Terror and Its Networks: Disappearing Trails in Cyberspace (DRAFT)

Recommended Citation

Vinay Lal, "Terror and Its Networks: Disappearing Trails in Cyberspace (DRAFT)", Global Problem Solving, April 25, 2002, https://nautilus.org/global-problem-solving/terror-and-its-net-orks-disappearing-trails-in-cyberspace-draft/

By Vinay Lal
Associate Professor, Department of History
University of California, Los Angeles (UCLA)

I: Prologue: Cyberspace and the Politics of Networks

Much has been made in the American and international press of the "al-Qaeda network", an organization said to have been responsible for the attacks on the World Trade Center and the Pentagon. The word "network" brings to mind a number of associations, and there is the clear imputation of a rather far-flung and rather sinister organization whose members, while appearing to have acted with perhaps some degree of independence and autonomy, have similar ideological sentiments. There was even some speculation, in the immediate aftermath of September 11th, that the attacks had been carried out by an al-Qaeda cell without the knowledge of Osama bin Laden, much in the way in which revolutionary cells in colonial Algeria generally operated, during the movement of resistance to French rule, independent of other cells. However, the precursors to the al-Qaeda network, as that term is deployed in the mainstream American media, appear to be "the terrorist networks" that allegedly operated at the behest of the former Soviet Union.[1] When Reagan described the then-Soviet Union as an "evil empire", one can reasonably assume that he had in mind more than communism: his political rhetoric fixated on the Soviet Union's sponsorship of terror, and administration officials spoken often of a widespread terrorist network that was calculated to foment revolution in Third World countries and destabilize the industrialized nations of the North and their free market allies in the South. Something at once "sinister" – reeking of conspiracy, calling to mind the shadowy world of espionage, political assassination, the cult of violence, and ruthless self-aggrandizement – and ominously grand in scope – men of steely determination with indeterminate sources of funding backed by the power of "rogue" states and widely dispersed around the world – was called to mind in the evocation of "terror networks"

There is, evidently, a more common usage associated with the word "network", a usage which points to the more alarmist and far-reaching possibilities that are sought to be conjured in the evocation of terror networks. In the American idiom, "networks" have preeminently meant "media networks", and it is CNN, CBS, and other principal media outlets that are being evoked in this usage. No one, needless to say, has ever suggested that these “media networks” and “terror networks” are quite the same thing; indeed, it is no exaggeration to suggest that media networks in the United States have entirely lent their services to the work of counterterrorism. When, for example, Secretary of Defense Donald Rumsfeld suggested that the bin Laden videotapes being broadcast by al Jazeera television were most likely conveying coded messages to bin Laden’s followers and other al-Qaeda terrorists, and therefore ought not to be broadcast by American networks, both patriotism and the media’s self-appointed role as a functionary of counterterrorism demanded immediate compliance with the sentiments of the Pentagon. Media networks have done more than any government agency to promote an impoverished conception of terrorism as political acts of desperate individuals who carry out their political agendas without any regard for civilians or any consideration for the sanctity and dignity of human life.

Yet, from the standpoint of a dissenting and radical politics, American media networks are something like terror networks: they point to the inextricable connections between mass media, the corporate domination of American political and public life, and the corridors of political power. The synchronization of the worlds of politics, business, and media such that they together embody the purposeful and orchestrated exercise of power constitutes its own form of terror, all the more frightening and totalizing for appearing to work in the name of democracy. The shadowy world of “terror networks” would certainly seem to mimic the “media networks” of American society, with their expansive reach, control over large segments of civil society, political influence, ample funding, accessibility to men with power, and even the relatively easy transgression of borders and boundaries. The exponents of globalization may not have been thinking of terrorism when they were championing unregulated entry of goods, ideas, and American-style youth culture into the remotest parts of the world, but it is precisely this disdain for borders which seems to characterize the political aspirations and movements of members of the al-Qaeda network. In retrospect, whatever the political realities of the “al-Qaeda network” or of its ideologues whose political life is commonly thought to be defined by the twin towers of a radical commitment to Islam and an equally radical hatred for the political fabric of American life, al-Qaeda will be viewed as one of the earliest and clearly unanticipated manifestations of globalization in practice.

