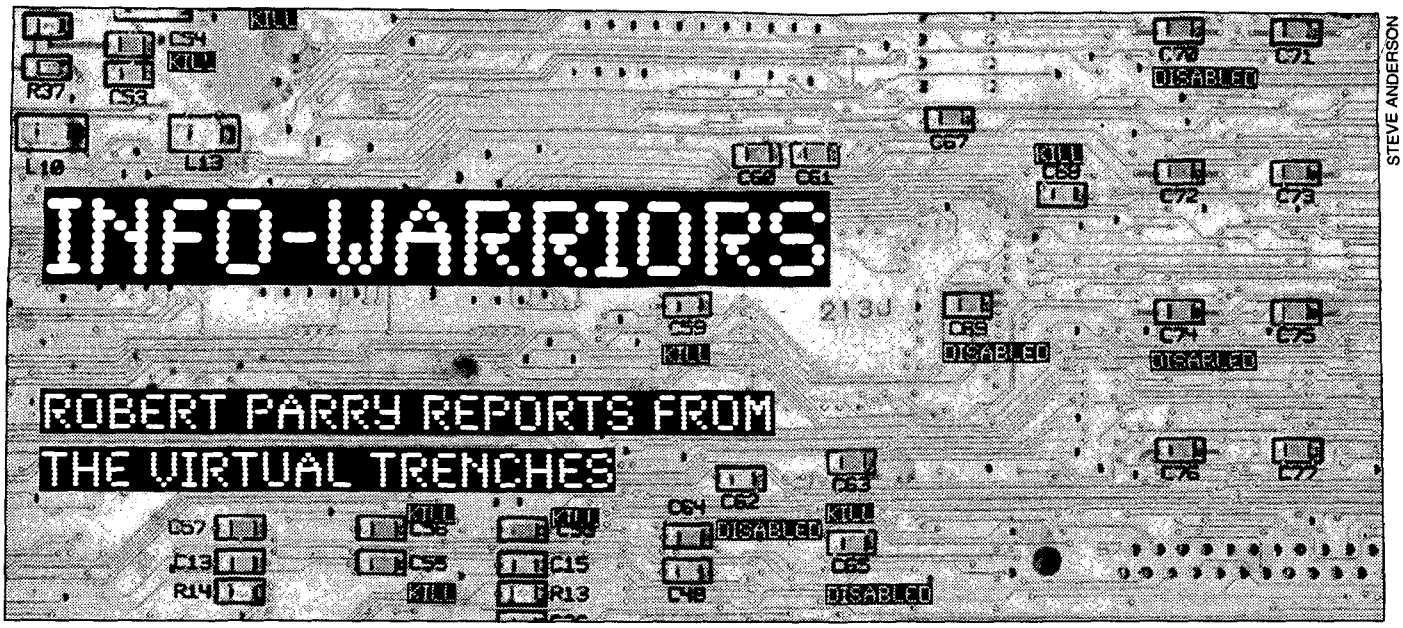


STEVE ANDERSON

NATO's war for Kosovo is pressing the edges of modern "information warfare." Through the early phases of the conflict, NATO concentrated its attacks on command-and-control centers, power stations and propaganda outlets. Those attacks included sophisticated electronic assaults on computers directing Serbian air defenses and so-called "soft bombs" to short out electrical lines.

But by April, President Clinton privately indicated that he might opt for a far more expansive high-tech assault to punish the Yugoslavian government for the atrocities in Kosovo. Though these "info-war" techniques rarely are acknowledged officially, government sources say Clinton is poised to apply Big Brother military capabilities. According to these sources, U.S. info-warriors have the capacity to plant viruses in civilian computer systems, alter bank records and generally wreak havoc on Yugoslavia's infrastructure—from disrupting electrical utilities to shutting down the phone system.

Clinton's info-war planning was first reported in *iF Magazine* in early May. That report was corroborated in the May 31 issue of *Newsweek*. In the magazine, senior intelligence officials acknowledged that Clinton issued a top-secret "finding" in mid-May that instructed the CIA "to conduct a cyberwar against [Slobodan] Milosevic, using government hackers to tap into foreign banks and, in the words of one U.S. official, 'diddle with Milosevic's bank accounts.' " According to *Newsweek*, the United States has "identified banks in several countries, including Russia, Greece and Cyprus, where the Serb leader has hidden millions of dollars."

