Chapter Eight

ACTIVISM, HACKTIVISM, AND CYBERTERRORISM: THE INTERNET AS A TOOL FOR INFLUENCING FOREIGN POLICY

Dorothy E. Denning

Editors' abstract. Netwar is not mainly about technology—but good information technology sure makes a difference. In this chapter, Denning (Georgetown University) examines how activists, hacktivists, and cyberterrorists use the Internet, and what influence they have been able to exert on policymakers. Social activists seem the most effective of these netwar actors. Hacktivists and cyberterrorists have not posed much of a real threat to date—but this could change if they acquire better tools, techniques, and methods of organization, and if cyberdefenses do not keep pace. In this swiftly evolving area, today's tools and techniques are often soon outdated; yet Denning's analytic approach should prove conceptually sound for years to come. The original version of this paper was sponsored by the Nautilus Institute and presented at a conference on "The Internet and International Systems: Information Technology and American Foreign Policy Decision Making," The World Affairs Council, San Francisco, December 10, 1999 (www.nautilus.org/info-policy/workshop/papers/denning.html). Reprinted by permission.

The conflict over Kosovo has been characterized as the first war on the Internet. Government and nongovernment actors alike used the Net to disseminate information, spread propaganda, demonize opponents, and solicit support for their positions. Hackers used it to voice their objections to both Yugoslav and NATO aggression by disrupting service on government computers and taking over their web sites. Individuals used it to tell their stories of fear and horror inside the con-

flict zone, while activists exploited it to amplify their voices and reach a wide, international audience. And people everywhere used it to discuss the issues and share text, images, and video clips that were not available through other media. In April 1999, the *Los Angeles Times* wrote that the Kosovo conflict was "turning cyberspace into an ethereal war zone where the battle for the hearts and minds is being waged through the use of electronic images, online discussion group postings, and hacking attacks."[1] Anthony Pratkanis, professor of psychology at the University of California, Santa Cruz, and author of *Age of Propaganda: The Everyday Use and Abuse of Persuasion,* observed,

> What you're seeing now is just the first round of what will become an important, highly sophisticated tool in the age-old tradition of wartime propaganda . . . . The war strategists should be worried about it, if they aren't yet.[2]

Just how much impact did the Internet have on foreign policy decisions relating to the war? It clearly had a part in the political discourse taking place, and it was exploited by activists seeking to alter foreign policy decisions. It also affected military decisions. While NATO targeted Serb media outlets carrying Milosevic's propaganda, it intentionally did not bomb Internet service providers or shut down the satellite links bringing the Internet to Yugoslavia. Policy instead was to keep the Internet open. James P. Rubin, spokesman for the U.S. State Department, said "Full and open access to the Internet can only help the Serbian people know the ugly truth about the atrocities and crimes against humanity being perpetrated in Kosovo by the Milosevic regime."[3] Indirectly, the Internet may have also affected public support for the war, which in turn might have affected policy decisions made during the course of the conflict.

The purpose of this chapter is to explore how the Internet is altering the landscape of political discourse and advocacy, with particular em-

---

[1]Ashley Dunn, "Crisis in Yugoslavia—Battle Spilling over onto the Internet," *Los Angeles Times*, April 3, 1999.

[2]Quoted in Rick Montgomery, "Enemy in Site—It's Time to Join the Cyberwar," *Daily Telegraph* (Australia), April 19, 1999, p. 19.

[3]David Briscoe, "Kosovo-Propaganda War," *Associated Press*, May 17, 1999.

phasis on how it is used by those wishing to influence foreign policy. Emphasis is on actions taken by nonstate actors, including both individuals and organizations, but state actions are discussed where they reflect foreign policy decisions triggered by the Internet. The primary sources used in the analysis are news reports of incidents and events. These are augmented with interviews and survey data where available. A more scientific study would be useful.

The chapter is organized around three broad classes of activity: activism, hacktivism, and cyberterrorism. The first category, activism, refers to normal, nondisruptive use of the Internet in support of an agenda or cause. Operations in this area includes browsing the web for information, constructing web sites and posting materials on them, transmitting electronic publications and letters through email, and using the Net to discuss issues, form coalitions, and plan and coordinate activities. The second category, hacktivism, refers to the marriage of hacking and activism. It covers operations that use hacking techniques against a target's Internet site with the intent of disrupting normal operations but not causing serious damage. Examples are web sit-ins and virtual blockades, automated email bombs, web hacks, computer break-ins, and computer viruses and worms. The final category, cyberterrorism, refers to the convergence of cyberspace and terrorism. It covers politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage. An example would be penetrating an air traffic control system and causing two planes to collide. There is a general progression toward greater damage and disruption from the first to the third category, although that does not imply an increase of political effectiveness. An electronic petition with a million signatures may influence policy more than an attack that disrupts emergency 911 services.

Although the three categories of activity are treated separately, the boundaries between them are somewhat fuzzy. For example, an email bomb may be considered hacktivism by some and cyberterrorism by others. Also, any given actor may conduct operations across the spectrum. For example, a terrorist might launch viruses as part of a larger campaign of cyberterrorism, all the while using the Internet to collect information about targets, coordinate action with fellow conspirators, and publish propaganda on web sites. Thus, while this chapter

distinguishes activists, hacktivists, and terrorists, an individual can play all three roles.

The following sections discuss and give examples of activity in each of these three areas. The examples are drawn from the Kosovo conflict, cryptography policy, human rights in China, support for the Mexican Zapatistas, and other areas of conflict. The examples are by no means exhaustive of all activity in any of these areas, but are intended only to be illustrative. Nevertheless, they represent a wide range of players, targets, and geographical regions.

The main conclusion here is that the Internet can be an effective tool for activism, especially when it is combined with other communications media, including broadcast and print media and face-to-face meetings with policymakers. It can benefit individuals and small groups with few resources as well as organizations and coalitions that are large or well-funded. It facilitates such activities as educating the public and media, raising money, forming coalitions across geographical boundaries, distributing petitions and action alerts, and planning and coordinating events on a regional or international level. It allows activists in politically repressive states to evade government censors and monitors.

With respect to hacktivism and cyberterrorism, those who engage in such activity are less likely to accomplish their foreign policy objectives than those who do not employ disruptive and destructive techniques. They may feel a sense of empowerment, because they can control government computers and get media attention, but that does not mean they will succeed in changing policy. The main effect is likely to be a strengthening of cyberdefense policies, both nationally and internationally, rather than accommodation to the demands of the actors.

ACTIVISM

The Internet offers a powerful tool for communicating and coordinating action. It is inexpensive to use and increasingly pervasive, with an

estimated 300 million people online as of May 2000.[4] Groups of any size, from two to millions, can reach each other and use the Net to promote an agenda. Their members and followers can come from any geographical region on the Net, and they can attempt to influence foreign policy anywhere in the world. This section describes five modes of using the Internet: collection, publication, dialogue, coordination of action, and direct lobbying of decisionmakers. While treated separately, the modes are frequently used together, and many of the examples described here illustrate multiple modes.

Collection

One way of viewing the Internet is as a vast digital library. The web alone offers several billion pages of information, and much of the information is free. Activists may be able to locate legislative documents, official policy statements, analyses and discussions about issues, and other items related to their mission. They may be able to find names and contact information for key decisionmakers inside the government or governments they ultimately hope to influence. They may be able to identify other groups and individuals with similar interests and gather contact information for potential supporters and collaborators. There are numerous tools that help with collection, including search engines, email distribution lists, and chat and discussion groups. Many web sites offer their own search tools for extracting information from databases on their sites.

One advantage of the Internet over other media is that it tends to break down barriers erected by government censors. For example, after Jordanian officials removed an article from 40 print copies of *The Economist* on sale in Jordan, a subscriber found a copy online, made photocopies, and faxed it to 1,000 Jordanians. According to Daoud Kuttab, head of the Arabic Media Internal Network (AMIA), the government would have been better off leaving the print version intact. "We found this very exciting," he said. "For the first time the traditional censorship that exists within national borders was bypassed." Kuttab said AMIA opened Jordanian journalists to the non-Arab world

[4]Nua Internet Surveys, www.nua.ie. The site is updated regularly with the latest estimate.

and use of the web as a research tool. "In the Jordanian media, we have been able to detect a much more open outlook to the world as well as to Arab issues," he said.[5]

The Internet itself is not free of government censorship. According to Reporters Sans Frontiers, 45 countries restrict their citizens' access to the Internet, typically by forcing them to subscribe to a state-run Internet service provider, which may filter out objectionable sites.[6] Authoritarian regimes recognize the benefits of the Internet to economic growth, but at the same time feel threatened by the unprecedented degree of freedom of speech.

Chinese authorities block access to web sites that are considered subversive to government objectives. This has been only partially effective, however, and Chinese activists have found ways of slipping information past the controls. For example, the editors of *VIP Reference*, a Washington-based electronic magazine with articles and essays about democratic and economic evolution inside China, email their electronic newsletter directly to addresses inside mainland China. The email is sent from a different address every day to get past email blocks. It is also delivered to random addresses, compiled from commercial and public lists, so that recipients can deny having deliberately subscribed. As of January 1999, about 250,000 people received the pro-democracy publication, including people inside the government who did not want it. Chinese officials were not, however, complacent. When 30-year-old Shanghai software entrepreneur Lin Hai sold 30,000 email addresses to *VIP Reference*, he was arrested and later sentenced to two years in prison. In addition, authorities fined him 10,000 yuan (a little over $1,000) and confiscated his computer equipment and telephone. Lin was said to be the first person convicted in China for subversive use of the Internet. He claimed he was only trying to drum up business and was not politically active.[7]

---

[5]Alan Docherty, "Net Journalists Outwit Censors," *Wired News*, March 13, 1999.

[6]*The Twenty Enemies of the Internet,* press release, Reporters Sans Frontiers, August 9, 1999.

[7]Maggie Farley, "Dissidents Hack Holes in China's New Wall," *Los Angeles Times*, January 4, 1999. Adrian Oosthuizen, "Dissidents to Continue E-Mail Activity Despite Court Verdict," *South China Morning Post*, February 2, 1999.

During the Kosovo conflict, people in Yugoslavia had full access to the Internet, including Western news sites. In April 1999, the *Washington Post* reported that according to U.S. and British officials, the NATO governments controlled all four Internet access providers in Yugoslavia and kept them open for the purpose of spreading disinformation and propaganda. The *Post* also said that Belgrade, with a population of 1.5 million, had about 100,000 Internet connections.[8] Individuals without their own connections could get access at Internet cafes.

Even though Serbs had access to Western news reports, both through the Internet and through satellite and cable television, many did not believe what they saw and heard from Western media. They considered coverage on Western television stations such as CNN and Sky News to be as biased as that on the Yugoslav state-run station, citing instances when Western reports of Serbian atrocities turned out to be wrong. Alex Todorovic, a Serbian-American who spent time in Belgrade during the conflict observed, "By and large, Serbs mistrust the rest of the world's media. CNN, for example, is considered the official voice of Washington."[9] Some Yugoslav surfers did not even bother looking at Western news sites on the Internet. When asked if she visited web sites of Western news stations, one 22-year-old student replied, "No, I don't believe in their information, so why should I upset myself?"[10] Thus, it is not clear whether open Internet access in Yugoslavia undermined Milosevic's objectives. Further, given that people living in Yugoslavia personally witnessed and felt the effects of the NATO bombing and either disbelieved reports or heard little about Serb atrocities against the ethnic Albanians in Kosovo, it is not surprising that an anti-NATO discourse ran throughout Belgrade. As one pharmacist observed, "I have two children. The people who are bombing my kids are my only enemy right now."[11]

In addition to information relating to a particular policy issue, the web offers cyberactivists various information that can help them use the Net effectively. For example, NetAction offers a training guide for

[8]Michael Dobbs, "The War on the Airwaves," *Washington Post*, April 19, 1999.