Howsoever one might be inclined to view American media networks, one cannot but speculate whether the invocation of the “al-Qaeda network” was not also meant to call to mind the intricate web of networks created in cyberspace. As details of the simultaneous hijacking of four aircraft on the morning of September 11th began to emerge, a number of questions arose about the links between the hijackers, their modes of communication, and the wider networks to which they might have been attached. The initial supposition was that not all the hijackers were aware that their mission would end with their own deaths, and it has been argued that each of the four teams of hijackers, while equally bound to the authority of some commanding figure, might also have been unaware of the role or even presence of the other three teams in the macabre symphony of death planned for September 11th.[2] Thus, while disassociated from each other, the teams of hijackers might have been networked to a common source and perhaps to wider network neighborhoods. One scholar, Valdis Krebs, who has attempted to establish the links between the hijackers notes that they “appeared to have come from a network that had formed while they were completing terrorist training in Afghanistan.”[3]

Some appeared to have known each other from childhood; others were mates at university; a few shared lodgings; some seem to have been related by kinship ties; and all, apparently, were graduates of the bin Laden terrorist training school. Applying social network analysis to terrorist activity, Kerbs concedes that several difficulties are encountered in such analysis: the links are not always transparent, and can lend themselves to conflicting interpretations; moreover, “these networks are not static, they are always changing.”[4] Kerbs notes that even hijackers from the same team appear to have been at considerable distance from each other, and that the points of intercourse between the teams were largely allowed to lapse once the master plan had been hatched in order to prevent detection. Much as Chicago serves as the hub for United and Detroit does so for Northwest, Mohamed Atta appears to have been the nodal point for the terrorist activity that saw its culmination on September 11th.[5]

While social network analysis is not without its insights, a more obvious set of questions about the al-Qaeda network remains: how far did members of the al-Qaeda deploy the internet in furtherance of their designs? Can one reasonably speak of an online trail that the terrorists might have laid, or is it the precise characteristic of the internet that it facilitates terrorist activity as much as it assists those functionaries of the state and international agencies who are charged with the tasks of surveillance, interception of criminal activity, and the maintenance of “law and order” on the information superhighways?Can one, moreover, go so far as to aver that terrorist activity and cyberspace activism mirror each other, insofar as both rely upon some notion of nomadic politics, reject the idea that constitutional politics furnishes the appropriate parameters for political activity, and seek to bypass the “media networks”, as that term is generally understood, for the transmission of information? In seeking to understand the particular nexus, if any, between terrorist activity and cyberspace, is one compelled to revisit the arguments that have generally been advanced about the information superhighway as a space of either authoritarianism or democracy?[6] Is it any longer meaningful to speak of the use or abuse of the information superhighway and the internet, in the same way in which some people are still habituated to speaking of the use or abuse of science, and does this mean that the internet has been assimilated within the dominant frameworks of knowledge as merely another “form” of media which waits for “content” to be fulfilled?

II: Terrorism and Its Trails in Cyberspace

More than six months after the events of September 11th, the internet appears to be revealing few secrets about the al-Qaeda network or Osama bin Laden.Even the mere and frequently voiced assertion that bin Laden “uses the internet to communicate to his followers and to issue orders” remains largely unverified,[7] and a recent article published in the *New York Times* admits that simple measures to evade detection, such as moving from one internet café to another, or using websites – rather than email, which is more easily intercepted – to communicate messages appear to have thwarted intelligence agencies in their attempt to monitor suspected terrorist groups.[8] Some of the principal characteristics of the internet – its easy accessibility, low cost, and relative anonymity – make it attractive to terrorists.[9] Similarly, it is widely rumored that bin Laden and other terrorists use encryption programs – which scramble data or messages into existing pictures that can only be unlocked with a code known only to the recipient – to plan terrorist activities on the internet and relay messages to followers, and there has been a report that two computers recovered from Kabul and apparently in use at an al-Qaeda office contained files protected by encryption.[10] This, in itself, scarcely constitutes a revelation: the Anti-Defamation League, among other institutions, warned in its online “Terrorism Update” in Winter 1998 that terrorist groups, as well as other extremist political movements, were increasingly turning to encryption in an attempt to remain ahead of intelligence agencies.[11] Kim Schmitz, a German who runs an investment company and founded the Young Intelligent Hackers Against Terrorism (YIHAT) on September 15th, claims to have conducted a cyberwar against “web vandals sympathetic to Osama bin Laden” and reported uncovering $360 million in assets belonging to terrorists “by hacking into banks”, but no government agency has indicated a willingness to corroborate this claim. Less than a month later, YIHAT, claiming the vandalization of its web site, declared that it was going “underground.”[12]

