

The Internet in the Aftermath of the World Trade Center Attack

Briavel Holcomb, Philip B. Bakelaar, and Mark Zizzamia

A main purpose of the Internet, when first established in the late 1960s and early 1970s, was to provide a means of communication between command centers in various parts of the United States that would function in case of a national emergency when other methods of communication would be out of commission. The U.S. Defense Department's Advanced Research Projects Agency established ARPANET to link computers on the East and West coasts, as well as command centers in Utah and Illinois that could continue to communicate in the event of a nuclear attack. But it was over thirty years later on September 11, 2001, in the aftermath of the terrorist attacks on the World Trade Center (WTC) and the Pentagon, during which about 3,000 people were killed, that the Internet was used for the purpose for which it was originally designed. This paper was first written for the "Digital Communities: Cities in the Information Society" conference in November 2001 to explore both the function and the uses to which the Internet was put on 9/11 and the weeks that followed. It has been updated to include information on modifications to the Web in reaction to that "attack on America" and a discussion of the issue of security vs. privacy, an issue that is becoming increasingly controversial.

Journal of Urban Technology, Volume 10, Number 1, pages 111-128.

Copyright © 2003 by The Society of Urban Technology.

All rights of reproduction in any form reserved.

ISSN: 1063-0732 paper/ISSN: 1466-1853 online

DOI: 10.1080/1063073032000086353

Terrorists on the Internet

There is evidence that the terrorists who crashed two jetliners into the twin towers of the WTC, another into the Pentagon, and whose hijacked jet crashed in Pennsylvania short of their intended goal, conspired with a possibly far-flung network of terrorists in part by communicating via the Internet. Whether, and how, this was achieved is still a matter of some controversy. Initially, rumors and speculations spread in the media that there were coded orders for the attacks secretly hidden in pornographic Web images and that the terrorists used encryption or even steganography to communicate via the Internet. Encryption uses mathematical keys to scramble and unscramble a message, and while encryption is difficult to decipher, it can reveal who is communicating to whom “secretly” and, thus, may be of value to U.S. intelligence officials. Steganography, on the other hand, makes the message “disappear” by hiding it in a larger file such as a *.jpeg* or *.gif* image, or as an *.mp3* music file, although messages can be read by special software. Allegations that bin Laden’s followers were using encrypted messages hidden inside pornographic pictures made lurid news well before the WTC attack, though no actual proof has been found that Al Qaeda used this method. A former French defense ministry official is reported to have said that terrorists planning an attack on the U.S. Embassy in Paris used steganography. Others alleged that “terrorists have made a practice of putting encrypted messages, including maps of targets, inside seemingly innocent Internet chat rooms, bulletin boards, and other Web sites.” However, subsequent FBI analysis of hundreds of e-mail messages among the terrorist suspects have found no evidence of encryption beyond the possible use of such code words as referring to Osama bin Laden as the “director” or using the Arabic word for babyhood to mean “bomb.” In fact, the very mundaneness of their e-mails camouflaged them from surveillance. Web sites apparently hosted in China, Pakistan, and London may have provided communications among Al Qaeda operatives. As a computer security specialist remarked, the terrorists were successful because their activities had “none of the hallmarks of clandestine activity the intelligence agencies normally look for. They did nothing suspicious—until they did something abominable.” Nevertheless, this fact has not diminished calls for greater surveillance of the Internet and the demand that government be given “backdoors” to all encryption products. As will be noted, the debate about Internet surveillance has become heated.

Knight

Campbell

Kelley

“GIS and Steganography...”

Kolata

Lyman

Higgins et al.

Higgins et al.

Internet Uses and Functioning during the Crisis

Coughlin During the hijacking of the planes and the crumbling of the WTC, victims of the attacks made crucial digital communications. There are stories of final messages of love and farewell sent by cell phone and instant messaging from those who died at the WTC. Passengers in the plane headed possibly for the White House or Camp David were able to communicate with people on the ground and, alerted to the situation, fought with the hijackers, causing the plane to crash in Pennsylvania short of the terrorists' target, thus preventing even greater casualties. A corporate e-mail network gave evacuation orders to employees of the American International Group in six buildings in lower Manhattan.

It was in the hours immediately following the attack that the real test of the Internet came. Happening as it did in mid-morning Eastern Standard Time, news of the attack spread worldwide by telecommunications. While some media were at least partially compromised, the Internet withstood the attack remarkably well. Physical destruction of radio and television broadcasting antennae atop the WTC, and of fiber-optic and conventional telephone and data lines in the vicinity, temporarily crippled some local communications. The Verizon Communications building, near the north tower of the WTC, sustained heavy damage. Before the attack, it had been one of the nation's busiest telephone central switching stations, which, at full capacity, served a customer base comparable to a city the size of Cincinnati. But after power to the building was interrupted, service was temporarily disrupted for more than 300,000 phone lines and 3.6 million high-capacity data circuits, many serving Wall Street financial institutions.