[9]Alex Todorovic, "I'm Watching Two Different Wars," *Washington Post*, April 18, 1999.

[10]Dobbs, 1999.

[11]Todorovic, 1999.

the virtual activist. The guide provides information on the use of email for outreach, organizing, and advocacy; web-based outreach and advocacy tools; membership and fundraising; netiquette and policy issues; and various resources.[12]

Publication

The Internet offers several channels whereby advocacy groups and individuals can publish information (and disinformation) to further policy objectives. They can send it through email and post it to newsgroups. They can create their own electronic publications or contribute articles and essays to those of others. They can put up web sites, which can serve as a gathering place and source of information for supporters, potential supporters, and onlookers.

One reason the Internet is popular among activists is its cost advantage over traditional mass media. It is easier and cheaper to post a message to a public forum or put up a web site than it is to operate a radio or television station or print a newspaper. Practically anyone can afford to be a web publisher. In addition, the reach of the Internet is global. A message can potentially reach millions of people at no additional cost to the originator. Further, activists can control their presentation to the world. They decide what is said and how. They do not have to rely on the mass media to take notice and tell their story "right."

Kosovo. During the Kosovo conflict, organizations and individuals throughout the world used their web sites to publish information related to the conflict and, in some cases, to solicit support. Nongovernment organizations with Kosovo-related web pages included the press, human rights groups, humanitarian relief organizations, churches, and women's groups.

Government web sites on Kosovo tended to feature propaganda and materials that supported their official policies. An exception was the U.S. Information Agency (USIA) web site, which presented a survey of news stories from around the world, some of which were critical of

[12]*NetAction's Virtual Activist Training Guide,* www.netaction.org/training.

NATO actions.[13] Jonathan Spalter, USIA chief information officer, commented that "The measure of our success is the extent to which we are perceived not as propaganda but anti-propaganda."[14] The British government's Foreign Office used their web site, in part, to counter Serb propaganda. Concerned that the Yugoslav public was getting a highly distorted view of the war, Foreign Secretary Robin Cook posted a message on the office's web site intended for the Serbs. The message said that Britain has nothing against the Serbs but was forced to act by the scale of Yugoslav President Slobodan Milosevic's brutality.[15] British Defence Secretary George Robertson said the Ministry of Defence (MoD) had translated its web site into Serbian to counter censorship of the news by Belgrade.[16]

The Yugoslav media was controlled by the Serbian government and served to promote Milosevic's policies. Yugoslavia had an independent, prodemocracy radio station, B92, but it was raided by the police in the early days of the Kosovo conflict and turned over to a government-appointed station manager.[17] B92 had had a run-in with the government earlier, in late 1996, when government jammers tried to keep it from airing news broadcasts. At that time, however, B92 prevailed, in part by encoding their news bulletins in RealAudio format and posting them on a web site in Amsterdam. Radio Free Europe acquired tapes of the news programs and rebroadcasted them back to the Serbs, circumventing the jammers, who then gave up.[18] But when the government took over B92's facility in 1999, B92's then-managers ceded to the government and also discontinued posting materials on their web site, which had offered viewers a reliable source of information about the conflict. This was considered a great loss to Yugoslavia's

[13]See www.usia.gov.

[14]David Briscoe, "Kosovo-Propaganda War," *Associated Press*, May 17, 1999.

[15]"Conflict in the Balkans—Cook Enlists Internet to Send Serbs Message," *Daily Telegraph*, London, April 2, 1999, p. 9.

[16]Rebecca Allison, "Belgrade Hackers Bombard MoD Website in 'First' Internet War," *PA News,* March 31, 1999.

[17]Leander Kahney, "Yugoslavia's B92 Goes Dark," *Wired News*, April 2, 1999.

[18]Bob Schmitt, "An Internet Answer to Repression," *Washington Post*, March 31, 1997, p. A21.

prodemocracy movement and general public, which had rallied behind Belgrade's top-rated news station.

A few individuals inside Yugoslavia posted to the Internet firsthand accounts of events as they were being witnessed or shortly thereafter. Their stories told of fear and devastation, the latter caused not only by the Serb military, but also by NATO bombs. By all accounts, the situation inside Yugoslavia was horrible for citizens everywhere, whether Serbian or ethnic Albanian. The stories may have inspired activists and influenced public opinion, but it is not clear what if any effect they had on government decisionmaking.

New-media artists used the web to voice their opinions on the Balkans conflict. In late March, artist and high school teacher Reiner Strasser put up a site called Weak Blood, which featured works of visual poetry, kinetic imagery, and interactive art, all making an antiviolence statement. Strasser vowed to add one or two pieces a day "as long as bombs are falling and humans are massacred" in the region.[19]

Some Serbs with Internet access sent emails to American news organizations calling for an end to the NATO bombing. Many of the messages contained heated rhetoric that was anti-NATO and anti-U.S. One letter directed to the Associated Press ended, "To be a Serb now is to be helpless . . . to listen to the euphemistic and hypocritical phrases as 'peace-making mission,' 'moral imperative.'" Other messages contained human stories about how their lives were affected. Tom Reid, London correspondent to the *Washington Post*, said he received 30–50 messages a day from professors at universities and activists all over Yugoslavia. The general tenor of the messages was the same, "'Please remember there are human beings under your bombs,'" he said.[20]

The Serbs used email distribution lists to reach tens of thousands of users, mostly in the United States, with messages attacking the NATO bombing campaign. One message read

[19]Matthew Mirapaul, "Kosovo Conflict Inspires Digital Art Projects," *The New York Times (Cybertimes)*, April 15, 1999.

[20]Larry McShane, "Yugoslavs Condemn Bombs over E-mail to U.S. Media," *Nando Times*, April 17, 1999, www.nandotimes.com.

> In the last nine days, NATO barbarians have bombed our schools, hospitals, bridges, killed our people but that was not enough for them now they have started to destroy our culture monuments which represents [sic] the core of existence of our nation.

Most recipients were annoyed by this unwanted "spam," which the *Wall Street Journal* dubbed "Yugospam."[21]

Dennis Longley, a professor in the Information Security Research Centre at Australia's Queensland University of Technology, said they received a suspicious email from Serbia. The message had two paragraphs. The first was the usual friendly greetings, while the second was a rant about NATO that read like pure propaganda, characterizing NATO as a "terrorist organization" that "brought nothing but a gigantic humanitarian disaster to Kosovo," while attributing the cause of the problem to "Albanian terrorist and separatist actions, not the repression by the government security forces." The second paragraph exhibited a style unlike the first and a standard of English well below that of the sender, leading them to speculate that Serb authorities had modified the email.[22] If that is so, one is left wondering how much other anti-NATO talk hitting the Net was the work of the Yugoslav government.

Of course, not all of the messages coming out of the Balkans were anti-NATO. Shortly after the Kosovo conflict began, I found myself on a list called "kcc-news," operated by the Kosova[23] Crisis Center from the Internet domain "alb-net.com." The messages included Human Rights Flashes from Human Rights Watch, Action Alerts from the Kosova Task Force, and other appeals for support in the war against the Serbs. One message contained a flier calling for "sustained air strikes until total Serb withdrawal" and "ground troops to STOP GENOCIDE now." The flier included links to web pages that documented Serb atrocities and aggression.

---

[21]Ellen Joan Pollock and Andrea Petersen, "Unsolicited E-Mail Hits Targets in America in First Cyberwar," *Wall Street Journal*, April 8, 1999.

[22]Dennis Longley, personal communication, July 15, 1999.

[23]The task force uses the spelling "Kosova" in its name and in all references to Kosovo.

Even though the Yugoslav government did not prohibit Internet activity, fear of government reprisals led some to post their messages through anonymous remailers so they could not be identified. This allowed for a freer discourse on Internet discussion groups and contributed to the spread of information about the situation inside Belgrade and Kosovo. Microsoft Corp. initiated a section called "Secret Dispatches from Belgrade" on the web site of its online magazine *Slate*. An anonymous correspondent gave daily reports of both alleged Serb atrocities and civilian suffering inflicted by NATO bombs.[24]

After human rights organizations expressed concern that the Yugoslav government might be monitoring Internet activity and cracking down on anyone expressing dissenting views, Anonymizer Inc., a provider of anonymous web browsing and email services, launched the Kosovo Privacy Project web site. The site, which went online in April 1999, offered surfers anonymous email and instant, anonymous access to Voice of America, Radio Free Europe, and about 20 other web sites. According to *Federal Computer Week*, Anonymizer planned to add NATO and other Western government information sites to the Kosovo list, and to launch similar projects for human rights situations in other parts of the world, for example, China.[25] However, the effectiveness of the Kosovo project was never established. In August 1999, *USA Today* reported that activists said the project was little noticed inside Kosovo, where traditional media seemed unaware while the fighting knocked out Internet trunk lines in short order.[26]

Internet Policy Issues. The Internet has raised numerous policy issues in such areas as privacy, encryption, censorship, electronic commerce, international trade, intellectual property protection, taxation, Internet governance, cybercrime, and information warfare, all of which have a foreign policy dimension. As the issues surfaced and took on some urgency, existing industry and public-interest groups began to address them. In addition, both national and international

[24]Rick Montgomery, "Enemy in Site—It's Time to Join the Cyberwar," *Daily Telegraph*, Australia, April 19, 1999.

[25]Daniel Verton, "Net Service Shields Web Users in Kosovo," *Federal Computer Week*, April 19, 1999.

[26]Will Rodger, "Online Human-Rights Crusaders," *USA Today*, August 25, 1999.

advocacy groups sprung up specifically devoted to Internet issues. They all operate web sites, where they publish policy papers and information about issues, events, and membership. Many also send out email newsletters and alerts.

In the area of encryption policy, for example, the major players include Americans for Computer Privacy (ACP), the Center for Democracy and Technology (CDT), Cyber-Rights & Cyber Liberties, the Electronic Frontier Foundation (EFF), the Electronic Privacy Information Center (EPIC), the Global Internet Liberty Campaign (GILC), and the Internet Privacy Coalition. The ACP has perhaps the largest group of constituents, being composed of 40 trade associations, over 100 companies, and more than 3,000 individual members.[27] GILC is one of the most global, with member organizations from Europe, North America, Australia, and Asia.

In July 1999, nine leading U.S.-based Internet companies joined forces to become the voice of the Internet on such issues as privacy, consumer protection, and international trade. The industry group, called NetCoalition.com, includes America Online, Amazon.com, eBay, Lycos, Yahoo!, DoubleClick, Excite@Home, Inktomi, and Theglobe.com. The companies represent seven of the top ten Internet sites, and more than 90 percent of the world's Internet users visit one of the sites at least once a month. The group plans to focus on 150 Internet-related bills that were introduced in Congress.[28]

Hackers and Terrorists. The Internet is used extensively as a publication medium by hackers (including hacktivists) and terrorists. Hackers publish electronic magazines and put up web sites with software tools and information about hacking, including details about vulnerabilities in popular systems (e.g., Microsoft Windows) and how they can be exploited, programs for cracking passwords, software packages for writing computer viruses, and scripts for disabling or breaking into computer networks and web sites. In March 1997, an article in

[27]See www.computerprivacy.org.