The use of cyberspace by terrorists is generally understood to have two dimensions, both of which have attracted considerable critical scrutiny.[13] First, an argument has been advanced that terrorist organizations, taking their cue from some guerrilla and liberation movements, are increasingly resorting to the internet to disseminate their views to a wider public, and that they have come to the realization that establishing their presence in cyberspace is nearly just as critical to their long-term success as any military triumph or act of sabotage. The web has become their most critical resource for the solicitation of funds, and according to one source, the Lashkar-e-Taiba, a mujahideen group which is fighting the Indian army in Kashmir, has become the envy of other like-minded groups on account of its ability to attract donors through its extensive web site with its versions in Urdu, English, and Arabic.[14] As has been noticed by several other commentators, HAMAS [Islamic Resistance Movement], Hizbollah [The Party of God], the Tamil Tigers of Eelam,[15] the Mojahedin-e Khalq [of Iran], the Hezb-e-Islami, the Revolutionary Armed Forces of Colombia (FARC),[16] and the Algerian Armed Islamic Group, among other terrorist organizations, are well-represented on the world wide web; as are indeed, in the United States, a plethora of neo-Nazi and white supremacist groups.[17]

Both militia groups in the US and Islamic fundamentalist organizations, which are united at least by their disdain for the US government, have been known to post bomb-making instructions and manuals on the web, a matter of sufficient interest to the Congress that it sought to regulate such activity on the web through congressional legislation.[18] HAMAS webpages carry military communiqués issued by the leaders of various armed Palestinian resistance movements, besides furnishing a catalog and visual montages of atrocities perpetrated by Israel (especially upon Palestinian children) and exhortations to carry out attacks against Israel and Jews.[19] The extent of Hizbollah's presence on the web can be gauged by the fact that its principal work is distributed among three sites, one of which largely documents attacks on Israeli targets. This dispersal of business, so to speak, is sound political practice, since the closure of one site still keeps Hizbollah afloat in cyberspace; it is also illuminative of the diasporic characteristics of cyberspace, which terrorist groups and non-state actors, among many other agents, are particularly poised to exploit.[20]

The story, consequently, of the cyberspace presence of terrorist groups, revolutionary and secessionist movements, and other political organizations that operate largely outside the realm of constitutional and legislative politics creates its own intricate web and has barely begun to be told. In 1998, nearly half of the 30 organizations designated as Foreign Terrorist Organizations under the Antiterrorism and Effective Death Penalty Act of 1996 [AEDPA] maintained websites[21]; by the end of 1999, nearly all terrorist groups had established their presence on the net.[22] These websites, whatever other language versions they might be available in, are invariably in English and pose complex and hitherto unexplored questions about the constituencies which find cyberspace hospitable for the fulfillment of their political designs. Moreover, since the preponderant number of these groups are presumed to be hostile to Westernization and globalization (not that the two are by any means congruent), most commentators have assumed that the use of English, a more global language than any other, points ultimately to the ineffectiveness of resistance to globalization. Similarly, the hostility of many of these organizations towards the United States in no manner prevents them from using American internet providers, or being hosted by American groups: thus, to take one example, the political manifesto and communiqués of the Peruvian revolutionary organization MRTA (Movimiento Revolucionario Tupac Amaru), which has been designated a Foreign Terrorist Organization by the State Department, are readily found on a website operated by students at the University of California, San Diego.[23]

With what confidence and skill do terrorists or others with extreme political persuasions use English on the web, and what are the different registers of the language with they work? Should the wide use of English alert us to the possibility that the constituencies attracted by such websites themselves hail from relatively privileged backgrounds, and that virtual terrorists, so to speak, have not arisen (as is commonly argued about terrorists) from backgrounds of poverty and deprivation, but rather they are the products (as was demonstrably clear from the profiles of the terrorists associated with the September 11thevents) of Western universities and secular institutions? The deployment of the internet by political extremists may yet be the most ironical instantiation of the disenchantment with modernity.

If the internet and the world wide web is a fecund ground for the dissemination of political ideologies, there is also considerable apprehension that terrorists and other political extremists could wage cyberattacks on computer networks and therefore cripple or at least disable the military, financial, and service sectors of advanced economies. An entire arsenal of words – cybercrime, cyberwar, infowar, netwar, cyberterrorism, cyber harassment, cyber break-ins – has found its way into our lexicon to describe the network piracy characteristic of what some military and political strategists describe as the "new terrorism" of our times.[24] In 1997, the Internet Black Tigers, which is affiliated with the Tamil Tigers of Eelam, a secessionist movement that has fought the Sri Lankan state to a stalemate over the last two decades, "flooded" Sri Lankan embassies throughout the world with email messages and rendered their computer systems inoperable. A year later, the Department of Defense was reporting 60 cyberattacks on its website every week, and there have been periodic reports of systemic efforts by, if I may coin this neologism, "computerrorists" to disable Pentagon computing systems. The Pentagon did not take these attacks lying down, and struck back with a Java applet that loads and reloads an empty browser on the attacker's desktop, forcing him or her to reboot the computer.[25] That same year, pursuant to India's nuclear tests, web activists waged concerted attacks on the website of the Homi Bhabha Research Center, the country's preeminent agency for nuclear research, and superimposed peace slogans, an image of a mushroom cloud, and data on the probable effects of nuclear war on the site.[26]

