Global Information Assurance Certification Paper

Ethics of Hacktivism

Julie L.C. Thomas

January 12, 2001

What is Hacktivism?

"HACKTIVISM: a policy of hacking, phreaking or creating technology to achieve a political or social goal."[1]

This is the definition proffered by one of the groups who can be said to be at the leading edge of the fight, Cult of the Dead Cow. The members of Electronic Disturbance Theater present themselves as the major proponents of electronic civil disobedience and describe it thus: "The same principals of traditional civil disobedience, like trespass and blockage, will still be applied, but more and more these acts will take place in electronic or digital form."[2] Professor Dorothy Dunning of Georgetown University defines hacktivism as "…[T]he convergence of hacking with activism, where 'hacking' is used here to refer to operations that exploit computers in ways that are unusual and often illegal, typically with the help of special software ('hacking tools'). Hacktivism includes electronic civil disobedience, which brings methods of civil disobedience to cyberspace."[3]

Hacktivists claim that the roots of hacktivism can be traced to the roots of civil disobedience itself, the classic work On Civil Disobedience by Henry David Thoreau.[4] Hacktivists claim that they are doing no more and no less than following in the tradition of Gandhi and Martin Luther King, Jr., by attempting to bring about social change through non-violent means. Whereas activists in the past trespassed and blockaded physical positions of power, hacktivists now would seize control of the new positions of power—cyberspace—and without all those nasty guns, water cannons, dogs, billy clubs, tear gas, etc.

Hacktivism is often confused with and overlaps with on-line activism and/or cyberterrorism. Boundaries between the three areas are necessarily blurred depending on one's definition of concepts such as "damage", however distinctions may be drawn in terms of some rather sweeping generalities. On-line activism can be defined as non-disruptive and legal; hacktivism is intended to be disruptive, though usually not damaging, and may or may not be illegal; cyberterrorism is intended to be not only disruptive, but also damaging, and is probably illegal. On-line activism is simply activist activities taking place via the Internet: the Bluewater Network,[5] for example, wages a continual campaign against personal watercraft and snowmobiles in national parks on-line. They advocate electronic and written communication with relevant governmental officials on a person-to-person basis. They distribute status reports, alerts, calls-for-action, addresses and phone numbers via an electronic newsletter. No one could argue that there is anything illegal involved in these actions. On-line activism could become hacktivism, however, if an organization were to advocate that all their supporters should e-mail multiple copies of a protest letter to several officials with the intent that their

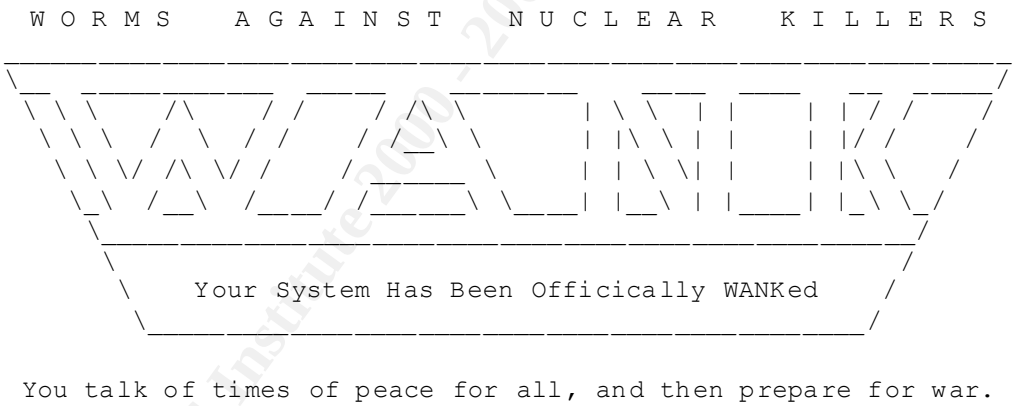
electronic mailboxes would be filled with messages. The mailserver might then crash and, therefore, unable to receive messages from those holding differing opinions. Cyberterrorism can be described as the use of hacking activities to commit terrorism, *i.e.*, "(threats of) violent action for political purposes."[6] The technique of mail-bombing described above would turn from hacktivism to cyberterrorism if the mailserver in question were also providing 911 service to the surrounding community. Crashing the server could then result in the loss of life or property.

The Hacktivism Toolbox

Common hacktivist techniques are computer break-ins, including website defacement as well as worm and virus infections; and denial-of-service attacks (DoS), including website sit-ins and e-mail bombings.

