

October 31, 1998

'Hacktivists' of All Persuasions Take Their Struggle to the Web

By AMY HARMON

Until they declared "Netwar" against the Mexican government, Ricardo Dominguez and Stefan Wray earned their activist credentials the old-fashioned way, attending rallies in support of the Zapatista rebels, handing out pamphlets, shouting political slogans.

Now, the two New Yorkers organize "virtual sit-ins" and recruit computer programmers to attack the World Wide Web sites of any person or company they deem responsible for oppression. Their new rallying cry: "The revolution will be digitized."

Wray, 37, and Dominguez, 39, are co-founders of the Electronic Disturbance Theater. It is one of several groups around the world that are beginning to experiment with computer hacking, so far largely nuisance attacks and the equivalent of electronic graffiti, as a means to a political end.

"We see this as a form of electronic civil disobedience," Wray told a group of about 75 people who had gathered in New York's East Village for an "anti-Columbus Day" event in October. "We are transferring the social-movement tactics of trespass and blockade to the Internet."

The notion is a departure for both radical activists and hackers, whose distinct, subversive subcultures have rarely intersected until recently. In some ways, the two psychologies are polar opposites.

Hackers, while reliably anti-authoritarian, tend to limit their critique of the military-industrial complex to its imperfect computer security apparatus. Enamored of their image as the cowboys of the electronic frontier, most at least pay lip service to the hacker mantra, "information wants to be free."



Christine M. Thompson

But whatever capacity they might have to disrupt the social order has so far been largely restricted to pointless vandalism and pinching the occasional credit card number.

Political activists, on the other hand, preoccupied as they are with the power structure, have typically paid little heed to the information infrastructure on which it rests. Motivated by the desire for social change, they generally see building communities of support and cooperation as essential.

But the rapid growth of the Internet has transformed what was once a hacker playground into, among other things, a far-reaching political platform. What's more, the tricks invented by hackers have become easier for activists to learn and adopt because they are now widely published on how-to Web sites.

As a result, radical groups are discovering what hackers have always known: Traditional social institutions are more vulnerable in cyberspace than they are in the physical world. Likewise, some members of the famously sophomoric hacker underground are finding motivation in causes other than ego gratification.

In recent months, groups as diverse as the Animal Liberation Front, a militant animal-rights group; Radio4All, which supports pirate broadcasting, and international teams of teen-agers with cyber pseudonyms like Milworm and causes like anti-imperialism have increasingly begun pumping political protest through the Internet's security holes.

On Oct. 27, a day after China's human rights agency announced its new Web site, the official view of that nation's human rights record was replaced with an electronic trespasser's manifesto: "China's people have no rights at all, never mind human rights. How can the United States trade millions and millions of dollars with them and give them most-favored trade status when they know what is happening?"

Earlier in October, computer intruders scrawled "Save Kashmir" over the opening screen of a Web site that the Indian government set up last summer to provide information about the region, whose ownership is disputed by Pakistan and several separatist groups. The hacked site included photographs of Kashmiris allegedly killed by Indian forces, overlaid with the words "massacre" and "extra-judicial execution."

In June, after the Indian government conducted nuclear tests, college students in Britain and the Netherlands claimed credit for placing the image of a mushroom cloud on the Web site of India's major nuclear weapons research center.

In September, Portuguese hackers modified the sites of 40 Indonesian servers to display the slogan "Free East Timor" in large black letters, and they added hypertext links to Web sites describing Indonesian human rights abuses in the former Portuguese colony.

No slouches in packaging and self-promotion, the burgeoning computer underground has adopted a catchy term for the trend: they call it "hacktivism."

Related Articles "Hacktivism is a way to be heard by millions," a group of three Mexican hackers known as X-Ploit wrote in an e-mail

[The Hacker Myth
Crumbles at Convention](#)
(August 2, 1998)

[California ISP Says It
Tracked Teen-Agers in
Pentagon Hacking](#)
(March 10, 1998)

message to a reporter. "We want to speak out about what we and many, many people disagree with in this treasonous and corrupt government. If we protest both on line and off line, we'll have better chances to see a change."

The tactic is not limited to one end of the political spectrum. A group of Serbian computer hackers this month claimed responsibility for crashing a Web site promoting the ethnic Albanian cause in the Serbian province of Kosovo. The Serbian newspaper Blic quoted one of the hackers as saying, "We shall continue to remove ethnic Albanian lies from the Internet."

Wednesday, the group, called Black Hand, after a clandestine Serbian military organization at the turn of the century, attacked the site of the Croatian state-owned newspaper Vjesnik. Croatian hackers counterattacked the next day, inserting messages like "Read Vjesnik and not Serbian books" on the Web site of the Serbian National Library, Vjesnik reported Friday.

Guerrilla attacks on Web sites may seem more of a headline-grabbing ploy than true information warfare. But security experts said the recent spate of digital vandalism underscores the risk to companies and governments that increasingly rely on the Internet for commerce and communication.

"What this demonstrates is the capacity of groups with political causes to hack into systems," said Michael Vatis, chief of the National Information Protection Center, a new federal agency formed to protect the nation's crucial infrastructure. "I wouldn't characterize vandalizing Web sites as cyber-terrorism, but the only responsible assumption we can make is there's more going on that we don't know about."