Romero Furthermore, since it would take five years and millions of dollars to build alternative systems for all the telephone lines served by the Verizon building, there are no plans to do so. A year after the attack, it was reported that the failure of a "repeater"—an electronic device designed to boost radio transmissions in high-rise buildings—in the North Tower probably contributed to the loss of lives by impeding communications among firefighters. Meanwhile, the Internet continued to function at near-normal performance levels despite the rapid spike in traffic. Matrix.net, Internet performance measurement experts, reported that shortly after the attack, a significant performance degradation of the Internet was apparent as measured by increased packet loss and decreased "reachability", but the spike, though significant, was short-lived. IP traffic returned nearly to normal within an hour.

Dwyer and Flynn

Matrixnet

Although some sites slowed, neither the destruction of fiber

optic lines nor the heavy traffic on the Web caused major disruptions. Keynote Systems, which tracks the performance of 40 highly visited business sites, reported that while in the first few hours, a home page took three or four times as long to load as usual, things soon returned to normal. Nevertheless, Infoworld.com reported that the performance of the Internet was “affected more than during the California energy crisis, the Code Red worm, [and] the Baltimore train disaster” according to statistics provided by Mercury Interactive.

Tedeschi

Harrell and Grygo

There are several reasons why the Internet functioned so well, especially compared to other media. Unlike traditional phone calls, which require an open circuit between two people, data sent via the Internet travels in discrete packets, which can move over many different channels at the same time to be reunited at their destination. This enables packages to avoid bottlenecks, if necessary, by temporarily storing data packets, and then forwarding them when routes open. Packet switching and built-in redundancies enabled most messages to get through with minimal delays. A second reason for Internet success during the crisis was that media companies that received particularly heavy traffic took drastic steps to cut all but the most vital information from their sites. *CNN.com* and the *New York Times* on the Web both cut photos, graphics, extraneous text, and ads from the first page users reached, enabling users to download information more quickly. *CNN.com*'s home page before the attack held “more than 255 kilobytes of information: the slimmed-down version was about 20 kilobytes.” Another way companies coped was to divert servers from one use to another. *CNN.com*, for example, converted servers that were normally devoted to financial and sports news to news of the crisis. Thus *CNN.com* was able to cope with a nearly tenfold traffic surge.

Guemsey

Tedeschi

Schiesel and Hansell

Another reason for the survival of the Internet on September 11 was the rapid decrease in traffic on various categories of sites. Some commercial sites that are commonly very busy (e.g., Amazon.com and eBay) had fewer visitors than usual, though in the case of eBay this may have been partly attributable to the fact that the company halted trading on items purportedly from the disaster sites, which were offered for auction. Travel sites saw a decrease in visitors and advertising was minimized. Travelocity removed all ads from the Web, TV, and radio for a week, feeling that advertising was simply “inappropriate.” Given the proximity of Wall Street to the WTC, the financial industry was, of course, hard hit and E*Trade stopped taking orders for the rest of the day.

Tedeschi

Constructive Uses of the Internet in the Aftermath

Perhaps the most impressive function the Internet served on and soon after September 11, 2001 was to transmit millions of messages of inquiry and reassurance between survivors of the attack and their loved ones. There can be few people on the Net in the New York metropolitan region who did not send and receive messages concerning the crisis with its victims and survivors. Within hours, the authors (based in New Jersey) had received inquiries from as near as Manhattan and as far away as Europe, Asia, and Africa from relatives and friends. International students at Rutgers University reported similar messages from concerned families in many parts of the world. A Pew report published in September 2002 noted that many new Web sites, Weblogs (online logs or journals), and online discussion groups were posted in response to the events, and that while television may have been a better medium in delivering breaking news, the Internet had the advantage of offering depth of information, making available wider perspectives (including international ones), and providing a much more personal medium. “During a disaster, it’s a natural human impulse to reach out to others, and the Internet is nonpareil in bridging the distance that often separates us.”