Some info-war advocates argue that computer sabotage is a far more humane way to wage war than dropping bombs and firing off missiles. They note the obvious: Electronic attacks do not carry the immediate physical risk to civilians that explosives do. But there are ethical concerns, too, about attacking a nation's computer infrastructure and severely destabilizing its economy. Plus, there are fears that a computer virus or a similar tactic could backfire and infect computers far beyond Yugoslavia. An info-war "first strike" could invite retaliation against America's computer-dependent economy.

American officials rarely have discussed info-war developments publicly, and they're careful not to mention the United States as a participant in this new arms race. CIA Director George Tenet testified to Congress that "several countries have or are developing the capability to attack an adversary's computer systems." He added that "developing a computer attack capability can be quite inexpensive and easily concealable. It requires little infrastructure, and the technology required is dual-use." Left unsaid was that the U.S. government, with the world's most powerful computers and most sophisticated software designs, has led the way both in offensive info-war strategies and defensive countermeasures.

When info-war gets mentioned in the American news media, it usually is in the context of a real or potential threat from an enemy seeking to damage the United States and its allies. On March 31, one week into NATO's air war, NATO spokesman Jamie Shea prompted headlines in U.S. newspapers when he complained that hackers in Belgrade had disrupted the official NATO Web site. But NATO computer experts acknowledged that the low-grade harassment was more "spamming" than hacking, and that no sensitive computer systems were entered.

The U.S. military first demonstrated the revolutionary potential of information warfare during the Gulf War. With air attacks and electronic means, U.S. forces destroyed Saddam Hussein's command-and-control structure before concentrating on his tanks and troops. Scattered journalistic reports at the time noted U.S. success in planting viruses in Iraqi military computer systems.

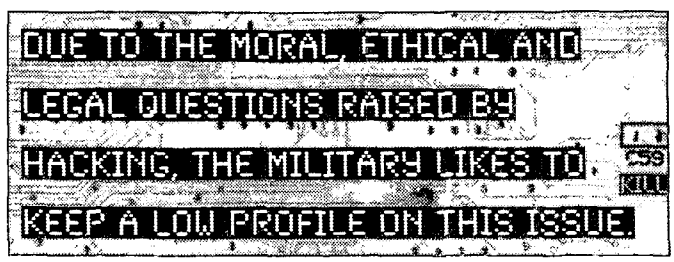
The CIA also has utilized info-war techniques to fight the drug war. According to a U.S. government source, in the mid-'90s, U.S. intelligence learned of a South American drug lord's plan to bribe a politician. After the money was transferred, U.S. government hackers accessed the politician's bank account and electronically deleted the money. In the fall-out from the disappeared funds, the drug lord blamed a hapless bookkeeper who reportedly was killed. The CIA has

jealously protected its info-war capability so that targets remain unsuspecting and other countries don't mount defensive or retaliatory operations.

However, the potential for info-war became such a hot topic within the U.S. military that the Pentagon hired an outside consultant to summarize some of the most salient features of digital combat in a chatty, 13-page booklet entitled *Information Warfare for Dummies*. The booklet, obtained from a government official, was designed to clue in some of the Pentagon's more unplugged officers. It begins by explaining the first objective for any lap-topped GI fighting a future information war: "Destroy (or weaken) the bad guy's system and protect your own."

The manual describes info-war tactics as "fairly groundbreaking stuff for our nation's mud-sloggers." It adds: "Theft and the intentional manipulation of data are the product of devilish minds. ... Pretty shady, those Army folks."

The high-tech techniques can be divided into "hard kill" acts of physical destruction and "soft kill" methods of electronic or psychological disruption. The pamphlet notes, "Their commonality lies in their emphatic focus on information—destroying it, corrupting it, and denying it."



More traditional information warfare targets an enemy's battlefield command-and-control structure to "decapitate" the fighters from their senior officers, thereby "causing panic and paralysis." But "network penetrations"—or hacking—"represents a new and very high-tech form of warfighting." The disruptive strategies in the U.S. arsenal include "insertion of malicious code (viruses, worms, etc.), theft of information, manipulation of information, denial of service." Such techniques can both damage the functioning of enemy computers or subtly alter data, such as financial records, to spread confusion.