Conflicts on the ground are echoed, as one can imagine, in cyberspace. This should not surprise us: an earlier generation relentlessly waged cartographic wars, a matter that confounds those who are accustomed to thinking of maps as scientific representations of physical geographies and political boundaries.When India and China went to war briefly in 1962 over disputed territory in the former North-east Frontier Agency (NEFA), maps were produced on both sides to advance their respective claims;[27] and, again, both India and Pakistan have conducted cartographic wars over disputed territory in Kashmir and along other sectors of the border between the two countries. Cyberspace offers even more fertile territory for sabotage, misinformation, and what in the cliched formulation is termed the war over minds. An oft-mentioned case is that of Kosovo, which is sometimes described as the stage for the first internet war.[28] Both Milosevic and his opponents, in and outside Yugoslavia, and some opposed to NATO as much as to Serbian nationalists, took to cyberspace – as did indeed civilians caught in the fray, who found it a medium for the expression of sentiments about life under the twin tyrannies of dictatorship and carpet bombing.

A reporter for the *Los Angeles Times* appeared to have caught traces of this conflict over cyberspace early in the spin war, and observed that the dispute over Kosovo 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."[29] In Britain, the *Daily Telegraph* reported that it had learned of an order passed by President Clinton that authorized "American government computer hackers to break into Slobodan Milosevic's foreign bank accounts and drain his hidden fortune as part of a clandestine CIA plan to overthrow the Yugoslav president,"[30] but a more reasoned assessment of the utility of untethered cyberwar against Milosevic appears to have been offered by James Rubin, spokesperson for the US State Department, when he stated that it was American policy to keep internet service providers in Yugoslavia in business. “Full and open access to the Internet”, Rubin remarked, “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.”[31]

The second intifada, likewise, lurched straight into cyberspace when negotiations between Israel and the Palestinian National Authority broke down in October 2000. Israeli hackers subjected Hezbollah and other Palestinian sites to FloodNet attacks, and Hezbollah’s web logo, “a raised fist clenched around an automatic weapon”, was replaced by “photos of Israelis captured by Hezbollah set against a field of waving Israeli flags.”[32] Palestinians responded with attacks on the web sites of the Israeli military, the Tel Aviv Stock Exchange, the Bank of Israel, and the finance ministry. Some Israeli online activists then constituted themselves into the Israeli Internet Underground (IIU) and stated it as their mission “to inform and provide solutions wherever we can and therefore protect our sites against political cyber vandalism.”[33] Meanwhile, Palestinian activists came together in a group called Unity, which one commentator has described, without furnishing any evidence, as a “Muslim extremist group with ties to Hezbollah and other terrorist groups”.[34] Palestinian chatrooms are said to be abuzz with talk of “e-jihad” and “cyber-jihad”.

Wars that go cold on the ground -- or perforce cannot be conducted with arms -- might still remain hot in the air, howsoever lopsidedly. When a mid-air collision between an American spy plane and a Chinese jet fighter took place in April 2001, leading to heated exchanges between the two countries, activists immediately took to cyberspace. An American group known as PoizonBox was said to have attacked over 100 Chinese websites in the first two weeks following the collision; a Chinese retaliation, promised for the week beginning May 1st, was announced with the claim that the “crackers” intended to persuade the American people to influence their government from pursuing war-like gestures.[35] An American hacker known as “PrOphet” conceded that the cyber war amounted to little, and had not generated any political influence, but he described the goal as “just to fuck with China in any little way we can.”[36] One might think, of course, that the Americans were bound to have the edge over the Chinese. There were, in the year 2001, at least 10 times as many computers in the US as in China, and American computing power dwarfs that of China, estimated recently as 42 times greater.[37]

By the same token, as has been argued often enough, this makes the United States, where financial, commercial, military, educational, and administrative systems are entirely computerized, more vulnerable. Some of the strengths of the United States might also be the source of its weaknesses, though therein lies another tale which has yet to be told. But what is immediately striking in the cyberwar between Chinese and American hackers is that no commentator has thought it desirable to term them cyber-terrorists, as though this designation had to be reserved for Islamic fundamentalists, whose use value for Western commentators as exemplary terrorists can scarcely be disguised, or for those cyber activists, whether belonging to the Shining Path or the Revolutionary Armed Forces of Colombia (FARC), whose stated avowal of Marxist-Leninist ideologies, or disdain for free-trade arguments, immediately renders them suspect. Now that China has been admitted to the WTO, and is clearly veering towards a consumer-type society, it will most likely not be producing terrorists.

