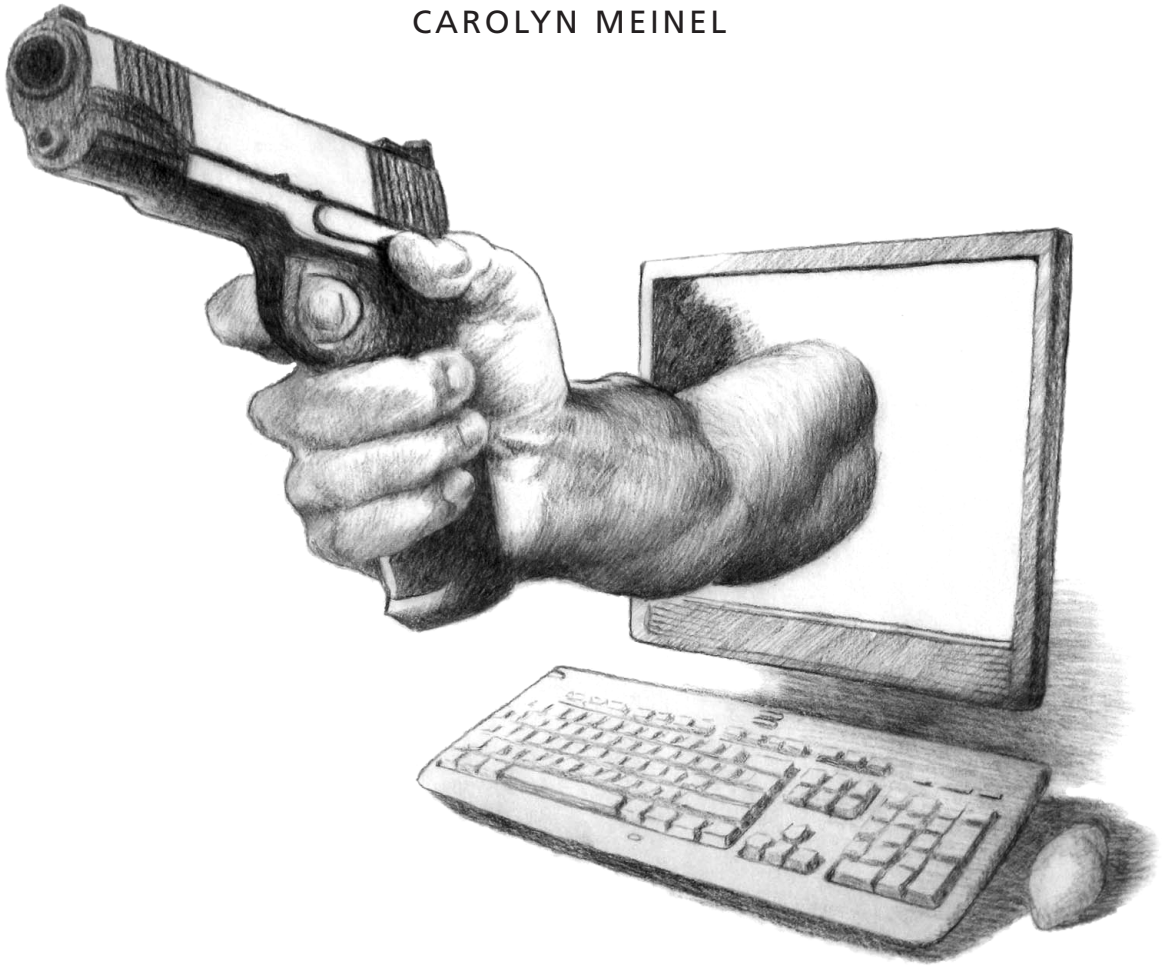
Hoaxers, Hackers, and Policymakers

How Junk Science Persuaded the FBI to Divert Terrorism Funding to Fight Hackers

Hoaxers warned of an imminent and deadly electronic Pearl Harbor. Consequently, the FBI diverted resources and attention away from terrorism and toward fighting hackers. This may have contributed to the September 11, 2001, attacks. Use of critical inquiry and the scientific method could have avoided this misdirection.