The booklet notes that these tactics do have advantages over more traditional military operations: "The intrusions can be carried out remotely, transcending the boundaries of time and space. They also offer the prospect of 'plausible deniability' or repudiation." It's difficult to trace a network penetration to its source—and because viral infections can be so subtle, adversaries may be unaware they've been attacked.

The info war goes beyond hacking. *Information Warfare for Dummies* mentions other *Buck Rogers*-type weapons, such as electromagnetic pulse (EMP) bombs. "The high-energy pulse emitted by an EMP bomb can temporarily or permanently disable all electronics systems, including computers, for a radius of several kilometers," the manual says. "Put simply, EMP weaponry fries electronic circuitry. EMP weapons can be launched by airborne platforms or detonated inside information centers (banks, corporate headquarters, telephone exchanges, military command posts). The explosion needed to trigger the electromagnetic pulse apparently is minor compared to a conventional blast, theoretically resulting in fewer human casualties." Though EMP bombs are believed to be part of the U.S. arsenal, there has been no official acknowledgment that they have been used in combat.

Info-war also offers the potential for high-quality "psyops [psychological operations] and deception" to confuse and demoralize a targeted population. "Future applications of psyops may include realistic computer simulations and 'morphed' imagery broadcasts of bogus news events," the booklet explains.

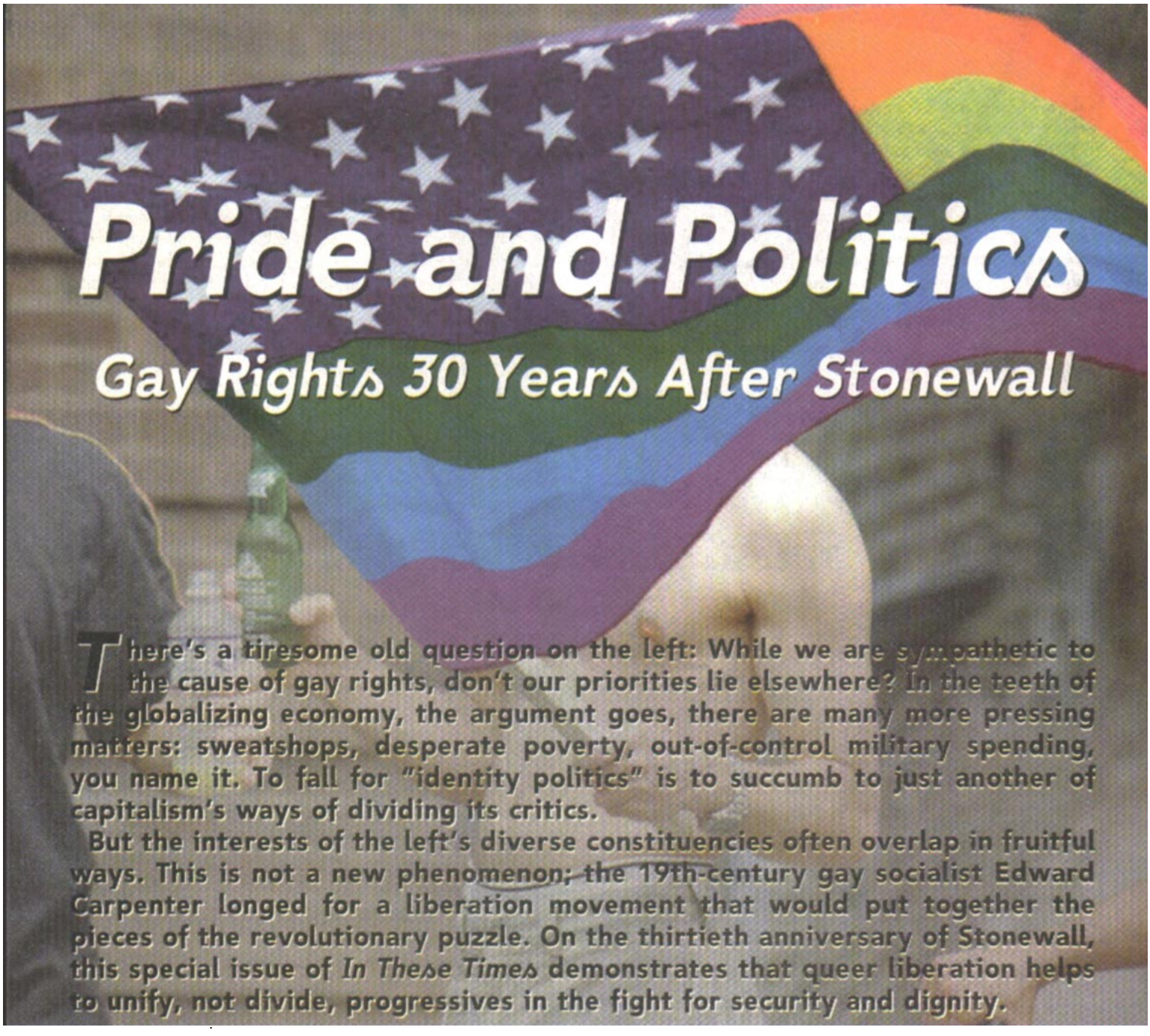
The Pentagon does recognize the taboo nature of information war. "Due to the moral, ethical and legal questions raised by hacking, the military likes to keep a low profile on this issue," the primer explains. It cites several ethical questions: "Is penetrating another nation's computer system somehow 'dirty' and 'wrong'—something the U.S. military has no business doing? Are electronic attacks against a nation's financial transaction computers too destabilizing and perhaps immoral?"