III: Terrorism, Virtual Reality, and Nomadism: Some Concluding Observations

In a frequently cited article, Dorothy Denning distinguishes between three forms of political activity on the internet, with particular reference to attempts to influence foreign policy.[38] She refers to activism as “normal, non-disruptive use of the internet in support of an agenda or cause”: such activity includes browsing the web, compiling a digital library, submitting electronic petitions, or coordinating political meetings open to the public. This form of activism has varying degrees of success, however that may be measured: for instance, the arrest of the Kurdish rebel leader Abdullah Ocalan became known in a matter of hours to Kurds scattered around the world, and they responded more quickly than did governments[39]; but demonstrations staged around the world, while they put the world on notice that the “Kurdish problem” remains unresolved, could not influence the Turkish government into releasing Ocalan or showing him clemency.

Hacktivism, Denning suggests, is a different order of political activity, and represents the marriage of hacking and activism; it generally shades into activity of dubious ethical import, and is often unlawful.

It takes many forms: in a sit-in or blockade, activists generate immense traffic against a targeted website and thus prevent legitimate users from reaching it.A more complex form of civil disobedience entails the creation of a special website with software that, once it is downloaded, accesses the targeted site every few seconds. Tellingly, such sites are called FloodNet sites, and activists term this form of political engagement, with perhaps an inadequate comprehension of how far the idea of theater and spectacle is integral to terrorism (as the sight of aircraft slamming into the World Trade Center towers indubitably established) Electronic Disturbance Theater (EDT). Hacktivism’s arsenal extends beyond all this, as Denning observes, to swarming, email bombing, computer break-ins, creating mirror and mimic websites, and introducing viruses and worms into computer networks.

Finally, to round up her discussion, Denning adverts to cyberterrorism, a term coined by Barry Collin, of the Institute for Security and Intelligence (California), to suggest the marriage of terrorism” and cyberspace”.[40] She finds adequate the definition furnished by a FBI agent: “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.”[41] It is the distinctive characteristic of cyberterrorism that it recognizes no boundaries and aims specifically to target the critical infrastructures of the enemy country or organization.

It is instructive, and alarming, that Denning takes her cues, in speaking of cyberterrorism, from figures of the political and defense establishment, since nearly all of the purportedly theoretical literature on information warfare, the larger category under whose rubric cyberwar, cyberterrorism, and internet terrorism are generally subsumed and discussed, has been generated by officials working for the Pentagon, Air Force, the National Defense University, other branches of the military and intelligence services,[42] and so-called think tanks, such as the RAND Institution.[43]

Surprisingly, there is little if any theorizing in this literature on what constitutes “information”, how it comes to be assessed as information, and its politics -- and how it is to be distinguished from “knowledge”. Cliches about the “information revolution” proliferate, and its votaries are profuse in expressing sentiments whose inanity matches their crudity: thus, we are told, information struggles or wants to be free, and information belongs to all.

The definition of information warfare furnished by the Department of Defense is accepted as a template by nearly every commentator: “Actions taken to preserve the integrity of one’s own information system from exploitation, corruption, or destruction, while at the same time exploiting, corrupting, or destroying an adversary’s information system and in the process achieving an information advantage in the application of force.”[44] Information warfare is perceived as a zero-sum game, as another aspect of man’s innate tendency to gravitate towards competition, the preservation and enhancement of self-interest, and the destruction of the interests of others. Speaking in a particularly American idiom, which recognizes only “winners” and “losers”, the two principal officers of the US Air Force opine that “the competition for information is as old as human conflict”, predating “the dawn of history”, “virtually a defining characteristic of humanity”; more to the point, “Nations, corporations, and individuals each seek to increase and protect their own store of information while trying to limit and penetrate the adversary’s.”[45] Cyberterrorism is, understandably, placed within this framework: it represents an attempt, by non-state actors, to “deny, exploit, corrupt, destroy, or protect information.”[46]

[Here will follow several paragraphs about the use of the internet in Chiapas, the Zapatista network, the place of the internet in the organization of the Seattle demonstrations, and the Electronic Intifada.]

To unravel the politics of the discourses around cyberterrorism, it becomes imperative to ask who produces knowledge about terrorism, how terrorism is constituted, and the politics of knowledge disguised by conventional definitions of terrorism. If our understanding of terrorism, as I would argue, derives primarily from the counterterrorism experts, it may help illuminate why government officials, military strategists, policy planners, and the consultants who work for RAND and the like are so resistant to any definition of terrorism that seeks to exonerate states and fixates only on subnational, transnational, and other non-state actors. . . . . .