CAROLYN MEINEL



Beginning in late 1996, Fred J. Villella, calling himself the former "executive secretary to the national security adviser," squired "Dr. Mudge" and "Se7en," to meetings where they warned federal policymakers of a looming electronic Pearl Harbor (Richtel 1998, Radcliff 1998). Their adventures appeared in many news stories, and for good reason. This was back when the Internet and the Dot Com revolution were big and scary and most people had no idea what it all meant. The policymakers were as clueless as anyone. They were the sorts who had their secretaries print out their e-mails so they could read them—if they even had e-mail. And here were these geniuses telling them what to think: Be afraid. Be very, very afraid. Villella's hackers seemed believable because they exploited the archetype of trickster gods of technology such as the Sumerian Enki and Norse Loki. Movies such as *War Games* and *The Matrix* updated the archetype, with hackers as the modern incarnations. Their trickster god auras must have worked, for these policymakers paid no attention to the murky pasts of these men.

The hackers' messages may have contributed to an entrapment scheme. The missing piece in their electronic Pearl Harbor story was whether hackers were actually collaborating with enemies of the U.S. This soon changed. On May 11, 1998, the FBI arrested Indian immigrant Khalid Ibrahim for "willfully and knowingly" filing a false affidavit on behalf of an al Qaeda operative. At the perp walk, the federal prosecutor told the press that they were conducting "extensive discussions" about a plea bargain, "a disposition that would be termed mutually beneficial" (Moreno 1998). After this publicity, al Qaeda could never trust Ibrahim. Clearly, the FBI was targeting him elsewhere.

A few days later, Ibrahim contacted "Chameleon," a hacker whom the FBI believed had defaced the Army's artificial intelligence Web site with UFO pictures and theme music to *The X-Files*. Ibrahim introduced himself as an Indian terrorist living in New Delhi, India. He offered to pay Chameleon for military secrets. Shortly thereafter, Ibrahim mailed him $1,000. Days later, the FBI raided the home where Chameleon lived with his mother and two sisters (McKay 1998).

Chameleon turned out to be Marc Maiffret, age seventeen. A high school dropout, he spent two years trying to find out whether the Pentagon was conspiring with extraterrestrials. Maiffret was never indicted, which suggests that the FBI failed to find evidence of stolen military secrets. Despite this, many news stories (e.g., McKay 1998, Burrough 2000) and books (Penenberg 2000, Mitnick 2005) hyped the raid to say that hackers were in league with al Qaeda.

Carolyn Meinel is a consultant and science writer. She has assisted the Defense Advanced Research Projects Agency (DARPA) with its Intrusion Detection Evaluation Program and its Cyberadversary Workshop, and consults for Systems Advisory Group Enterprises, Inc. (www.sage-inc.com), the Institute for Advanced Technology (www.iat.utexas.edu/), and the Santa Fe Institute (www.santafe.edu/). She may be reached at carolyn.meinel@techbroker.com.

Stir into this media frenzy a feud between Louis Freeh, the head of the FBI, and President Clinton's terrorism and cyberspace czar, Richard A. Clarke (Freeh 2005). Consequently, Freeh habitually froze Clarke out of the loop. All Clarke could have known about Maiffret's supposed al Qaeda adventure was what he saw in the news.

Even other parts of the FBI had little or no knowledge of what was going on. Department of Justice regulations known as "The Wall" kept agents who worked the foreign intelligence beat from sharing information with those handling domestic crimes (Coulter 2004).

All this confusion had a predictable result. In January of 1999, Clarke announced, "There is a problem convincing people that there is a threat. . . . They think I'm talking about a fourteen-year-old hacking into their Web sites. I'm talking about people shutting down a city's electricity, shutting down 911 systems, shutting down telephone networks and transportation systems. You black out a city, people die. Black out lots of cities, lots of people die. It's as bad as being attacked by bombs" (Weiner 1999).

A few days after Clarke's statement, Se7en was exposed as a faker who could barely navigate a keyboard (Silberman 1999). Villella turned out to be just an ex-FEMA bureaucrat who had resigned when caught with his hands in the cookie jar—and on a protesting female security guard (Vranesevich 1999, Kurtz 1984, Earley 1984). These exposés came on top of the fact that news stories had already warned that Dr. Mudge was not the expert he claimed to be (see, for example, Lange 1997 and Wells 1998).