Computer Break-ins

One of the earliest documented cases of hacktivism computer security compromise is the WANK worm attack on the Goddard Space Flight Center. A worm is a self-replicating program that infects computers over a network. The goal of the WANK work was to stop the launch of the shuttle carrying the Galileo space probe. On October 16, 1989, users at Goddard were greeted with the following banner:



The work attack did not stop the shuttle launch, but recovery from the attack did require a massive expenditure of money and effort.[7]

More recently, several hacktivists have launched attacks against the Chinese government to protest government censorship of Internet content. A group known as the Hong Kong

Blondes claims to have hijacked a Chinese communication satellite.[8] This attack would have the potential to affect the operations of Chinese governmental and military institutions, as well as foreign countries doing business in China. Two hackers known as Bronc Buster and Zyklon also compromised a firewall system in China, allowing Internet users in that country unrestricted access to the Web for a brief period of time.[9] They also defaced several Chinese governmental websites.

Website defacement has been a weapon of choice in recent global conflicts. During the war in Kosovo and, more recently, in the Israeli-Palestinian conflict both sides have attacked the other's governmental and private websites to tell their versions of the truth. The AntiOnline website maintains an archive of such hacked websites. Among them are Yugoslavian sites that were altered by Dutch hackers Meestervervalser and Xoloth1 of www.dutchthreat.org (now-defunct) to display pro-NATO sentiments.[10] Likewise, Serb hackers altered NATO websites.[11] In the Israeli-Palestinian crisis both sides traded cyber volleys as the Hebrew University and Netanya Academy websites were replaced with diatribes against Israel, the United States and the Arab governments.[12] Israeli hackers targeted the Hizbollah Party webserver and the Politics Forum of Albawaba with other methods such as denial-of-service attacks and message bombing.[13]

Denial-of-Service

A web sit-in occurs when the attackers generate a sufficient volume of traffic to a website such that no legitimate traffic can access the site. What is generally accepted as the first web sit-in is the 1995 attack by a group known as the Strano Network against the French government in response to their nuclear and social policies.[14] On December 21, 1995, the Strano Network organized a Net-Strike attack that lasted an hour. At the appointed time, collaborators worldwide pointed their browsers at various governmental websites and continually reloaded the sites. It was reported that the attackers were successful in rendering some websites unreachable for that period of time.

A more well-known web sit-in was organized by the Electronic Disturbance Theater in 1998. EDT is "a small group of cyber activists and artists engaged in developing the theory and practice of Electronic Civil Disobedience (ECD)."[15] The developmental work done by members of EDT provided an important milestone in the execution of electronic civil disobedience. The web sit-in in 1998 was the first to utilize a tool called FloodNet. FloodNet was developed by Carmen Karasic and Brett Staulbaum of EDT. The software allows users to go to EDT's website at click on an icon. The icon launches FloodNet against the target website, accessing the site approximately 10 times per minute. The web sit-in initiated by EDT on September 9, 1998, was directed at the Mexican presidency, the Pentagon, and the Frankfurt Stock Exchange. The targets were chosen to support the Mexican guerrilla group called Zapatistas, protest the United States military, and protest a symbol of international capitalism. EDT reports that 20,000 people accessed FloodNet during the two days of September 9 and 10.[16] EDT released FloodNet to the general population on January 1, 1999. It is now part of the Disturbance Developer Kit.[17]

While e-mailbombing has, in all likelihood, been in existence as long as e-mail has been in existence, the first generally recognized incident of e-mail bombing by a terrorist organization occurred in 1998. An offshoot of the Liberation Tigers of Tamil Eelam launched an e-mail bomb attack against the mail servers of Sri Lankan consulates. The message read "We are the Internet Black Tigers and we're doing this to disrupt your communications."[18] Servers in Seoul, Ottawa, and Washington, D.C., were crashed.[19] The attack achieved the goal of generating a level of fear in the victims. William Church, an authority in the study of warfare, responded to the attack by saying that cyber warfare was preferable to real warfare and encouraged the Tigers to continue electronic attacks to the exclusion of attacks on real people.[20]

The Ethics of Hacktivism

A well-known incident in which hacktivists achieved their goal is the combination of mailbombing and denial-of-service (DoS) attacks that forced the Internet service provider Institute for Global Communications (IGC) to remove the website for the Euskal Herria Journal (EHJ), a Basque separatist publication.[21] After a militant branch of the Basque separatists murdered a popular politician in northern Spain, IGC was flooded with demands that the website be removed. The demands escalated into calls for mailbombings and DoS attacks. At one point a Spanish newspaper, *El Pais*, supported the mailbombing activity and listed e-mail addresses for IGC. After a sustained attack over a period of several days, IGC reluctantly removed the EHJ site.