Pew Research Center

Several registries were established almost immediately on the Web where both survivors and missing people could be registered. One of the first was hosted at the University of California at Berkeley, www.safe.millennium.berkeley.edu, but such sites proliferated causing some problems such as the need to register on multiple sites, all of which were not easily locatable. Some people, not finding their loved one on a register of survivors, may have needlessly been plunged into despair. Conversely, the absence on a victim list of a friend who worked at the WTC may have given false hope to others. The Greater New York Hospital Association eventually posted a list of patients admitted to hospitals from the WTC site, thereby arguably compromising patient privacy. More than a year after the attacks no complete list of victims, missing persons, or “survivors” exists. A CNN victim list contained 2,970 persons while the *september11victims.com* list had 3003 persons in October 2002. As late as November 2002, two “missing” persons on the list were “found,” and there are still 56 missing victims for whom no death certificate has been issued.

WTC Internet Remembrance Campaign

Lipton

An important function the Internet served immediately after the attack was to provide information about where to go for assistance and where to offer assistance. The non-media sites that received the

greatest increase in traffic that day included *disasterrelief.org* (with a 2,324 percent increase) and *redcross.org* (1,494 percent). The Port Authority of New York and New Jersey, which built and owned the WTC saw a 7,715 percent increase as people sought information. The Red Cross, America's largest disaster relief organization, received 20,959 visitors and received \$1,024 in donations the day before the attack (September 10). But on Tuesday, the number of visitors rose to 243,974 and within 12 hours \$1 million had been donated. Since the Red Cross site was so swamped, AOL, Amazon, and Yahoo accepted donations on their sites for the Red Cross, and by the end of the week \$39.5 million had been raised online. Before that, the most that had been raised online was \$2.5 million in response to earthquakes in India and Central America earlier in 2001. For the first time, online donations outpaced those to a toll-free number. As well as money, relief supplies such as clothing, blankets, and food poured into New York partly in response to online requests. The Internet became a way that people far from the disaster site could donate and feel useful. The "Internet has really come about as a great place for people to act quickly—almost impulse donate rather than impulse buy," said an Internet analyst at Nielsen/netRatings. The Salvation Army received \$1.5 million in online donations their first week, and a spokesman remarked that the Web "really affords people an opportunity to be generous and spontaneous in a new way, so we're very pleased with that."

Christensen

Mariano

Mariano

The Red Cross raised so much money so fast that on October 30 fund raising for the 9/11 victims was suspended since the \$547 million pledged was adequate for relief efforts. Controversy ensued when the Liberty Fund was set up within the Red Cross to manage funds donated for 9/11 and to prevent funds from being diverted to other chapters, but with a suggestion that \$200 million be set aside for use in the event of future terrorist attacks. The president of the Red Cross resigned over the furor. A year later in September 2002, the Red Cross reported receiving more than \$1 billion for the Liberty Fund and having distributed \$643 million, with \$200 million more expected to be distributed by the end of the year.

Barstow and Seelye

American Red Cross

Web sites were quickly set up to coordinate donations of office supplies, furniture, and rental space for displaced businesses. Information about the location of blood donation centers was available both on Web sites and sent by e-mail to many list-serves. The American Medical Association set up a database of doctors who volunteered for duty at the WTC site. The Red Cross set up 225 computers donated by Compaq in locations in New York and Washington to enable displaced survivors to post information about themselves and to e-

mail family and friends. Microsoft programmers in Redmond, Washington helped set up a family registration system for this effort. Within hours of the attacks a volunteer site called *siliconalleycares.org* was created “to organize and prepare groups of volunteers to effectively help the Red Cross in its management of the crisis.” Indeed, this disaster has “seen the integration of Internet technology that will better prepare the Red Cross and other relief agencies for the next disaster....It has just come together so quickly....The fact that this could be in place when the next hurricane or earthquake occurs and we could just throw a switch and turn this on is just mind-boggling,” according to a Red Cross official. Perhaps this integration of the Internet into crisis response can be viewed as one of the few silver linings of the event. The 2002 Pew report noted that in the cross-sectional sample of Web sites relating to 9/11, 36 percent allowed visitors to provide assistance to victims and 26 percent allowed individuals to seek assistance from others and from relief organizations.

Immediately after the collapse of the WTC, and continuing a year later, the Internet has seen a plethora of Web sites and e-mail messages offering poems, prayers, pictures, expressions of patriotism, personal accounts of the events, sympathy messages, sources for counseling, and the like. One could light a memorial cyber-candle (as did 1.1 million people the first week), or a real one at 10:30 P.M. one night in response to an e-mail stating that NASA planned to take a satellite picture as a memorial to the attack victims (which NASA never intended). One could add one’s name to numerous petitions pleading for peace, download American flags to print out and display, volunteer to create squares for the WTC Memorial Quilt at *www.wtcmemorialquilt.com*, or join a prayer circle at *Beliefnet.com*. Some may have wished to join the “cyberangels” to express support for our armed forces. A much-forwarded “tribute to the United States” by a Canadian TV commentator, Gordon Sinclair, which was reportedly read into the Congressional Record, called Americans “the most generous and possibly the least appreciated people on all the earth” (although that paean to the United States was actually written in 1973). But more critical analyses of the situation, such as one by Noam Chomsky pointing out the widespread famine and dire situation in Afghanistan prior to 9/11/01, were also circulated. The Internet thus became a very open forum for the free expression of ideas and opinions about the crisis. Without doubt, it served an important therapeutic function, allowing people to simply record their experiences and feelings. But it also facilitated a wide range of information about, perspectives on, and interpretations of the event from sources ranging from official government sites to Arabic media sites, from