Clarke never connected the dots. He persuaded Clinton to form the National Infrastructure Protection Center (NIPC), and tasked it to battle both terrorists and cyber attackers. This meant that the money to fight both threats came out of the same pot. Consequently, fears of an electronic Pearl Harbor led NIPC to use all funding increases that Congress earmarked against terrorism to hire FBI agents for the hacker beat (Benjamin 2002). For example, in fiscal year 2000, NIPC spent only $4.9 million on counterterrorism. Of this, nearly $3 million went to buy office equipment, and another million went for training (GAO 2001). Therefore, the FBI lacked the resources to follow up on an agent's warning of al Qaeda members at U.S. flight schools (Posner 2003).

In February 2000, Clarke arranged for Dr. Mudge to meet with and advise President Clinton. In early 2001, Clarke appointed Dr. Mudge to advise the National Security Council (NSC). Not until after September 11, 2001, did Dr. Mudge lose his influence.

Ignoring the Scientific Method

None of this would have happened had federal policymakers heeded the scientific method and thought critically about the issues.

1. Create a hypothesis that is falsifiable, meaning that it is possible to run experiments that, if the data were to come out a certain way, would disprove it.
2. Conduct experiments.
3. Publish the hypothesis and results of experiments, and in so doing, credit prior research.

4. Compare with experimental results obtained by independent researchers.

Let's examine how this process could be applied to the hacker threat.

Se7en's hypothesis. His gang, the Dis.org Crew, claimed to know how to build a cheap, lightweight HPM (high power microwave) gun that could destroy electronic devices at great ranges. This was a big deal because these are not available on the open market. Anyone who wishes to use an HPM weapon must first design and build one. As will become apparent below, there is a good reason for this.

Their experiments. They promised to demonstrate their HPM gun at the 1997 Defcon hackers' convention. However, they never demonstrated it there or anywhere else. Their Web site, www.dis.org, simply claims that they successfully completed this research project.

Their publication. In the June 3, 1996, issue of *Forbes* they made claims of a HERF (high energy radio frequency) gun that could generate a pulse with two million watts of power for a thousandth of a second (2000 joules). "Have you ever heard of a device that directs magnetic signals at hard disks and can scramble the data? . . . That will cook your internal organs, man . . . $300: a rucksack full of car batteries, a microcapacitor and a directional antenna and I could point it at Oracle over there. . . . We could cook their whole office. . . . If you had a Cessna . . . you could fly over Silicon Valley and—POW!—there goes Sun Microsystems—POW!—there goes Intel! . . . You could be a half-mile away and take out a computer in Oracle" (Poole 1996). They failed to credit any other research, for example, HPM programs funded by the U.S. Department of Defense.

Independent experimental results. On a February 1999 *20/20* newsmagazine program, inventor David Schriner demonstrated a device with approximately the same power as the alleged *Forbes* weapon against an idling Corvette. At a range of some ten feet, with the hood up and the weapon pointed directly into the engine compartment, the HERF gun made the idling corvette . . . run roughly (Smith 1999, Schwartau 2005).

At the September 1999 Infowarcon conference, Schriner demonstrated a circa 1880 Hertzian generator equipped with a four-foot parabolic antenna, but reportedly was only able to crash (but not burn out) a computer, and only when within twenty feet (Poulsen 1999, Schwartau 2005).

Why, one might ask, did Schreiner risk this exposure? "Tuning frequency is crucial," says Jeff Schleher, an HPM researcher with defense contractor SAIC. "Each individual vehicle," he says, can have a different vulnerable frequency. An HPM weapon that can stop one vehicle cold might only make another run roughly.

Under a U.S. Army contract, Fiori Industries, Inc. is currently assessing "feasibility of using HPM to immobilize engines" at its Albuquerque, New Mexico, test facility. Although the project is classified, its existence suggests a practical application still is in the research phase.

Diehl GmbH und Co. of Roethanbach, Germany, is said to be selling an HPM weapon, but only to approved governmental entities. No mention of this product appears on its Web site. However, two of its scientists presented a paper on their HPM power source research at the Euro Electromagnetics Conference, July 12–16, 2004. A Google search fails to turn up other vendors of HPM weapons.

Countless news stories and at least two books on computer crime have claimed that hacker HPM weapons are serious threats.