[28]"Internet Heavies Back New Net-Policy Group," IDG, July 14, 1999.

The New York Times reported that there were an estimated 1,900 web sites purveying hacking tips and tools, and 30 hacker publications.[29]

Terrorist groups use the Internet to spread propaganda. Back in February 1998, Hizbollah was operating three web sites: one for the central press office (www.hizbollah.org), another to describe its attacks on Israeli targets (www.moqawama.org), and the third for news and information (www.almanar.com.lb).[30] That month, Clark Staten, executive director of the Emergency Response & Research Institute (ERRI) in Chicago, testified before a U.S. Senate subcommittee that "even small terrorist groups are now using the Internet to broadcast their message and misdirect/misinform the general population in multiple nations simultaneously." He gave the subcommittee copies of both domestic and international messages containing anti-American and anti-Israeli propaganda and threats, including a widely distributed extremist call for *jihad* (holy war) against America and Great Britain.[31] In June 1998, *U.S. News & World Report* noted that 12 of the 30 groups on the U.S. State Department's list of terrorist organizations are on the web. As of August 1999, it appears that virtually every terrorist group is on the web, along with a mishmash of freedom fighters, crusaders, propagandists, and mercenaries.[32] Forcing them off the web is impossible, because they can set up their sites in countries with free-speech laws. The government of Sri Lanka, for example, banned the separatist Liberation Tigers of Tamil Eelam, but they have not even attempted to take down their London-based web site.[33]

---

[29]Steve Lohr, "Go Ahead, Be Paranoid: Hackers Are out to Get You," *The New York Times*, March 17, 1997.

[30]John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar, and Information-Age Terrorism," in Ian O. Lesser et al., *Countering the New Terrorism*, RAND, 1999, p. 66. The authors cite "Hizbullah TV Summary 18 February 1998," *Al-Manar Television World Wide Webcast*, FBIS-NES-98-050, February 19, 1998, and "Developments in Mideast Media: January–May 1998," Foreign Broadcast Information Service (FBIS), May 11, 1998.

[31]Clark L. Staten, testimony before the Subcommittee on Technology, Terrorism and Government Information, U.S. Senate Judiciary Committee, February 24, 1998.

[32]Bob Cromwell's site at Purdue has an excellent collection of links: http://RVL4.ecn.purdue.edu/~cromwell/lt/terror.html.

[33]Kevin Whitelaw, "Terrorists on the Web: Electronic 'Safe Haven,'" *U.S. News & World Report*, June 22, 1998, p. 46. The State Department's list of terrorist organizations is at www.state.gov/www/global/terrorism/index.html.

Dialogue

The Internet offers several venues for dialogue and debate on policy issues. These include email, newsgroups, web forums, and chat. Discussions can be confined to closed groups, for example through email, as well as open to the public. Some media sites offer web surfers the opportunity to comment on the latest stories and current issues and events. Government officials and domain experts may be brought in to serve as catalysts for discussion, debate issues, or answer questions. Discussion can even take place on web sites that themselves lack such facilities. Using Gooey software from the Israeli company Hypernix, for example, visitors to a web site can chat with other Gooey users currently at the site.[34]

Internet discussion forums are frequently used to debate, blast, and maybe even attempt to influence government policies. Encryption policy, for example, is discussed on the email lists "cypherpunks" and "ukcrypto" and on several newsgroups, including alt.privacy and sci.crypt.

The ukcrypto list was created in early 1996 by two academics, Ross Anderson (Cambridge) and Paul Leyland (Oxford), and one person then in government, Brian Gladman (NATO SHAPE), who was acting outside his official capacity. Motivated by a concern that a lack of public discussion and debate in the United Kingdom on cryptography issues was allowing the government to set policies that they believed were not in the interests of the United Kingdom and its citizens, they formed the list with the objective of affecting cryptography policy. They were concerned both with domestic policy, particularly proposals to restrict the use of cryptography by U.K. citizens, and foreign policy, particularly export controls. As of May 1999, the list had 300 subscribers, including government officials responsible for U.K. policy and persons in other countries, including the United States. Many of the key contributors held influential positions in other policymaking fora. The focus is on U.K. policy issues, but items of international interest are also discussed, including export controls adopted under the Wassenaar Arrangement (31 countries participate);

[34]Chris Oaks, "Every Web Site a Chat Room," *Wired News*, June 14, 1999.

policy changes adopted by France, the United States, and other countries; policy statements from the European Union and other organizations; and some technical issues.[35]

Gladman believes the list has made four contributions: (1) educating many about the policy issues and encouraging journalists and writers to write about them; (2) bringing individual and industry views closer together and allowing U.K. industry to see more clearly that agreeing with their government may not be a good thing if private citizens do not support government policy; (3) encouraging the more progressive voices in government to speak out and argue from within government that their views represent those of the public; and (4) bringing groups together that were previously campaigning separately. "The most significant contribution of ukcrypto is not direct," Gladman said. "It is the contribution that it has made in promoting an educated community of commentators and a forum for the review of what government is doing that is fully open."

On the downside, some postings on ukcrypto may alienate the very government officials the authors hope to influence. According to Gladman,

> discussions on the list can become slinging matches that quickly put those in government on the defensive and hence inclined to discount what is being said. It would be more effective if we had a way of focusing on the issues and not the personalities.[36]

But Andrew Brown gave ukcrypto high marks, crediting it with most of the thought and coordination behind the successful campaign to keep strong cryptography legal and widely available. He wrote in *New Statesman,*

> There, for the past two years, the civil servants responsible for policy have actually been available, more or less, to the people who disagree with them. . . . They have had to justify their actions, not to the

[35]Brian Gladman, personal correspondence, May 4, 1999, augmented by my own observations from subscribing to the list since the beginning.

[36]Ibid.

> public, but to a small group of geographically dispersed experts. . . . It's a kind of updated version of Lions *v* Christians.[37]

Nigel Hickson, one of the principal players in the policy debates from the U.K. Department of Trade and Industry (DTI), agrees the Internet and ukcrypto in particular have played a role in shaping U.K. cryptography policy.[38] But he was also critical of the list:

> Whilst ukcrypto has undoubtedly had an influence on the development of U.K. encryption policy, it has tended to polarise the debate into extremes. This may be because there tends to be a large "silent majority" on the list who do not directly contribute because of commercial or policy reasons.[39]

Besides participating in ukcrypto, the DTI has published draft consultation documents on the web for comment. Many of the comments they receive arrive through electronic mail. DTI has also met with industry groups and participated in non-Internet forums, such as conferences and seminars. These have also helped shape policy decisions.

There are Usenet newsgroups and other interactive forums that focus on practically every conceivable topic relating to foreign (and domestic) policy. Whether these are effective or not in terms of influencing policy is another matter. After studying the effects of the Net on the American political system, Richard Davis, a political science professor at Brigham Young University and author of *The Web of Politics*, observed that

> In Usenet political discussions, people talk past one another, when they are not verbally attacking each other. The emphasis is not problem solving, but discussion dominance.[40]

---

[37]Andrew Brown, "Editors Wanted," *New Statesman*, April 26, 1999.

[38]Nigel Hickson, private conversation, April 29, 1999.

[39]Nigel Hickson, private communication, July 28, 1999.

[40]Richard Davis, *The Web of Politics*, Oxford University Press, 1999, p. 177.

Davis also found interactivity on the Internet to be primarily an illusion:

> Interest groups, party organizations, and legislators seek to use the web for information dissemination, but they are rarely interested in allowing their sites to become forums for the opinions of others.[41]

Coordination of Action

Advocacy groups can use the Internet to coordinate action among members and with other organizations and individuals. Action plans can be distributed by email or posted on web sites. Services are cheaper than phone and fax (although these services can also be delivered through the Internet), and faster than physical delivery (assuming Internet services are operating properly, which is not always the case). The Internet lets people all over the world coordinate action without regard to constraints of geography or time. They can form partnerships and coalitions or operate independently.

One web site was created to help activists worldwide coordinate and locate information about protests and meetings. According to statements on Protest.Net, the web site serves "to help progressive activists by providing a central place where the times and locations of protests and meetings can be posted." The site's creator said he hoped it would "help resolve logistical problems that activists face in organizing events with limited resources and access to mass media."[42] The site features news as well as action alerts and information about events.

The power of the Internet to mobilize activists is illustrated by the arrest of Kurdish rebel leader Abdullah Ocalan. According to Michael Dartnell, a political science professor at Concordia University, when Turkish forces arrested Ocalan, Kurds around the world responded with demonstrations within a matter of hours. He attributed the swift action in part to the Internet and web. "They responded more quickly than governments did to his arrest," he said. Dartnell contends the Internet and advanced communication tools are changing the way peo-

[41]Davis, 1999, p. 178.

[42]See www.protest.net.

ple around the world play politics. Antigovernment groups are establishing alliances and coalitions that might not have existed before the technology was introduced.[43]

The force of the Internet is further illustrated by the day of protest against business that took place on June 18, 1999. The protests, which were set up to coincide with a meeting of the G8 in Cologne, Germany, was coordinated by a group called J18 from a web site inviting people to plan individual actions focusing on disrupting "financial centres, banking districts and multinational corporate power bases." Suggested activity included marches, rallies, and hacking. In London, up to 2,000 anticapitalists coursed through the city shouting slogans and spray-painting buildings.[44] According to the *Sunday Times*, teams of hackers from Indonesia, Israel, Germany, and Canada attacked the computers of at least 20 companies, including the Stock Exchange and Barclays. More than 10,000 attacks were launched over a five-hour period.[45]

During the Kosovo conflict, the Kosova Task Force used the Internet to distribute action plans to Muslims and supporters of Kosovo. A March 1999 Action Alert, for example, asked people to organize rallies in solidarity with Kosovo at local federal buildings and city halls on April 3 at 11 a.m.; organize public funeral prayers; make and encourage others to make daily calls or send email to the White House asking for Kosovo independence, sustained air strikes until there was total Serb withdrawal from Kosovo, and arming of ethnic Albanians in Kosovo; and make and encourage others to make calls to their representatives and senators. An April 18 alert asked every community in the United States to establish a Kosova Room for action and information. Each room was to be equipped with a bank of phones for making 1,000 calls to the White House and Congress in support of resolution #HCR 9, calling for independence of Kosovo.

---

[43]Martin Stone, "Prof to Build Archive of Insurgency Groups," *Newsbytes*, March 3, 1999.

[44]Edward Harris, "Web Becomes a Cybertool for Political Activists," *Wall Street Journal*, August 5, 1999, B11; Barbara Adam, "J18 Hackers Could Target Australian Companies on Friday," *Australian Associated Press*, June 16, 1999.

[45]Jon Ungoed-Thomas and Maeve Sheehan, "Riot Organisers Prepare to Launch Cyber War on City," *Sunday Times*, August 15, 1999.