“patriots” to “peaceniks.” Harris Interactive found that while American adults turned first to TV as their main source of information on September 11, 47 percent discussed the events online, and 23 percent said that using the Internet helped them deal with the events.

O’Connell

The Pew report, published a year later, noted that of their sample of Web sites, 75 percent were expressions of sadness, grief, and condolences; 61 percent expressed religious or spiritual thoughts; and 46 percent expressed patriotism. But anger, fear, and hate appeared on 52 percent of the sites. Harmon noted that virtual memorials on the Web have allowed mourners to do the equivalent of visiting a “grave site” for a loved one whose physical remains are not found, and, in some cases to write messages to their lost loved ones in cyberspace.

“Powerful Attack Upsets...”

Harmon 2002

The Internet acted not only as a source of information but a medium for testimony and recording the experience for posterity. Many accounts were posted on *www.worldnewyork.org* (a defunct site a year later) and the Library of Congress worked with the Internet Archive to collect Web sites related to the attacks (see *www.webarchivist.org*). The WTC disaster is the most documented event in human history. The documentation is in all media from print, to video, to photography, to the Web. Images of the disaster, its victims, personal accounts, news stories, and a huge amount of similar archival material is on the Web (see <http://911digitalarchive.org> for links to some of these). Online discussion groups have greatly facilitated public input to plans for the redevelopment of the WTC site, allowing people who cannot go to public meetings to voice their ideas and concerns.

Negative Uses of the Internet in the Aftermath of 9/11

There were, inevitably, destructive uses of the Internet, in which hoaxes were circulated, hackers disrupted sites designed to help, hate speech was evident, and efforts to profit financially from the disaster appeared on the Web. Some of these were fairly harmless, such as the fake photo of a tourist atop the WTC observation deck oblivious to the plane approaching just behind him, or the quotation from Nostradamus supposedly predicting the tragedy. The tourist was depicted wearing a heavy coat and hat on a beautiful day and, as the Observation Deck did not open until 9.30 A.M. (the first plane crashed into the North Tower at 8.45 A.M.), the question of how the camera and film survived is moot! A year later, the same tourist was depicted on the Web in other imaginary disaster locations. The predictive quotation from Nostradamus made the book a sudden best seller on *Amazon.com*,

but the supposed quotation, said to have been written in 1654, is not in the book, and Nostradamus died in 1566. Nevertheless, Nostradamus joined “sex” and “mp3” on the list of terms most frequently entered on Internet search engines. The photographer who took the picture of the burning WTC that seems to contain a face (bin Laden? The devil?) in the smoke transmitted the image to AP within 15 minutes of the attack, and he did not notice the face at the time. Nevertheless, he received over 4,000 e-mails from people, some of whom thought he was a divine messenger, others that he had doctored the image. Some rumors were more problematic. Early rumors of cell-phone messages from victims still alive beneath the rubble raised hopes unnecessarily and complicated rescue efforts. An e-mail sent to hundreds of people claiming the city’s water supply had been poisoned created paranoia. A much forwarded e-mail ostensibly from a friend of a woman who was dating an Afghanistani man who begged her not to go on any commercial airlines on 9/11 and not to go to any malls on Halloween...and then disappeared, was refuted formally by the FBI. An imaginative array of possible terrorism attacks posted on *MSNBC.com* included such things as smallpox spread by suicide disease carriers and disguised production workers contaminating consumer goods such as vitamins and baby powder, but such fears “could easily prove contagious” heightening paranoia.

As the 2002 Pew study noted, “the Web was an incubator of rumor as well as an inoculator—knocking down rumors and other fanciful tales.” While Nostradamus received the most searches on Google in September 2001, the first site returned (*Nostradamus-repository.org*) actually refuted the idea that he had predicted the attack, and a site devoted to verifying “urban legends”—Snopes—set up a separate section for 9/11 rumors.

