The Joan Shorenstein Center on the Press, Politics and Public Policy

Working Paper Series

The War on Terrorism Goes Online: Media and Government Response to First Post-Internet Crisis

By Andrew J. Glass
Shorenstein Fellow, Fall 2001
Senior Editor, *The Hill*

#2002-3

The Joan Shorenstein Center
PRESS ▪ POLITICS
▪PUBLIC POLICY▪
Harvard University
John F. Kennedy School of Government

THE WAR ON TERRORISM GOES ONLINE:
Media and Government Response to First Post-Internet Crisis

By Andrew J. Glass

Discussion Paper
December 2001

The Joan Shorenstein Center
John F. Kennedy School of Government
Harvard University

Introduction

For the first time, all the headline-making events that have happened since the terrible Tuesday in September on which the United States was successfully attacked by foreign terrorists have occurred during the Internet Age. While the parameters of today's online communications' systems were in place during the 1991 Persian Gulf War, that relatively brief struggle occurred shortly before the advent of the World Wide Web and, consequently, before millions of people across the planet could access and exchange information in real time on Internet-enabled computers.

This paper investigates the multifaceted role that the Internet has played in the initial phases of the equally multifaceted campaign against global terrorist networks in what Defense Secretary Donald Rumsfeld calls this "so-called war." It is an effort that, necessarily, seeks to evaluate a moving target. Nevertheless, some the unique aspects of the post 9-11 Internet environment were already evident three months after the attacks.

Moreover, the broader questions of U.S. information policy have strong implications for the Net, which can be made to respect national borders only under the kind of draconian conditions that have yet to be widely imposed in the West and that, in any event, would pose significant technical, legal and administrative challenges were they to be implemented.

In theory at least, an terrorist based in the Middle East equipped with a satellite-enabled link to the Internet could read today's issue of The New York Times -- replete with uncensored strategic and tactical battle reports -- online in the same time frame as any Manhattan-based reader. (Making such a satellite-based data phone call, to be sure, could also attract the interest the National Security Agency.)

Conversely, one the hottest Internet sites in the hours that followed U.S. military retaliation against the then Taliban rulers in Afghanistan in early October 2001 was a site based in Qatar, a small oil-rich nation on the Persian Gulf.

The first pictures of the Oct. 7 bombing strikes on Kabul appeared on aljazeera.net, the Arab world's equivalent of CNN and MSNBC. Although the site is in Arab, enterprising netizens could make out the gist of the stories through an Arab-English translation site such as tarjim.ajeeb.com/ajeeb.

Said Peter Brown, an editorial page columnist for the Orlando Sentinel: "In this Internet age, when the terrorists can read the Washington Post instantaneously in Kabul, there is reason to carefully limit logistical information about U.S. forces. This is a new kind of war. If the changes that this new kind of warfare requires limits the news media's ability to do their job, then that's

too bad. However, let's not whine about it. It would be nice if everyone understands that we are in this together."

In comparison to other recent military operations, President Bush and his advisers appear to have gone to greater lengths to conceal information, which has direct implications for the freewheeling Net culture. Even while it identified Osama bin Laden as its primary suspect, the White House initially refused to provide any of the evidence it possessed linking bin Laden's organization to the attacks. Instead, Americans got their information indirectly when British Prime Minister Tony Blair outlined the case in a speech to Parliament and immediately posted a dossier on the evidence on the Internet, which was then widely linked to news sites around the globe.

As illustrated by the Blair posting, the potential use and misuse of cyber-technology has become integrated into the post-Sept. 11 world. Thus, the Internet has also served as the source of many, if surely not all, of the 250,000 tips received by the FBI to date since the attacks. Persons interested in collecting the $25 million reward for Osama's capture are able to download the full particulars of the offer on the Justice Department's anti-terrorism Web site.

Another Internet staple application - chat room logs that record Web data transfers -- could be, and probably already have been, used by the FBI and CIA to locate the terrorist networks. There are also indications that the U.S. government is seeking to use highly sophisticated cyber techniques to deplete the terrorists' financial networks, although, in most cases, foreign government need to cooperate with such endeavors.

In sum, all this suggests that, in more ways than one, the Internet nowadays is serving as a double-edged sword, an information tool that at once both propagates and ameliorates these high crimes.

Crisis News on the Net

For some Americans, the Internet proved to be an immediate boon in helping them to deal with the horrific events of Sept. 11. Instant web sites and "white pages" were set up as a means to help search for and identify missing persons. News groups, listservs and newsletters became beacons of guidance seeking to cut through the chaos.

In the ensuing hours after the attacks, American Data Technology Inc., one of the nation's largest dedicated Web host firms, posted a notice on its site that pleaded with its clients of Internet Service Provides "to limit [their connections] to the network as much as possible" in order to allow critical voice and data traffic to get through. Nevertheless, on the whole, the Net did not fail even as the weakest links in the system proved to be the servers that support major news Web sites.

Meanwhile, clogged telephone lines - which utilize a big chunk of the same Net infrastructure that served news sites -- prevented family members from reaching loved ones feared missing or dead. In some poignant cases, e-mail proved to be the last resort and the final means of communication from the twin World Trade Center twin towers before their catastrophic collapse.

The big picture, however, reveals that the terrorist attack on U.S. soil immediately increased Internet usage of online-enabled Americans. According to a study by Jupiter Media Metrix, an authoritative source of online demographics, an average of 11.7 million Americans visited online news sites on each day in the week after the Sept. 11 attacks -- nearly double the 6 million who had visited news sites in the week before the attack. A follow-up Harris Interactive survey found that two weeks after the attacks, the number of wired Americans logging onto news sites had

more than doubled. (In addition to news sites, the Red Cross Web site [RedCross.org] averaged 398,000 unique visitors a day during the week.)

The chart below, extracted from the Jupiter data, reviews the viewership response at major news portals that drew a million or more unique visitors during the week:

Online Site	Number of unique visitors	% increase from previous week
CNN	17,247,000	23.2
MSNBC	14,994,000	20.2
ABC News	5,469,000	7.4
CBS	4,842,000	6.5
New York Times	4,536,000	6.1
Washington Post.com	4,430,000	6.0
Slate	3,443,000	4.6
USAToday.com	3,367,000	4.5
Fox	2,934,000	4.0
BBC	2,624,000	3.5
Los Angeles Times	1,343,000	1.8
Associated Press	1,221,000	1.6
Boston Globe	1,006,000	1.4

Another study by the Pew Research Center for the People & the Press -- conducted between September 12th and 13th among a sample of 1,226 adults, 18 and older -- revealed that Americans mostly relied on television in the immediate aftermath of the attacks -- even as they sharply raised their Internet usage in order to stay in touch with loved ones, friends and business associates.

Given the networks' collective response to the first instance of megaterror of American soil, it is not at all surprising that the Internet initially played a second-fiddle role as an information medium. The "Big Four" networks suspended all of their regular programming and substituted wrap-around news coverage for at least the first 90 hours of the crisis -- exceeding the continuous airtime they had devoted to the assassination of President John F. Kennedy in 1962 and the start of Operation Desert Storm in 1991.

Nevertheless, for millions of Americans with access to the Internet, cyberspace played an important paramount or supplementary role as an effective communications tool, furnishing both via e-mail and instant messaging services in addition to access to news sources within the United States and abroad.

However, according to Pew, only 3 per cent of Internet users said that they had gotten most of their information about the attacks from the Internet. By contrast, 81 percent of all Americans got most of their information from television. Interestingly, there was no measurable statistical difference between Internet users and non-users in their reliance on TV news.

Some 11 percent got most of their information from radio. Again, there was no statistical difference between the responses of Internet users and non-users. (A quarter of Internet users multitasked on that fateful Tuesday by having their TV sets or radios on while they surfed or dealt with their e-mail.)

On Sept. 11, the day of the attack, 15 percent of all Internet users sent e-mail messages concerning that traumatic event to family members and 12 percent sent e-mail to friends. In addition, 6 percent of Internet users sent instant messages to on that Tuesday -- about the same level of usage of instant messaging services that takes place on any given day online.

On an overall basis, 36 percent of Internet users sought news online in the first two days in the immediate aftermath of the attacks. On that Tuesday alone, 29 percent of Internet users -- some 30 million people -- sought news online. That is one-third greater than the normal news-seeking online audience on a normal news day.

In the first 48 hours after the crisis, 13 percent of Internet users logged into virtual meetings or participated in virtual communities by reading or posting comments in chat rooms, online bulletin boards, or e-mail list servers. On a typical day, only 4 percent of online Americans visit chat rooms.

Of the Internet users who sought to obtain news of the crisis online on the day of the attacks, 43 percent of them said they experienced problems reaching their desired sites. Within this group, 41 percent kept on trying; 38 percent went in search of news to other sites and 19 percent gave up entirely.

In sum, the Pew survey concluded that while the Internet was not a primary resource for news or outreach for most Americans immediately after the terror attacks, it still served as a useful supplement, particularly through the use of e-mail and instant messaging, and as a news source.

No doubt, a lack of accessibility was one reason why online news services failed to measure up in the immediate wake of the attacks. The average "reachability" of the Internet dropped just over 8 percent from 96 percent to 88 percent around 10 a.m. EDT, about one hour and 15 minutes after the attacks began, according to Jupiter Metrix.Net.

At major news sites, which normally take between 2.5 and 3.5 seconds to access a Web page, the access time proved to be between 20 and 40 seconds. Moreover, for nearly three hours after the attack, some of the Internet's foremost news sites -- including MSNBC, CNN and ABC -- were unavailable because their primary servers had been destroyed in the collapse of the World Trade Center towers.