The manual also warns that the info-war attacks, especially viral infections, could backfire and harm U.S. interests. It worries, too, whether the Army will have success in recruiting "hacker-types and nerds"—and whether these recruits will "go bad" and sell their skills to another country to help penetrate U.S. computers.

There is also the question of whether these info-war techniques could be turned against U.S. citizens. While executive orders ban the CIA from influencing U.S. politics, new anti-terrorism laws have expanded government police powers in many security areas. Though there is no evidence that it has been used in that way, info-war certainly offers a tempting capability for waging a "dirty tricks" campaign against domestic "threats."

It is too early to tell how effective the information warriors will be against Milosevic and his government. But, depending how aggressive President Clinton chooses to be, the Balkan war could turn into an important testing ground for these new tactics. The conflict could become what the president might call a warfare bridge to the 21st century. ■

Robert Parry *is the editor and publisher of* iF Magazine *and* www.consortiumnews.com, *where a version of this story originally appeared.*



Pride and Politics

Gay Rights 30 Years After Stonewall

There's a tiresome old question on the left: While we are sympathetic to the cause of gay rights, don't our priorities lie elsewhere? In the teeth of the globalizing economy, the argument goes, there are many more pressing matters: sweatshops, desperate poverty, out-of-control military spending, you name it. To fall for "identity politics" is to succumb to just another of capitalism's ways of dividing its critics.

But the interests of the left's diverse constituencies often overlap in fruitful ways. This is not a new phenomenon; the 19th-century gay socialist Edward Carpenter longed for a liberation movement that would put together the pieces of the revolutionary puzzle. On the thirtieth anniversary of Stonewall, this special issue of *In These Times* demonstrates that queer liberation helps to unify, not divide, progressives in the fight for security and dignity.

Taking Care of Business

By Hans Johnson

The King of Beers was in trouble. A Bud Light ad showing two men holding hands no sooner had appeared in a St. Louis gay newspaper in April than Jerry Falwell was railing against "homosexual images coming into our homes through reckless advertising" and the Family Research Council was denouncing Anheuser-Busch's "steps to promote homosexuality."

Instead of calling in the Clydesdales, the brewer with the multimillion-dollar promotional budget called on the public to phone in reactions to the brouhaha. And the Human Rights Campaign (HRC), the nation's largest gay lobbying group, rushed to the company's defense, urging activists to write Busch praising the ad.

Welcome to a widening front of the gay rights movement, where gay groups like HRC direct grassroots advocacy not to Capitol Hill but corporate headquarters. The shift in focus stems in part from a GOP logjam blocking national legislation to recognize hate crimes and ban workplace discrimination based on sexual orientation. But the shift is also about business—and the gay movement's tightening embrace of it. The bid to save the Bud ad, which the brewer seems poised to resurrect once the dust settles, is the latest in