Other Web sites displayed dismaying levels of hate, xenophobia, and vengeance. The site for *DeadArab.com*, which proclaimed itself as “the best anti-Osama bin Laden and Taliban site around,” featured bin Laden hanging from a noose attached to a pole from the wreckage of the WTC with firefighters observing below. The site offered sales of tee-shirts festooned with depictions of Arabs hanging from trees, games in which the goal was to shoot bin Laden and other Al Qaeda members, and hate messages directed towards anyone who resembles an Afghanistani. (Strangely, a year later in October 2002 the *DeadArab.com* site provided links to casinos on the net, insurance, careers, and completely unrelated material.) Similar sites proliferated (e.g., *www.killosama.com*) and included such messages as “the Middle East should be nuked and paved for a European parking lot.” At the same time, there was a surge of hacking incidents on Middle

Eastern networks including web pages and governmental databases. The Taliban Web site (<http://www.talibonline.com>) was hacked into, and its information replaced by a proclamation that “The United States will Destroy You! ... Project Afganistand!!! (*sic*) Knock them Out! Hacked by MaxMouse... You will pay for this you stupid fools!!!!...” (*sparkhost.com 2001*). Some pages that actually opposed bin Laden and the Taliban, such as www.AfghanGovernment.org, were mistakenly hacked into by groups that mistook them for supporters. The *AfghanGovernment* site was flooded with over 10,000 hate messages after the attacks, and within a few days hackers were able to take it down completely. In October 2001, the site contained a letter from President Burhanuddin Rabbani who was recognized by the U.N. and many countries as the official ruler of Afghanistan. A year later, in October 2002, the *AfghanGovernment.org* site led one to sites offering tapestry throws, Afghan dog tee-shirts, and handcrafted dog jewelry!

“Crisis”

Other Web sites appeared to support the terrorists including one with a heading “The Road to Jihad,” which included an urban skyline in flames with burning U.S. and Israeli flags. One had “animations of dripping blood, Kalashnikov automatic weapons and admonitions to vanquish the ‘enemies of Allah’ by any means necessary” (8). Another gave advice on handling guns and suggested wearing gloves to avoid fingerprints. A site with audio and video clips of speeches by bin Laden asked supporters to send money to a bank in Pakistan for which account numbers were provided. Most such sites were removed within a few days either by the hosting companies or whoever posted them in the first place.

Lohr

Lohr

As noted earlier, the Web performed an excellent service in raising funds for victims of the attacks, but perhaps inevitably, it also bred scams. Web sites “festooned with American flags, had buttons viewers could click to make donations to the Red Cross or the Victims Survivors Fund.” On clicking a button one was taken to another site that asked for a credit card number. The site was shut down shortly after the FBI was informed. Another e-mail message asked for donations to help find Osama bin Laden and asked for wire transfer of money to a bank in Estonia. Various unofficial Web sites asked for donations for families of firefighters, children orphaned by the attacks and similar groups of victims, though it is doubtful that donations reached intended recipients.

Peterson

Peterson

Other somewhat crass efforts to capitalize upon the tragedy included the rush to register topical URLs (especially including bin Laden) that could later be sold to the highest bidder. Domains such as *09112001.com* or *worldtradecenterdisaster.com* were bought, though

whether for profit or to memorialize the victims was not clear at the time. Although the owner of the latter domain was initially rumored to have received an offer of \$1.47 million, in fact he paid \$30 to register *worldtradecenterdisaster.com/org/net* and *worldtradecentermemorial.com/org/net*. “I registered them a few minutes after the attack, which I witnessed live on TV...I wanted to do something helpful, so I immediately put up the Web site that’s still there today. Later I contributed *worldtradecentermemorial.com/org/net* to a nonprofit organization that was making an online memorial.”

Although he did receive an indirect offer from an unnamed insurance company for all the domain names, they did not mention a price. A year later, *worldtradecenterdisaster.org* was a quite comprehensive site, offering memorials, links, information, and the message that \$110,266,000 had been collected online (by October 16, 2002) for disaster relief.

Network Solutions removed *Twintowers09112001.com*, which had an asking price of \$65,000, from its auction service to prevent inappropriate uses. However, a year later *www.twintowers911.com* leads one to *www.usretaliation.com* with images of the American eagle sharpening its talons and holding bin Laden in its beak and the message “Never Forget: Never Surrender.” Others sought profit from the sale of patriotic gore. One could, for example, buy a T-shirt or mouse pad online both of which are decorated with the image of the side of a milk carton and bin Laden’s face in the “Missing Person” section of the carton. Also available were hats or handkerchiefs embellished with “Evil will be Punished,” or buttons with the stars and stripes with the declaration, “These colors don’t run.” Within hours of the attack, a drawing of the WTC that was selling for \$5 on eBay leapt to \$250 before eBay banned sales of WTC items since pieces of the ruins began to appear. That policy was later changed to allow memorabilia to be sold for charity.