The International Campaign to Ban Landmines (ICBL), a loose coalition of over 1,300 groups from more than 75 countries, has made extensive use of the Internet in efforts to stop the use, production, stockpiling, and transfer of antipersonnel landmines, and to increase international resources for humanitarian mine clearance and victim assistance. According to ICBL's Liz Bernstein, the Net has been the dominant form of communication since 1996.[46] It has been used to coordinate events and committee functions, distribute petitions and action alerts, raise money, and educate the public and media. Although most direct lobbying is done through face-to-face meetings and letters, email has facilitated communications with government policymakers. Bernstein said the Net "has helped the nature of the campaign as a loose coalition, each campaign setting their own agenda yet with common information and communication."[47] Ken Rutherford, cofounder of Land Mine Survivors Network, noted that the Internet also helped establish bridges from North America and Europe to Asia and Africa, and helped enable quick adoption of the 1997 landmine treaty.[48] It became international law on March 1, 1999, and, as of September 16, 1999, has been signed by 135 countries and ratified by 86. In 1997, the Nobel Peace Prize was awarded to the ICBL and its then coordinator, Jody Williams.[49]

Human rights workers increasingly use the Internet to coordinate their actions against repressive governments. One tool that has become important in their battles is encryption, because it allows activists to protect communications and stored information from government interception. Human rights activists in Guatemala, for example, credited their use of Pretty Good Privacy (PGP) with saving the lives of witnesses to military abuses.[50] Encryption is not the ultimate solution, however, since governments can outlaw its use and arrest those who do not comply.

---

[46]Liz Bernstein, private communication, October 4, 1999.

[47]Ibid.

[48]Ken Rutherford, private communication, October 6, 1999.

[49]See also the ICBL web site at www.icbl.org and the web site of the Land Mine Survivors Network at www.landminesurvivors.org.

[50]Alan Boyle, "Crypto Can Save Lives," *ZDNet*, January 26, 1999. PGP provides both file and electronic-mail encryption.

Terrorists also use the Internet to communicate and coordinate their activities. Back in 1996, the headquarters of terrorist financier Osama bin Laden in Afghanistan was equipped with computers and communications equipment. Egyptian "Afghan" computer experts were said to have helped devise a communication network that used the web, email, and electronic bulletin boards.[51] Hamas activists have been said to use chat rooms and email to plan operations and coordinate activities, making it difficult for Israeli security officials to trace their messages and decode their contents.[52]

The U.S. government's program to establish an Advanced Encryption Standard (AES) illustrates how government can use the Internet to invite and coordinate participation in a decisionmaking process of international significance. The Department of Commerce National Institute of Standards and Technology (NIST) set up a web site with information about the AES program and AES conferences, a schedule of events, candidate encryption algorithms (more than half from outside the United States), documentation and test values, and links to public analysis efforts all over the world. The site contains an electronic discussion forum and Federal Register call for comments. Public comments are posted on the site and NIST representatives contribute to the online discussions and answer questions.[53] Because the AES will offer a foundation for secure electronic commerce and privacy internationally, involving the international community from the beginning will help ensure its success and widespread adoption. Cryptographers from all over in the world have been participating.

NIST's use of the Internet to aid a decision process seems to be unusual. While most government sites provide an email address for making contact, they do not support discussion forums or even ac-

---

[51]John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar, and Information-Age Terrorism," in Ian O. Lesser et al., *Countering the New Terrorism*, RAND, 1999, p. 65. The authors cite "Afghanistan, Saudi Arabia: Editor's Journey to Meet Bin-Laden Described," *London al-Quds al-'Arabi*, FBIS-TOT-97-003-L, November 27, 1996, p. 4, and "Arab Afghans Said to Launch Worldwide Terrorist War," 1995.

[52]Ibid. The authors cite "Israel: U.S. Hamas Activists Use Internet to Send Attack Threats," *Tel Aviv IDF Radio*, FBIS-TOT-97-001-L, October 13, 1996, and "Israel: Hamas Using Internet to Relay Operational Messages," *Tel Aviv Ha'aretz*, FBIS-TOT-98-034, February 3, 1998, p. 1.

[53]The NIST AES web site is at csrc.nist.gov/encryption/aes/aes_home.htm.

tively solicit comments on specific pending policy decisions. However, to the extent that government agencies invite or welcome email messages and input through electronic discussion groups, the Internet can serve the democratic process. Because it is easier to post or send a message on the Internet than to send a written letter, professionals and others with busy schedules may be more inclined to participate in a public consultation process or attempt to influence policy when policymakers are readily accessible through the Internet.

Lobbying Decisionmakers

Whether or not government agencies solicit their input, activists can use the Internet to lobby decisionmakers. One of the methods suggested by the Kosova Task Force for contacting the White House, for example, was email. Similarly, a Canadian web site with the headline "Stop the NATO Bombing of Yugoslavia Now!" urged Canadians and others interested in stopping the war to send emails and/or faxes to the Canadian Prime Minister, Jean Chretien, and all members of the Canadian Parliament. A sample letter was included. The letter concluded with an appeal to "stop aggression against Yugoslavia and seek a peaceful means to resolve the Kosovo problem."[54]

Email has been credited with halting a U.S. banking plan aimed to combat money laundering. Under the "Know Your Customer" policy, banks would have been required to monitor customer's banking patterns and report inconsistencies to federal regulators. Recognizing the value of the Internet to its deliberations, the Federal Deposit Insurance Corporation (FDIC) put up a web site, published an email address for comments, and printed out and tabulated each message. By the time the proposal was withdrawn, they had received 257,000 comments, 205,000 (80 percent) of which arrived through email. All but 50 of the letters opposed the plan. FDIC's chair, Donna Tanoue, said it was the huge volume of email that drove the decision to withdraw the proposal. "It was the nature and the volume [of the comments]," she

[54]See www.aeronautix.com/nato/yugoslavia.html.

said. "When consumers can get excited about an esoteric bank regulation, we have to pay attention."[55]

Most of the email was driven by an online advocacy campaign sponsored by the Libertarian Party. About 171,000 (83 percent) of the email messages were sent through the party's web site. The party advertised its advocacy campaign in talk radio interviews and by sending a notice to its email membership list.[56] One could argue that the results were due more to the efforts of a large nongovernment organization than to a grassroots response from the citizens.

Indeed, many email campaigns have been driven by nongovernment organizations. The organizations send email alerts on issues to electronic mailing lists, offer sample letters to send members of Congress and other decisionmaking bodies, and, in some cases, set up email boxes or web sites to gather signatures for petitions. The petition process can be automated, making it possible to gather huge volumes of signatures across a wide geographic area with little effort and cost. One web site, e-The People, offers hundreds of petitions to choose from and 170,000 email addresses of government officials.[57]

Computer Professionals for Social Responsibility (CPSR) organized an Internet petition campaign in early 1994 to protest the U.S. government's proposal to adopt the Clipper encryption chip as a standard.[58] The chip offered strong encryption but would have given law enforcement agencies the capability to decrypt a subject's messages when conducting a court-ordered wiretap against the subject. Despite numerous safeguards to ensure that government agencies could not violate the privacy of users of the chip,[59] Clipper was strongly opposed for privacy (and other) reasons, and the general sentiment expressed

---

[55]Rebecca Fairley Raney, "Flood of E-Mail Credited with Halting U.S. Bank Plan," *The New York Times (Cybertimes)*, March 24, 1999.

[56]Ibid.

[57]Edward Harris, "Web Becomes a Cybertool for Political Activists," *Wall Street Journal*, August 5, 1999, B11. The web site is at www.e-thepeople.com.

[58]The persons organizing the campaign went on to form the Electronic Privacy Information Center shortly thereafter.

[59]For example, each chip was uniquely keyed and decryption was not possible without getting the keys to the subject's chip from two separate government agencies.

on Internet newsgroups and email discussion lists was strongly anti-Clipper. CPSR announced its petition through email and set up an email address whereby people could sign on. Tens of thousands of signatures were collected, but it is not clear the petition had much impact. The government moved forward with the standard anyway, although Clipper eventually met its death.[60]

Because of the low cost of operation, individuals can run their own advocacy campaigns. For example, during the heart of the impeachment process against President Clinton, Joan Blades and Wes Boyd, a husband and wife team in Berkeley, founded MoveOn.org and put up a web site inviting citizens to sign a one-sentence petition: "The Congress must immediately censure President Clinton and move on to pressing issues facing the country." In just four months, the petition gathered a half-million signatures. Another petition that read "In the Year 2000 election, I will work to elect candidates who courageously address key national issues and who reject the politics of division and personal destruction" was sent to every member of the House and Senate. MoveOn.org received pledges of $13 million and more than 650,000 volunteer hours for congressional candidates in the 2000 election who supported its position.[61] It is difficult to assess the effects of the site on the impeachment process, but it may have amplified public opinion polls, which showed the American public supported Clinton and wanted Congress to turn to other issues.

While activists can attempt to influence policymakers through email, it is not clear that most policymakers listen (the FDIC, which asked for comments, was an exception). Richard Davis found that

> the Internet has not lived up to its promise as a forum for public expression to elected officials. In fact, while publicly encouraging e-mail, members are becoming increasingly disenchanted with it. If the most idealistic members originally envisioned e-mail as the impetus for intelligent communication with constituents, they have

[60]For an interesting discussion of the Internet campaign against Clipper, see Laura J. Gurak, *Persuasion and Privacy in Cyberspace*, Yale University Press, 1997.

[61]Chris Carr, "Internet Anti-Impeachment Drive Yields Big Pledges of Money, Time," *Washington Post*, February 7, 1999. The site is at www.moveon.org.

> seen e-mail deteriorate into a mass mailing tool for political activists. . . . [M]embers may even discount e-mail communication."[62]

According to the *Wall Street Journal*, Senator Charles Schumer's office gives first priority to old-fashioned letters. Persons sending an email to his account get back an automatic response telling them to submit a letter if they want a personal reply.[63]

The most successful advocacy groups are likely to be those that use the Internet to augment traditional lobbying methods, including personal visits to decisionmakers and use of broadcast media to reach the public. These operations can be time consuming and expensive, favoring groups that are well-funded. They also require a network of long-term and trusted relationships with policymakers, sponsors, and voters. This supports Davis's conclusion that the promise of the Internet as a forum for participatory democracy is unlikely to be realized. Davis found that existing dominant players in American politics—the media, interest groups, candidates, and policymakers—are adapting to the Internet to retain preeminence; and that the Internet is not an adequate tool for public political movement.[64]

HACKTIVISM

Hacktivism is the convergence of hacking with activism, where "hacking" is used here to refer to operations that exploit computers in ways that are unusual and often illegal, typically with the help of special software ("hacking tools"). Hacktivism includes electronic civil disobedience, which brings methods of civil disobedience to cyberspace. This section explores four types of operations: virtual sit-ins and blockades, automated email bombs, web hacks and computer break-ins, and computer viruses and worms. Because hacking incidents are often reported in the media, operations in this category can generate considerable publicity for both the activists and their causes.

---

[62]Davis, 1999, p. 135.

[63]Edward Harris, "Web Becomes a Cybertool for Political Activists," *Wall Street Journal*, August 5, 1999, B11.

[64]Davis, 1999, p. 168.

Virtual Sit-Ins and Blockades

A virtual sit-in or blockade is the cyberspace version of a physical sit-in or blockade. The goal in both cases is to call attention to the protestors and their cause by disrupting normal operations and blocking access to facilities.

