Source: Summary of Defense Information Systems Agency figures in Brian Lewis, "Information Warfare." Available January 26, 2001 at <http://www.fas.org/irp/eprint/snyder/infowarfare.htm>.

in control or out of it ?

Governments and non-governmental organizations recently have taken both offensive and defensive measures to address the emerging conflict taking place over our information networks.

On the domestic front, the government first tackled the nebulous term "information warfare" by trying to define it. In 1996, the Brown Commission, tasked with conducting a review of US intelligence programs, defined information warfare as "activities taken by government, groups, or individuals to gain electronic access to information systems in other countries . . . as well as actions undertaken to protect against it." Several critics argue that the commission did not pay enough attention to information warfare issues, and that the definition it provided was vague and inadequate.

Law enforcement agencies and public-private consortiums are working to prevent computer attacks. Under Presidential Decision Directive-63 (PDD-63), signed by President Clinton in May 1998, the FBI's Computer Investigations and Infrastructure Threat Assessment Center expanded "into a full-scale National Infrastructure Protection Center," including people from the FBI, US Secret Service, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the DoD and the intelligence community. Other domestic efforts include Carnegie Mellon University's CERT (Computer Emergency Response Team) Coordination Center, which was established in 1988 after an Internet "worm" stopped ten percent of the computers connected to the Internet.

Much of the public focus in Europe has been in opposition to US-led information-gathering programs that stave off network-based threats. For example, the European parliament and the French national assembly are taking legal action against a US-led electronic eavesdropping system called Echelon. Echelon is believed to monitor phone conversations and look for keywords in emails and other data traffic that could be classified as potential threats.

Because of the extensive attention given to Echelon in Europe, US civil liberties organizations, including the ACLU and Electronic Frontier Foundation, have made these systems a focus of their legal efforts. They have raised concerns about the Foreign Intelligence Surveillance Act, the Terrorism Act of 1997, and other

learn the lingo

semantic attack—a system under semantic attack operates. . . correctly. . . but it will generate answers at variance with reality.*

simula-warfare—a prediction of warfare to come in which there will be a computerized simulation of physical war.**

trojan horse—the most elementary form of malicious code. . . This kind of program appears to do something useful or. . . entertaining, such as putting up an attractive screensaver. . . [S]uch a program may destroy files or create a "back door". . . that enables an intruder to access your system.**

virus—commonly inserts itself into other program files. . . [like] a virus in nature. . . When the infected program runs, the virus code gets a chance to inspect its environment and look for and infect new carriers in the form of other program files.**

worm—a self-replicating program that does not alter files but resides in active memory and duplicates itself by means of computer networks. Worms use facilities of an operating system that are meant to be automatic and invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.**

Source: *Martin Libicki, *What is Information Warfare?* Washington, DC: National Defense University, 1995. **A paraphrase of Libicki. ***Peter Coffee, "Trojan Horse, Virus, or Worm?" Available January 26, 2001 at <http://www.zdnet.com/zdhelp/stories/main/0,5594,2435378,00.html>.

legislation, which they claim permits intelligence agencies to spy on US citizens. Their fears seemed to be somewhat justified following revelations of an FBI system called "Carnivore," which enables the government to download the private e-mail of any individual subject to an investigation. Critics protest that the privacy of third parties may be violated by expansive government searches.

Despite current controversies like Echelon and Carnivore, much of the discourse within the information warfare profession focuses on the future. Analysts at National Defense University (NDU) and RAND are responsible for envisioning the battlefield of the future. One of NDU's recent publications was entitled *Sun Tzu and the Art of Information Warfare*. It included essays from experts in information warfare. One expert presented a scenario in which Serbian paramilitaries undermine a NATO peacekeeping mission by tampering with NATO military networks, causing the deaths of a dozen soldiers. Then, according to the scenario, the paramilitaries use the Internet to mobilize Western public opinion against NATO involvement. Some analysts speculate that a future like *The Matrix*, in which warfare is conducted completely in virtual-reality spaces, could even be feasible one day. Other similar scenarios pervade research funded by the US government.

is it a virus? it depends what the definition of "is" is . . .