The Air Force Research Laboratory in Albuquerque has conducted many lethality experiments. Its smallest HPM test device delivers ten million joules per attack, five hundred times as much as the supposed weapon of the Dis.org Crew. The capacitor bank that delivers the pulsed power for this device fills a large room. Other experiments at this facility have used pulses of hundreds of millions of joules. These require detonation of large quantities of explosives and operate at ranges far shorter than half a mile (AF Research Lab Fact Sheet 2002).

Despite all this evidence—and lack of evidence—countless news stories and at least two books on computer crime have claimed that hacker HPM weapons are serious threats (Vacca 2002, Adams 1998).

Dr. Mudge

Dr. Mudge's hypothesis. "Dr. Mudge" has repeatedly claimed he can single-handedly crash the Internet—and keep it crashed for days (Kohl 2005). Furthermore, he and others have said that an Internet crash would cause vast disruptions in the nation's infrastructure.

On May 19, 1998, the Senate Governmental Affairs Committee held a hearing on "Weak Computer Security in Government: Is the Public at Risk?" Peter Neumann of SRI International testified "that the underlying information infrastructure of the U.S. such as power generation, transmission and distribution; air traffic control; and telecommunication" were at risk. "It may take a Chernobyl-scale event to raise awareness levels. . . ."

Dr. Mudge's testimony was equally startling. Chairman Fred Thompson asked, "I'm informed that you think that within thirty minutes . . . you could make the Internet unusable for the entire nation. Is that correct?"

"That's correct," said Dr. Mudge, "Actually . . . with just a few [keystrokes]." He added that, "it would definitely take a few days for people to figure out what was going on" (Trigaux 1998, Wells 1998)

Experiments: Dr. Mudge has never publicly demonstrated anything relevant to his claim.

Publications: None. When asked in a phone interview where he had published his research, he said only that it had been reviewed "for years by the National Security Council" (NSC). When asked who on the NSC evaluated it, he replied "I am not at liberty to divulge this information" and hung up. The NSC is not a research organization.

Despite predictions, this electronic Pearl Harbor was a flop. Wherever the Internet crashed, the phones kept on working, the lights stayed on, the trains ran on time—and nobody died.

Dr. Mudge, aka Peiter Zatko.

Independent experimental results: In July 2001, the Code Red v2 worm infected almost half a million Webservers on the Internet. Soon the traffic of all these worms seeking new victims was flooding the Internet. Amid this, a train crash in a Baltimore tunnel severed a major Internet backbone. Consequently, portions of the Internet crashed (FEMA Technical Report 2001, Moore 2002).

Despite predictions, this electronic Pearl Harbor was a flop. Wherever the Internet crashed, the phones kept on working, the lights stayed on, the trains ran on time—and nobody died. These systems were inaccessible from the Internet, a detail that had escaped the alarmists.

Critical Analysis About E-Terrorism

Here is how legitimate researchers have investigated the electronic Pearl Harbor hypothesis.

Winn Schwartau first publicly introduced the "electronic Pearl Harbor" hypothesis at a 1991 Congressional hearing (Schwartau 1991). He also has published his theories in many articles and books, and has always made it clear that an electronic Pearl Harbor would be difficult to achieve. He also has sponsored public demonstrations of HPM weapons, which he calls HERF (high-energy radio frequency) guns.

Admittedly, advertisements for these demonstrations lacked sobriety. Said one, "This year we have more home-brew terrorist capable HERF devices for hands-on play and education!" (O'Hearn 2003). However, Schwartau must sound sympathetic to the claims of hackers in order to get them to come out of the woodwork.

These demonstrations have shown that these weapons fall drastically short of the performance claimed in that 1996 *Forbes* story. Some have been outright irrelevant. At Schwartau's Infowarcon 2003, a seventeen-year-old Russian student used an EMP device to launch full soda cans. At one event, Schreiner showed off a "HERF pen" that he said could "blow up the chips" in ATM machines (Schwartau 2005). How this could be as effective for extracting money as a sledgehammer is unclear.

By contrast, several textbooks on HPM weapons are available that rely upon the scientific method to distinguish fact from fantasy. Examples include *Electronic Warfare in the Information Age* by D. Curtis Schleher and *High-Power Microwave Systems and Effects* by Clayborne D. Taylor and D.V. Giri.

Regarding research on ways to crash the Internet, "How to 0wn [*sic*] the Internet in your spare time" (Staniford 2002) is an example of using the scientific method.

