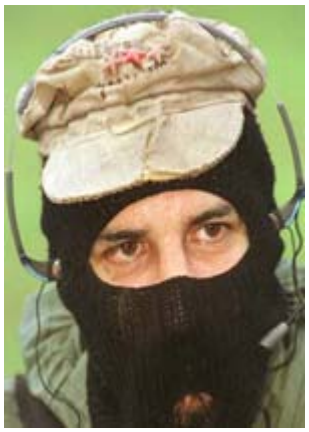
steal this modem

by Nuno Andrade

Is the new form of digital protest known as hacktivism a "destructive and unconstitutional use of technology," as one critic charges, or the last, best hope for political dissent in a digital age?



Subcommandante Marcos of the EZLN, Chiapas, Mexico. March 12th, 2001. Photo: Chiapas Media Project

On Tuesday, April 15, 2002 at exactly 12:00 AM GMT, the Israeli government was attacked, not by Palestinian suicide bombers or Hezbollah fighters wielding rifles, but by activists armed with nothing but computers and Internet connections.

The attacks, conducted on Israeli government information systems, were organized by the Electrohippie Collective, a group of activists and computer experts intent on using the Internet to further their political agenda. In a mass e-mail sent the day of the cyber-attacks, the Collective stated, "In response to...the recent Israeli military incursions into the major settlements of the West Bank, the Electrohippie Collective is mounting an online 'electronic civil disobedience action' against the information systems of the Israeli government."

The Electrohippie Collective is one of many groups that fall under the rubric of "hacktivism" — activism practiced by Web-savvy activists, some of them hackers (computer whizzes known for their prowess at breaking into computer systems).

This trend can be traced back to January 1, 1994, when a revolutionary group called the Zapatista National Liberation Army (or Ejército Zapatista de Liberación Nacional, in Spanish — EZLN for short) began a "low-intensity" guerrilla war against the Mexican government by seizing four towns in the southern state of Chiapas as a protest against the government's treatment of rural Mayan communities. In the years since, the EZLN's greatest weapon has not been its rifles, but its ability to disseminate information detailing the reasons for, and goals of, its actions. Confined to hideouts in Chiapas, the group's favorite communications medium has been the Internet. Through numerous e-mail communiqués, the Zapatistas have managed to turn a small insurrection in an even smaller Mexican town into a global event.

"Digital Zapatismo is one of the most politically effective uses of the Internet," said Ricardo Dominguez, who on January 4, 1994 became a founding member of the New York Zapatistas (The New York Committee for Democracy in Mexico). A recognized hacktivist, Dominguez believes that it is the EZLN's press savvy that keeps it alive. If not for the Zapatistas' ability to communicate with the outside world, he maintains, the Mexican government would have ended their insurrection by force, long ago. The Zapatistas' tactical use of e-mail and webpages has created "an electronic force field" around the Mayan dissidents, says Dominguez.

But distribution of information is not the only way that Zapatistas and their supporters have taken advantage of the Internet. In 1998, in response to the deaths of 45 Zapatista men, women, and children at the hands of Mexican paramilitary police in the village of Acteal in Chiapas, Mexico, sympathizers formed The Electronic Disturbance Theater (EDT). According to political theorist and activist Stephan Wray, who with Dominguez co-founded the Theater, the EDT is "a small group of cyber activists and artists engaged in developing the theory and practice of Electronic Civil Disobedience (ECD)."

Ricardo Dominguez, hacktivist.

The EDT has perfected the guerrilla tactic of the virtual sit-in, wherein users repeatedly hit the "Refresh" buttons on their browsers in an attempt to block access to a site. By continually calling up the website on their computers, visitors can cause a digital traffic jam that prevents anyone else from viewing the site.

Brett Stalbaum and Carmin Karasic, members of the EDT, created FloodNet, a software program that automates the process of repeatedly clicking on a Web browser's "Refresh" button. A public version of FloodNet, the Disturbance Developers Kit (DDK), is available through Wray's website.

The EDT's best-known exploit occurred on Thursday, January 31, 2002, when protestors used a tool much like Floodnet to block access to the World Economic Forum (WEF) website. According to Dominguez, over 50,000 people downloaded the application; at 10 AM EST on January 31, the WEF website crashed. The following day, the site was back in service, but WEF officials weren't certain whether the crash was a result of hacktivists or increased interest in the site. Dominguez doesn't believe hacktivists alone were responsible, saying in numerous interviews that perhaps the website's "infrastructure is as badly built as the WEF's economic vision during the last 31 years."

Cult of the Dead Cow member Oxblood Ruffin, incognito. Photo: Chris Bolin, National Post

Regardless of the success of EDT's tactics, there are those who don't believe that what the EDT does is hacktivism at all. The hacker who goes by the *nom de guerre* Oxblood Ruffin believes that the EDT is merely transplanting '60s-style street protests into cyberspace. "In the first place, I don't accept the term 'electronic civil disobedience,'" said Ruffin. "There are some things in the physical world that don't translate well into cyberspace, and this is one of them."