With a sit-in, thousands of activists simultaneously visit a web site and attempt to generate so much traffic against the site that other users cannot reach it. A group calling itself Strano Network conducted one of the first such demonstrations as a protest against French government policies on nuclear and social issues. On December 21, 1995, they launched a one-hour Net'Strike attack against the web sites operated by various government agencies. At the appointed hour, participants from all over the world were instructed to point their browsers to the government web sites. According to reports, at least some of the sites were effectively knocked out for the period.[65]

In 1998, the Electronic Disturbance Theater (EDT) took the concept of electronic civil disobedience a step further. They organized a series of web sit-ins, first against Mexican President Zedillo's web site and later against President Clinton's White House web site, and the web sites of the Pentagon, the School of the Americas, the Frankfurt Stock Exchange, and the Mexican Stock Exchange. The purpose was to demonstrate solidarity with the Mexican Zapatistas.[66] According to EDT's Brett Stalbaum, the Pentagon was chosen because "we believe that the U.S. military trained the soldiers carrying out the human rights abuses." For a similar reason, the School of the Americas was selected.[67] The Frankfurt Stock Exchange was targeted, Stalbaum said,

> because it represented capitalism's role in globalization utilizing the techniques of genocide and ethnic cleansing, which is at the root of the Chiapas' problems. The people of Chiapas should play a key role

[65]Information provided to the author from Bruce Sterling; Winn Schwartau, *Information Warfare*, 2nd ed., Emeryville, Calif.: Thunder's Mouth Press, 1996, p. 407.

[66]For an in-depth analysis of the Zapatista's "netwar," see David Ronfeldt, John Arquilla, Graham E. Fuller, and Melissa Fuller, *The Zapatista "Social Netwar" in Mexico*, Santa Monica, Calif.: RAND, MR-994-A, 1998.

[67]Niall McKay, "Pentagon Deflects Web Assault," *Wired News*, September 10, 1998.

> in determining their own fate, instead of having it pushed on them through their forced relocation (at gunpoint), which is currently financed by western capital.[68]

To facilitate the strikes, the organizers set up special web sites with automated software. All participants had to do was visit one of the FloodNet sites. When they did, their browser would download the software (a Java Applet), which would access the target site every few seconds. In addition, the software let protesters leave a personal statement on the targeted server's error log. For example, if they pointed their browsers to a nonexistent file such as "human_rights" on the target server, the server would return and log the message "human_rights not found on this server." Stalbaum, who wrote the software, characterized FloodNet as "conceptual net art that empowers people through active/artistic expression."[69]

EDT estimated that 10,000 people from all over the world participated in the sit-in on September 9, 1998, against the sites of President Zedillo, the Pentagon, and the Frankfurt Stock Exchange, delivering 600,000 hits per minute to each. According to *Wired News'* Niall McKay, the Pentagon "apparently struck back." Stalbaum recalled the incident:

> They [Pentagon programmers] were redirecting any requests coming by way of the EDT Tactical FloodNet to a page containing an Applet called "HostileApplet." This Applet . . . instantly put all the FloodNet protestors' browsers into an infinite loop by opening a small window which tried to reload a document as fast as [possible]. . . . I had to restart my [computer] to recover control.

President Zedillo's site did not strike back on this occasion, but at a June sit-in, that site used software that caused the protestors' browsers to open window after window until their computers crashed. The Frankfurt Stock Exchange reported that it was aware of the protest but believed that the protest had not affected its services. The exchange normally gets about 6 million hits a day. Overall, EDT considered the

---

[68]Brett Stalbaum, private correspondence, July 23, 1999.

[69]Brett Stalbaum, "The Zapatista Tactical FloodNet," www.thing.net/~rdom/ecd/ZapTact.html.

attack a success. "Our interest is to help the people of Chiapas to keep receiving the international recognition that they need to keep them alive," said Stalbaum.[70]

When asked about the effects of its web strikes, EDT's Ricardo Dominguez responded,

> Digital Zapatismo is and has been one of the most politically effective uses of the Internet that we know of since January 1, 1994. It has created a distribution network of information with about 100 or more autonomous nodes of support. This has enabled the EZLN [Zapatista National Liberation Army] to speak to the world without having to pass through any dominant media filter. The Zapatistas were chosen by *Wired* as one of the 25 most important people online in 1998. . . . The Zapatista network has, also, held back a massive force of men and the latest drug war technologies from annihilating the EZLN in a few days.

Regarding FloodNet, specifically, he said the main purpose of the Electronic Disturbance Theatre's Zapatista FloodNet performance

> is to bring the situation in Chiapas to [the] foreground as often as possible. The gesture has created enough ripples with the Pentagon and the Mexican government that they have had to respond using both online and offline tactics. Thus, these virtual sit-ins have captured a large amount of traditional media attention. You would not be interviewing us if this gesture had not been effective in getting attention to the issues on a global scale.[71]

EDT also conducted web sit-ins against the White House web site to express opposition to U.S. military strikes and economic sanctions against Iraq. In the "Call for FloodNet Action for Peace in the Middle East," EDT articulated the group's philosophy.

---

[70]Niall McKay, "Pentagon Deflects Web Assault," *Wired News*, September 10, 1998; Brett Stalbaum, personal communication, January 30, 1999.

[71]Ricardo Dominguez, personal communication, February 2, 1999.

> We do not believe that only nation-states have the legitimate authority to engage in war and aggression. And we see cyberspace as a means for non-state political actors to enter present and future arenas of conflict, and to do so across international borders.[72]

Animal right's activists have also used EDT's FoodNet software to protest the treatment of animals. Over 800 protestors from more than 12 countries joined a January 1999 sit-in against web sites in Sweden.[73] And on June 18, 1999, FloodNet was one of the tools used in the anti-capitalist attack coordinated by J18.[74]

Whether web sit-ins are legal is not clear. Mark Rasch, former head of the Department of Justice's computer crime unit, said that such attacks run the risk of violating federal laws, which make it a crime to distribute a program, software code, or command with the intent to cause damage to another's site. "It may be an electronic sit-in, but people get arrested at sit-ins," he said.[75] A related question is the legality of using a denial-of-service (DoS) counteroffensive. In the case of the Pentagon, the response most likely would be considered lawful, because it is permissible for a nation to take "proportional" actions to defend against an attack that threatens its security.

The tools used to conduct web sit-ins have evolved so that protestors need not all congregate on a central site at once. Instead, they can download the software anytime or get it via email and then run it at the appointed hour. The software remains, however, fundamentally different from that used in standard DoS and distributed DoS attacks, such as those launched against Yahoo! and other e-commerce web

---

[72]See www.aec.at/infowar/NETSYMPOSIUM/ARCH-EN/msg00633.html.

[73]*Day of Net Attacking Against Vivisection,* communiqué from the Animal Liberation Front, December 31, 1998. *The First Ever Animal Liberation Electronic Civil Disobedience Virtual Sit-In on the SMI Lab Web Site in Sweden,* notice from Tactical Internet Response Network, http://freehosting.at.webjump.com/fl/floodnet-webjump/smi.html. *ECD Report—SMI Shuts Down Their Computer Network!!!,* www.aec.at/infowar/NETSYMPOSIUM/ARCH-EN/msg00678.html, January 15, 1999.

[74]Jon Ungoed-Thomas and Maeve Sheehan, "Riot Organisers Prepare to Launch Cyber War on City," *Sunday Times*, August 15, 1999.

[75]Carl Kaplan, "For Their Civil Disobedience, the 'Sit-In' Is Virtual," *Cyberlaw Journal, The New York Times on the Web,* May 1, 1998. The law is Title 18 U.S.C. section 1030 (a)(5)(A).

sites in February 2000. It does not compromise any systems or spoof source addresses, and it usually does not shut down the target. Further, thousands or tens of thousands of people must hit the target at once to have any effect, a phenomena sometimes referred to as "swarming." Swarming ensures that the action being protested is reprehensible to more than just a single person or small group.

The Electrohippies Collective, another group of hacktivists, says that its web sit-ins must substitute the deficit of speech by one group with a broad debate on policy issues, and that the event used to justify the sit-in must provide a focus for the debate. The group also espouses a philosophy of openness and accountability.[76] The group conducted a sit-in in conjunction with the WTO protests in Seattle in late 1999. In April 2000, it planned a sit-in against the genetics industry but backed out when visitors to their web site voted a lack of support. The sit-in was to be part of a broader "E-Resistance is Fertile" campaign, which also included a low-level email lobbying campaign.[77]

Individuals acting alone or in small groups have used DoS tools to disable Internet servers. During the Kosovo conflict, Belgrade hackers were credited with conducting such attacks against NATO servers. They bombarded NATO's web server with "ping" commands, which test whether a server is running and connected to the Internet. The effect of the attacks was to cause line saturation of the targeted servers.[78]

Email Bombs

It is one thing to send one or two messages to government policymakers, even on a daily basis. But it is quite another to bombard them with thousands of messages at once, distributed with the aid of automated tools. The effect can be to completely jam a recipient's incoming email box, making it impossible for legitimate email to get through. Thus, an email bomb is also a form of virtual blockade. Al-

[76]See www gn.apc.org/pmhp/ehippies.

[77]Ibid.

[78]Rebecca Allison, "Belgrade Hackers Bombard MoD Website in 'First' Internet War," *PA News,* March 31, 1999.

though email bombs are often used as a means of revenge or harassment, they have also been used to protest government policies.

In what some U.S. intelligence authorities characterized as the first known attack by terrorists against a country's computer systems, ethnic Tamil guerrillas were said to have swamped Sri Lankan embassies with thousands of electronic mail messages. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your communications."[79] An offshoot of the Liberation Tigers of Tamil Eelam, which had been fighting for an independent homeland for minority Tamils, was credited with the 1998 incident.[80]

The email bombing consisted of about 800 emails a day for about two weeks. William Church, editor for the Centre for Infrastructural Warfare Studies (CIWARS), observed that

> the Liberation Tigers of Tamil are desperate for publicity and they got exactly what they wanted . . . considering the routinely deadly attacks committed by the Tigers, if this type of activity distracts them from bombing and killing then CIWARS would like to encourage them, in the name of peace, to do more of this type of "terrorist" activity.[81]

The attack, however, was said to have had the desired effect of generating fear in the embassies.

During the Kosovo conflict, protestors on both sides email bombed government sites. According to *PA News,* NATO spokesman Jamie Shea said the NATO server had been saturated at the end of March by one individual who was sending 2,000 messages a day.[82] Fox News reported that when California resident Richard Clark heard of attacks against NATO's web site by Belgrade hackers, he retaliated by sending an email bomb to the Yugoslav government's site. Clark said that a few

---

[79]"E-Mail Attack on Sri Lanka Computers," *Computer Security Alert*, No. 183, Computer Security Institute, June 1998, p. 8.

[80]Jim Wolf, "First 'Terrorist' Cyber-Attack Reported by U.S.," Reuters, May 5, 1998.

[81]*CIWARS Intelligence Report*, May 10, 1998.