> We begin with a mathematical model derived from empirical data of the spread of Code Red I in July, 2001. We discuss techniques subsequently employed for achieving greater virulence by Code Red II and Nimda. In this context, we develop and evaluate several new, highly virulent possible techniques: hit-list scanning (which creates a *Warhol* worm), permutation scanning (which enables self-coordinating scanning), and use of Internet sized hit-lists (which creates a *flash* worm).
>
> We then turn to the threat of *surreptitious* worms that spread more slowly but in a much harder to detect "contagion" fashion. We demonstrate that such a worm today could arguably subvert upwards of 10,000,000 Internet hosts.

According to the Citeseer Web site, which tracks citations of scientific publications (http://citeseer.ist.psu.edu/staniford02how.html), forty-six other scientific papers have cited this paper. According to one of the co-authors, Nicholas Weaver, factors that led to the value of their research came straight out of the scientific method: ". . . testability through simulation and enough details for others to evaluate. Also, there is a fine line: you have to give enough details for evaluation, but you can't give *too* much detail because you don't want to give

attackers too many ideas. And also . . . we don't have a perfect understanding: E.g., on our worst-case estimate, we were careful on both the details we elided and noting where we really didn't have an understanding" (Weaver 2005).

Remarkably enough, at age eighteen, Marc "Chameleon" Maiffret, the kid the FBI failed to entrap as an al Qaeda collaborator, cofounded eEye Digital Security. In contrast with Dr. Mudge, Maiffret and his research team followed the scientific method, and to a fault. Because his credibility was under attack, Maiffret often published explicit details of the computer security flaws they uncovered. This made it easy for others to replicate his findings, but also inadvertently assisted criminals. One of his analyses provided a sequence of keystrokes that was incorporated in the Code Red v2 worm. This inspired FBI agents to pay him another unpleasant visit. However, they found no evidence against him.

On August 29, 2001, Maiffret testified before the House Subcommittee on Government Management, Information, and Technology about threats to the Internet. Unlike Dr. Mudge in his 1998 Senate testimony, Maiffret provided a detailed and sober analysis. He concluded, "I referenced the Code Red worm heavily . . . because I feel by analyzing it closely we can learn a lot about what went wrong and what we can do in the future . . . the biggest problem facing security today is that there are too many people talking about what we could do or what the threat is, and not enough people doing real work that will result in the mitigating or abolishment of those threats" (Maiffret 2001).

Maiffret hit the nail on the head. Too many self-described computer security researchers have made terrifying claims, but failed to substantiate them. Fortunately, a few researchers have published their hypotheses and subjected them to experiments and peer review. We simply need to act on those findings that have scientific validity, and ignore the flimflam and hoaxes.

The next time some hacker claims to have god-like powers over technology, perhaps we can persuade our leaders that neither Enke nor Loki have incarnated themselves as this latest fear monger.

References

Adams, James. 1998. *The Next World War: Computers Are the Weapons and the Front Line Is Everywhere*. New York: Simon & Schuster.

Benjamin, Daniel, and Steven Simon. 2002. *The Age of Sacred Terror*. New York: Random House.

CSX tunnel fire. 2001. FEMA Technical Report Series, USFA-TR-140, July. Available at www.usfa.fema.gov/downloads/pdf/publications/tr-140.pdf.

Coulter, Ann. 2004. Clinton's policies invited 9/11. FrontPageMagazine.com, April 15. Available at www.frontpagemag.com/Articles/Printable.asp?ID=13009.

Earley, Pete. 1984. Key FEMA official accused of sexually harassing aide. *The Washington Post*, August 2, Thursday, Final Edition, A9.

Evron, Gadi. 2005. RE: router worms and international infrastructure [was: re: IOS exploit]. Message posted on the Bugtraq mailing list, September 19. Available at http://msgs.securepoint.com/bugtraq/.

Fact sheet: High-power microwaves. 2002. Air Force Research Laboratory, Office of Public Affairs, September. Available at www.de.afrl.af.mil/Factsheets/ HPM.pdf.

Freeh, Louis J., with Howard Means. 2005. *My FBI: Bringing Down the Mafia, Investigating Bill Clinton, and Fighting the War on Terror*. New York: St. Martins.

General Accounting Office report: Critical infrastructure protection: Significant challenges in developing national capabilities. 2001. GAO-01-323, April.