IGC had a second response to the mailbombing and DOS attacks, however, that focused attention on the ethics of the attacks. The issue at the heart of IGC's response was freedom of expression. IGC's first step was to draw attention to the fact that the attacks were taking place. Their goal was to emphasize that if IGC could be forced to remove content that some users found objectionable, any ISP anywhere could face a threat from similar tactics. IGC also published their own response on their server. After being forced to remove the EHJ website, IGC replaced it with a site of their own,[22] protesting the attacks. IGC further organized against what they perceived to be an attempt to censor the content of their hosted websites. IGC received support from numerous anti-censorship organizations including NetAction, Computer Professionals for Social Responsibility, the Electronic Frontier Foundation, and UK-based Cyber-Rights and Cyber-Liberties.[23] IGC also received statements of support from their parent organization, the Association for Progressive Communications (APC),[24] as well as APC partners globally, including those in Spain. One statement from a Brazilian group equated the mailbombing of IGC with "burning a bookstore to protest a book."[25] Finally, IGC ensured the continuing survival of the EHJ website by arranging for the site to be hosted and mirrored by several other servers worldwide.[26]

In the statements of support for IGC described above, IGC's defenders decried the mailbombing and declared that censorship is unacceptable, regardless of the source. Audrie Kraus, Executive Director of NetAction stated, "The mailbombers need to know that vigilante censorship is just as unacceptable as government censorship."[27]

Instituto Brasileiro de Análises Sociais e Econômicas (IBASE) condemned that action of the militant Basque separatists, Euskadi Ta Askatasuna (ETA), but also denounced the attack on IGC for interrupting the Internet service to the other 13,000 IGC customers. "While IBASE joins its protest with thousands of people horrified by the brutality of tactics such as the ones adopted by ETA…it cannot endorse any terrorist response which affected thousands of legitimate civil society groups and communities legally struggling for just sustainable development, social justice and human rights."[28]

Computer Professionals for Social Responsibility (CPSR) also spoke on behalf of freedom of expression and against the burden that mailbombings and DDoS attacks place on ISPs and their surrounding networks. "We simply support the rights of organizations to carry on electronic communications without deliberate disruption, and the right to freedom of expression…We also condemn denial-of-service attacks in general. Not only are they an undemocratic way of trying to censor a particular speaker, but they misuse the Internet by weighing down a Internet provider and the networks through which the attacks pass, thus forcing users across the Internet to pay for the attack and suffer some of its consequences."[29]

The issue of free speech has also come up in a debate between the proponents and opponents of FloodNet. After FloodNet was released to the general population (see above) it was rapidly installed and utilized by many hacktivist groups. One group that has made extensive use of FloodNet and other DoS techniques is *the electrohippies collective*, the self-proclaimed "Headquarters for Electronic Civil Disobedience (ECD)."[30] Since acquiring FloodNet *the electrohippies* have launched an attack (called an "action") in early December of 1999 protesting the World Trade Organization. Another attack was planned in early April of 2000 protesting genetically modified crops, however this attack was called off after a vote on their website failed to return a simple majority in favor of the attack.[31]*Theelectrohippies* prepared a defense of their actions in which they compare distributed denial-of-service (DDoS) attacks to Jesus' attack on the merchants in the temple: "As Jesus ransacked the temple in Jerusalem because it had become a house of merchandise, so the recent attacks on e-commerce web sites are a protest against the manner of it's [sic] recent development."[32] *The electrohippies* describe the Internet as a "public space" which is being exploited by the "unsustainable consumerism" of e-commerce, and defends DoS attacks as a potential means to restore the Internet to "the more philanthropic basis of the 'Nets [sic] original use."

The electrohippies distinguish between a "server-side" DDoS attack and a "client-side" DDoS attack. A server-side attack is the result of a small number of anonymous people "abusing the routers of web servers to generate huge numbers of incomplete requests." A server-side attack, they claim is "[e]ffective, but the manner of the action, and it's [sic] covert nature…mean that it does not have any particular democratic legitimacy." A client-side DDoS attack, on the hand, according to *theelectrohippies*, arises from a mandate from the masses: "Our method has built within it the guarantee of democratic accountability. If people don't vote with their modems (rather…than voting with their feet) the action would be an abject failure."