[82]Rebecca Allison, "Belgrade Hackers Bombard MoD Website in 'First' Internet War," *PA News,* March 31, 1999.

days and 500,000 emails into the siege, the site went down. He did not claim full responsibility but said he "played a part." That part did not go unrecognized. His Internet service provider, Pacific Bell, cut off his service, saying his actions violated their spamming policy.[83]

An email bombing was conducted against the San Francisco–based Internet service provider Institute for Global Communications (IGC) in 1997 for hosting the web pages of the *Euskal Herria Journal*, a controversial publication edited by a New York group supporting independence of the mountainous Basque provinces of northern Spain and southwestern France. Protestors claimed IGC "supports terrorism" because a section on the web pages contained materials on the terrorist group Fatherland and Liberty, or ETA, which was responsible for killing over 800 people during its nearly 30-year struggle for an independent Basque state. The attack against IGC began after members of the ETA assassinated a popular town councilor in northern Spain.[84]

The protestors' objective was censorship. They wanted the site pulled. To get their way, they bombarded IGC with thousands of bogus messages routed through hundreds of different mail relays. As a result, mail was tied up and undeliverable to IGC's email users, and support lines were tied up with people who couldn't get their mail. The attackers also spammed IGC staff and member accounts, clogged their web page with bogus credit card orders, and threatened to employ the same tactics against organizations using IGC services. The only way IGC could stop the attack was by blocking access from all of the relay servers.[85]

IGC pulled the site on July 18, but not before archiving a copy so that others could put up mirrors. Within days of the shutdown, mirror sites appeared on half a dozen servers on three continents. Chris Ellison, a spokesman for the Internet Freedom Campaign, an English

[83]Patrick Riley, "E-Strikes and Cyber-Sabotage: Civilian Hackers Go Online to Fight," Fox News, April 15, 1999.

[84]Rebecca Vesely, "Controversial Basque Web Site Resurfaces," *Wired News*, August 28, 1997; "Two More Basque Politicians Get ETA Death Threats," Reuters, San Sebastian, Spain, December 16, 1997.

[85]"IGC Censored by Mailbombers," letter from Maureen Mason and Scott Weikart, IGC, www.infowar.com.

group that was hosting one of the mirrors, said they believe "the Net should prove an opportunity to read about and discuss controversial ideas." A New York–based journal maintained its objective was to publish "information often ignored by the international media, and to build communication bridges for a better understanding of the conflict."[86] An article by Yves Eudes in the French newspaper *Le Monde* said the email bomb attack against the IGC site represented an "unprecedented conflict" that "has opened up a new era of censorship, imposed by direct action from anonymous hackers."[87]

About a month after IGC threw the controversial Basque *Euskal Herria Journal* off its servers, Scotland Yard's Anti-Terrorist Squad shut down Internet Freedom's U.K. web site for hosting the journal. According to a press release from Internet Freedom, the squad claimed to be acting against terrorism. Internet Freedom said it would move its news operations to its U.S. site.[88]

The case involving *Euskal Herria Journal* illustrates the power of hacktivists on the Internet. Despite IGC's desire to host the controversial site, they simply could not sustain the attack and remain in business. They could have ignored a few email messages demanding that the site be pulled, but they could not ignore an email bombing. The case also illustrates the power of the Internet as a tool for free speech. Because Internet venues for publication are rich and dispersed throughout the world, it is extremely difficult for governments and hacktivists alike to keep content completely off the Internet. It would require extensive international cooperation, and, even then, a site could operate out of a safe haven that did not sign on to international agreements.

---

[86]Rebecca Vesely, "Controversial Basque Web Site Resurfaces," *Wired News*, August 28, 1997.

[87]Yves Eudes, "The Zorros of the Net," *Le Monde*, November 16, 1997.

[88]*Anti-Terrorist Squad Orders Political Censorship of the Internet,* press release from Internet Freedom, September 1997.

Web Hacks and Computer Break-Ins

The media is filled with stories of hackers gaining access to web sites and replacing some of the content with their own. Frequently, the messages are political, as when a group of Portuguese hackers modified the sites of 40 Indonesian servers in September 1998 to display the slogan "Free East Timor" in large black letters. According to *The New York Times*, the hackers also added links to web sites describing Indonesian human rights abuses in the former Portuguese colony.[89] Then in August 1999, Jose Ramos Horta, the Sydney-based Nobel laureate who represents the East Timor independence movement outside Indonesia, warned that a global network of hackers planned to bring Indonesia to a standstill if Jakarta sabotaged the ballot on the future of East Timor. He told the *Sydney Morning Herald* that more than 100 hackers, mostly teenagers in Europe and the United States, had been preparing the plan.[90]

In June 1998, a group of international hackers calling themselves Milw0rm hacked the web site of India's Bhabha Atomic Research Center (BARC) and put up a spoofed web page showing a mushroom cloud and the text "If a nuclear war does start, you will be the first to scream . . . ." The hackers were protesting India's recent nuclear weapons tests, although they admitted they did it mostly for thrills. They said that they also downloaded several thousand pages of email and research documents, including messages between India's nuclear scientists and Israeli government officials, and had erased data on two of BARC's servers. The six hackers, whose ages range from 15 to 18, hailed from the United States, England, the Netherlands, and New Zealand.[91]

Another way in which hacktivists alter what viewers see when they go to a web site is by tampering with the Domain Name Service so that

---

[89]Amy Harmon, "'Hacktivists' of All Persuasions Take Their Struggle to the Web," *The New York Times*, October 31, 1999.

[90]Lindsay Murdoch, "Computer Chaos Threat to Jakarta," *Sydney Morning Herald*, August 18, 1999, p. 9.

[91]James Glave, "Crackers: We Stole Nuke Data," *Wired News*, June 3, 1998; Janelle Carter, "Hackers Hit U.S. Military Computers," *Associated Press*, Washington, D.C., June 6, 1998; "Hackers Now Setting Their Sights on Pakistan," *Newsbytes*, June 5, 1998.

the site's domain name resolves to the Internet protocol address of some other site. When users point their browsers to the target site, they are redirected to the alternative site.

In what might have been one of the largest mass homepage takeovers, the antinuclear Milw0rm hackers were joined by Ashtray Lumberjacks hackers in an attack that affected more than 300 web sites in July 1998. According to reports, the hackers broke into the British Internet service provider (ISP) EasySpace, which hosted the sites. They altered the ISP's database so that users attempting to access the sites were redirected to a Milw0rm site, where they were greeted with a message protesting the nuclear arms race. The message concluded with ". . . use your power to keep the world in a state of PEACE and put a stop to this nuclear bullshit."[92]

Several web sites were hacked during the Kosovo conflict. According to Fox News, the *Boston Globe* reported that an American hacking group called Team Spl0it broke into government web sites and posted statements such as "Tell your governments to stop the war." Fox also said that the Kosovo Hackers Group, a coalition of European and Albanian hackers, had replaced at least five sites with black and red "Free Kosovo" banners.[93] The Bosnian Serb news agency SRNA reported that the Serb Black Hand hackers group had deleted data on a U.S. Navy computer, according to the Belgrade newspaper *Blic*. Members of the Black Hand group and Serbian Angel planned daily actions that would block and disrupt military computers operated by NATO countries, *Blic* wrote.[94] Black Hand had earlier claimed responsibility for crashing a Kosovo Albanian web site. "We shall continue to remove [ethnic] Albanian lies from the Internet," a member of the group told *Blic*.[95]

---

[92]Jim Hu, "Political Hackers Hit 300 Sites," *CNET*, July 6, 1998. The Milw0rm page is shown at www.antionline.com.

[93]Patrick Riley, "E-Strikes and Cyber-Sabotage: Civilian Hackers Go Online to Fight," Fox News, April 15, 1999.

[94]"Serb Hackers Reportedly Disrupt U.S. Military Computers," SRNA (Bosnian Serb news agency), March 28, 1999.

[95]"Serb Hackers Declare Computer War," *Associated Press*, October 22, 1998.

In the wake of NATO's accidental bombing of China's Belgrade embassy in May 1999, angry Chinese allegedly hacked several U.S. government sites. *Newsbytes* reported that the slogan "down with barbarians" was placed in Chinese on the home page of the U.S. Embassy in Beijing, while the Department of Interior web site showed images of the three journalists killed during the bombing, crowds protesting the attack in Beijing, and a fluttering Chinese flag.[96] According to the *Washington Post,* Interior spokesman Tim Ahearn said their computer experts had traced their hacker back to China. The newspaper also reported that the Department of Energy's home page read:

> Protest U.S.A.'s Nazi action! Protest NATO's brutal action! We are Chinese hackers who take no cares about politics. But we can not stand by seeing our Chinese reporters been killed which you might have know. Whatever the purpose is, NATO led by U.S.A. must take absolute responsibility. You have owed Chinese people a bloody debt which you must pay for. We won't stop attacking until the war stops![97]

NATO did not, of course, declare an end to the war because of the hacking. The effect on foreign policy decisions, if any at all, likely paled in comparison to the bombing itself. Following the accident, China suspended high-level military contacts with the United States.[98]

Acting in the name of democracy and human rights, hackers have targeted Chinese government computers. One group, called the Hong Kong Blondes, allegedly infiltrated police and security networks in an effort to monitor China's intelligence activities and warn political targets of imminent arrests.[99] According to OXblood Ruffin, "foreign minister" of the Cult of the Dead Cow, the Blondes are an under-

---

[96]Martyn Williams, "Federal Web Sites Under Attack After Embassy Bombing," *Newsbytes*, May 10, 1999.

[97]Stephen Barr, "Anti-NATO Hackers Sabotage 3 Web Sites," *Washington Post*, May 12, 1999.

[98]"China Suspends Contacts with U.S.," *Associated Press*, Beijing, May 9, 1999.

[99]Niall McKay, "China: The Great Firewall," *Wired News*, December 1, 1998. See also Sarah Elton, "Hacking in the Name of Democracy in China," *The Toronto Star*, July 4, 1999.

ground group of Chinese dissidents who aim to destabilize the Chinese government. They have threatened to attack both Chinese state-owned organizations and Western companies investing in the country.[100]

The *Los Angeles Times* reported that a California computer science student who calls himself Bronc Buster and his partner Zyklon cracked the Chinese network, defacing a government-run web site on human rights and interfering with censorship. The hackers said they came across about 20 firewall servers blocking everything from Playboy.com to Parents.com, and that they disabled the blocking on five of the servers. He said they did not destroy any data, but only moved files.[101]

Bronc Buster belonged to a group of 24 hackers known as the Legion of the Underground (LoU). In a press conference on Internet Relay Chat (IRC) in late December 1998, an LoU member declared cyberwar on the information infrastructures of China and Iraq. He cited civil rights abuses and said LoU called for the complete destruction of all computer systems in China and Iraq.[102]

The declaration of cyberwar prompted a coalition of other hacking groups to lash out against the campaign in early 1999. A letter co-signed by *2600*, the Chaos Computer Club, the Cult of the Dead Cow (CDC), !Hispahak, L0pht Heavy Industries, Phrack, Pulhas, and several members of the Dutch hacking community denounced the cyberwar, saying "Declaring 'war' against a country is the most irresponsible thing a hacker group could do. This has nothing to do with hacktivism or hacker ethics and is nothing a hacker could be proud of." Reid Fleming of the CDC said "One cannot legitimately hope to improve a nation's free access to information by working to disable its data networks."[103]

---

[100]Neil Taylor, "CDC Says Hackers Are Threat," *IT Daily*, August 26, 1999.

[101]Maggie Farley, "Dissidents Hack Holes in China's New Wall," *Los Angeles Times*, January 4, 1999.

[102]See www.hacknews.com/archive.html?122998.html.

[103]Letter of January 7, 1999.

By the time the letter went out on January 7, LoU had already issued a statement that day saying that the declaration of war on IRC did not represent the position of the group.