Once they were viable again, some news sites, such as CNN, recognized their backup servers' overload problems and redesigned their pages to strip out graphics, ads, and other time-consuming downloadable features, thereby increasing their throughput capacity. Once back in operation, CNN saw record traffic, reaching 9 million page views an hour, compared to ordinary volume of 11 million page views per day. Having streamlined its site, was CNN able to connect effectively to the enormous online community thirsting for up-to-the-minute news of the crisis and resume some kind of service.

The Harris data closely tracked the Pew findings. Thus Harris reported that on Sept. 12, 2001, television proved to be the primary source of information for 78 percent of Americans with online access in the 24 hours immediately following the attacks -- followed by radio at 15 percent and the Internet at 3 percent.

However, a Harris poll completed three weeks later showed that the Internet has achieved statistically significant gains, with 8 percent of the population using the Internet as their primary source of news, while both television (at 76 percent) and radio (at 8 percent) experienced a modest decline.

"There can no longer be any doubt that, for Americans who have online access, the Internet is second only to television as the medium of choice for news and information," said Michael

Zimbalist, acting executive director of the Online Publishers Association. "And unlike any other medium, the Internet audience continues to experience rapid worldwide growth."

According to Harris, the percentage of people using the Internet as one of their information sources, if not their primary source, jumped from 64 percent to 80 percent in the two weeks since the attacks, overtaking radio (72 percent) and second only to television, with 98 percent.

The top reasons given for using the Internet as a news and information source were:

-- It provides information users want when they want it (63 percent of the respondents).

-- It delivers more detailed information (43 percent).

-- It offers more up to date information (42 percent).

-- The news is accessible at work (42 percent).

Harris reported that in the wake of the attacks 35 percent of the people interviewed said their number of visits to news websites had increased and that 47 percent said the amount of time they spent on news websites had also risen appreciably.

Yet another metric came from MeasureCast Inc., which reported that AM News/Talk stations that streamed their programs over the Internet pumped out more hours of coverage to larger audiences as various aspects crisis enfolded.

Evidence of this growing trend occurred on Monday, Nov. 12, 2001 when American Airlines flight 587 crashed in Queens, New York, near John F. Kennedy International Airport and was at first suspected to be another terrorist act. MeasureCast chief executive Edward Hardy said "many terrestrial AM News/Talk stations streaming their programs over the Internet streamed more hours that day than they did the previous Monday. We saw the same thing happen on September 11th, but the ... audience size increases were more dramatic."

Online Journalism

"The Internet has had a good war," says David Brooks, senior editor of The Weekly Standard, a Washington-based opinion journal which, quite typically nowadays, puts its own work online for subscribers to its paper edition.

Online journalism may be sponsored by a parent cable or print outlet, such as CNN or The Wall Street Journal. Or it may be a stand-alone effort, such as Slate, which is wholly owned by Microsoft Corp., or Salon, which solicits both ads and $6-a-month subscriptions in order to read the full content. Or it may take the form of an independent Web site that is maintained by an already well-known journalist such as Andrew Sullivan (www.AndrewSullivan.com), or Michael Barone (www.MichaelBarone.com). Sometimes, the cyber-based news material is duplicated in another medium, either in the same or in an altered form.

Online journalism has been around for nearly a decade. It is yet another example of "re-positioning" -- the effort of media owners to diversify their holdings with interlocking and competing media. Nearly every major U.S. newspaper has hedged its investments by creating its own online site, with news as a key element in the cyber mix.

San Diego's "Sign On" carries a full share of crisis-related reports to a local audience that is heavily engaged in military affairs. Launched in 1996, "SignOnSanDiego" set up its own desk operation within the Union-Tribune newsroom in 2001, linked to newsroom staff of 20 in a separate building.

"SignOn," said Gene Bell, chief executive of the Union-Tribune Newspapers, a member of the Copley newspaper chain, "is simply a different way of providing our content. We are no longer

limited to print. We can add value for readers with this synergy. Newspapers must grow beyond the print product."

"Online coverage of the anti-terrorist effort reflects both our strengths and weaknesses," David Plotz, Slate's Washington bureau chief, told a Shorenstein Center audience in November 2001. "Without a doubt," Plotz added, "from bad times come good stories."

Plotz noted "an enormous surge of traffic" to the Slate site. The weeks following the Sept. 11 attack brought some 10 million unique visitors to the online service, against 3 million who would normally visit in a month.

On the plus side, Plotz said, the Internet has raised the velocity of news coverage. "The rate at which people demand news is becoming faster and faster," he observed. "The Web is able to provide more substance than the all-news cable outlets. People want analytic information very quickly. They are being barraged with disparate facts from all over the world."

Accordingly, within 24 hours of the terrorist strikes, Slate provided a detailed civil engineering explanation of why the twin towers had imploded in lower Manhattan after being struck by jumbo jets. During that early time frame, the Web site was also able to offer up a full profile of Osama bin Laden, then still a shadowy figure in the minds of many people.

"It is very reassuring for people to have their news in synthesized form and not just images of towers falling and planes crashing," Plotz said. "We're able to be there more quickly than the traditional news magazines. In fact, there's an increasing feeling out there that [the news weeklies] are always a week out of date."

Online stories must be short," Plotz said. "People don't have the patience to read long-form journalism online. The best we can hope for is a `conceptual scoop'" -- one which he defined as "the ability to put a set of facts together in a different sort of way so that they make sense to people." But, he added, "there's an inherent tension between how fast you should do something and how well you should do something."

Despite Slate's high viewer volume, Plotz reported that it was much harder for him to get his calls returned then is usually the case for journalists who work for more established press outlets. Ploltz noted that at times he had to call upon Michael Kinsley, Slate's editor -- who is based in Washington state (but who is well known in the other Washington) and who writes a weekly column for The Washington Post -- to run interference for him with top government officials.

There are some other negative aspects to online journalism as well, particularly in wartime. Thus, Plotz lamented "how little original material we are able to contribute to the facts" involving the American-led war in Afghanistan. "Most of the news gathering," he said, "is still being done by the wires, the large national newspapers and the television networks."

"There's very little original reporting online. That's still the Achilles heel of Web journalism. We are mainly a re-packaging operation, rather than a primary gatherer of news. It would be great to be driving White House coverage but we're not doing that." Moreover, Plotz added, as a group "we're still adolescents. At least sometimes we behave as adolescents."

In this respect, Plotz possibly had in mind Ann Coulter, a onetime contributing editor and columnist for National Review Online. Coulter was dropped after writing a column that recommended the United States invade Muslim countries, kill their leaders and convert them to Christianity.

Reflecting on that action, Kathleen Parker, a columnist for the Orlando Sentinel, wrote: "One might expect to lose some readers with that kind of commentary. Like [Bill] Maher, [host of the late-night television talk show "Politically Incorrect,"] Coulter is provocative -- especially when she appears on "Politically Incorrect" in those microscopic skirts. But," Parker asked, "was she

fired for her commentary, or was she fired for calling her editors wimps for declining to run her next `swarthy-male' column?"

Life online, it seems, mirrors the more traditional news world. For, as Parker concluded, "...[If] I liked my job and wanted to keep it, even though I might disagree with an editor's decision (it happens), I probably wouldn't publicly insult the guy cutting my paycheck. That's called self-censorship, also known as being a grown-up."

Purported signs of "adolescense" aside, Plotz believes that in a crisis setting online journalism "forces everybody else to keep up with the same pace. There's very little patience, the people driving the system constantly demand a new story."

As he put it at the Shorenstein meeting: "Now things have to run on Internet time. The big downside of that is we're demanding that this war be fought on Internet time. And that's just not reasonable. You want to throw up big headlines very fast -- even before you've reported it. CNN throws up a headline and you have to wait for the [real] story."

Plotz characterized the situation as "The Drudge Effect," in keeping with the website maintained by Matt Drudge, which is devoted in large part to breaking exclusive stories that are often gleaned, however, on a derivative basis. To some extent, online news coverage is caught up in that whirlwind as well. But, as Plotz noted, while in television news the words and pictures flash by quickly, "things live longer on the Web." In fact, since storage in cyberspace is essentially infinite and free, such accounts often archived or stored on repositories maintained by secondary sites for months and even years on end.

The Wall Street Journal maintains an extensive free-of-charge site for columns and other features that mirror the editorial page of the newspaper's print edition (OpinionJournal.com). James Taranto, the online editor and former deputy editorial features editor of The Wall Street Journal, also prepares a "Best of Web" compilation that can only be found on the Internet. The result is a hybrid form of journalism that seamlessly combines hard reporting, news analysis and personal commentary.

The posting for Dec. 7, 2001 discussed in detail the encounter between a CIA agent named John Spann and an American Taliban fighter named John Walker in a form that did not appear in any U.S. newspaper. Spann was killed shortly after the interview in a Taliban prison uprising.

In a dispatch entitled "The Voice of Treason Goes Mute," Taranto wrote: "Well well. It turns out John Walker, the Marin County weirdo whose "spiritual journey" led him to join the Taliban, was interrogated by two CIA officers, the late Johnny "Mike" Spann and another man identified only as Dave, at the Qala Jangi prison in Afghanistan. Newsweek has a transcript of the videotaped confrontation, in which Walker said ... nothing:

Spann: What's your name? Hey. [He snaps his fingers twice in front of Walker's face. Walker is unresponsive]

Spann: Who brought you here? Wake up! Who brought you here? How did you get here? Hello?

Later, Dave walks up. Spann and Dave speak to one another, within a few feet of Walker, loudly enough for the prisoner to hear them.

Spann [to Dave]: I explained to him what the deal is.

Spann [to Walker]: It's up to you.