According to George Smith, editor of *The Crypt Newsletter*, even our law enforcement officials have fallen for widely circulated hoaxes. In the December 1996 issue of the FBI's *Law & Enforcement Bulletin*, two academics reported of a "Clinton virus" that was "designed to infect programs, but . . . eradicates itself when it cannot decide what programs to infect." The same authors wrote in an earlier paper of hackers who "reportedly broke into a NASA computer responsible for controlling the Hubble telescope and are also known to have rerouted telephone calls from the White House to Marcel Marceau University, a mining institute." As it turned out, both the Clinton virus and "Marcel Marceau University" were two pranks in a computer magazine's April Fool's Day column.

eastern europe: the wild west of information warfare

According to an article by David S. Bannahum in the November 1997 issue of *Wired*, the brief history of computer viruses and attacks began, of all places, in the Communist-controlled Bulgaria in the early 1980s. As a result of a government initiative, Bulgaria was the Eastern Bloc's production center for Apple IIe knockoffs which the government provided for home use. State-sponsored technical clubs were the training ground for an emerging community of computer virus programmers. In 1989, over ten percent of the world's viruses came from Bulgaria. Most came from a mysterious programmer who operated under the moniker "Dark Avenger." As a result of Bulgarian and other viruses, as many as 63 percent of North American companies had been hit by viruses by 1991. But by 1993, perhaps because of the collapse of Soviet communism, Dark Avenger disappeared and Bulgaria stopped being a major virus source. To this day, no one has been able to track him or her down.

trade war and information war

The United States relies upon foreign intelligence in its trade negotiations. According to Brian C. Lewis, US agents allegedly hacked into the computers of the European Commission to steal political and economic secrets. European officials claim that the United States later used the information in 1996 negotiations over the General Agreement on Tariffs and Trade (GATT). The United States refuses to acknowledge the intrusion. It instead claims to be investing primarily in defensive measures that would stop hacker or terrorist attacks and has not declared any offensive information warfare capability.

(anything but a) conclusion

Experts disagree over the definition and extent of information warfare. While several computer attacks have caused extensive damage, there have been few documented instances of large-scale, state-sponsored strategic attacks. Most attacks come from "lone wolves" who are not organized and may be more like high-tech vandals than terrorists or warriors.

Civil liberties advocates warn that governments may be inflating the looming threat of information terrorism to justify violation of personal privacy. They point to several large programs that make it easy for the government to snoop in individuals' electronic files. Some also are concerned that part of the US research may be offensive and not defensive in nature.

How do **you** answer the **tough questions**

According to the US government's Brown Commission, "Information warfare is activities taken by government, groups, or individuals to gain electronic access to information systems in other countries . . . as well as actions undertaken to protect against it." Do you believe this definition is adequate, or can you think of other activities that might fall under the rubric of information warfare?

Consider how documented information warfare attacks are the work of individuals, very rarely terrorist organizations, and thus far, not countries. Based on what you have read, do you expect that states will soon be conducting network attacks in conflicts like the recent Kosovo air war? Would it be good for the US to spend more money on offensive information warfare? Why or why not?



For years, governments have eavesdropped on the phone calls of criminal suspects, as well as law-obeying dissidents, by tapping phone lines. Under a recently passed measure, the United Kingdom would become the only country to require Internet users to turn over their encryption keys. Refusal to hand over encryption keys to their computer systems when requested to by police could result in an automatic two-year jail sentence. Do you believe that the risk from network-based dangers merits such a measure? Why?

The victims of the most costly information warfare attacks often have been businesses. To what extent should the private sector bear the burden for the defense against an information offensive? Is this the province of the military, like other matters of national security? Or should defending against all kinds of attacks simply be treated as "costs of doing business" and left to the private sector?



.....

- The Persian Gulf War was environmentally
- devastating, leading to the largest oil spill in
- history and oil well fires that blazed for
- months. Can you imagine how war over
- computer networks could be less
- environmentally damaging than war is
- today? How could it make war worse for the
- environment?

.....

What privacy rights should people have when they are using communications networks? Are current privacy laws adequate, or is it necessary, as the American Bar Association recently suggested, to draft international rules of conduct for online communication?

Some suggest that the solution to the challenges posed by information warfare is to lessen society's dependence on technology. Do you agree? Why?