Ruffin is the foreign minister of the waggishly named hacker group, the Cult of the Dead Cow (cDc). Unlike the EDT, which is a social-justice group using the Internet to spread its message, the cDc is a hacker cabal hell-bent on using technology for the betterment of humanity. One of the cDc's major accomplishments is the development of a tool called Peekabooty, which allows residents of countries with strict Internet censorship to bypass that censorship and view restricted webpages.

Ruffin is especially critical of the EDT's denial-of-service (DoS) attacks. "Denial-of-service attacks, however they are positioned by the EDT, qualify as a destructive — and in my opinion unconstitutional — use of technology," he said. "[They] are a violation of the First Amendment, and of the freedoms of expression and assembly. No rationale, even in the service of the highest ideals, makes them anything other than what they are — illegal, unethical, and uncivil. One does not make a better point in a public forum by shouting down one's opponent."

Dominguez shrugs off Ruffin's criticisms, defending the EDT's mass actions as populist, versus the SWAT-like actions of hacker groups like the cDc, which look like elite paramilitary operations by comparison.

"We promote mass social performances that create a disturbance based on [the] amount of folks who participate," said Dominguez. "Our VR Sit-In tool does not and cannot destroy, disrupt or crash servers," he said, differentiating between crashing a website by hacking and temporarily blocking access to a website by conducting a virtual sit-in. "But it does create a social disturbance." To Dominguez, the significance of EDT's actions is strongly dependent on their symbolism. "The point of the Virtual Sit-Ins is to get across how widespread the protest is," he said.The EDT's activism "represents the unbearable weight of beings saying, '*Ya Basta!*' Enough is enough!" As Dominguez emphasizes, hacktivism precedes real-world action. As he puts it, "Code [alone] will not save us from some very difficult and human problems."

Setting aside the cultural politics of hacking versus hacktivism, a larger question remains: Is hacktivism legal?

Dorothy Denning
Photo: Peter Denning.
© Dorothy Denning, 2002

Dorothy E. Denning, Professor of Computer Science at Georgetown University and Director of the Georgetown Institute for Information Assurance and author of *Information Warfare and Security*, thinks hacktivism is one of three classes of activity — activism and cyberterrorism are the other two — that threaten to alter "the landscape of political discourse and advocacy."

Although she does not think activism and hacktivism are as serious as cyberterrorism, she does believe that the lines between the three are blurry. According to Denning, the question of hacktivism's legality turns on the effects of the actions taken. "I don't think it is clear whether a Web sit-in is legal or not," she said in an e-mail interview. "It may depend on the level of traffic generated against the site."

In a statement to the House Armed Services Committee Special Oversight Panel on Terrorism, in May 2000, Denning drew a distinction between Web sit-ins and cyberterrorism. "Sit-ins require mass participation to have much effect, and thus are more suited to use by activists than by relatively small groups of terrorists operating in secrecy," she said. "EDT view their operations as acts of civil disobedience, analogous to street protests and physical sit-ins, not as acts of violence or terrorism. This is an important distinction. Most activists, whether participating in a street march or Web sit-in, are not terrorists."

According to the Electrohippie Collective, actions such as those undertaken against the Israeli government are absolutely legal because they do not involve "computer abuse." In their view, such actions are undertaken by "thousands of people across many countries [using] the computer systems precisely as they are intended to be used — but coordinated in a way that causes significant disruption or closure of the services."

Information-security expert Winn Schwartau. Courtesy of nicekids.net

Legal or not, what information security expert Winn Schwartau calls "cyber-civil disobedience" is, in his estimation, "potentially highly effective." Schwartau is the author of *Cybershock* and *Information Warfare* and numerous articles on information security. In his 1995 *Information Week* article, "Would Thoreau Approve?," Schwartau writes, "Twenty-five years ago, a protest required massive organization and the physical congregation of huge numbers of people. Now, cyberspace provides the '90s alternative to conventional assembly." Cyber-civil disobedience, says Schwartau, is "the protest means of choice for the Information Age."

Although he downplays hacktivism's threat—"Floodnet attacks are disruptive, not destructive in the classic sense of the word," he writes, in *Network World Fusion*—he is wary of the notion of releasing programs such as Floodnet to the general public, calling it a "potentially disturbing event that could further empower push-button hackers." In the final analysis, however, he does not view Ricardo Dominguez as a threat: "From where I stand, [Dominguez] is a political dissident, not a hacker with an attitude of technical supremacy; he merely wants to make political statements."

Although the jury is out on the legality and ethics of their virtual protests, the actions of the Zapatistas and hacktivists offer inarguable proof that it is increasingly impossible to separate real-world social problems from our online lives.

"The Internet can be an effective tool for activism," says Denning, "especially when it is combined with other communications media, including broadcast and print media and face-to-face meetings with policy makers." Computers themselves will not solve society's problems, but to Dominguez and other hacktivists like him, they are powerful engines for social change.

This article originally appeared in ReadMe.