Dave [to Spann]: The problem is, he's got to decide if he wants to live or die. If he wants to die, he's going to die here. Or he's going to f---ing spend the rest of his short f---ing life in prison. It's his decision, man. We can only help the guys who want to talk to us. We can only get the Red Cross to help so many guys.

Taranto concludes: "Sad to say, the wrong American died -- though this encounter raises the intriguing possibility of charging Walker in connection with Spann's death...."

The fight against the terrorists began at a time when the economics of the Internet were in a perilous state. Salon, often cited as Slate's main competition, is in David Plotz' words, "just clutching the edge of the cliff." (Slate itself is protected by Mircosoft's deep pockets and is, Plotz reported close to breaking even.)

The wide-ranging iconoclastic nature of online commentary can be further exemplified by an article entitled "Round up the Jews!" and written for Salon by Ron Unz, a theoretical physicist and founder and chairman of Wall Street Analytics, Inc.

Unz' point is that if it's all right to racially profile Muslims and Arabs in the wake of the Sept. 11 attacks as potential fifth-columnists, then it should have been all right also to single out Jews during the 1950s Communist-spy panic.

Unz notes that "[i]t's an undeniable historical fact that Jews made up an extraordinarily high fraction of America's leading Communist Party members and Communist spies even though the overwhelming majority of Jewish Americans were loyal and law-abiding patriotic Americans ..."

But he points out "no figure of authority even on the extreme right ever did so publicly. Sen. Joseph McCarthy, whose name is synonymous with extreme anti-Communism, actually appointed a young Jewish aide, Roy Cohn, as his most prominent lieutenant. Similarly, American leaders ensured that both the prosecutors and the judge who sent Julius and Ethel Rosenberg to their deaths for spying were themselves Jewish."

So Unz concludes "intellectual honesty requires that anyone calling for the ethnic profiling of Arabs and Muslims as possible terrorists today should retrospectively endorse the ethnic profiling of all American Jews as possible traitors 50 years ago. And if such a statement chokes in his throat, perhaps he should reconsider its present-day analogue."

So-called "hyperlinks," which enable people to easily surf between sites, are a vital aspect of online journalism and can be found in nearly all the examples cited in this discussion. "You may lose a few people who never come back to the original site," Plotz noted. "But, in general, people are resentful if you don't give them the original documentation on which your account is based."

Online press criticism of crisis-related news accounts can also often be found at InstaPundit.Com. Thus, on Dec. 7, 2001, writer Glenn Reynolds took on a front page New York Times piece by Fox Butterfield alleging that "the Justice Department has refused to let the FBI check its records to determine whether any of the 1,200 people detained after the Sept. 11 attacks had bought guns. (Reynolds also reprinted the entire section of the penal code that governs this situation.)

As David Brooks noted, also online, Reynolds' analysis "highlights a fact that Butterfield conveniently left out of his story: U.S. law specifically forbids the Justice Department from allowing such checks. (According to Reynolds, the law allows law enforcement to trace a firearm captured at a crime scene, but it does not allow officials to go fishing through the gun records in search of somebody who owns a gun and might have committed a crime.)

Brooks concludes: "If true, this explodes the whole ideological intent of Butterfield's story," although Brooks felt that the language in the penal code "is less open and shut than Reynolds makes out."

The complex online relationships in the press among Brooks, Reynolds and Butterfield comes to the fore in Brooks' overall summary. Reynolds, Brooks tells us, "provides some historical background on Butterfield. Those of us in the media know that Butterfield is someone who often

lets his ideology shape his reporting, but there's no reason others shouldn't know this. The web links it all together."

Independent Journalists

In conducting his tour of online news and opinion sites, the Weekly Standard's David Brooks said he found "truckloads of absolutely essential information every day." A separate search of news- and opinion-oriented Web sites in the second week of December related to the crisis confirms the accuracy of Brooks' comment.

Among the more valuable virtual news clearing houses in cyberland is Hotline World Extra, a compendium of most that has been written, said, or thought about the war in Afghanistan in the English-language press over the past 24 hours. As Brooks noted, "the `Hotline' has a domestic edition which is a depressingly exhaustive bible of the pundit class and carries a hefty subscription fee. But the war edition is free."

One of the independent online journalists whom Brooks admires is Andrew Sullivan, a former editor of the New Republic, who still frequently contributes to that journal as well as to the New York Times Sunday Magazine.

Sullivan prepares a virtual concoction which he calls the "Daily Dish," heavily laced with press criticism that is unavailable elsewhere and that, along with similar sites, serves to deepen and enrich the crisis coverage.

For example, on Dec. 8, 2001, Sullivan tore into one of his favorite targets, the British-based Guardian newspaper, which he described as "the leading Western anti-war newspaper." In this instance, Sullivan, whose political slant is difficult to pigeonhole, dissected a Guardian editorial which conceded that while the war in Afghanistan isn't all over, humanitarian problems will no doubt continue.

While all that he says is true, Sullivan nevertheless declaims in cyberspace that the Guardian editorial "absolutely misses the bigger picture, which is that the U.S.-led campaign in Afghanistan continues to be far more successful than the pessimists, and even most optimists, ever thought possible." Sullivan concludes "moderate liberals are now denying that there ever was an anti-war left; and left-liberals are now announcing that they were wrong about the war. Does it get any sweeter than that?"

Mickey Kaus is another such independent online journalist, albeit one with a liberal bent, whose often provocative reports, known as the "Kausfiles," are rarely mirrored or even widely cited in the mainstream press.

On Dec. 6, 2001, in a typical posting, Kaus raised the question of whether it is in Bush's political interest to prolong the war in Afghanistan. Before the Sept. 11 attacks, Kaus argued, "it seemed pretty clear that President Bush, though popular, might have trouble getting re-elected. Having passed his tax cut, and almost passed his education reform, he'd essentially run out of things to do on the domestic front ...Worse, he faced a potential independent presidential campaign by Sen. John McCain."

Kaus postulates that the Arizona senator would have challenged Bush and won. But, he adds, "all that is moot, of course, thanks to the terrorist attacks. It's inconceivable that a military man like McCain would challenge Bush now while there's a war on."

The Kaus online filing argues: "What is becoming increasingly, glaringly clear -- even as, with U.S. troops engaged in combat, it remains unmentionable -- is that the continuation of the war works in Bush's political interest. It's not just that Bush, as an effective wartime leader, is

popular. It's that as long as there is a war, Bush doesn't have to worry about McCain. As long as there is a war, he doesn't have to worry about anyone focusing too intensely on his nonexistent domestic agenda."

While such observations may or may not be "unmentionable" in the mainstream press, they are patently mentionable online. Thus, Kaus concludes "if Bush doesn't want to repeat his father's mistakes -- which does seem a guiding principle of his administration -- he'll be leery of a too-early termination of the current conflict. Not just for policy reasons, but also, if he thinks about them, for sound political reasons. As long as the war against terrorism is going as well as it seems to be going, then the longer it goes on, the better the chances that Bush will be a two-term commander."

In closing his essay, Kaus predicts that his online site "will be roundly condemned as unpatriotic" for having run a controversial political analysis of Bush's wartime strategy. Nevertheless, Kaus forecasts that "within two months the essential point -- that it's in Bush's political interest to keep the war going -- will be such a staple of punditry that you will switch channels when you hear it."

Andrew Ferguson, among others, represents a conservative viewpoint in what is a broad ideological spectrum of wartime coverage to be found online. Along with Brooks, Furguson writes regularly as a contributing editor for the Weekly Standard and is an online columnist for Bloomberg News (www.bloombergnews.com/columns/) His commentaries are preceded by the disclaimer that "[t]he opinions expressed are his own." As several other such writers in cyberland, Ferguson also devotes a good deal of attention to press criticism of war-related events.

For instance, on Dec. 4, 2001, Ferguson filed a 900-word report entitled "John Ashcroft Becomes All-Purpose Bad Guy." Quite typically, Ferguson's file amounts to a commentary-laced essay on recent news events.

"I've never been much of a fan of Attorney General John Ashcroft," Ferguson begins. "But anybody who gets trashed by four -- yes, four -- New York Times columnists over the course of a single weekend can't be all bad.

"He's not a particularly appealing figure on his own," Ferguson continues. "As a politician he's poorly suited to the tastes of the television age. His voice rolls out in a sleepy monotone, and let's not talk about the haircut. When he ran for re-election to his Missouri Senate seat last year, he lost to an opponent who had been dead for a month. Voters couldn't tell them apart.

"Ordinarily such men are dismissed as dull. But Ashcroft has managed to excite a large number of public people -- not merely New York Times columnists but also professional activists, his fellow politicians, and civil libertarians of the left and the right. Cartoonist Pat Oliphant depicts him as a Taliban mullah. Bill Goodman of the Center for Constitutional Rights last week called Ashcroft and his Justice Department the Constitution's `main enemies right now.' Osama bin Laden comes in second, I guess."

Ferguson goes on to cite the anti-communist raids of the 1920s conducted by a prior Attorney General, Mitchell Palmer, as an unseemly precedent. He argues that the best argument against implementing the new Ashcroft anti-terrorist rules revolves around the constitutional separation of powers – noting "Ashcroft's tactics will have a better chance of passing the inevitable legal challenges if they're undertaken with congressional consent." Ashcroft, he concludes, should meet these unilteralist objections to his policies squarely "as a dull defender of the Constitution rather than the enemy that his more hysterical critics imagine him to be."

Irreverency can play a role in cyber-journalism as well, even when it comes to such acknowledged serious issues as national security. Jonah Goldberg, one such practicioner on the light side of the news, filed a "non-column column" on Dec. 7, 2001 on his Web niche (www.nationalreview.com/goldberg/goldberg.shtml) reporting that he would be skipping his regular offering because on the due date, he would be "on a secret assignment for National Review."