According to the 1998 National Science Foundation report on *Women, Minorities, & Persons With Disabilities in Science and Engineering*, only thirty-five percent of US computer and math bachelor's degrees were earned by women in 1995. Do you think this affects the hacker culture or even US policy with respect to information warfare? Why or why not?

Imagine the "digital Pearl Harbor" that some analysts predict. Nationwide networks would be shut down, leaving people without electricity, water, or telephone service. What would be an adequate response to such an attack? If it were discovered that the attack had come from an individual, how should reprisal be meted out? What if it were to come from a terrorist group, or another country?

Information warfare, beyond its involvement with computer viruses, is a topic rarely discussed. Do you think US universities should teach courses on information warfare? Why or why not?



Some advocates of disarmament suggest that we are in the midst of an arms race involving computing. They point to large supercomputing projects at the same laboratories that design nuclear weapons. Are they right to be concerned? Why or why not?

some reading to "hack" through

- *In Athena's Camp: Preparing for Conflict in the Information Age*. John Arquila et. al. consider warfare in the context of new information technologies. War will entail "swarming" actions, rather than mass movements. Santa Monica, CA: RAND, 1997.
- *Cyberspace and the Use of Force*. Walter G. Sharp, Sr., Aegis Research Corp, 1999.
- "Cyberterrorism Hype," Johan J. Ingles, *Janes Intelligence Review*, 21 October 1999, available January 25, 2001 at <http://jir.janes.com/sample/jir0525.html>.
- *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Alan D. Campen (editor), et. al. Articles on information warfare. Fairfax, VA: Acea International, 1996.
- *Information Warfare and Security*. Dorothy Denning's summary of the various facets of information warfare, with case studies. New York: Addison-Wesley, 1998.
- "Information Warfare," Brian C. Lewis expands on work done by recent commissions. Available January 26, 2001 at www.fas.org/irp/eprint/snyder/infowarfare.htm.
- *Information Warfare: Principles and Operations*. Edward Waltz gives an in-depth systems-level consideration of information warfare. London: Artech House, 1998.
- "On Physics and National Security," special edition of *Physics Today*, December 2000. See also the *Physics Today* online archive at www.physicstoday.org/pt/vol-53/iss-12/current.html, which includes a September 1997 article by Martin Libicki, "Information Warfare: A Brief Guide to Defense Preparedness."
- "Networks, Netwar, & Information-Age Terrorism," a chapter by John Arquila, David Ronfeldt, and Michele Zanini in *Countering the New Terrorism*. Ian O. Lesser, et. al. Santa Monica, CA: RAND, 1999. Pp. 39 - 84.
- *Powershift: Knowledge, Wealth, and Violence in the 21st Century*. Alvin Toffler, prophet of the "information society," writes that information wars will be ubiquitous at many levels in the future. New York: Bantam, 1991.
- *Risks to the US Infrastructure from Cyberspace*. Testimony by Robert H. Anderson before a Governmental Affairs subcommittee. Santa Monica, CA: RAND, 1996.
- *Securing the US Defense Information Infrastructure: A Proposed Approach*. Robert Anderson (editor). Could US forces be vulnerable to information warfare? Santa Monica, CA: RAND, 1999.
- *Strategic Information Warfare: A New Face of War*. How would the United States respond to a cyber attack? Santa Monica, CA: RAND, 1996.
- *Sun Tzu and Information Warfare*. A collection of winning papers from a writing competition sponsored in honor of Sun Tzu, the ancient Chinese war theorist. Washington, DC: National Defense University Press, 1997. Available January 25, 2001 at www.ndu.edu/inss/siws/cont.html.
- *What is Information Warfare?* Martin C. Libicki. Washington, DC: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, 1995.

check it out !**technological goofiness**

- *NetForce*. Tom Clancy and Steve Pieczenik imagine a new computer security agency in 2010 when "computers are the new superpowers." Check out this series of novels for a bit of light, if not lofty, reading.
- *Neuromancer*. Before *The Matrix* came William Gibson's award-winning novel on fighting in cyberspace. New York: Ace Fiction, 1984.
- *Sneakers*. Starring Robert Redford, an implausible action comedy about a box that can decode anything. Good for laughs.
- *Enemy of the State*. Will Smith and Gene Hackman dodge corrupt National Security Agency operatives in this Jerry Bruckheimer (*Flashdance*, *Top Gun*, *Crimson Tide*) production.