“The Stuff of Patriotism...”

The Future of the Internet after the “Attack on America”

Three years before the WTC disaster, the U.S. Department of Defense created an office to defend the United States from cyberattack. Its mission is primarily to safeguard infrastructure. The FBI also established the National Infrastructure Protection Center at about the same time, and the Commerce Department created a Critical Infrastructure Assurance Office shortly afterward. Nevertheless, when the new Office of Homeland Security (now a Cabinet Department) was established in the days after the attack, Senator Joseph Lieberman

suggested that it spearhead the country's anti-cyberterrorism efforts. Within days of the attack, President Bush appointed a new special advisor for cyberspace security who reports both to Homeland Security and the National Security Advisor. Given the potential for cyberterrorists to cause tremendous damage by disrupting financial records, air traffic controls, electrical grids, pipelines, or production lines of pharmaceutical industries, to mention just a few, the need for greater surveillance of the Internet was recognized, and increased security measures were also seen as being necessary. Two days after the attack, the Senate approved an amendment as part of a Justice Department spending bill that makes it easier for law enforcement to "wiretap" Internet communications. The F.B.I. already uses its Carnivore system to monitor communications between suspects.

Both federal and state governments have also begun removing information from the Web. The "location and operating status of nuclear power plants, maps of the nation's transportation infrastructure, and an array of other data suddenly deemed too sensitive for general consumption" have been taken down. The Environmental Protection Agency (EPA) removed a database with information on chemicals used at 15,000 industrial sites, although that information remains available at reading rooms around the country. The U.S. Geological Survey (USGS) removed nuclear facility maps from its "National Atlas of the United States" Web site; Los Alamos National Laboratories have removed various reports; the U.S. Department of Energy's site for the National Transportation of Radioactive Materials has been removed; and Risk Management Plans are no longer on EPA's site. New Jersey removed its Community Right to Know information on about 30,000 private-sector facilities that store chemicals, despite the fact that firefighters accessed this database en route to fires. Similarly, New York State, along with many other states, removed material potentially useful to terrorists. Obviously, there has been criticism of these actions since such information is useful to the public, but even the Federation of American Scientists removed data on nuclear weapons facilities from its Web site.

The relative importance of freedom of information and national security is the subject of an ongoing debate. In early 2002, a new Information Awareness Office (IAO) within the Defense Department, headed by John Poindexter (who was the national security advisor and a controversial figure in the Iran-contra scandals during the Reagan Administration) was established. Its mission is "total information awareness" which includes biometric signatures of humans, and cognitive aids to allow humans and machines to "think

Garretson

"When Terrorists Log On"

Collin
Schwartz "Securing the Lines..."

Alvarez

Schwartz "In Investigation..."

Toner

Meuser

McKinley

together,” often using the Internet. Civil libertarians and others are concerned with the invasion of privacy implied (perhaps especially so since the IAO’s logo includes the “all-seeing eye” of the Freemasons seal!). In September 2002, the Bush Administration released a draft report on “The National Strategy to Secure Cyberspace,” but it was criticized both by high-tech companies and by civil liberties advocates. The following month a bipartisan report, “Protecting America’s Freedom in an Information Age” called for decentralized information systems which could both protect privacy and prevent terror, and for greater sharing of information between different levels of government. In November 2002, the Information Awareness Office was reportedly building a “vast electronic dragnet” which could “data mine” commercial, governmental, and personal data bases (including phone logs and bank records), though the 1974 Privacy Act would have to be amended to deploy the system.

Schwartz “Revamped Proposal...”

Miller

Markoff

Private-sector companies also feared an increase in cyber terrorism and increased security by upgrading firewalls and intrusion detection systems. Now that the Office of Homeland Security has become a federal department, increasing funding and attention are being given to Internet security issues.

Markoff

There are indications that e-commerce grew in the immediate aftermath of the attacks as a reaction to people’s disinclination to shop in crowded places. Certainly, online sales of Cipro boomed as the anthrax scare grew. Similarly, anthrax sent through the U.S. postal system caused many to turn to e-mail for communications. Even the Direct Marketing Association urged its members in this \$528 billion industry to send e-mail in conjunction with mass mailing campaigns. Likewise, videoconferencing company shares rose soon after the attacks as people avoided air travel when possible. The longer lasting effects of the attacks on commercial communications are impossible to separate from the effects of the subsequent economic downturn.