As Goldberg explained it: "I will be at an undisclosed airport or airports somewhere on the Eastern seaboard reporting on the current state of our homeland security. (I will be carrying one National Review Online T-Shirt for anybody who comes up to me and says `the fat man bathes in dirty moonlight' -- World War II code for `give me the damn t-shirt you dork.'")
I wouldn't even tell you this much, except for the unfortunate fact that
I do not trust the suits at NR to pay for what would be my exorbitant legal expenses should I get put in airport jail without my trusted readers knowing I went missing on official business."
Virginia Postrel, another independent (and independent-minded) online columnist takes on such issues as alleged Saudi discrimination against female U.S. military personnel.

In a Dec. 7 posting, Postrel describes in detail the suit filed by Air Force Lt. Col. Martha McSally, the service's highest-ranking female fighter pilot, against the U.S. Department of Defense for sex and religious discrimination. Its genesis: a Pentagon rule that requires American servicewomen to wear the abaya, a full-length robe, and sit in the backseat of cars when they go off base in Saudi Arabia. McSally, an active Christian, objected not only on the basis of sex discrimination but also to being required to wear a garment that is a mark of Muslim faith. A full copy of her legal action is available on the Web site, an extra service that would not to be possible in a common newspaper or magazine setting.

Postrel concludes: "I'm wary of dress-code suits, particularly in a military context, but this one strikes me as a good "don't throw me in the briarpatch" case. The regulations exceed even restrictive Saudi laws, don't apply to non-military personnel, and are basically designed to kiss up to the Saudis. The suit could give the administration a good excuse for ending the obsequiousness. Alternatively, we could require Muslim women visiting this country to wear crucifixes or dress like Britney Spears."

The idiosyncratic liberal-left viewpoint online is represented by such writers as Joshua Micah Marshall, a former Washington editor of the American Prospect who is currently completing his doctoral dissertation in Colonial American history at Brown University. Marshall is also the editor of the "Talking Points Memo," a Web site (www.j-marshall.com/talk) that serves up well-written commentary about the current crisis that is available only online.

For example, in a Dec. 7, 2001 posting, Marshall termed John Ashcroft's performance before the Senate Judiciary Committee on the previous day as "offensive (and) even disgusting." Marshall added: "On attitude and lack of forthcoming-ness alone, it was bad. But to argue that those who raise questions about civil liberties are somehow aiding the terrorists is offensive and, frankly, requires an apology.

"Even if you don't think the Justice Department has done anything wrong or over-stepped on any count, you should still be glad that some people are raising these questions."

"Wartime and crisis often require steps that would be unwarranted and even unacceptable in peacetime. But there must some counter-balance to the government which, in the nature of things, will try to push the ball as far as it can...."

Marshall concluded: "Anti-war critics are always permissible, but I'm not sure they're always necessary. Civil liberties critics are always necessary. Even when they're wrong. This is the

problem with Ashcroft. Both in his penchant for secrecy and his intolerance of criticism, his flaws of character and untoward belligerence get him in trouble even when he's right on the merits."

The War for Public Opinion

Since Sept. 11, the Internet has played a useful role as an alternate source of news and opinion. While all the available evidence as 2001 wound to an end indicated that the Bush administration was continuing to prevail in what might be termed "the war for public opinion," it was equally evident that the Internet gave people a meaningful choice of viewpoints.

"The Bush administration has had to contend with a new set of media forces arising from the 'Information Revolution,'" said Tamara Straus, senior editor of AlterNet.org, one such online alternative voice.

As Straus saw it, "the war on terrorism is the world's first war for the Internet and foreign news outlets. Never before have so many people ostensibly had access to so much news and opinion from so many sources. Never before has it been possible to gauge so many views -- not only in the United States -- but from Europe and the Middle East... Public opinion is now vulnerable to what is reported outside the [America's] news borders."

Straus' own Dec. 10 online essay illustrates her point. "The Pentagon's tactics in the media war have been less than subtle," she wrote. "For starters, they bought up access to all commercial satellite photographs of the region, preventing any news outlets from obtaining them. They also have prevented journalists from accompanying soldiers or airmen on most missions, or even from interviewing them afterward.

"Meanwhile, television news has been behaving more like a wing of the military than an objective Fourth Estate, with anchors like CBS Dan Rather pledging his allegiance on air: 'Wherever [Bush] wants me to line up, just tell me where.'"

I. The Steganographic Scene

In ensuing months after the Sept. 11 attacks, many accounts appeared in newspapers, news magazines and on the air reporting that the suicidal terrorists had cloaked their planning through coded Internet messages. Steganographic messages do not need to be encrypted -- they are hidden in plain sight in the vastness of cyberspace.

Thus CNN.com cited a "law-enforcement theory about how the al-Qaeda network disseminates instructions to operatives in the field" -- suggesting that Osama bin Laden had been hiding messages to his operatives on pornographic web sites, where investigators presumably were less likely to spot them. (note: CNN.Com 11/12)

The CNN report and similar ones alleged that computers and the Internet were used in some unspecified covert ways to facilitate the first mass terrorist attacks on U.S. soil of the digital era. For the most part, the accounts cited as sources independent analysts and security consultants who had left their governmental posts.

Ever since the Internet became a mass communication medium, the potential use by terrorists of online encryption techniques have been a central concern of intelligence agencies. Those concerns have been echoed by lawmakers pressing to close digital loopholes through further legislation. Well before the Sept. 11 attacks, in both open and closed testimony on Capitol Hill, officials from within the Department of Defense, the Central Intelligence Agency,

the Federal Bureau of Investigation and National Security Agency demanded legislative curbs on Internet privacy. Some even called for an outright ban of all encrypted messages that could not be successfully decoded by government monitors.

Throughout the 1990s, the information technology community largely focused on the question of whether security software that employed encryption techniques should also be subject to so-called "escrow" methodology. Such techniques require special "keys" which allow private messages to be decoded by the government -- presumably only after in- place judicial rules had been followed.

In December 1999, however, the federal government abruptly scuttled its efforts to impose monitoring controls on the use of supposedly unbreakable encryption techniques as technologically unfeasible. They did so after privacy champions, joined by such security software programmers as Microsoft Corp., had persuaded key members of Congress that banning exports of American-made "strong encryption" could not prevent terrorism but that it could -- and, indeed, probably would -- significantly damage e-commerce. They argued that it would do so by triggering a wholesale shift of the multi-million-dollar online security business to overseas suppliers unbound by any ground rules that the U.S. government might seek to enforce. In short, the inherent trans-national nature of the Internet had seemingly undermined the would-be code breakers' agenda.

II. Terrorism and Internet Encryption

Within hours of the Sept. 11 carnage, however, the pre-2000 debate resumed. It was widely asserted that Internet encryption must have been used to coordinate the attacks. Attorney General John Ashcroft demanded that Congress plug the loopholes. And Congress rapidly and dutifully sought to do so by passing on Oct. 26 the so-called USA Patriot Act.

Even earlier, on Sept. 13, just two days after the attacks on the World Trade Center and the Pentagon, Congress also passed the Combating Terrorism Act of 2001 (CTA), which significantly lowered the legal standards necessary for the FBI to deploy a surveillance system once known as Carnivore -- currently the government's most potent device for spying on the private e-mail of American citizens within the confines of the United States..

Still pending on the legislative agenda is the proposed Mobilization Against Terrorism Act (MATA). If enacted in its present form, the law would empower U.S. attorneys throughout the nation to order up a Carnivore installation without first obtaining a court order. It would also permit federal prosecutors to use electronic evidence gathered abroad, including Internet files, even when that evidence failed to follow Fourth Amendment guarantees against unreasonable search and seizure.

"These are the kinds of things that law enforcement has asked us for," said Sen. Jon Kyl, Republican of Arizona and a co-sponsor of the already enacted CTA. "This combination is relatively modest in comparison with the kind of terrorist attack we have just suffered," he added.

Much of the early reporting on these issues reflected a seven-month-old story in USA Today which claimed that bin Laden and his followers operated an Internet communications network based on encrypted messages that were concealed within pornographic pictures. (note: Jack Kelley: "Terror groups hide behind Web encryption." USA Today Feb. 5, 2001.) These techniques, known as steganography, (from the ancient Greek word for hidden writing), enable users to mask a coded message within a digital, a picture, or music file by making small changes

to data that are then nearly impossible to detect without employing special sophisticated software.

In the wake of the attacks, reports appeared on several Internet privacy-related Web sites to the effect that FBI agents had ordered EarthLink, the nation's third-largest Internet service provider (ISP), to install Carnivore. These reports said that the ISP, long a strong advocate of online privacy, had refused to do so.

The reality, however, differs somewhat from these accounts, and, in fact, had been widely reported in the trade press well before the attacks occurred. In December 1999, shortly after the FBI rolled out its Carnivore software, EarthLink told the agency that it would not allow the technology to be installed on its network. Subsequently, the parties, seeking to avoid a protracted court battle, cut a deal. That bargain permitted EarthLink to use its own software, rather than Carnivore, to monitor its e-mail traffic. At the same time, the ISP agreed to turn over all the data the FBI was entitled to inspect under any relevant subpoenas or court orders that the agency produced.

III. U.S. Government Response

A week after the attacks occurred, Ronald Dick, an assistant FBI director and chief of the U.S. National Infrastructure Protection Center, a coordinating body, informed reporters that the hijackers had used the Internet, and had "used it well." (note: AP, etc.)