[INCOMPLETE]

[1] Valdis E. Krebs, “Uncloaking Terrorist Networks”, *First Monday*: *Peer-Reviewed Journal on the Internet* 7, no. 4 (April 2002), seems to be wholly unaware of the pre-history of “terrorist networks”, though Krebs is right in advancing the claim that “in the non-stop stream of news and analysis” following the events of September 11th, “one phrase was continuously repeated – ‘terrorist network.’” On-line (accessed 8 April 2002) at: http://www.firstmonday.dk/issues/issue7_4/krebs/index.html

The phrase “terror network” was first made famous by Claire Sterling, *The Terror Network* (New York: Holt, Rinehart & Winston/Reader’s Digest, 1981), a work whose “scholarly” merit can be surmised from the involvement of “Reader’s Digest”; an apt rejoinder to her, which dissects the idea of “networks”, is Edward S. Herman, *The Real Terror Network*: *Terrorism in Fact and Propaganda* (Boston: South End Press, 1982).

[2] A videocassette prepared by Osama bin Laden and released on or around 13 December 2001 appears to confirm the existence of different cells which appear to have acted independently of each other: “Those who were trained to fly”, bin Laden is heard saying, “didn’t know the others. One group of people did not know the other group.” See: http://www.defenselink.mil/news/De2001/d20011213ubl.pdf for the full transcript. A similar argument about independent cells may reasonably be advanced about the American Embassy bombings in Kenya and Tanzania, which have been linked to bin Laden and which, like the attacks of September 11th, took place within minutes of each other.

[3] Krebs, “Uncloaking Terrorist Networks”, p. 2.

[4] Ibid.

[5] Ibid., pp. 3-8.

[6] For a brief resume of, and reflection on, these arguments see Vinay Lal, “The Politics of History on the Internet: Cyber-Diasporic Hinduism and the North American Hindu Diaspora”, *Diaspora* 8, no. 2 (Fall 1999), pp. 137-73, esp. pp. 137-43.

[7] “Osama Bin Laden: Planning Terrorist Attacks on the Internet”, accessed 10 Jan. 2002 online at:<wysiwyg://122/http://www.allfreecontests.com/bin_laden/bin_laden_web.htm>

[8] Susan Stellin, “Terror’s Confounding Online Trail”, *New York Times* (28 March 2002), accessed online (16 April 2002) at:<http://www.nytimes.com/2002/03/28/technology/circuits/28TERR.html?>

[9] Charles Piller, “Terrorists Taking Up Cyberspace”, *Los Angeles Times* (8 Feb. 2001), p. A1; Varvara Mitliaga, “Cyber-Terrorism: A Call for Governmental Action?”Paper presented at the 16th BILETA Annual Conference (April 2001), Edinburgh, online (accessed on 15 January 2002) at:http://www.bileta.ac.uk/01papers/mitliaga.html. A lengthier treatment of these issues is offered by Michael Whine, “Cyberspace: A New Medium for Communication, Command and Control by Extremists” (April 1999), online at: http://www.ict.org.il/articles/cyberspace.htm (accessed 25 March 2002). The anonymity of the internet – for example, both Hotmail and Yahoo make it possible to set up a free and anonymous email account, and some technologies, such as AOL’s “Instant Messages”, make no provision for the storage of messages – is cited most frequently as the reason why terrorist activity online is hard to track down. Where a sophisticated technology for the interception of messages does exist, there remain questions, on which the literature is profuse, about how security and privacy concerns must be reconciled. A technology known colloquially as “Carnivore” to monitor electronic communications watches “for specific words or codes” and saves “copies of any messages containing these elements.” See Jason Krause, “New Tools sought to track terror online”, Chicago Tribune (15 October 2001), online at:http://www.chicagotribune.com/technology/chi-0110150199oct15.story?null. The language of cyberspace will doubtless soon find deserving lexicographers, grammarians, and semanticians.

[10] Stellin, “Terror’s Confounding Online Trail”.

[11] See http://www.adl.org/Terror/focus/16_focus_a4.html, accessed on 10 January 2002.

[12] Erik Baard, “Outside Chance”, *Village Voice* (7-13 November 2001), online at: sysiwyg://57/http://www/villagevoice/com/issues/0145/baard.php

[13] Mitliaga, “Cyber-Terrorism: A Call for Governmental Action?”, offers a brief summary. Online (accessed on 15 January 2002) at:<http://www.bileta.ac.uk/01papers/mitliaga.html>

[14] Piller, “Terrorists Taking Up Cyberspace”, p. A15.

[15] http://www.eelam.com

[16] http://www.farc-ep.org/pagina_ingles [English version]

[17] A useful CD-ROM compendium of such websites, though slightly dated, is *Digital Hate 2000* (Los Angeles: Simon Wiesenthal Center, 1999).