Henriques

Festa and Konrad

Non

Most assessments agree that the Internet passed its first big test in the WTC crisis and will continue to grow. However, it was not the target of the attack on September 11, and some anticipate that we could still face a “cyber Pearl Harbor” and warn that we are “sitting on a cyber time bomb.” In October 2002, an electronic attack briefly crippled 9 of the 13 computer servers that manage global Internet traffic in the “largest and most sophisticated assault on the servers in the history of the Internet.” Although the attack was short lived and hardly noticed, future attacks may be less easily deflected. The Internet continues to hold great promise and peril. As the “father” of the Internet, Vinton Cerf, remarked the day after the attack: “Now,

Meuser

“Powerful Attack Upsets...”

more than ever, the Internet must be wielded, along with other media, to cast bright lights on all who would destroy freedom in the world. Information is the torch of truth, and its free flow is the bloodstream of democracy.”

Bibliography

- L. Alvarez, "Spying on Terrorists and Thwarting Them Gains New Urgency," *New York Times* (September 14, 2001), A17.
- P. Atfab, "Cyberangels Special Message: Terrorist Attack on the United States" (September 2001) <www.cyberangels.com> (Accessed September 20, 2001).
- American Red Cross, *September 11 Report* (September 5, 2002) <www.redcross.org/disasters> (Accessed November 3, 2002).
- D. Barstow and K. Seelye, "Red Cross Halts Collections for Terror Victims," *New York Times* (October 31, 2001) B11.
- A. Batey, "Can He Save the World?" <MediaGuardian.co.uk> (October 29, 2001).
- D. Campbell, "How the Terror Trail Went Unseen," *Telepolis* (October 8, 2001) <www.heise.de/tp/english/inhalt/te/9751/1.htm> (Accessed November 5, 2001).
- V. Cerf, "Words for All of Us from Vinton Cerf" (September 12, 2001) <www.icdri.org> (Accessed October 26, 2001).
- J. Christensen, "Relief Agencies Retool to Handle Online Flood," *New York Times* (September 26, 2001) H1, H8.
- B. Collin, "The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge," paper presented at the Eleventh Annual Symposium on Criminal Justice Issues of the Institute for Security and Intelligence (Chicago, 1996) <<http://afgen.com/terrorism1.html>> (Accessed October 31, 2001).
- K. Coughlin, "Internet Becomes Only Link after Cell Phones Fail," *Star Ledger* (September 12, 2001) 28.
- "Crisis," Blogspot.com <<http://crisis.blogspot.com>> (Accessed October 27, 2001).
- J. Dwyer and K. Flynn, "911 Tape Raises Added Questions on Radio Failures," *New York Times* (November 9, 2002) A1, B4.
- M. Farley, "Hoaxes, Rumors, and Wishful Thinking Spawned Trauma," *Los Angeles Times* (September 28, 2001) <www.latimes.com> (Accessed September 28, 2001).
- P. Festa and R. Konrad, "Anthrax Worries Find Answer in E-mail," *Zdnet News* (October 16, 2001) <<http://netscape.zdnet.com>> (Accessed October 25, 2001).
- D. Filkins, "As Thick as the Ash, Myths Are Swirling," *New York Times* (September 23, 2001) Section 4, 2.
- C. Garretson, "Senator Says New Office Should Cover Cyber Terrorism," *IDG News Service, Washington Bureau* (September 21, 2001).

- "GIS and Steganography-Part I: Hidden Secrets in the Digital Ether," *Directions Magazine* (April 9, 2002) <www.directionsmag.com> (Accessed November 7, 2002).
- L. Guernsey, "Keeping the Lifelines Open," *New York Times* (September 20, 2001) G1, G6.
- A. Harmon, "The Search for Intelligent Life on the Internet," *New York Times* (September 23, 2001) Section 4, 1.
- A. Harmon, "Real Solace in a Virtual World: Memorials Take Root on the Web," *New York Times* (September 11, 2002) 39.
- H. Harreld and E. Grygo, "U.S. Attack: Internet Performance after Attack Could Be Worst Ever," *Infoworld.com* (September 12, 2001) <www.inforworld.com/articles/hn/xml/oi/09/12/01092hyperformance.xml> (Accessed November 1, 2001).
- D. Henriques, "Anthrax Drug Is Promoted on Web Sites," *New York Times* (October 15, 2001) C8.
- A. Higgins, K. Leggett, and A. Cullison, "How Al Qaeda Put Internet to Use" *Wall Street Journal* (November 11, 2002) <www.msnbc.com> (Accessed November 11, 2002).
- D. Hopkins, personal e-mail communication, (October 21, 2002).
- M. Kakutani, "Fear, the New Virus of a Connected Era," *New York Times* (October 20, 2001) A13.
- J. Kelley, "Terror Groups Hide Behind Web Encryption," *USA Today* (February 5, 2002) <www.usatoday.com> (Accessed January 26, 2003).
- W. Knight, "Controlling Encryption Will Not Stop Terrorists," *New Scientist* (September 18, 2001) <www.newscientist.com> (Accessed September 18, 2001).
- G. Kolata, "Veiled Messages of Terror May Lurk in Cyberspace," *New York Times* (October 30, 2001) F1,4.
- E. Lipton, "Sept. 11 Death Toll Declines as 2 People are Found Alive," *New York Times* (November 3, 2002) A17.
- S. Lohr, "Internet Access Providers Curb Both Terrorist Postings and an Anti-Islamic Backlash," *New York Times* (September 17, 2001) C8.
- E. Luening, "VeriSign Bars 'Offensive' Net Name Auctions" (September 2001) <<http://news.cnet.com/news/0-1005-200-7228509.html>> (Accessed September 19, 2001).
- J. Lyman, "How Terrorists Use the Internet," *Newsfactor.com* (October 2001) <www.newsfactor.com/perl/story/7731.html> (Accessed October 11, 2001).
- G. Mariano, "Web Donors Give Millions in Relief" *CNETNews.com* (September 17,