Dick said FBI investigators -- by obtaining records from both ISPs and by reviewing computer files stored in various public libraries -- had been able to locate hundreds of e- mail communications dispatched some 30 to 45 days before the attacks took place. These messages, written in both English and Arabic, were sent from both within the United States and from abroad.

Both in open briefings and in background sessions, Dick and other FBI officials repeatedly stressed that bin Laden's terrorist gang knows its way around the Internet. The supposed ringleader, Mohamed Atta, who flew the hijacked Boeing 767 into one of the World Trade Center's twin towers, reserved his seat on Americanairlines.com. Others communicated through Yahoo and Hotline e-mail accounts. Both services enable anonymous "handles," one reason, presumably, for their early adoption and continued popularity.

The terrorist cell members, the government also let it be known, went online to research the possibility of utilizing the chemical-dispersing facilities of crop dusting planes to engage in urban chemical or bioterrorism. At the same time, the government briefers took care to note that all of these messages were sent "in the clear," without resort to any encryption techniques.

Dick also accused civil libertarians of, in effect, aiding and abetting criminals: "Quite simply," he told reporters, "the balance described in the Constitution, which provides the government with the capacity to protect the public, is eroding. In its place, the privacy of criminals and foreign enemies is edging toward the absolute."

While the government avowed otherwise, a Time magazine story in mid-November reported that "secret Internet messages, known as steganography, may be the most insidious way that bin Laden has taken his terrorist movement online." (note: Adam Cohen "When Terror Hides Online" TIME, 11-12-01 issue)

The Time article speculated that "a terrorist mastermind" could insert plans for blowing up a nuclear reactor in, say, the digital image of a nose of a puppy posted on a pet- adoption web

site. Operatives in the field, when told which nose to look for, "could then check for their marching orders."

Time deduced that bin Laden's followers may have learned about steganography "when it burst on the pop-culture scene in such recent movies as "Along Came a Spider," in which a detective locates a key piece of evidence in a digitized picture of Charles Lindbergh's nose.

The magazine further reported that the "FBI has been close-mouthed on whether it has found any steganographic images from bin Laden's al-Qaeda network." As noted above, that reporting contradicted the FBI's official stance, which held that none of the conspirators had used encryption technology or otherwise sought to conceal their messages. Once located, the FBI had said, their e-mails could be easily and openly read.

The unnamed Time source who linked bin Laden's followers to steganographic techniques was a "former government official in France [who] has said that suspects who were arrested in September for an alleged plan to blow up the U.S. embassy in Paris were waiting to get their orders through an online photo." Many other accounts that took a similar tack cited no official sources in alleging that terrorists were using encryption methods.

As it happened, only a few days before the Sept. 11 attacks, a computer team from the University of Michigan reported they had searched for Internet images that might have contained terror-laden plans. They did so by using a network of computers to look for the tell-tale digital "signature" of steganography. Researchers at the university's Center for Information Technology Integration said they "analyzed two million images but have not been able to find a single hidden message." (Note: www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf) Their pre-attack Michigan study has been widely ignored in the mainstream press.

Nevertheless, there are indications that law enforcement authorities, armed with the new antiterrorism statute that broaden their powers to intradict Internet communications, have stepped up their targeting of technology that could both prove useful to terrorist organizations and that, if spotted in a timely way, could conceivably help foil further plots.

To be sure, these Internet sweeps are also subject to deliberate attempts to spread disinformation. It is known in the intelligence community that the terrorist networks are familiar with disinformation techniques -- a favorite ruse of clandestine agencies in the Cold War era. What's not known is how sophisticated the anti-terrorist watchdogs are in ferreting out any disinformation they may encounter.

IV. Internet Privacy Concerns

For their part, civil libertarians continue to contend in the wake of the Sept. 11 attacks that in due course Americans may come to regret having granted law enforcement agencies too much power to monitor American citizens and legal aliens. In the view of John Perry Barlow, co-founder of the Electronic Freedom Foundation and an Internet pioneer: "These provisions may seem semi-innocuous taken separately by the government we have at the moment. But it has the possibility of turning into a massive surveillance system, where anything you do online can be used against you by a government that is not as benign." (Adam Cohen - Online mag)

Recent surveys suggest that the Bush administration's anti-terrorist thrusts, with their online aspects, enjoy wide public support. The prevailing mood appears to hold that if you're not doing anything wrong, you have nothing to worry about and that if you are doing something wrong, the government has some new-found tools to find you and punish you.

Nevertheless, a vocal minority in the press -- from both the new libertarian right and the more traditional liberal left -- have spoken out against the post-Sept. 11 legislative and administration actions. Their common meeting point appears to be privacy -- what a Supreme Court justice once called "the right to be left alone."

Thus, in the December 2001 issue of "Yahoo! Internet Life," Robert Scheer wrote: "Big Brother is back big-time, and Americans are welcoming him warmly"

"The fact is," Scheer added, "ordinary citizens will be affected far more by the Internet-oriented parts of this legislation than will terrorists."

Privacy advocates note that under the newly enacted legislation the federal government has gained expanded powers to spy on web surfing activities of all Americans, including specific terms that are entered into Internet search engines. The government need merely inform any federal judge of its choosing that its spying activities could conceivably lead to information that is "relevant" to an ongoing criminal investigation. The person being spied upon need not be a target of the investigation. The new law removes all judicial discretion: the application must be granted. Furthermore, the government is not obligated to report to the court or tell the person spied up what it has done.

The USA Patriot Act also raises the threshold of how much information the government may obtain about users from ISPs, such as Yahoo!, or others who handle or store their online communications. First, it permits ISPs to voluntarily hand over all "non-content" information to law enforcement without the need for any court order or subpoena. Secondly, it expands the records that the government may seek with a simple subpoena, without the requirement of a court review, to include records of specific online session times and durations, temporarily assigned network Internet Protocol (IP) addresses and the means and sources of payments, including credit card and/or bank account numbers.

One big winner in the new national climate will be the aforementioned Carnivore. Originally named for its ability to get at the "meat" in large quantities of e-mail and instant messaging, it has recently been renamed DCS1000 because the original name sounded so creepy. The DSC1000 technology was spawned in the FBI's own labs. The FBI is close-lipped about how it works, and ISPs that install it are under court order to keep quiet about its technological gizzards. It has been reported in the trade press to be a stealthy looking black box dedicated computer that runs on an Intel Pentium III chip under the Windows NT operating system. Its sole dedicated task is to "sniff out" Internet packets, the building block of all non-wire online communications. When the FBI has a suspect in its sights whose e-mail it wants to poke through, it gets a court order similar to traditional ones used for phone wiretaps employed with traditional point-to-point circuit-switched networks. It then takes the DSC1000 out of storage in its Quantico, Va., technical field headquarters and works with an individual ISP's engineers to hook it up to that server's packet-switched network. Once it's hooked up, the computer can search through e-mail traffic in a variety of ways -- by names on "To" and "From" lines, by trolling for an Internet Protocol (IP) address and by filtering for keywords within the header or body of an e-mail message. In its official description of the DSC1000, the FBI insists that its software was designed to spy with "surgical" precision (note: www.fbi.gov/hq/lab/carnivore/carnivore2.htm) on specific individuals.

But the machine's critics are not so sanguine. They say that once the device is hooked up to an ISP's network, it can be used to do keyword searches -- for, say, "hijack" or "bin Laden" -- on every single e-mail which passes through the datastream. "They're sucking on the hose," said Lee Tien, senior staff attorney with the Electronic Freedom Foundation. "It's conceivable they're

taking every bit and deciding whether they're entitled to it or not, but maybe they're looking at every bit."

It's a fair bet that there will be a lot more DSC1000's installed in the weeks and months ahead. After Sept. 11, according to widespread trade press accounts, the FBI fanned out and installed the data-capturing devices on ISPs throughout the country, without any further publicity and without any vocal opposition from the ISPs.

Just what information the FBI can collect in the altered national climate depends on what kind of court order the agency has procured. For circuit-switched phone wiretaps, routine orders call for so-called "trap-and-traces," which allow law enforcement authorities to record the phone numbers that a suspect dials, and to perform "pen-registers," which log the phone numbers and the time of incoming calls. Similar secret court orders, it is widely believed, are currently being issued for the DSC1000 in order to obtain e-mail addresses. But to actually gain access to the substance of a packet-switched e-mail message, under current law the FBI needs a full-blown content wiretap order, which the courts have been more wary in granting.

When the DSC1000 was first introduced as Carnivore, civil libertarians hoped to stop it cold. But after EarthLink settled with the FBI, for fear of losing its court case on appeal -- and in the absence of any groundswell of popular opposition -- privacy advocates have increasingly redirected their efforts to halting what they see as potential abuses in how the FBI might deploy the technology.

"We're not trying to stop them from doing their jobs," said Ari Schwartz, a policy analyst at the Center for Democracy & Technology. "What we're talking about is oversight."

These critics would like to be sure that when the DSC1000 is installed on an ISP the data collection that is done is truly the equivalent of a "surgical strike" -- so that the FBI avoids any "collateral damage" by further downloading information about non-targets that it also happens to intercept. Moreover, the critics charge that the FBI is already misusing pen-registers and trap-and-traces. The government has argued that those limited wiretaps entitle it to e-mail headers -- the brief subject headlines at the top of each message aimed at summarizing the contents. To get access to headers, Carnivore's critics say, the FBI should have to meet the higher standard for a content wiretap. They would also like to see rules instituted that would require the FBI to throw out collected evidence once an investigation is over, rather than allowing the government to store the data in a semi- permanent database.