> The LoU does not support the damaging of other nations' computers, networks or systems in any way, nor will the LoU use their skills, abilities or connections to take any actions against the systems, networks or computers in China or Iraq which may damage or hinder in any way their operations.[104]

Bronc Buster said the IRC declaration was issued by a member before he left and never came back.[105]

In August 1999, a cyberwar erupted between hackers in China and Taiwan. Chinese hackers defaced several Taiwanese and government web sites with pro-China messages saying Taiwan was and would always be an inseparable part of China. "Only one China exists and only one China is needed," read a message posted on the web site of Taiwan's highest watchdog agency.[106] Taiwanese hackers retaliated and planted a red and blue Taiwanese national flag and an anti-Communist slogan—"Reconquer, Reconquer, Reconquer the Mainland"—on a Chinese high-tech Internet site. The cyberwar followed an angry exchange by Chinese and Taiwanese in response to Taiwan's President Lee Teng-hui's statement that China must deal with Taiwan on a "state-to-state" basis.[107]

One of the consequences of hacking is that victims might falsely attribute an assault to a foreign government rather than the small group of activists that actually conducted it. This could strain foreign relations or lead to a more serious conflict.

The Chinese government has been accused of attacking a U.S. web site devoted to the Falun Gong meditation sect, which has been outlawed by Chinese authorities. Bob McWee, a sect practitioner in Mid-

---

[104]Statement of January 7, 1999.

[105]James Glave, "Confusion Over 'Cyberwar,'" *Wired News*, January 12, 1999.

[106]"Pro-China Hacker Attacks Taiwan Government Web Sites," *Reuters*, August 9, 1999.

[107]Annie Huang, "Hackers' War Erupts Between Taiwan, China," *Associated Press*, Taipei, Taiwan, August 9, 1999.

dleton, Maryland, said his site had been under a persistent electronic assault in July 1999. In addition to a continuous denial-of-service attack, someone had tried breaking into his server. He said he was able to trace the penetration attempt to the Internet Monitoring Bureau of China's Public Security Ministry.[108] According to the *South China Morning Post,* additional attacks took place in April 2000 against at least five Falun Gong sites: three in the United States and two in Canada. The group's main web site, www.Falundafa.org, had received an anonymous tip-off warning that the police software security bureau had offered to pay a computer company money to hack into the sites.[109] If these attack did indeed originate with the Chinese police, this would have major foreign policy implications. It would suggest that the Chinese government views web sites operating on foreign soil as legitimate targets of aggression when those sites support activities prohibited on home soil.

Web hacks and computer break-ins are extremely common, and targets include commercial and educational computers as well as government ones. The results of *Information Security* magazine's "1999 Industry Survey" showed that the number of companies experiencing penetrations jumped from 12 percent in 1997 to 23 percent in 1998 (almost double).[110] About 26 percent of respondents to the "ERRI/EmergencyNet News Local/County/State Computer 'Hacking' Survey" said they thought they had been the victims of an unauthorized intrusion or attack on their computer systems.[111] And 30 percent of respondents to the "1999 CSI/FBI Computer Crime and Security Survey" reported intrusions from outsiders.[112] Most of the attacks, however, were probably not motivated by politics (hacktivism), but rather by thrills, curiosity, ego, revenge, or financial gain. In the area of web

---

[108]"Beijing Tries to Hack U.S. Web Sites," *Associated Press*, July 30, 1999. McWee's web site is at www.falunusa.net.

[109]"Web Sites of Falun Gong Hit," *South China Morning Post*, April 14, 2000.

[110]See www.infosecuritymag.com/articles/1999/julycover.shtml/.

[111]Clark Staten, private email, July 19, 1999.

[112]Richard Power, "1999 CSI/FBI Computer Crime and Security Survey," *Computer Security Issues & Trends*, Vol. V, No. 1, Winter 1999.

hacks alone, Attrition.org recorded more than 1,400 cases of vandalism by July 1999 for the year.[113]

Computer Viruses and Worms

Hacktivists have used computer viruses and worms to spread protest message and damage target computer systems. Both are forms of malicious code that infect computers and propagate over computer networks. The difference is that a worm is an autonomous piece of software that spreads on its own, whereas a virus attaches itself to other files and code segments and spreads through those elements, usually in response to actions taken by users (e.g., opening an email attachment). The boundary between viruses and worms, however, is blurry and not important to the discussion here.

The first protest to use a worm occurred about a decade ago, when antinuclear hackers released a worm into the U.S. National Aeronautics and Space Administration's SPAN network. On October 16, 1989, scientists logging into computers at NASA's Goddard Space Flight Center in Greenbelt, Maryland, were greeted with a banner from the WANK worm (see Figure 8.1).

At the time of the attack, antinuclear protestors were trying to stop the launch of the shuttle that carried the Galileo probe on its initial leg to Jupiter. Galileo's 32,500-pound booster system was fueled with radioactive plutonium. John McMahon, protocol manager with NASA's SPAN office, estimated that the worm cost them up to half a million dollars of wasted time and resources. It did not have its intended effect of stopping the launch. The source of the attack was never identified, but some evidence suggested that it might have come from hackers in Australia.[114]

Computer viruses have been used to propagate political messages and, in some cases, cause serious damage. In February 1999, the *London Sunday Telegraph* reported that an Israeli teen had become a national hero after he claimed to have wiped out an Iraqi government

[113]Ted Bridis, "Hackers Become an Increasing Threat," *Associated Press*, July 7, 1999.

[114]Ibid.

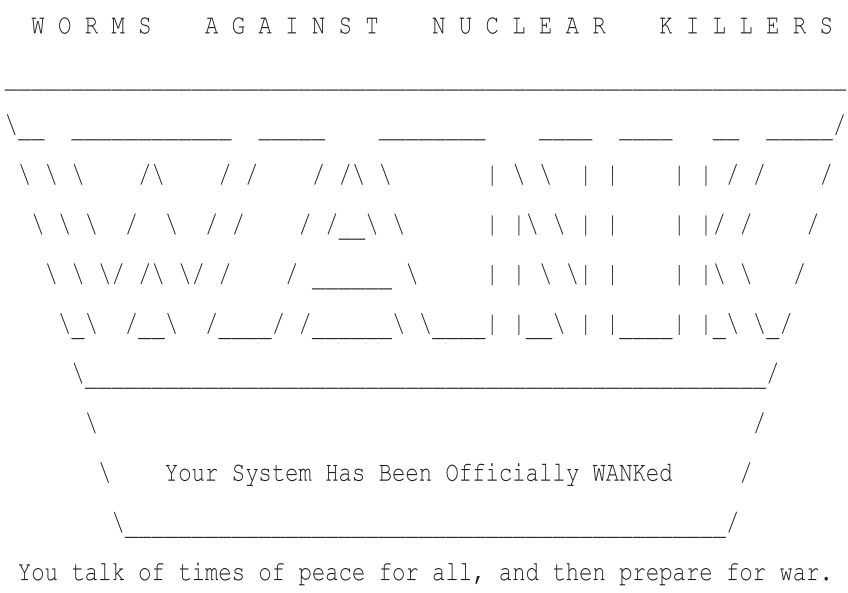

Figure 8.1—WANK Worm

web site. "It contained lies about the United States, Britain and Israel, and many horrible statements against Jews," 14-year-old Nir Zigdon said.[115] "I figured that if Israel is afraid of assassinating Saddam Hussein, at least I can try to destroy his site. With the help of some special software I tracked down the site's server to one of the Gulf states."[116] The Tel Aviv hacktivist then sent a computer virus in an email attachment to the site. "In the e-mail message, I claimed I was a Palestinian admirer of Saddam who had produced a virus capable of wiping out Israeli websites," Zigdon said. "That persuaded them to open the message and click on the designated file. Within hours the site had

[115]Tom Gross, "Israeli Claims to Have Hacked Saddam Off the Net," *London Sunday Telegraph*, February 7, 1999.

[116]Ibid.

been destroyed. Shortly afterwards I received an e-mail from the site manager, Fayiz, that told me to 'go to hell.'"[117]

During the Kosovo conflict, businesses, public organizations, and academic institutes received virus-laden emails from a range of Eastern European countries, according to mi2g, a London-based Internet software company. "The contents of the messages are normally highly politicised attacks on NATO's unfair aggression and defending Serbian rights using poor English language and propaganda cartoons," the press release said. It went on to say "The damage to the addressee is usually incorporated in several viruses contained within an attachment, which may be plain language or anti-NATO cartoon."[118] In an earlier press release, mi2g warned that "The real threat of cyber warfare from Serbian hackers is to the economic infrastructure of NATO countries and not to their better prepared military command and control network."[119]

It is extremely difficult, perhaps impossible, for an organization to prevent all viruses, because users unwittingly open email attachments with viruses and spread documents with viruses to colleagues. Although antiviral tools can detect and eradicate viruses, the tools must be kept up-to-date across the enterprise, which may have tens of thousands of computers, and they must be installed and used properly. While viruses bearing political messages may not seem to pose a serious problem, an organization hit by one may have to shut down services to eradicate it from its network.

Viruses, especially those carrying destructive payloads, are a potentially potent tool in the hands of cyberterrorists. Other tools of hacktivism, including computer network attacks, could likewise be put to highly destructive ends. This is the topic discussed next.

---

[117]Ibid.

[118]*mi2g Cyber Warfare Advisory Number 2*, April 17, 1999, M2 Communications, April 19, 1999.

[119]M2 Communications, April 8, 1999.

CYBERTERRORISM

In the 1980s, Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, coined the term "cyberterrorism" to refer to the convergence of cyberspace and terrorism.[120] Mark Pollitt, special agent for the FBI, offers a working definition:

> Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by subnational groups or clandestine agents.[121]

Politically motivated attacks that cause serious harm, such as severe economic hardship or sustained loss of power or water, might also be characterized as cyberterrorism.

The Threat

As previously discussed, terrorist groups are using the Internet extensively to spread their message and to communicate and coordinate action. However, there have been few, if any, computer network attacks that meet the criteria for cyberterrorism. The 1998 email bombing by the Internet Black Tigers against the Sri Lankan embassies was perhaps the closest thing to cyberterrorism that has occurred so far, but the damage cause by the flood of email, for example, pales in comparison to the deaths of 240 people from the physical bombings of the U.S. embassies in Nairobi and Dar es Salaam in August of that year.

Is cyberterrorism the way of the future? For a terrorist, it would have some advantages over physical methods. It could be conducted remotely and anonymously, it would be cheap, and it would not require the handling of explosives or a suicide mission. It would likely garner extensive media coverage, since journalists and the public alike are fascinated by practically any kind of computer attack. One highly ac-

---

[120]Barry Collin, "The Future of Cyberterrorism," *Crime and Justice International*, March 1997, pp. 15–18.