Established by Attorney General Janet Reno this year, the center is in part a response to the perception that "political forces which could not take on the United States in conventional military terms stand a better chance on an electronic battlefield," said Vatis.

The potency of the sling-shot approach is not lost on would-be hactivists, either. "If you have 10 people at a protest, they don't do much of anything," said a Toronto-based computer jockey who calls himself Oxblood Ruffian. "If you have 10 people on line, they could cripple a network."

Oxblood is a member of Cult of the Dead Cow, a hacker group that recently reserved the Web address www.hactivism.org as an Internet distribution hub for tools to assist others in subversive digital activism. He said the group was planning to attack the Internet operations of U.S. companies doing business with China.

But the effectiveness of such actions is unclear, prompting a debate over how best to implement the hactivist brand of political protest.

Under U.S. law, terrorism is defined as an act of violence for the purpose of intimidating or coercing a government or a civilian population. And breaking into a computer system and altering data are felonies.

For that reason, the members of the Electronic Disturbance Theater emphasize that

the software they use to attack Web sites disrupts Internet traffic but does not destroy data. In the tradition of civil disobedience protests, they encourage mass participation and use their real names.

The group was forged in an online discussion among several American supporters of the Zapatistas, the first armed revolutionaries known to have solicited public sympathy for their struggle by publishing their communiques over the Internet.

On Nov. 22, the group says, it plans to attack the Web site of the School for the Americas, a U.S. Army training center for foreign military personnel, some of whom have been accused of human rights abuses.

Recent targets have included the sites of Mexican President Ernesto Zedillo and of the U.S. Defense Department.

When online activists heed the call to "commence flooding!" they visit the group's Web site and click on an icon that launches a program called FloodNet. The software points their Web browser to the target of the attack, where it requests the same page over and over again at a rate of about 10 times per minute.

This tactic is a variation of what is known in Internet security-speak as a "denial of service attack." An unusually large volume of requests will overwhelm the computer that is serving up the target's Web pages. This can cause legitimate visitors to see error messages instead of the pages they are seeking, and it can even crash the server computer.

"This isn't cyber-terrorism," insisted Carmin Karasic, a Quincy, Mass., software engineer who designed the FloodNet program. "It's more like conceptual art."

The U.S. Defense Department does not agree. Alerted to a planned FloodNet attack on its public site on Mexican Independence Day, the agency responded by diverting the requests to a nonexistent Internet address, a spokesman said.

"If it wasn't illegal it was certainly immoral -- there are other constructive methods of electronic protest," the spokesman said.

The victims of such attacks are not the only ones to criticize the digital desperados. In their quest for support from a public already suspicious of hackers and anxious about online safety, some political activists deride such methods as counterproductive.

And hackers faithful to the ethic of electronic exploration for its own sake deride Web site intrusions as the work of "script kiddies," an epithet for people who break into systems by using schemes developed by others rather than by searching out new security holes of their own. Script kiddies have been responsible for a recent surge in attacks throughout the Internet -- of which politically motivated hacks are a small fraction.



But in e-mail and telephone interviews, several hackers promoting a political agenda -- all of whom refused to give their real names -- insisted that their motives were pure.

Barbara Alper for The New York Times

Increasingly, activists have adopted computer hacking as a tool. Stefan Wray, Carmin Karasic and Ricardo Dominguez of the Electronic Disturbance Theater spoke at a panel discussion in New York this month.

"We have hundreds of servers we could hack, and we don't," said Secretos, a Portuguese hacker in his early 20's whose group, the Kaotik Team, has taken up the cause of East Timor independence. "By contrary, we even help them to fix their bugs. The main objective of our hacking pages is to transmit the message. It is not, 'We are groovy, we have power.'"

John Vranesevitch, editor of Antionline, an Internet publication that tracks hacker activities, said the apparent political awakening among hackers reflects a generation's coming of age.

"We're starting to see right now the first generation of people who have grown up on the Internet," said Vranesevitch, who at 19 counts himself among that group. "These hackers are entering the ages where people are most politically active. This is their outlet."

And some are trying to make that outlet more accessible. A 26-year-old University of Toronto dropout calling himself Perl Bailey, after a computer language popular among Web developers, said he had earned a living as a software developer and had dabbled in not entirely legal computer exploration for several years. Now, he is writing a tool to arm computer novices with basic hacktivist techniques.

"After you reach a certain point, it feels like you are dressed up with nowhere to go," he said. "I want to make people doing questionable business dealings with countries that have no respect for human rights worry that someone who doesn't have a grade school education can sit down and go click-click and create havoc. That to me is very powerful."

Amy Harmon at amy@nytimes.com welcomes your comments and suggestions.

[Home](#) | [Site Index](#) | [Site Search](#) | [Forums](#) | [Archives](#) | [Marketplace](#)

[Quick News](#) | [Page One Plus](#) | [International](#) | [National/N.Y.](#) | [Business](#) | [Technology](#) | [Science](#) | [Sports](#) | [Weather](#) | [Editorial](#) | [Op-Ed](#) | [Arts](#) | [Automobiles](#) | [Books](#) | [Diversions](#) | [Job Market](#) | [Real Estate](#) | [Travel](#)

[Help/Feedback](#) | [Classifieds](#) | [Services](#) | [New York Today](#)

Copyright 1998 The New York Times Company