The terrorist attacks will also probably increase the use of "computer forensics," detective work that turns criminals' own computers against them. One of the hottest tools in the field right now is keystroke logging -- law enforcement's surreptitious installation of software, or even a rigged keyboard, to log every keystroke a suspect types into his or her computer. Computer forensic techniques are usually kept under wraps. But keystroke logging techniques became public in the trial of Nicodemo S. Scarfo, an accused New Jersey bookmaker. The FBI used keystroke logging to ascertain the password to an Internet encryption program Scarfo allegedly used to relay gambling and loan-sharking data. Nevertheless, keystroke logging is hard for law enforcement to employ because it's usually a "black-bag job" -- an agent must actually show up and install the monitoring device. Those techniques could yet prove to be a crucial asset in uncovering terrorist plots before attacks actually occur.

V. Online Community Response

Privacy advocates say they will keep fighting these battles -- before judges, in Congress and in the media. But they also realize it's become a hard sell try to rein in the carnivorous beast, a situation that is likely to persist for some time. "No matter how you feel about Carnivore, if the smoke is still coming off the World Trade Center, no one is going to tell the FBI they can't install it," said David McClure, president of the U.S. Internet Industry Association.

"Laws made in crisis mode seldom vanish once the wartime footing ends," notes Brendan I. Koerner, a Markle Fellow at the New America Foundation. For example, in response to rumors that TWA Flight 800 had been downed by a terrorist bomb, Congress made it easier to expel legal aliens. However, when mechanical failure was revealed to be the culprit, the law remained on the books. Said Koerner: "Even if Al Qaeda is somehow dismantled in the coming years, one suspects that technology's carefree days were also a victim of September 11."

"We were probably poised to have much better privacy protections, and I think this is going to create a lot of resistance," said Jamie Love, executive director of the Consumer Project on Technology. He foresees a backlash against programs that enable anonymous Web browsing -- and, perhaps, even an end to all anonymous surfing on U.S.-based public-access terminals.

In the aftermath of the attacks, one prominent remailer operator shut down his system. In a note to his fellow operators, Len Sassaman explained his move by writing: "I don't want to get caught in the middle of this. I'm sorry. I'm currently unemployed and don't have the resources to defend myself. At this point in time, a free-speech argument will not gain much sympathy with the Feds, judges, and general public."

In hindsight, some of the privacy alarms that went off after the Sept. 11 attacks now appear to have been false. In the hours after the attacks, there were scattered reports that several anonymous proxies -- services that allow users to surf the Internet or send e-mail without revealing their identity -- voluntarily shut down or cut back on services. Privacy advocates were concerned that the government might start to force anonymous proxies to stop operating, in the name of national security.

But so far, no evidence has emerged that the terrorists used anonymizers. In fact, they may have intentionally avoided them. "If you're a terrorist, your main goal is not to be noticed at all," says Lance Cottrell, president of Anonymizer.com. "Using an anonymizer gets you noticed." Investigators now believe some of the hijackers accessed the Internet through computers in public libraries in Florida and Virginia. Those personal computers offered them anonymity because they do not require log-ons or passwords. Their sign-in sheets are (or at least were until recently) thrown out at the end of the day, and at least some of the computers came with wrap-around "shields" that prevented other patrons from reading what was on the screen.

VI. Foreign Operations

The drive to root out radical Islamic terrorist cells is also likely to give a boost to an even more sweeping eavesdropping system: Echelon, the National Security Agency's (NSA) top-secret global wiretapping network. Echelon grew out of a 1945 agreement to share information obtained by bugging hostile powers, particularly the Soviet Union. It was developed and is now operated as a joint effort of the NSA and the intelligence operations of England, Canada and New Zealand. Echelon has been shrouded in mystery -- so much so that its very existence was long doubted. But a report by the European Parliament in July confirmed that it is quite real. That report suggested the technology is able to intercept virtually any telephone conversation, e-mail, Internet connection or fax on a worldwide basis. Echelon is believed to work somewhat

akin to a global police scanner. It is reportedly able to search out specific keywords like "hijack" or "bomb." Not surprisingly, the biggest stumbling block to the system is said to be the gigantic volume of data that is being collected -- upwards of 3 million messages a minute, according to the estimates in the European Parliament report -- that must then be sorted and analyzed. Clearly, if Echelon was working before Sept. 11, it didn't prevent what occurred in Lower Manhattan, Northern Virginia and in the Pennsylvania countryside.

The American Civil Liberties Union and other privacy advocates have long fought Echelon. Among their chief concerns is that Echelon will be used to spy on Americans, even though Americans are outside the NSA's jurisdiction, because Internet traffic takes such roundabout paths. For its part, the NSA, which has reportedly had to lobby Congress hard for Echelon funding, will now presumably have a far more receptive audience. Included in the items likely to be high on the NSA's wish list: funding to hire large numbers of staff, especially Arabic speakers, to sift through voluminous data.

VII. The Road Ahead

Immediately after the Sept. 11 attacks, when rumors were rampant that the terrorists had encrypted their e-mail messages, it appeared that there would be a crackdown on encryption programs. Sen. Judd Gregg, Republican of New Hampshire, began drawing up legislation that would require encryption programs to contain a "backdoor" that would be accessible to U.S. law enforcement. But the anti-encryption campaign gained little momentum.

In part, it was because law enforcement began to doubt that the terrorists had bothered to use encryption. But just as important, the last prior attempt to crack down on encryption, during the Clinton administration, was abandoned when even its supporters began to doubt it would help. One key flaw: there's no way for the U.S. intelligence authorities to ensure that every encryption program sold in the world has a backdoor accessible to American law enforcement. "Why would terrorists use encryption with a backdoor we had access to?" asked Dorothy Denning, a Georgetown University computer-science professor who has abandoned her past support for rules requiring backdoors. "There are a lot of good encryption companies outside the U.S. they could go to."

Besides, as noted above, there's little evidence that terrorists have used encryption. Brian Gladman, who once headed up electronic security for Britain's Ministry of Defense and NATO, argues that the Sept. 11 hijackers attackers probably eschewed encrypted messages because they would have stood out and been more likely to have been picked up by the National Security Agency. (Although texts may not be able to deciphered in a timely way by even the most powerful computers, other information, such as routing addresses, which cannot be encrypted on a packet-switched Internet network, could prove useful to the authorities in locating terrorist cells.)

In the wake of the Sept. 11 attacks, the Internet community braced for a truly draconian privacy crackdown. Cottrell, the "atomizer" provider, heard talk of requiring Internet users to have an Internet ID card, with a smart-card reader or bio-optic identification, to go online, or imposing an affirmative duty on all ISPs to track their users. Richard Smith, chief technology officer of the Brookline, Mass.-based Privacy Foundation, talked of his fears that the government would require web sites to log and save visitor IP addresses, and ISPs to save e-mail, for a period of years.

As a result of the post Sept. 11 crisis, there will almost certainly be some changes on the margins in privacy on the Internet. There will likely be more e-mail and Internet monitoring of specific suspects, pursuant to court orders. Echelon is likely to spy more than ever on overseas communications. And ISPs and other Internet players are already approaching requests from law enforcement with altered attitudes. "In the old days it was easy to take a stand and say anything goes on our ISP," says Internet association president McClure. "Now they're going to be quicker to say, `unless there's a reason to think you're breaking the law.'" Still, some privacy advocates hope the changes won't be overwhelming. "There seem to be a lot of voices out there saying, `Wait a minute, take this a little slower,'" says Cottrell. "We don't want to trample our civil liberties, particularly if there's no gain."

Some civil libertarians argue, in fact, that as the war on terrorism continues, there could even be a renewed appreciation for privacy. After all, secrecy can also help the good guys. Anonymizer.com is making its service available for free to investigators. That will allow law enforcement at all levels to look at terrorist web sites without tipping off the groups that they're being watched. And there's another group that has traditionally relied on privacy: informants. Anonymizer.com has created a special gateway to the FBI web site where anonymous tips can be left about bin Laden and his terror network. It's something legislators may want to keep in mind when they reconsider the laws of cyberspace in the years ahead. After all, private e-mail, anonymized Web surfing and encrypted messages could hide not only terrorists but a wavering member of a terror network seeking to summon up the courage to turn them in.

VIII: National Security Issues

Free speech faces the strongest challenges during times of crisis. So it should come as no surprise that the U.S. government's response to the terrorist attacks of September 11, 2001 has had a chilling effect on the availability of information on the Internet as well as on some of the people who seek to provide information through that powerful medium..

On the other hand, a wealth of specific military and intelligence information is available online. One such content-rich sites is Globalsecurity.org, which is based in Alexandria, Va., near the Pentagon. (On Oct. 15, ABC News quoted John Pike, the site's proprietor, as having received a request from low-level military officials that he remove data he had gathered from military web sites.)

To be sure, a Web search in early December found no web sites that had been shut down by a direct federal order. Such an action, on its very face, would violate the First Amendment since U.S. courts have repeatedly ruled that the Internet, as a mass medium of communication, is subject to constitutional protection.

Commercial Internet service providers have been more active in shutting sites. For example, Yahoo, one of the largest such providers, has unilaterally removed 55 "jihad-related" sites since Sept. 11.

Similar rights may not be found in other nations, however. For example, in early October, the British government shut down qoqaz.net on the grounds that the site was run by London-based Azzam Publications, which it said advocated support of Muslim-run terrorism in the Caucasus, the donation of funds to the Taliban and military training for the battling the West.

A cached copy of the British Web site, preserved by Google, includes an illustration captioned "Jihad in Afghanistan." Superimposed over a map of Afghanistan is a black cross dripping with red blood. A blue Star of David is positioned over the center of the cross. (Google

has told both government agencies and private organizations that it will delete, at their request, cached versions of their Web pages where the originals have been removed.)

