

STATE OF THE ART

A CONTINUING SURVEY OF TECHNOLOGY AND SOCIETY

| | |
|----------------------------|--------------------------------|
| Dot-Com Terrorism | Red Planet, Wet Planet |
| Campaigning for Stem Cells | Miles Still to Go |
| Daniel J. Boorstin, RIP | The Science of Human Potential |
| Gaga Over Google | One of Us |
| Life from Scratch | 'The Course We Must Maintain' |
| Science Goes Hollywood | Notes & Briefs |

Dot-Com Terrorism

How Radical Islam Uses the Internet to Fight the West

Al Qaeda has been dealt heavy blows in Afghanistan and elsewhere, but the war against radical Islamic terrorism continues, and cyberspace is among its most active fronts.

The Internet is host to thousands of websites run by terrorist groups and their supporters, with Al Qaeda exerting a dominant influence on their bloodthirsty content. After September 11, as Paul Eedle observed in *Jane's Intelligence Review*, Al Qaeda launched an online campaign to win the hearts and minds of the Muslim world—to advance its ideology of total war with the West and discredit those few Muslim leaders who spoke out against terrorist jihad. Today, the jihadis clearly have the advantage in Islamic cyberspace: Radical Islamist websites have proliferated, while Muslim websites devoted to moderate alternatives are few in number.

The online deluge of political and religious tracts preaching anti-Americanism and anti-Semitism is mind-boggling. Some sites monger conspiracy theories: The pernicious rumor, still widespread in the

Muslim world, that Jews were the real masterminds of the September 11 attacks was started and disseminated by Islamist “news” websites. Other websites, such as those run by Hamas, spread the violent Islamist theology of martyrdom by glorifying suicide bombers and other fallen jihadis.

Online video brings home the jihadi message of violence with terrible vividness. Video clips of suicide bombers are readily available, and some analysts have speculated that Al Qaeda deliberately staged and filmed the murder of *Wall Street Journal* reporter Daniel Pearl for the purpose of circulating the footage on the Internet. The grisly murder of American contractor Nicholas Berg in Iraq was likewise released to the world via online video.

Since at least the time of the Bosnian conflict in the late 1990s, militant Islam has used the Internet to recruit new jihadis for its wars in Chechnya, Kashmir, Afghanistan, and against Israel and the United States. Beginning last year, analysts have observed Al Qaeda using websites and online chat rooms to draw fresh

mujahideen from around the world to the battlefields of Iraq. "Al Qaeda's use of the Internet is amazing," said Rita Katz, director of the Search for International Terrorist Entities Institute, in the *New York Post*. "We know from ... captured Al Qaeda fighters who say they joined up through the Internet ... that this is one of the principal ways they recruit fighters and suicide bombers."

A growing number of European-language websites have sprung up to persuade Muslims living in Western countries to join the cause of radical Islam. The website of Al-Muhajiroun, a London-based group that exalted the September 11 hijackers as the "Magnificent 19," has entreated Muslims to become radical Islam's "fifth column" in the West. A few months ago, the group's website displayed a picture of the U.S. Capitol in flames. For anyone unclear about the meaning of this image, a caption below it read: "How the Khilafah [caliphate] will be restored and man-made law destroyed."

For the apprentice jihadi, cyberspace abounds with training manuals and other useful information for war preparations. In 2002, Hamas founded an online "military academy" with live instructors offering courses on how to build explosives, including the weapon-of-choice for Hamas militants, the exploding belt. Since being bombed out of their Afghan training centers, Al Qaeda has been publishing a monthly e-magazine called *Al-Battar*. Recent editions include detailed instructions on physical fitness training, the use of firearms, how to plot an assassination, wilderness survival skills, and how to organize and manage a terrorist cell.

Militant Islam's use of the Internet as a fundraising tool is also well-documented. In recent years, the American government

has cracked down on several Islamic charities, most of them with online collections operations, that have channeled funds to support terrorist operations. In Europe, however, there are fewer restrictions on such charities, and because the Internet provides a great degree of anonymity, many fundraising operations have survived in cyberspace by simply re-branding themselves. New ones have also emerged. As noted in a recent report from the United States Institute of Peace, a group called Hizb ut-Tahrir—a rising star in terrorism circles—uses websites across Europe and Africa to solicit funds for its operations. Its message: Kill nonbelievers and enemies of Islam wherever you find them.

Al Qaeda in particular has placed a great deal of emphasis on developing its ability to use computers for coordinating and planning attacks, as documented in a new study from Dartmouth's Institute for Security Technology Studies. Computers confiscated in Afghanistan suggest that the September 11 attacks were largely coordinated via encrypted e-mail, and planned with intelligence gathered online. One Al Qaeda training manual found in Afghanistan said that "it is possible to gather at least 80 percent of all information required about the enemy" by "using public sources openly and without resorting to illegal means."

As one expert put it in the U.S. military journal *Parameters*: "We can say with some certainty, Al Qaeda loves the Internet." In fact, because of its Internet aptitude, Al Qaeda has been able to retain some of its command and control structure and its ability to launch future attacks, despite being bombed out of Afghanistan. In recent years, as intelligence agencies have sought to disrupt the organization by intercepting

encrypted messages and breaking other lines of communication, the Internet jihadis have responded with high-tech savvy. One Al Qaeda site, *alqeda.com*, after being repeatedly kicked off its host servers, stayed online by “parasiting” itself into the directories of other websites. And rather than using encryption technologies, which draw the attention of intelligence agencies, Al Qaeda has relied heavily on communicating through anonymous e-mail accounts and in chat rooms and discussion groups.

In waging war against terrorist groups, government investigators and prosecutors have increasingly found that citizen-experts are among the most resourceful and effective online combatants. In his book *Against All Enemies*, former cybersecurity czar Richard Clarke says the FBI failed so miserably at gathering information on Islamic terrorist groups that he was compelled to turn to private researchers. One private group, The Investigative Project, furnished Clarke and his colleagues with a wealth of intelligence on terrorist organizations—including who they are, how they’re structured and financed, and what their agendas are. Much of this information was collected online. Another citizen group, the Northeast Intelligence Network, was founded after September 11 in the belief that scouring the Internet and trans-

lating its vast backwaters of jihadi material might yield intelligence to help thwart future attacks.

Still other private groups have taken up the war against the Internet jihadis directly. The Internet Haganah (Hebrew for “defense”) is described by its director as “a volunteer effort to research, report on, and stop the use of the Internet as a communications and propaganda tool by Islamist terrorist groups, their supporters and apologists.” Internet Haganah has helped to shut down hundreds of Islamist websites by alerting their Internet service providers. In retaliation, self-proclaimed “Internet terrorists” have launched cyberattacks against Haganah’s service provider.

Fighting radical Islamic terrorism requires a multi-pronged strategy, including military and economic actions, intelligence and counter-intelligence, and aggressive public diplomacy. The fight has gone online, too, insofar as the Internet has become central to the recruiting, training, and planning of terrorism. If there is an irony here, it is that those who supposedly despise modern civilization have skillfully adopted its tools to fuel their mission. And if we are going to win the war on terrorism, we will need to take the front in cyberspace seriously, lest it become a permanent source of rage and instability.