top pick

• Federation of American Scientists (site contains numerous links to articles and other sites on information warfare)—www.fas.org/irp/wwwinfo.html

best of the rest

- Carnegie Endowment for International Peace (this organization has a special program on the information revolution and world politics)—www.ceip.org/files/projects/irwp/irwp_home.ASP
- Cyberspace Policy Institute at George Washington University—www.cpi.seas.gwu.edu
- CIA Center for the Study of Intelligence (contains links to articles on information warfare)—www.cia.gov/csi
- Covert Action Quarterly (monitors the activities of intelligence agencies)—www.caq.com
- Journal of Electronic Defense (a journal that deals broadly with electronic defense, from radar to cyberwar)—www.jedefense.com
- National Infrastructure Protection Center (FBI's center to prevent information attacks)—www.nipc.gov
- Infowar.com (a site with links to numerous resources related to information warfare)—www.infowar.com
- Terrorism Research Center (an independent group that provides next generation terrorism analysis)—www.terrorism.com/infowar/index.shtml
- Wired (online periodical that includes frequent updates on developments in the technology sector and feature articles on information warfare)—www.wired.com

web power!**cyberspace**

This *mind•full* was written by Clayton Nall, University of Wisconsin Student Pugwash, with input from Chitra Kumar, MIT Student Pugwash. Clayton was chapter program summer intern and a chapter representative on the Student Pugwash USA board of directors. Chitra is currently a chapter representative on Student Pugwash USA's board of directors, previously she was chapter activities associate Student Pugwash USA. Special thanks to Paul Guinnessy, Online Editor, *Physics Today* for his comments. Any errors are the responsibility of Student Pugwash USA. ©2001 Student Pugwash USA.

board of directors

Eric Roberts, Chair
 Elizabeth Fader
 Natalie Goldring
 Paul Jellinek
 Judith Kass
 Amber Kerr
 Chitra Kumar
 Jeffrey Leifer
 Alan McGowan
 Benjamin Silverman
 Dann Sklarew
 Eric Tapley
 Yonette Thomas
 Frank von Hippel

board of advisors

Sissela Bok
 Hal Harvey
 John Holdren
 Walter Kohn
 Sally Lilienthal
 Shirley Malcom
 Victor Rabinowitch
 Victor Weisskopf
 Herbert York

but wait, there's more!

- **Chapter Organizing Guide.** Provides chapter members with an A to Z guide to getting a campus-based chapter up and running.
- **mind•full: a brainsnack for future leaders with ethical appetites.** Volume two issues available: pugwash conferences; exploring human genetics; science, technology, & culture; communications technologies; beyond nuclear weapons; nuclear energy; computers and human genetics; energy and international security; science, ethics, and education; environment and energy; war-free world. Volume three issues available: genetic testing; terrorism and weapons of mass destruction; technology and human rights; women and science; and pledges, oaths, & scientists.
- **Jobs You Can Live With, Web Edition.** Our former print publication, *Jobs You Can Live With*, a comprehensive guide to getting a socially responsible job or internship, with a special focus on jobs at the intersection of science, technology, and society, is now in an online format.
- **Pugwatch.** The chapter newsletter.
- See other resources on our Web site: www.spusa.org/pugwash.

recent supporters

Compton Foundation
 Cyrus Eaton Foundation
 Ford Foundation
 W. Alton Jones Foundation
 Jeffrey Leifer (founder)
 John D. and Catherine T. MacArthur Foundation
 National Institutes of Health
 The New-Land Foundation
 Novartis International AG
 The David and Lucile Packard Foundation
 Ploughshares Fund
 Price Family Charitable Fund
 Mary Stuart Rogers Foundation
 Samuel Rubin Foundation
 San Diego Foundation, Dr. Seuss Fund
 Surdna Foundation
 Trust for Mutual Understanding
 University of California, San Diego
 US Pugwash
 Individual Contributors

STUDENT

PUGWASH
U S A

student pugwash usa
815 15th street, nw, suite 814
washington, dc 20005 usa

address service requested

how to find us

telephone: 202-393-6555 or 1-800-wow-a-pug • fax: 202-393-6550
 e-mail: spusa@spusa.org • Web: <http://www.spusa.org/pugwash/>