The electrohippies acknowledge that DDoS attacks and web sit-ins violate the First Amendment, both in terms of restricting freedom of speech and freedom of association. They state, however, that it is justified when "the acts or views perpetrated by the targets of a [D]DoS action must be reprehensible to many in society at large, and not just to a small group." A DDoS attack launched by *the electrohippies* follows the guidelines of proportionality, substitution for the deficit of speech, openness, and accountability. A DDoS attack is acceptable, they claim, if it does not "disrupt the communications of an organisation on a general basis" and focuses attention on a single issue, rather than the organization as a whole, *i.e.*, proportionality. The instigators of the attack, furthermore, should provide information on both sides of the contested issue so that participants in the attack are well educated, *i.e.*, substitution for the deficit of speech. Finally, all participants in the attack should provide their real names, *i.e.*, openness and accountability.

Other hacktivists, however, are of the opinion it is never acceptable to violate another's First Amendment rights, regardless of motive. Oxblood Ruffin, a member of Cult of the Dead Cow, offered a rebuttal to *theelectrohippies*' paper on client-side DDoS attacks. In it he states that "Denial of Service attacks 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. Say something more intelligent or observe your opponents' technology and leverage your assets against them in creative and legal ways."[33] He further takes issue with *the electrohippies* assertion that the number of people participating in an attack establishes its legitimacy. He compares a server-side attack versus a client-side attack in terms of the difference between "blowing something up and being pecked to death by a duck."[34]

The issues at the heart of hacktivism appear to be the same issues that are at the heart of activism and civil disobedience in the physical world. If a building is blockaded by protestors, is it civil disobedience or infringement on freedom of assembly? Is a book burning activism or censorship? And, finally, when are causes more important than rights? An added dimension in cyberspace, however, is the character of the protestors, and the relative values of skill versus participation. Some hacktivists claim that the ease, relative safety, and non-violent nature of virtual sit-ins and mailbombings encourage the apathetic, fearful, and technologically non-savvy masses to raise their voices in protest. Tools such as FloodNet allow everyone with a computer to participate in the processes governing our world and make their opinions heard. On the other side are those who support the rights of freedom of expression and assembly on the Internet. They call virtual sit-in participants cowards, claiming that it takes neither commitment nor courage to hit "reload" on a browser. Often present in such claims is the one-upsmanship that is the lifeblood of the hacker community. This mandates that if one were a "real" hacker activist one would use one's own formidable hacking skills to right the wrongs of this world. Hacktivism, then, as with any social and political change, comes down the age-old question of whether the end justifies the means.

References

[1]Cult of the Dead Cow on the now-defunct website URL: http://www.hacktivism.org as reported in "Underground View" Underground View is a quarterly column written by the Research, Outreach Strategy and Engineering (ROSE) Group of ICSA Inc. URL: http://www.infosecuritymag.com/feb99/underground.htm. (January 3, 2001)

[2] Wray, Stephan. "The Electronic Disturbance Theater and Electronic Civil Disobedience." June 17, 1998. URL: http://www.thing.net/~rdom/ecd/EDTECD.html. (January 3, 2001).

[3] Denning, Dorothy E. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." February 4, 2000. URL: http://www.nautilus.org/info-policy/workshop/papers/denning.html (January 3, 2001).

[4] Wray, Stephan. "On Electronic Civil Disobedience." March, 1998. URL: http://www.thing.net/~rdom/ecd/oecd.html. (January 12, 2001.)

[5] URL: http://www.bluewatenetwork.org

[6] URL: http://dictionary.cambridge.org/define.asp?key=terrorism*1%2B0. (January 4, 2001).

[7] Dreyfus, Suelette. *Underground*, Mandarin, Australia, 1997.

[8] Paquin, Bob. "E-Guerrillas in the Mist." The Ottawa Citizen June 16, 1999. URL: http://www.infowar.com/hacker/99/hack_061799a_j.shtml. (January 8, 2001).

[9] Farley, Maggie. "'Great Firewall' breached." Los Angeles Times, 1999. URL: http://www.vinsight.org/1999news/0105.htm. (January 9, 2001).