Assam.com has also been shut down by multiple ISPs in the United States, although it is still available via some others, particularly those affiliated with educational institutions such as Harvard. The dead links are explained on the still active site as "due to freedom of speech being taken away in the West."

The U.S.-based Assam site contains an English-language version of Osama bin Liden's 13,000-word "Declaration of War Against the Americans Occupying the Land of the Two Holy Places," subtitled "Expel the Infidels from the Arab Peninsula," and written in 1996. The manifesto is preceded by a disclaimer stating "Azzam Publications has provided this document for information purposes and as a reference for other media organizations only. It does automatically mean that we agree with or endorse everything written in this document."

(To be sure, the Internet site enables people to read and evaluate bin Laden's polemic in toto, without editing or commentary. (A typical passage reads: "It should not be hidden from you that the people of Islam had suffered from aggression, iniquity and injustice imposed on them by the Zionist-Crusaders alliance and their collaborators; to the extent that the Muslims' blood became the cheapest and their wealth as loot in the hands of the enemies. Their blood was spilled in Palestine and Iraq ...")

Here are some other examples of post-crisis self-censorship:

-- Amazon.com, the leading bookseller on the Internet, deleted a photograph of a Arabic book jacket that shows a plane flying through the top of a building under construction in Riyadh, Saudi Arabia, that has a top shaped like the eye of a needle. The sole link to the World Trade Center is that the building in Riyadh has being financed by Prince Alwaleed bin Talal bin Abdul Aziz al-Saud, whose $10 million donation to the Twin Towers Fund was refused by Mayor Rudolph Giuliani of New York, because along with expressing condolences, the prince urged the United States to re-examine its policy toward Israel.

-- Actress Barbra Streisand removed anti-Bush articles from her web site, explaining that "in light of recent events, I strongly believe we must support our government despite our disagreements on certain policies, such as those relating to environmental, educational, social and other specific issues. My past concerns about such matters still pertain, but at this point in time, I have removed several articles from my web site in an effort to encourage national unity instead of partisan divisions."

-- Steven Aftergood, who administers the Project on Government Secrecy for the Federation of American Scientists, has pulled some 200 pages of previously posted information from the Internet out of concern that terrorists might find them useful. They included floor plans of National Security Agency and Central Intelligence Agency facilities and images of foreign nuclear weapons plants.

-- MSNBC removed from an article formerly entitled "Ashcroft Seeks Sweeping Powers" and now called "House Approves $343 Billion Defense Bill" a section about how the House Judiciary Committee's Republican staffers ordered television camera crews to leave a hearing on terrorist attacks after Ashcroft testified.

-- The WhatDemocracy.com web site removed content critical of "right-wing politics, including President Bush and the Republican Party, in the aftermath of the terrorist attacks "due to the potential of endangerment to our staff." It noted "we would love to address the current terrorism situation, and we should have the right to safely address our opinions, but who will step up to the plate and protect us, and how?"

Some official web sites that do not bear directly on freedom of speech issues but could prove useful to watchdog groups that monitor government accountability in budgetary and regulatory matters have also left the Internet in the wake of the crisis.

Here are some instances that have come to light:

-- The Agency for Toxic Substances and Disease Registry dropped a report critical of chemical plant security. And the Army Corps of Engineers site that contained information about an underground military command center near Washington was placed behind a firewall so a username and password are now required for access.

-- The Department of Energy, National Transportation of Radioactive Materials site has been replaced with the note "This site temporarily unavailable."

-- The Department of Transportation (DOT) has limited access to the National Pipeline Mapping System of the Office of Pipeline Safety, which lays out the network of high-pressure natural gas pipelines throughout the nation and the site of the Geographic Information Services section of the DOT's Bureau of Transportation Services. Access to these highly detailed maps of roads and utilities is now limited to federal, state, and local government officials.

-- The Environmental Protection Agency has pulled from its site risk management plans, which contain detailed information about the dangers of chemical accidents -- such as toxic plume maps and emergency response plans after a refinery explosion.

-- The Federal Aviation Administration has pulled data from a site listing enforcement violations such as weaknesses in airport security.

-- The Federal Energy Regulatory Commission has removed documents that detail specifications for energy facilities from its web site.

-- The International Nuclear Safety Center has removed its reactor maps and left the following message: "If you requested access to the maps of nuclear power reactor locations, these maps have been taken off-line temporarily pending the outcome of a policy review by the U.S. Department of Energy and Argonne National Laboratory." (The nuclear site locations page in National Atlas of the United States is also missing, yielding a broken link.)

-- The Los Alamos National Laboratory has removed a number of reports from its laboratory publications page.

-- The John Glenn Research Center of the National Aeronautics and Space Administration (NASA) noted "public access to many of our web sites is temporarily limited. We apologize for any inconvenience."

-- The Nuclear Regulatory Commission (NRC) displays only "select content" while "performing a review of all material" on their web site, although most of the information has been there for years and "nothing top secret was on the Web site to begin with," according to William Beecher the NRC spokesman.

-- The U.S. Geological Survey has removed a number of pages from its registered online water-resources reports database.

IX: Online Rumors

While rumors traditionally flourish in times of crisis, the Internet offers a particularly warm soil for planting them. E-mails bearing tales of purported events on Sept. 11 and beyond -- hidden from the public and either unknown to or masked by the mass media -- have traveled quickly and propagated rapidly.

Sorting through the overwhelming number of rumors and images can be daunting. But most experts believe the Internet also offers a means to find out quickly what is true and what is not. "We try on different theories, myths and we discard them pretty quickly if they don't make sense," said Steve Jones, a professor at the University of Illinois at Chicago and president of the Association of Internet Researchers.

Jones noted that while people are pretty good at discarding rumors that don't make sense, "the problem with the Internet is that we don't have the same type of conversation online that we do offline. As he put it: "The Internet continues to throw up new, possible fictions that we keep sorting through. It's too easy to rehash. People come into the debate at different times. It's almost as if the rumors recur,"

"Who would have imagined two weeks ago that suddenly we would look at our mail as a source of potential death?" said Gary Alan Fine, a sociology professor at Northwestern University. "In times of ambiguity, things we once thought of as normal seem frightening, and we become more open to rumor."

Aaron Lynch, a scholar in thought contagion analysis who is based at Northwestern University in Evanston, Ill., said people are drawn to pass on terrorism warnings online by the "gratifying" sense that they might be saving the life of others, who might come back to thank them someday.

One such e-mail, attributed to an acquaintance, said a woman had gone to the apartment of her Middle Eastern boyfriend, only to find he had moved out, leaving her a note not to fly on Sept. 11.

That particular rumor received some extra veracity because the sender, Laura Katsis, had included her California phone number and this cover message: "I think you all know that I don't send out hoaxes and don't do the reactionary thing and send out anything that crosses my path. This one, however, is a friend of a friend and I've given it enough credibility in my mind that I'm writing it up and sending it out to all of you."

The information, however, is false, according to www.snopes2.com, one of several Internet sites devoted to investigating rumors and so-called urban legends. "A public information officer at the FBI's National Press Office told us that they've fielded many calls about this message, they've checked it out, and they have received no letter of warning from a girl with an Afghan boyfriend," the proprietors of the Web site, Barbara and David said.

Deluged with queries, Katsis's employer, Volt Information Sciences, shut down her phone extension and e-mail service. Inquiries were met either with a recorded statement or an automatic e-mail response from company officials denying any direct knowledge of the incident.

Such rumors, Barbara Mikkelson said, can be "hugely comforting in the strangest way. We're reducing terrorism -- which can strike anywhere, anytime, to anybody -- to `We know the place and time, so just avoid being there.' So it restores a sense of control back into an out-of-control world."

Each of the entries in the "rumors of war" category on the Mikkelson's Web site is color-coded: red is for false, green is for true, yellow an represents ambiguous situation and white signifies an unknown origin. A rumor that garlic cures anthrax, for example, is coded red.

On the site white bullets are the ones most commonly associated with "pure" urban legends -- entries that describe plausible events so general that they could have happened to someone, somewhere, at some time, and are therefore essentially unprovable. Some legends that describe events known to have occurred in real life are also put into this category if there is no evidence that the events occurred before the origination of the legends.

Green bullets are used for two similar but distinct types of entries: claims that are demonstrably true, and urban legends that are based on real events. For the former, "demonstrably true" means that the claim has been established by a preponderance of (reliable) evidence; for the latter, a green bullet indicates that the legend described is based on an actual occurrence. (The word "based" is key here: many legends describe events that have taken place in real life, but those events did not occur until the related legend was already in circulation.)

Yellow bullets generally describe disputed claims -- factual items which the available evidence is too contradictory or insufficient to establish as either true or false. This category also includes claims that have a kernel of truth to them but are not literally true as stated. (For example, an entry that read "Soupy Sales was fired for asking children to send him 'little green pieces of paper' on his TV show" would fit this classification because even though Soupy Sales did make such a request, he was not fired for doing so.) Some legends also fall into this classification when it cannot be determined whether the legends preceded similar real life events, or vice-versa.

Red bullets mark claims which cannot be established as true by a preponderance of (reliable) evidence. Some urban legends are also placed into this category because they describe invents too implausible to have actually occurred, or too fantastic to have escaped mention in the media of the day.

Links send surfers to a full takeout on the rumor, the verdict on its veracity and sometimes several pages worth of information the Mikkelsons have been to collect.

"The first thing I do is use news databases to see what I can find out about the facts" of any rumor, Barbara Mikkelson said. "We perform various searches of a number of online databases, sometimes we call the people involved in the stories, we use what we know about related legends and stories ... Or we go to UCLA (University of California at Los Angeles) to look into their microfilms archives."