[121]Mark M. Pollitt, "Cyberterrorism: Fact or Fancy?" *Proceedings of the 20th National Information Systems Security Conference*, October 1997, pp. 285–289.

claimed study of the risks of computer systems began with a paragraph that concludes "Tomorrow's terrorist may be able to do more with a keyboard than with a bomb."[122] However, there are also drawbacks to terrorists using cyberweapons over physical ones. Because systems are complex, it may be harder to control an attack and achieve a desired level of damage. Unless people are injured, there is also less drama and emotional appeal. Further, terrorists may be disinclined to try new methods unless they see their old ones as inadequate.[123]

In a 1997 paper, Collin describes several possible scenarios for cyberterrorism. In one, a cyberterrorist hacks into the processing control system of a cereal manufacturer and changes the levels of iron supplement. A nation of children get sick and die. In another, a cyberterrorist attacks the next generation of air traffic control systems. Two large civilian aircraft collide. In a third, a cyberterrorist disrupts banks, international financial transactions, and stock exchanges. Economic systems grind to a halt, the public loses confidence, and destabilization is achieved.[124]

Analyzing the plausibility of Collin's hypothetical attacks, Pollitt concludes that there is sufficient human involvement in the control processes used today that cyberterrorism does not *at present* pose a significant risk in the classical sense. In the cereal contamination scenario, for example, he argues that the quantity of iron (or any other nutritious substance) that would be required to become toxic is so large that assembly line workers would notice. They would run out of iron on the assembly line and the product would taste different and not good. In the air traffic control scenario, humans in the loop would

[122]National Research Council, *Computers at Risk*, Washington, D.C.: National Academy Press, 1991.

[123]Kevin Soo Hoo, Seymour Goodman, and Lawrence Greenberg, "Information Technology and the Terrorist Threat," *Survival*, Vol. 39, No. 3, Autumn 1997, pp. 135–155. See also unpublished RAND research by Martin Libicki, James Mulvenon, and Zalmay Khalilzad, on information warfare, which examines these issues in some detail.

[124]Barry Collin, "The Future of Cyberterrorism," *Crime and Justice International*, March 1997, pp. 15–18. In terms of scenario building, RAND's longstanding "The Day After . . . in Cyberspace" research effort has done much pioneering work. See, for example, Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War,* Santa Monica, Calif.: RAND, 1996.

notice the problems and take corrective action. Pilots, he says, are trained to be aware of the situation, to catch errors made by air traffic controllers, and to operate in the absence of any air traffic control at all.[125] Pollitt does not imply by his analysis that computers are safe and free from vulnerability. To the contrary, his argument is that despite these vulnerabilities, because humans are in the loop, a cyberattack is unlikely to have such devastating consequences. He concludes:

> As we build more and more technology into our civilization, we must ensure that there is sufficient human oversight and intervention to safeguard those whom technology serves.

There is little concrete evidence of terrorists preparing to use the Internet as a venue for inflicting grave harm. However, in February 1998, Clark Staten, executive director of the Emergency Response & Research Institute in Chicago, testified that it was believed that

> members of some Islamic extremist organizations have been attempting to develop a "hacker network" to support their computer activities and even engage in offensive information warfare attacks in the future.[126]

And in November, the *Detroit News* reported that Khalid Ibrahim, who claimed to be a member of the militant Indian separatist group Harkat-ul-Ansar, had tried to buy military software from hackers who had stolen it from U.S. Department of Defense computers they had penetrated. Harkat-ul-Ansar, one of the 30 terrorist organizations on the State Department list, declared war on the United States following the August cruise-missile attack on a suspected terrorist training camp in Afghanistan run by Osama bin Laden, which allegedly killed nine of their members. The attempted purchase was discovered when an 18-year-old hacker calling himself Chameleon attempted to cash a $1,000 check from Ibrahim. Chameleon said he did not have the soft-

---

[125]Mark M. Pollitt, "Cyberterrorism: Fact or Fancy?" *Proceedings of the 20th National Information Systems Security Conference*, October 1997, pp. 285–289.

[126]Clark L. Staten, testimony before the Subcommittee on Technology, Terrorism and Government Information, U.S. Senate Judiciary Committee, February 24, 1998.

ware and did not give it to Ibrahim, but Ibrahim may have obtained it or other sensitive information from one of the many other hackers he approached.[127]

Given that there are no instances of cyberterrorism, it is not possible to assess the effects of such acts. It is equally difficult to assess potential damage, in part because it is hard to predict how a major computer network attack, inflicted for the purpose of affecting national or international policy, would unfold. So far, damage from attacks committed for reasons other than terrorism—for example, to seek revenge against a former employer—have generally been confined to immediate targets. No lives have been lost.

Cyberdefense

The main effect of cyberthreats on foreign and domestic policy relates to defending against such acts, particularly attacks against critical infrastructures. At the international level, several countries, including the United States, have been addressing such issues as mutual legal assistance treaties, extradition, the sharing of intelligence, and the need for uniform computer crime laws so that cybercriminals can be successfully investigated and prosecuted even when their crimes cross international borders, as they so often do. This effort is not focused on either cyberterrorism or hacktivism, but rather addresses an array of actions that includes all forms of hacking and computer network attacks, computer and telecommunications fraud, child pornography on the Net, and electronic piracy (software, music, etc.). It also covers state-sponsored cyberwarfare operations that use hacking and computer network attacks as a military weapon.

At the initiative of the Russian Federation, the U.N. General Assembly adopted a resolution related to cybercrime, cyberterrorism, and cyberwarfare in December 1998. Resolution 53/70, Developments in the Field of Information and Telecommunications in the Context of International Security, invites member states to inform the secretary-general of their views and assessments on (a) the issues of information security, (b) definition of basic notions related to information

[127]"'Dangerous' Militant Stalks Internet," *Detroit News*, November 9, 1998.

security, and (c) advisability of developing international principles that would enhance global information and telecommunications systems and help combat information terrorism and criminality.[128]

The United States has taken several steps to better protect its critical infrastructures. In July 1996, President Clinton announced the formation of the President's Commission on Critical Infrastructure Protection (PCCIP) to study the critical infrastructures that constitute the life support systems of the nation, determine their vulnerabilities to a wide range of threats, and propose a strategy for protecting them in the future. Eight infrastructures were identified: telecommunications, banking and finance, electrical power, oil and gas distribution and storage, water supply, transportation, emergency services, and government services. In its final report, issued in October 1997, the commission reported that the threats to critical infrastructures were real and that, through mutual dependence and interconnectedness, they could be vulnerable in new ways. "Intentional exploitation of these new vulnerabilities could have severe consequences for our economy, security, and way of life."[129]

The PCCIP noted that cyberthreats have changed the landscape:

> In the past we have been protected from hostile attacks on the infrastructures by broad oceans and friendly neighbors. Today, the evolution of cyberthreats has changed the situation dramatically. In cyberspace, national borders are no longer relevant. Electrons don't stop to show passports. Potentially serious cyberattacks can be conceived and planned without detectable logistic preparation. They can be invisibly reconnoitered, clandestinely rehearsed, and then mounted in a matter of minutes or even seconds without revealing the identity and location of the attacker.[130]

---

[128]G.A. Res. 53/70, U.N. GAOR, 53rd Sess., U.N. Doc. A/RES/53/70.

[129]*Critical Foundations: Protecting America's Infrastructures,* The Report of the President's Commission on Critical Infrastructure Protection, October 1997, report summary, www.pccip.gov.

[130]Ibid.

In assessing the threat from both physical and cyberattacks, the PCCIP concluded that

> Physical means to exploit physical vulnerabilities probably remain the most worrisome threat to our infrastructures *today*. But almost every group we met voiced concerns about the new cyber vulnerabilities and threats. They emphasized the importance of developing approaches to protecting our infrastructures against cyberthreats *before* they materialize and produce major system damage.[131]

The recommendations of the PCCIP led to Presidential Decision Directive 63, which established the National Infrastructure Protection Center (NIPC), the Critical Infrastructure Assurance Office (CIAO), the National Infrastructure Assurance Council (NIAC), and private-sector Information Sharing and Assessment Centers (ISACs).[132] The Department of Defense also established a joint task force—Computer Network Defense. The National Security Council's "National Plan for Information System Protection," issued in January 2001, provides an update on the most recent developments in this area.

That critical systems are potentially vulnerable to cyberattacks was underscored by a June 1997 exercise, code-named Eligible Receiver, conducted by the National Security Agency (NSA). The objective was to determine the vulnerability of U.S. military computers and some civilian infrastructures to a cyberattack. According to reports, two-man teams targeted specific pieces of the military infrastructure, including the U.S. Pacific Command in Hawaii, which oversees 100,000 troops in Asia. One person played the role of the attacker, while another observed the activity to ensure that it was conducted as scripted. Using only readily available hacking tools that could easily be obtained from the Internet, the NSA hackers successfully gained privileged access on numerous systems. They concluded that the military infrastructure could be disrupted and possible troop deployments hindered. The exercise also included written scenarios against

---

[131]Ibid.

[132]*Protecting America's Critical Infrastructures: PDD 63,* The White House, May 22, 1998. See also the White Paper *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63,* May 22, 1998, and "National Infrastructure Assurance Council," Executive Order, The White House, July 14, 1999.

the power grid and emergency 911 system, with resulting service disruptions. For the latter, they postulated that by sending sufficient emails to Internet users telling them the 911 system had a problem, enough curious people would phone 911 at once to overload the system. No actual attacks were made against any civilian infrastructures.[133]

The vulnerability of commercial systems to cyberattacks is repeatedly demonstrated by survey results such as those mentioned earlier. There is no evidence that nongovernment systems are any more or less vulnerable than government ones, or that the security posture of either group, as a whole, is generally improving—despite the availability and use of a growing supply of information security tools.

CONCLUSIONS

The Internet is clearly changing the landscape of political discourse and advocacy. It offers new and inexpensive methods for collecting and publishing information, for communicating and coordinating action on a global scale, and for reaching out to policymakers. It supports both open and private communication. Advocacy groups and individuals worldwide are taking advantage of these features in their attempts to influence foreign policy.

Several case studies show that when the Internet is used in normal, nondisruptive ways, it can be an effective tool for activism, especially when it is combined with other media, including broadcast and print media, and face-to-face meetings with policymakers. As a technology for empowerment, the Net benefits individuals and small groups with few resources as well as organizations that are large or well-funded. It facilitates such activities as educating the public and media, raising money, forming coalitions across geographical boundaries, distributing petitions and action alerts, and planning and coordinating events on a regional or international level. It allows activists in politically repressive states to evade government censors and monitors.

---

[133] *CIWARS Intelligence Report*, Centre for Infrastructural Warfare Studies, June 21, 1998; "Pentagon Computer Systems Hacked," *Info Security News*, June 1998; Douglas Pasternak and Bruce B. Auster, "Terrorism at the Touch of a Keyboard," *U.S. News & World Report*, July 13, 1998, p. 37.

In the area of hacktivism, which involves the use of hacking tools and techniques of a disruptive nature, the Internet will serve mainly to draw attention to a cause, since such incidents are regularly reported by news media. Whether that attention has the desired effect of changing policy decisions related to the issue at hand is much less certain. Hacktivists may feel a sense of empowerment, because they can control government computers and get media attention, but that does not mean they will succeed in changing policy. So far, anecdotal evidence suggests that for the majority of cases, they will not.

With regard to cyberterrorism, that is, the use of hacking tools and techniques to inflict grave harm such as loss of life, few conclusions can be drawn about its potential effect on foreign policy, because there have been no reported incidents that meet the criteria. What can be said is that the threat of cyberterrorism, combined with hacking threats in general, is influencing policy decisions related to cyberdefense at both a national and international level. If we look at terrorism in general for insights into the potential effects of cyberterrorism, we find that the effect of terrorism on the foreign policy issues at hand is similarly difficult to assess, but here again, the threat of terrorism, particularly chemical, biological, and nuclear terrorism, is having a significant effect on national defense policy.