

Ghosts in the Machine: The Impact of Hacktivism

Thomas Ling

Hacktivism is the combination of hacking with activism – the (mis)use of computer systems, often via the Internet, to achieve political objectives. It is distinguished from 'on-line activism', the use of the Internet to facilitate activism in the real world, and cyberterrorism, causing harm or fear in a population, though these areas overlap (1,2).

Hactivists have many tools at their disposal. As on-line activists, they may simply use the Internet to communicate

attack against the main Scientology website (4). Anonymous later declared 'war' on the Church of Scientology, citing the "misinformation; suppression of dissent; ...litigious nature" of the Church as its motivation, and stating their intention to "expel [the Church] from the Internet and systematically dismantle [it] in its present form". Real-world protests have also taken place, and it seems that with growing sympathy for their cause, Anonymous have decided to focus on legitimate forms of protest (5).

In the UK, hacking is prohibited by the Computer Misuse Act (1990), which forbids gaining "unauthorised" access to computer material (6). Changes to this Act in 2006 explicitly outlawed denial-of-service attacks, which had previously been a legal grey area (7). So how can such attacks be justified? Notably, a group called the Electrohippies has argued for the ethics of 'client-side' attacks, in which tens of thousands of participants (rather than a few individuals) are required to successfully shut down a website (8). Others respond that denial-of-service attacks violate freedom of expression, whatever their motivation, and the real question is when, if ever, that freedom can be withheld (2).

Hactivism will likely continue to accompany real-world conflict as communication via the Internet becomes ever more important. However, its long-term effectiveness is questionable. The illegal forms of protest it covers may do more harm than good to an activist cause. Countermeasures also exist; for denial-of-service attacks, the capacity of a web server to deal with attacks can be increased, or the target website may be held in multiple locations, making it very difficult to block access to all the 'mirrors' (1). Since much more commitment and personal risk is involved in a real-world protest than a virtual sit-in, hacktivism may come to be seen as a cowardly method of protest and hactivists stereotyped as computer-obsessed teenagers. Ultimately, for both good and ill, the ghosts in the machine will not rest as long as there are causes worth fighting.

Thomas Ling is a 2nd year reading Medicine at Emmanuel College. He is currently an Associate Editor for The Triple Helix, Cambridge.

References:

1. Denning, D., *Activism, Hacktivism, and Cyberterrorism*, 1999 www.iwar.org.uk/cyberterror/resources/denning.htm
2. Thomas, J., *Ethics of Hacktivism*, 2001 www.giac.org/certified_professionals/practicals/gsec/0530.php
3. Dreyfus, S. *Underground Chapter 1* 1997 www.xs4all.nl/~suelette/underground/justin/chapter_1.html
4. ABC News, *Hackers Hit Scientology with Online Attack*, 2008 abcnews.go.com/Technology/GadgetGuide/story?id=4194143
5. Anonymous, *Why We Protest*, 2008 www.whyweprotest.net/more-about-anonymous/
6. *Computer Misuse Act*, 1990 www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1
7. U.K. *Outlaws Denial-of-service Attacks*, www.news.com/2100-7348_3-6134472.html
8. Electrohippies, www.fraw.org.uk/download/ehippies/op-01.html



with other activists, for example to organise rallies and disseminate information. Some go further and commit acts of dubious legality. Denial-of-service attacks disrupt operations or prevent access to target websites by generating so many visitors to the website that it cannot function (called a "virtual sit-in"). E-mail bombs prevent communication by sending thousands of useless email messages to their targets. Worms and viruses are programs which multiply and spread from computer to computer; they can destroy data and disrupt operations. And of course hackers can gain control of a system, perhaps to modify the content of websites (often to display propaganda or otherwise-censored information); steal, change, or destroy data; or interfere with services controlled by the system (2). If the targeted system controls, for example, a public utility such as a water treatment plant, there may be casualties. Hactivists may be separated from cyber-terrorists by their intentions, but in terms of potential impact there is no difference between them.

An early case, in 1989, is the WANK worm, the first major worm carrying a political message. The worm initially infected a computer network at NASA's Goddard Space Flight Center, displaying an anti-nuclear message, and pretending to destroy information. It was an apparent attempt to stop the launch of the Galileo space probe, which was powered by plutonium and sparked protests over the use of nuclear material in space (3).

Hactivists have staged virtual sit-ins to publicise the Zapatistas' cause in Mexico; disrupted NATO and Serbian computer systems in the Kosovan War, and in Israel and Palestine; defaced US government websites after the accidental bombing of a Chinese embassy; disabled censorship on Chinese web servers; and forced the removal of a website representing the Basque separatist organisation ETA (2).

Most recently, a hactivist group called 'Anonymous' have targeted the Church of Scientology. On 18th January 2008 Anonymous launched a successful denial-of-service