2001) <<http://news.cnet.com/news/o-1005-200-7208068.html?tag=1>> (Accessed September 18, 2001).

J. Markoff, "Pentagon Plans a Computer System That Would Peek at Personal Data of Americans," *New York Times* (November 11) A12.

Matrixnet, "Internet Withstands Attack on America," press release (October 16, 2001) <www.matrix.net> (Accessed October 16, 2001).

J. McKinley, "State Restricts Data on Internet in Attempt to Thwart Terrorists," *New York Times* (February 26, 2002) B1, B5.

M. Meuser, "Post 9/11 Age of Missing Information" <www.mapcrusin.com> (Accessed March 14, 2002).

J. Miller, "Report Calls for Plan of Sharing Data to Prevent Terror," *New York Times* (October 7, 2002) A11.

S. Non, "Videoconferencing's New Appeal," *CNETNEWS.com* (September 18, 2001) <<http://news.cnet.com>> (Accessed September 18, 2001).

P.L. O'Connell, "Taking Refuge on the Internet: A Quilt of Tales and Solace," *New York Times* (September 20, 2001) G3.

M. Peterson, "Report of Scams Preying on Donors Are on the Rise," *New York Times* (September 28, 2001) A18.

Pew Research Center, "One Year Later: September 11 and the Internet" (September 5, 2002) <www.pewinternet.org/reports/> (Accessed November 3, 2002).

"Powerful Attack Upsets Global Internet Traffic," *New York Times* (October 23, 2002) A17.

Reuters, "Companies Fear Wave of Cyberterrorism," (September 18, 2001) <[wysiwyg:/8/http://netscape.zdnet.com:80](http://www.wysiwyg.com/8/http://netscape.zdnet.com:80)> (Accessed September 20, 2001).

S. Romero, "Attacks Expose Telephone's Soft Underbelly," *New York Times* (October 15, 2001) C4.

S. Schiesel and S. Hansell, "A Flood of Anxious Calls Clog Phone Lines," *New York Times* (September 12, 2001) A8.

J. Schwartz, "In Investigation, Internet Offers Clues and Static," *New York Times* (September 26, 2001) H1, 8.

J. Schwartz, "Revamped Proposal Suggests Strategies to Tighten Online Security," *New York Times* (September 18, 2002) A21.

J. Schwartz, "Securing the Lines of a Wired Nation," *New York Times* (October 4, 2001) G1, G8.

Siliconalleycares.org, *Homepage* (September 2001) <www.atnewyork.com> (Accessed October 8, 2001).

G. Slabodkin, "New U.S. Office to Battle Cyberterrorism," *Newsbytes* (July 23, 1998) <wysiwyg://24/http://www.exn.ca/Stories/1998/07/23/58.asp> (Accessed October 31, 2001).

"The Stuff of Patriotism, and Cheap Too," *New York Times* (October 7, 2002) A11.

B. Tedeschi, "E-Commerce Report: The Internet Passes Its First Test as a Source of Communications in the Aftermath of a Disaster," *New York Times* (September 17, 2001) C6.

R. Toner, "Reconsidering Security, U.S. Clamps Down on Agency Web Sites," *New York Times* (October 28, 2001) B4.

"When Terrorists Log On," editorial, *New York Times* (October 14, 2001) Sec 4, 14.

WTC Internet Remembrance Campaign, "Internet Remembrance Campaign" <worldatwar.org> (Accessed October 16, 2002).