[10] URL: http://www.AntiOnline.com/archives/pages/www.carbo.co.yu/; URL: http://www.AntiOnline.com/archives/pages/www.italsrem.co.yu/; and URL: http://www.AntiOnline.com/archives/pages/www.pentagon.co.yu/. (January 12, 2001).

[11] Brewin, Bob. "Kosovo Ushered in Cyberwar." Federal Computer Week, September 27, 1999. URL: http://www.fcw.com/pubs/fcw/1999/0927/fcw-newscyberwar-09-27-99.html. (January 12, 2001).

[12] Salem, Fadi; Jarrah, Fawaz. "Israeli Palestinian Clashes Spur Hacking Attacks." Dabbagh Information Technology, October 18, 2000. URL: http://www.dit.net/itnews/newsoct2000/63.html. (January 12, 2001).

[13] *ibid*.

[14] Denning, Dorothy E. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." URL: http://www.nautilus.org/info-policy/workshop/papers/denning.html, (January 3, 2001), citing information provided to

the author from Bruce Sterling; Winn Schwartau, *Information Warfare*, 2nd ed., Thunder's Mouth Press, 1996, p. 407.

[15] Reference 2.

[16] Wray, Stephan. "Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics." November, 1998. URL: http://www.nyu.edu/projects/wray/wwwhack.html. (January 3, 2001).

[17] Available at URL: http://www.fakeshop.com/product_98/flood.html.

[18] "E-Mail Attack on Sri Lanka Computers," Computer Security Alert, No. 183, Computer Security Institute, June 1998, p. 8.

[19] Wolf, Jim. "First 'Terrorist' Cyber-Attack Reported by U.S." Reuters, May 5, 1998.

[20] Denning, Dorothy E. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." URL: http://www.nautilus.org/info-policy/workshop/papers/denning.html, (January 3, 2001), citing CIWARS Intelligence Report, May 10, 1998.

[21] Mason, Maureen. "IGC Fights Digital Censorship: Basque Website Attacked by Internet Mailbombers." 1997. URL: http://members.freespeech.org/ehj/html/igcehj.html. (January 9, 2001).

[22] URL: http://www.igc.org/ehj. (January 9, 2001).

[23] "Statements of Support for IGC." Institute for Global Communications, 1997. URL: http://www.igc.org/ehj. (January 10, 2001).

[24] Afonso, Carlos. "APC Statement on Mail Bombing as a Method of Political Protest." July 7, 1997. URL: http://www.apc.org/english/press/archive/apc_p013.htm (January 9, 2001).

[25] "IBASE condemns cyberterrorism against IGC." Instituto Brasileiro de Análises Sociais e Econômicas, July 22, 1997. URL: http://www.igc.org/ehj. (January 10, 2001).

[26] URL: http://members.freespeech.org/ehj; URL: http://www.contrast.org/mirrors/ehj/; URL: http://osis.ucsd.edu/~ehj to name a few

[27] Kraus, Audrie. "Statement from NetAction (San Francisco, California)." July 18, 1997. URL: http://www.igc.org/ehj. (January 10, 2001).

[28] Reference 20.

[29] "Statement from Computer Professionals for Social Responsibility (CPSR)." Computer Professionals for Social Responsibility, July 29, 1997. URL: http://www.igc.org/ehj. (January 10, 2001).

[30] URL: http://www.gn.apc.org/pmhp/ehippies/index.html. (January 4, 2001).

[31] "I-Defense and the Internet 'Thought Police': Misrepresenting the Facts to Create Media Panic." *the electrohippies collective*, April 6, 2000. URL: http://www.gn.apc.org/pmhp/ehippies/archive/communiques/communique-2000-04-h.html. (January 8, 2000.)

[32] DJNZ (an alias) and the action tool development group of *the electrohippies collective*. "Client-side Distributed Denial-of-Service: Valid campaign tactic or terrorist act?" February, 2000. URL: http://www.gn.apc.org/pmhp/ehippies/archive/papers/occasional-01-ddos-h.html. (January 4, 2001).

[33] Oxblood Ruffin (an alias). "Hacktivismo." July 7, 2000. URL: http://www.cultdeadcow.com/hacktivismo.html. (January 5, 2001).

[34] *ibid*.

See also: Dadok, Eva. "Hacktivism – A Free Form of Expression or a Digital Vandalism?" December 1, 2000. URL: http://www.sans.org/infosecFAQ/hackers/hacktivism.htm. (January 11, 2001).

I would like to thank Professor Dorothy Denning of Georgetown University for reveiwing this paper and offering useful suggestions.