[18] Senator Diane Feinstein (D-California) proposed new legislation that would make illegal the dissemination of bomb-making literature as a form of incitement to commit violence. An article published in the *Columbus Dispatch* (29 April 1996) provided details of several episodes of amateur bomb-making: see Mike Lafferty, “Blueprints for Bombs Are Not Hard to Find”, p. C1. The most well-known of such manuals goes by the name of the *Anarchist’s Cookbook*, first written by Jolly Roger in the mid 1980s and since published in several editions. The website [www.anarchistcookbook.net] on

which it is featured describes the book as a "collection of files compiled by a computer pirate detailing many underground activities such as hacking, phreaking (telephone hacking), pranks, drugs, explosives and home made bombs.The Cookbook has come under attack from many including the press in the past, but is essentially only a collection of publicly available information that can be found in your pubic library." Advocates of censorship on the net consistently encounter the rejoinder that information and material on the net deemed to be illegal, harmful, or exploitative is also found in more traditional forms, such as the print media.

[19] http://www.palestine-info.org

[20] The main home page is: http://www.hizbollah.org, while news and information are carried on: http://www.almanar.com.lb; attacks on Israeli targets are conveyed on http://www.moqawama.org

[21] Kevin Whitelaw, "Terrorists on the Web: Electronic Safe Haven", *U.S. News & World Report* (22 June 1998), p. 46.

[22] For links from one extraordinary site prepared by Barry Cromwell, and last modified on 19 April 2002, see < http://www.cromwell-intl.com/security/netusers.html >

[23] http://burn.ucsd.edu/~ats/MRTA. See also Robert Grollier, "Terrorists Get Web Sites Courtesy of U.S. Universities", *San Francisco Chronicle* (10 May 1997), online at: http://burn.ucsd.edu/archives/ats-1/1997.May/0042.html

[24] Bruce Hoffman, *Inside Terrorism* (London: Victor Gollancz, 1998). Describing the almost "revolutionary change in terrorism" induced by the internet, Hoffman remarks that "in the past, terrorists had to communicate through an act of violence and hope that the communiqué would effectively explain their ideological justification or their fundamental position." Quoted in Piller, "Terrorists Taking Up Cyberspace", p. A1.

[25] Niall McKay, "Pentagon Deflects Web Assault", *Wired News* (10 Sept. 1998), online (accessed on 17 April 2002) at:wysiwyg://6/http://www.wired.com/news/print/0%2C1294%2C14931%2C00.html

[26] James Glave, "Crackers: We Stole Nuke Data", *Wired News* (3 June 1998), online (accessed 28 March 2002) at: http://www.wired.com/news/print/0,1294,12717,00.html

[27] Unfortunately, John W. Garver, *Protracted Contest*: *Sino-Indian Rivalry in the Twentieth Century* (Seattle: University of Washington Press, 2001), though unusually comprehensive, is insensitive to such considerations.

[28] A recent documentary film, *Bringing Down a Dictator* (director Steve York, 2001), highlights the role of the student-led group, Otpor, which trained activists in non-violent action and maintained the channels of communication largely through the internet. The Balkans is also often the stage for imaginary scenarios of cyberwar:see Matthew G. Devost, Brian K. Houghton, and Neal A. Pollard, "Information Terrorism: Can You Trust Your Toaster?" (1996), available online from the archives of the Terrorism Research Center at www.terrorism.com

[29] Ashley Dunn, "Crisis in Yugoslavia – Battle Spilling Over Onto the Internet", *Los Angeles Times* (3 April 1999).

[30] Philip Sherwell, Sasa Nikolic, and Julius Strauss, "Clinton orders 'cyber-sabotage' to oust Serb leader", *Daily Telegraph* (7 April 1999), online at:<http://www.freerepublic.com/forum/a3780596c7940.htm>

[31] David Briscoe, “Kosovo-Propaganda War”, Associated Press (17 May 1999).

[32] Piller, “Terrorists Taking Up Cyberspace”.

[33] Cited by Larisa Paul, “When Cyber Hacktivism Meets Cyberterrorism” (19 February 2001), online (accessed 16 April 2002) at:http://rr.sans.org/hackers/terrorism.php

[34] Carmen J. Gentile, “Hacker War Rages in Holy Land”, *Wired news* (8 November 2000), online (accessed 17 April 2002) at:
wysiwyg://8/http://www.wired.com/news/print/0%2C1294%2C40030%2C00.html

The discrepancy in how Israeli and Palestinian cyberattacks are described tells its own story; it is enough to make allegations about the links of Palestinian cyber activists to the Hezbollah, and since the state is not seen as a perpetrator of terrorism, Israeli cyber activists are not seen in the same light.