Barbara Mikkelson is not surprised by the proliferation of rumors in the wake of the terrorist attacks. "It's a normal way for people to try and deal with times like this. What happened was horrifying, and part of the way we try to deal with something we can't comprehend is to try to fill in all the missing spots with information," she said.

"People want so badly to believe that we are not living in a world where anything can happen at any time. It's the truth, but it's too scary a truth for a lot of people," she added. "They'd much rather believe that there are prophets that can foresee everything, and that if bad stuff happens and people die, it's just because we didn't pay attention to what they said or we didn't interpret things correctly."

In the month after the Sept. 11 attacks, the Mikkelson's site received between 2 million to 2.5 million hits each day as Internet users sought the latest on post-attack rumors that range from a terrorist attack on a mall on Halloween to blue envelopes containing a deadly virus. Both both proved false.

The Mikkelsons have filled a void. Created six years ago, www.snopes2.com is one of the few sites devoted exclusively to ferreting out Internet rumors, the modern-day equivalent of urban legends. The terrorist attacks have, by far, generated a greater number of falsehoods - and public interest - than any other event in the site's lifetime.

"I use it a lot myself and I send students to it," said Sabina Magliocco, an assistant professor of anthropology at California State University, Northridge, who specializes in folklore. "I think it's very reliable."

And the couple who started the Web site as a hobby have now become experts on the topic, regularly appearing on TV news programs such as CNN and ABC as well as newspapers across the country, including The Dallas Morning News and the Seattle Post-Intelligencer.

"We work with them all the time," said Howard Fienberg, a research analyst with the Statistical Assessment Service, a Washington-based nonprofit research organization that works to improve the public's understanding of science and social research. He said the information on the site is well-researched and credible.

The Centers for Disease Control and Prevention lists the Web site as a source, though it includes a disclaimer stating it does not endorse it. The U.S. Department of Energy's Hoaxbusters page also links to www.snopes2.com.

Urban Legends and Folklore (urbanlegends.about.com), which also investigates Internet rumors, defines an urban legend as something that appears mysteriously, spreads spontaneously, contains elements of horror or humor, and makes good storytelling.

"It does not have to be false, although most are," the site says. Urban legends often have a basis in fact, "but it's their life after-the-fact that gives them particular interest."

But e-mail rumors can also threaten to disrupt urban life. Thus, Massachusetts officials braced for a potential terrorist strike after an e-mail circulated widely in the region stating that "a few drunk Arab men" had warned a Boston bartender that bloodshed would occur on Sept. 22.

Well into the fall, Harvard students circulated a rumor that their campus is No. 5 on a secret federal list of likely terrorist targets. Another e-mailed rumor, particularly widely propagated in the Middle East, held that the Israel Secret Service, known as the Mossad, was behind the Sept. 11 attacks.

One of the first rumors circulated by e-mail and on the Internet was that the French physician and astrologer Nostradamus in 1654 had made the prediction that World War III would start with the fall of the "two brothers," supposedly a reference to the World Trade Center towers.

Lee Rainie, director of the Pew Internet & American Life Project in Washington, said the Nostradamus rumor was an example of the self-policing element of the Internet. "Within a half hour of getting the Nostradamus e-mail, I got the debunking version," Rainie said. (The Mikkelsons further noted that the lines being attributed to Nostradamus [who actually died in 1566] were wriiten by a Canadian university student in 1997 and first appeared as a Web page essay.)

Rainie said researchers have found that Americans say they like to seek out different opinions on the Internet, although they are most comfortable with those that are consistent with theirs. "People obviously have to have their antenna out," he added "If it seems incredible, chances are it is incredible and uncredible."

In the Middle East, the rumors, spread via the Internet and other mass media channels, took on a more sinister coloration.

Mark Siegel, a Washington communications consultant who once represented former Pakistan President Benazir Bhutto and has had extensive dealings in the Muslim world, said the intellectual elite are receptive to the message from the West because they, too, are targets of fanatics. "The problem is the masses," Siegel said. "The governments of our allied Arab friends often spread in their state-controlled media the hate that fuels the masses."

He cited the example of the televised interview with the father of Mohammed Atta, a leader of the terrorists who participated in the Sept. 11 attacks. "Atta's father is a lawyer in Cairo, a middle-class guy," Siegel said. "He told the press that his son was innocent, that the attack on the United States was a Mossad [Israeli intelligence] operation, and that all the Jews were evacuated

from the World Trade Center before the attack. That insanity was on state-controlled media all over the Arab world and on Islamic Internet sites."

X. Bioterrorism

The Internet's inherent ability to widely spread vital public health information in a crisis has been put to its first significant test on the bioterrorism front, with both doctors and consumers turning to the World Wide Web for timely answers.

"Never before in my medical career have I had a more urgent need for just-in-time, on-demand health-care information and less time to obtain it than now," Dr. William Cordell, professor of emergency medicine at Indiana University, told Laura Landro of the Wall Street Journal.

Landro gave the reporter an account of an Indianpolis airport worker who came to a hospital emergency room showing classic symptoms of flu and diarrhea after anthrax was found on a mail sorting machine. Dr. Cordell consulted an anthrax response "flow chart" he had just received the day before via e-mail from a local poison center. With that as a guide, he obtained the needed cultures, prescribed antibiotic treatment and sought to calm the patient's fears. (So far, he has tested negative for the disease.)

The sheer amount of bioterrorism information on the Web is daunting: a search on Google for "anthrax" yields nearly a million results. One potential danger of the flood of bioterrorism data on the Web is that it could spur hypochondria and panic among the public. And even solid data can become quickly outdated, or hard to interpret.

In the aftermath of the anthrax attacks, health professionals sought to get the latest diagnostic and treatment data on the Web in an effort to allow doctors to easily obtain the information they need to battle bioterrorism and to give consumers practical advice on how to protect themselves.

The U.S. Centers for Disease Control (CDC) quickly moved into the forefront of those organizations getting important information to the public. The Atlanta-based CDC set up a special site for bioterrorism data (www.bt.cdc.gov) that in the immediate aftermath of the anthrax attacks saw more more than one million hits per day.

In addition to the CDC, several other sites sought to guarantee a reliable, level-headed and clearly presented source of information. Thus, the American Medical Association stressed such issues as the need to put the risks in perspective and to understand the dangers of taking unnecessary antibiotics. "Part of our mission has to be education for calming the public's fears," said AMA Chairman Timothy Flaherty. The association, which co-sponsors the CDC webcasts, offerred free access to its five recent articles on smallpox, botulism, plague, tularemia and anthrax via its www.ama-assn.org site. It also set up disaster-preparedness and medical-response Web pages. Dr. Flaherty noted that nearly 75 percent of AMA members use the Internet, thereby enabling them to quickly learn of changes in therapeutic regimens as more scientific evidence becomes available.

Even as New York University Medical Center presented a symposium on bioterrorism, emergency preparedness and chemical warfare in October 2001 for about 100 local doctors, some 8,000 more were able to watch a free Webcast of the event throughout the country. It was presented by World Medical Leaders, a for-profit site offering continuing medical-education credits for doctors who pay to hear experts lecture online. The group, which is owned by Omnicom Group, an advertising conglomorate, also has set up a bioterrorism resource center on

its site, offering CDC updates and lectures from Harvard University and the National Institute of Mental Health.

The American College of Emergency Physicians sponsored a live forum on its ACEP.org Web site. Doctors were able to posek questions to a CDC epidemiologist on;line. The group has also contacted 13,000 emergency doctors by e-mail, sending them its latest morbiity and mortality weekly reports, including updated treatment protocols for biologic agents.

Other previously closed professional sites, aimed primarily at doctors, have openedg their bioterrorism files to the public. For, example, Stanford University's online database for doctors, (Stanford Skolar MD,) allows consumers access its new biological and chemical terrorism resources by registering for a free ten-day trial on its Web site at www.skolar.com.

Similarly, the Medical Library Association has updated its bioterrorism resources on its mlanet.org site to offer pertinent information to consumers who are unfamiliar with medical jargon. And the Nemours Foundation's Center for Children's Health Media is using its KidsHealth.org Web site to offer articles for parents and for different child and teenage reading levels on "what you need to know about smallpox, anthrax and coping with the uncertainties we face today."

As is usually the case, there is also a dark side to bioterrorism dealings on the INternet, Thus, some 40 operators of Web sites have been warned by the Federal Trade Commission (FTC) to stop making what the agencyt called false claims that dietary supplements can prevent, treat or cure anthrax, smallpox and other health hazards. The warnings followed an Internet surfing project by the FTC, the Food and Drug Administration and state attorneys general in some 30 states.

J. Howard Beales III, the FTC's director of consumer protection, said the online investigation uncovered more than 200 Web sites that were marketing bioterrorism-related products, including gas masks, protective suits, mail sterilizers, homeopathic remedies and iohazard test kits, in addition to dietary supplements.

"We started right after September 11, both monitoring complaints and organizing a surf of the Internet to look for all the different ways people might try to take advantage of the September 11 tragedy to make money," Beales said. "We found claims that a variety of dietary supplements like colloidal silver or zinc mineral water or oregano oil would be remedies for anthrax or other biological agents. So far as we know there's no scientific evidence whatsoever that even suggests those kinds of claims might be true."

Conclusion

Three months after the massive terrorist blow, the evidence suggests that -- temporary and spotty overload problems aside -- the decentralized nature of the Internet provided -- and continues to provide -- a coherent and novel U.S. domestic communication channel in a quasi-wartime setting. But given the clearly more intrusive role of the federal government and the perceived threats to U.S. security posed by unfettered online communications, how that powerful forum evolves from this point forward still remains a major unresolved issue.