C:\ HACKERS, HACKTIVISTS, & SCRIPT KIDDIES

tobias c. van Veen

Can't tell a DoS attack from a DOS prompt? Never heard of Keven Mitnick? Think that Mafiaboy was a hacker? Get it right at the circuit party and roll hard with Capital's look at the anti-leaders of the Matrix, the hellraisers of the Net..

Now, any well-honed computer geek can bring down a system with a well planned attack and a bit of bug warez. Regardless of motive or politics, hackers of all bits and bytes—anarchist, libertarian, or just plain ignorant—are worms in the bowels of governments and corporations, phreaks whose legacy and actions are all the more important in the age of digital Big Brother.

1. Hackers. From the depths of the '80s, hackers phone phreaked into root telephone directories, sneaking around in the backbone of pre-Internet networks such as Telenet, ARPANET, and other government, bank, university, and military systems to quietly free information and gain a technical understanding of the grid. The motto was to leave no trace and to circulate the information gained. Most infamous of this era was the Legion of Doom (LOD). After a series of busts throughout the '80s, the LOD and other groups were finally dissolved in 1990 when the US Secret Service shut down hundreds of BBSs, but not before phone-ringing hacker wars broke out between members of the LOD and Masters of Deception (MOD). The scapegoat for this era is undoubtedly Kevin Mitnick, who spent 10 years of his life in and out of court and jail for his involvement in the "dark side of the internet."

In an ironic twist, many hackers went on to become security experts, either privately or for the government. Hence the two terms: White Hat and Black Hat hackers. White Hat hackers are usually security admins uncovering security holes, publicizing their results for the betterment of privacy (or the increasing impenetrability of corporate and military domains) whereas Black Hat hackers crack systems, software, and codes. White Hatters are often considered "good," whereas Black Hatters are often labelled malicious, although this distinction is generally wrong. Grey Hat hackers exist somewhere in the middle, but the whole "Hat" thing is kind of silly anyway, for most "hackers" today aren't hackers at all—they're script kiddies.

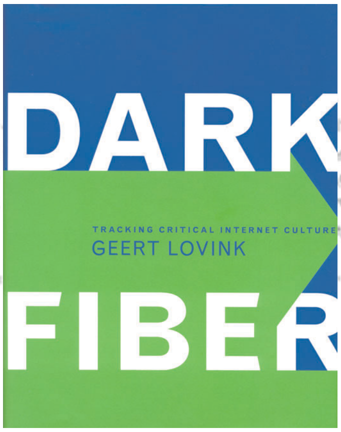
2. Hacktivists. Online activists come in two camps: Hacktivists are activists who use the Net to disseminate information and to organize through websites such as tao.ca or indymedia.org; Hacktivists are net-activists who use hacking and script techniques against corporate targets, such as Electronic Disturbance Theatre (EDT). Unlike Hackers, Hacktivists are public about their intrusions, and will conduct virtual sit-ins on the information superhighway to crash a corporate site. As this often brings down innocent routers and bottlenecks traffic, Hackers have a dislike for these public tactics, including the now well-known Denial of Service (DoS) attacks. Hacktivists, however, have been instrumental in publicizing wrongful actions: EDT's Floodnet software was used to cripple etoys.com after etoys tried to fuck over net-art site etoy.com, and EDT has held virtual sit-ins to highlight the fight of the Mexican Zapatista! rebels.

3. Script Kiddies & Graf. The problem with scripts like DoS is that almost any idiot can execute severe damage. So next thing you know you have 15 year old Canadian "Mafiaboy" bringing down CNN for about two hours, thus raising moralistic and totalitarian backlash against all "hackers." Likewise, most viruses, worms, and trojans that wreck indiscriminate havoc across the Net today are simple "script kiddy" programs that require only the most basic knowledge to run. Is this post-apocalyptic anarchy or just stupidity?

The same goes for web graff. While graffiting a web is usually a right-of-passage for the script-kiddy page (usually by uploading a page with porn and writing that says "h@x0rz oD !!!" or some other BS), it can also be used against worthwhile targets such as the infamous KKK hit. It's a tactic for the wise, but a weapon for the weak.

Dark Fiber: Tracking Critical Internet Culture

tobias c. van Veen



Geert Lovink
MIT Press 2002 | 382 pages |
$47.50 (CDN) | Hardcover
ISBN: 0-262-12249-9

Founder of the critical and political net.art discussion list Nettime.org, prominent media-access activist & Amsterdam squatter, member of theoretical group ADILKNO, Dutch hell-raiser—this is Geert Lovink, and these are his Nettime projectiles, a series of harvested essays from 1996-2001 on all things related to the Net. From the rise and fall of dotcom mania to the material access of cyberspace, from Radio B92 Belgrade and the Kosovo War to the dreams and failures of the Next Five Minutes internet conferences, Lovink offers a technologically savvy, theoreticallly tight, and—perhaps surprisingly—easily readable collection of "net.criticism," a practice he practically founded. Lovink is possessed with a thieve's ability to remix predilections for anarcho-theorists such as Hakim Bey and technological determinists such as Friedrich Kittler with observations on the technical specifics of internet protocols and the qualitative analysis of net.culture. He executes each trajectory with a quick wit of sharp keystrokes and straightforward soundbytes. One of few "intellectuals" who grasps the potentiality of the Net without subsuming it under outdated models (such as semiotics, metaphysics, or simulacra), Lovink navigates the curves of the Net on its own terms: virtual & fast. Theory & analysis at the speed of the Net. The question thus remains: is not a printed volume somewhat arcane? This text shines when it operates as an archival guide to today's digital dilemmas; to take this as a current manifestation of net.criticism would be a mistake. Its tactical transmissions serve as signposts that trace the growth and increasing corporatization and surveillance of the Net. Lovink offers analyses & tactics—while considering the positioning of these terms. And Geert's got guts, switching registers from a hacker conference one weekend to a rave the next (although he assures me that he's "not a raver"). For example, while discussing the work of Toronto-based independent news and political collective Tao.ca and the concurrent rise of indymedia.org, he ties in theorizations of the TAZ (Temporary Autonomous Zone) with the pragmatic organisation of Temporary Media Labs.

Critically, Lovink explores careful analyses of micropolitics that draw upon tht theories of Gilles Deleuze and Félix Guattari. He maps the successes, the failures, and—perhaps the best insight—the wrong turns. For example, he notes how "[The] TAZ was boiled down to a late 1980s concept, associating the Internet with rave parties" (239). The opposite can also be true: rave parties were boiled down to TAZs. As Lovink later notes, "Riots, raves, and other temporary autonomous experiences grow out of the desire to share directly, without mediation. In certain cases media have to be literally abandoned" (279). Lovink's missives are not only of media, but of that space where media meets meat: postcards from the digital divide. My only criticism of this volume—besides a desire to engage with Lovink's theories and methodology, which would overflow our space here—is that the copy-editing is the worst I have ever seen. Spelling and grammatical mistakes are found on practically every page. Whether trying to glasp the spleed of the Net or just prain laziness on behalf of MIT Prees is hard to spell.