[35] Michelle Delio, “Crackers Expand Private War”, *Wired News* (18 April 2001), and Michelle Delio”, “It’s (Cyber) War: China vs. U.S.”, *Wired News* (30 April 2001), both online (accessed 28 March 2002) at, respectively: wysiwyg://83/http://www.wired.com/news/print/0,1294,43134,00.html and wysiwyg://80/http://www.wired.com/news/print/0,1294,43437,00.html

[36] Delio, “Crackers Expand Private War”, p. 1.

[37] Mitliaga, “Cyber-Terrorism”, p. 3.

[38] Dorothy Denning, “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy”, online (accessed 14 January 2002) at:<http://www.terrorism.com/documents/denning-infoterrorism.html>

[39] Ibid., p. 8.

[40] Barry Collin, “The Future of Cyberterrorism”, *Crime and Justice International* (March 1997), pp. 15-18, online at: http://www.acsp.uic.edu/OICJ/CONFS/terror02.htm

[41] Denning, “Activism, Hacktivism, and Cyberterrorism”, p. 17, citing Mark M. Pollitt, “Cyberterrorism: Fact or Fancy?”, Proceedings of the 20^{th} National Information Systems Security Conference (October 1997), pp. 285-89, online (accessed 28 March 2002) at: http://www.cs.georgetown.edu/~denning/infosec/pollitt.html

[42] For a representative set of articles on “information warfare”, see Thomas G. Mahnken [Office of Naval Intelligence], “War in the Information Age”, *Joint Forces Quarterly* (Winter 1995-96), pp. 39-43; Lawrence E. Casper [US Army] et al, “Knowledge-Based Warfare: A Security Strategy for the Next Century”, *Joint Forces Quarterly* (Autumn 1996), pp. 81-89; Ronald R. Fogleman [Chief of Staff, US Air Force] and Sheila E. Widnall [Secretary of the Air Force], “Cornerstones of Information Warfare”, online on Infowar.com site at http://www.infowar.com/mil/_c4i/mil_c4ia.html-ssi (accessed 28 March 2002); Chris Morris, Janet Morris, and Thomas Baines [all Air University], “Weapons of Mass Protection: Nonlethality, Information Warfare, and Airpower in the Age of Chaos” [pdf. file]; Ronald R. Fogleman [Chief of Staff, US Air Force], “Information Operations: The Fifth Dimension of Warfare”, online (accessed 28 March 2002) at:http://www.defenselink.mil/speeches/1995/di1047.html; Dan Kuehl [National Defense University], “The Ethics of Information Warfare and Statecraft”, online at:http://www.infowar.com/mil_c4i/mil_c4ij.html-ssi (accessed 15 March 2002); Matthew G. Devost [Security Design International], “Organizing for Information Warfare: ‘The Truth is Out There’”,

online at: www. terrorism.com (accessed 15 March 2002); and Martin C. Libicki [National Defense University], “Information Dominance”, Strategic Forum, no. 132 (November 1997), online (accessed 28 March 2002) at: http://www.ndu.edu/inss/strforum/forum132.html. The pretensions of some commentators, who fancy themselves modern-day Sun Tzus, can be surmised from the papers published by the Institute for National Strategic Studies in its “Sun Tzu Art of War in Information Warfare” series. See, in particular, Brian Fredericks [US Army], “Information Warfare: The Organizational Dimension”; Charles B. Everett, Moss Dewindt and Shane McDade, “The Silicon Spear: An Assessment of Information Based Warfare (IBW) and U.S. National Security”; and John H. Miller, “Information Warfare: Issues and Perspectives”, all online at: http://www.ndu.edu/inss/siws.

[43] John Arquilla and David Ronfeldt of RAND (Santa Monica, California) have built an entire career around the ideas of “netwar” and other aspects of information warfare, but their numerous books all recycle a couple of ideas that are rather slim to begin with. See, for instance, *The Zapatista ‘Social Netwar’ in Mexico* (RAND, 1998); *In Athena’s Camp*: *Preparing for Conflict in the Information Age* (edited, RAND, 1997); and *Networks and Netwars*: *The Future of Terror, Crime, and Militancy*(edited, RAND, 2001).

[44] Cited by Devost, “Information Terrorism: Can You Trust Your Toaster”, p. 6.

[45] Fogleman and Widnall, “Cornerstones of Information Warfare”, p. 1.

[46] Ibid., p. 5.

Nautilus Institute
608 San Miguel Ave., Berkeley, CA 94707-1535 | Phone: (510) 423-0372 | Email: nautilus@nautilus.org