Kohl, Geoff. 2005. Accessed and compromised. SecurityinfoWatch.com, April 7. Available at www.securityinfowatch.com/article/article.jsp?siteSection=306&id=3562.

Kurtz, Howard, and Pete Earley. 1984. Hill panel probes FEMA official; agency funds said used for residence. *The Washington Post*, August 1, Wednesday, Final Edition, A3.

Lange, Larry. 1997. The rise of the underground engineer. *EETimes* (972) September 22.

Maiffret, Marc. 2001. What can be done to reduce the threats posed by computer viruses and worms to the workings of government? Testimony before the House Subcommittee on Government Management, Information, and Technology, Aug. 29.

McKay, Niall. 1998. Do terrorists troll the Net? (Part 1). November 4. Available at www.wired.com/news/news/politics/story/15812.html.

Mitnick, Kevin, and William L. Simon. 2005. *The Art of Intrusion*. Indianapolis: Wiley.

Moore, David, et. al. Code red: A case study of the spread and victims of an Internet worm. Available at www.caida.org/outreach/papers/ 2002/codered/codered.pdf.

Moreno, Sylvia. 1998. Herndon man accused of lying for terrorist. *The Washington Post*, May 12, Tuesday, Final Edition, Metro, B5.

O'Hearn, Betty. 2003. Infowar/Infowarcon News for 08/30/03. Message posted to several mailing lists.

Penenberg, Adam L., and Marc Barry. 2000. *Spooked: Espionage in Corporate America*. Cambridge, Massachusetts: Perseus.

Poole, Gary Andrew. 1996. Hack attack. *Forbes*, June 3.

Summary of Senate hearing: Weak computer security in the government: Is the public at risk? Available at http://hsgac.senate.gov/051998_summary.htm.

Posner, Gerald. 2003. *Why America Slept: The Failure to Prevent 9/11*. New York: Random House.

Poulsen, Kevin. 1999. Zap! . . . and your PC's dead. ZDNet News, Sept. 9. Available at http://news.zdnet.com/2100-9595_22-515644.html?legacy=zdnn.

Radcliff, Deborah. 1998. IT security opportunities: Sleeping with the enemy. *Computerworld* October 5. Available at www.computerworld.com/news/1998/story/0,11280,32868,00.html.

Richtel, Matt. 1998. Reformed crackers reveal their secrets to paying audiences of former victims. *The New York Times*, Feb. 12. Available at www.nytimes.com/library/cyber/week/021298hack.html.

Schwartau, Winn. 1991. Computer security. Hearing of the House Subcommittee on Technology and Competitiveness, Committee on Science, Space and Technology. June 27.

———. 1996. Information *Warfare—Cyberterrorism: Protecting Your Personal Security in the Electronic Age*. New York: Thunder's Mouth Press.

———. 2005. E-mail communication of November 11.

Silberman, Steve. 1999. Kid-porn vigilante hacked media, Wired.com, Feb. 8. Available at www.wired.com/news/print_version/culture/story/17775.html?wnpg=all.

Staniford, Stuart, Vern Paxsony, and Nicholas Weaver. 2002. How to 0wn the Internet in your spare time. Proceedings of the USENIX Security Symposium. Available at www.icir.org/vern/papers/cdc-usenix-sec02/index.html.

Taylor, Clayborne D., and D. V. Giri. 1994. *High-power Microwave Systems and Effects*. Washington, D.C.: SUMMA.

Trigaux, Robert. 1998. "Byte-sized crime crackers—the bad apples among hackers—find government and business easy prey. *The Toronto Star*, July 4, Saturday, 2nd Ed., Insight, E1.

U.S. official quits under fire. 1984. *The New York Times*, August 5, Sunday, Late City Final Edition, Section 1, Part 1, 36.

Vacca, John R. 2002. *Computer Forensics: Computer Crime Scene Investigation*. Boston: Charles River.

Vranesevich, John. 1999. What kind of hackers head the culture? April 23, AntiOnline.com.

Weaver, Nicholas. 2005. E-mail interview of Sept. 15.

Weiner, Tim. 1999. The man who protects America from terrorism. *The New York Times*, February 1, Section A; Page 3.

Wells, Rob. 1998. Hackers warn of crippling gaps. The Associated Press, May 19.

———. 1998. Net "crippled in 30 minutes"; hackers warn of threat to Nationwide News Pty. Limited, *The Advertiser*, May 21. □