2009

Culture Jamming: From Activism to Hactivism

Kay Hearn
Edith Cowan University

Rachel J. Mahncke
Edith Cowan University

Patricia A. Williams
Edith Cowan University

Originally published in the Proceedings of the 10th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 1st-3rd December, 2009

Culture Jamming: From Activism to Hactivism

Kay Hearn[1], Rachel J Mahncke[2] & Patricia A H Williams[2]
[1] School of Communications and Art
Edith Cowan University
Perth, Western Australia

[2] SECAU Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia

Abstract

A new kind of Internet threat has emerged. Hacking is increasingly being used as a weapon by individuals to promote their political ideologies by engaging in distributed citizen-based warfare. Their aim is to disrupt communications using internet enabled networks and organisations. Examples of these online assaults during 2009 were evident during the Iranian protests and the Melbourne International Film Festival. Such attacks use denial of service techniques and utilised social networking websites such as Facebook, Twitter and You Tube to post links to access hacking instructions. Posts on social networking websites and news stories from a variety of sources online, including official Chinese news websites and news sources from Australia, the United States of America and Britain, were extensively analysed. Medium theory has been used to framework the case studies as it assumes that tools such as the Internet are not neutral and are subject to human agency, and as such is useful for exploring the ways in which the medium has been employed for political purposes by groups outside of governments. An emerging trend for individual activists to engage in new Internet enabled technologies, such as social networking websites, to distribute their political ideologies and engage in online assaults. Hacktivism is justified by these individuals in the interests of promoting freedom of speech, as they perceived that global political or corporate superpowers have denied them this basic human right. Individuals have decided to harness the power of the global Internet medium to express opinions and to promote political ideologies. This new citizen-based warfare is a powerful weapon. In the case of the hack attacks on the Melbourne International Film Festival the hackers' message was consistent with the position of the Chinese Communist Party, and their line on the Uighur minority in Xinjiang province. The Internet has provided a new frontier for activists to develop powerful distributed strategies, such as hactivism, as a weapon to challenge political ideologies. The consequences of the development of the Internet and harnessing its global reach are increasingly challenging international relations, as was demonstrated during the Melbourne Film Festival. The hackers are in a sense really hacking to support the hegemonic practices of their respective countries, and that this kind of activity represents a new form of civic participation in international relations.

Keywords

Hactivism, hacking, activism, culture jamming, information warfare, cyberterrorism, social networking, Twitter.

INTRODUCTION

A new kind of Internet threat has emerged (Diebert & Stein, 2003). Hacking as a weapon is increasingly being used by individuals to promote their political ideologies by engaging in distributed citizen-based warfare. Hactivists, and associated with this is cyber- terrorists, have not yet posed a significant threat on the Internet, however as they become more organised and the tools for utilising this global network become more sophisticated, the use of this conduit for communication will have far reaching effects (Denning, 2001a). Whereas activism is defined as non-disruptive use of the Internet for ideological purposes, hactivism uses the tools of hacking to promote activists causes in a disruptive but not-serious or violent manner. Alexandra Samuel (2004) describes Hactivism as "a portmanteau of hack and activism, the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. These tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, virtual sabotage, and software development."

The progression of hactivism is to cyberterrorism, where politically motivated hacking is used to create loss of life and economic havoc. All three of these are collectively known as part of the new netwar era (Arquilla & Ronfeldt, 2001). “Hactivism is the fusion of hacking and activism; politics and technology” (metac0m, 2003). Hactivism is also now referred to as electronic civil disobedience and digital culture jamming. It is attractive to hactivists because of its global visibility, difficulty in prosecution and the low cost of operation (Denning, 2001). This paper discusses the concept of culture jamming and its link to hactivism and analyses two case studies involving political hactivism, and discuss how hacking was used as a means of social activism. In the case studies covered in this paper the attacks were spontaneous responses to political events.

THEORY

The theoretical framework used for this paper is medium theory and in particular the work of Harold Innis (1951). Medium theorists (Carey, 1989; Comor, 2001; Deibert, 1997; Drache & Beyer, 1996; Innis, 1951; McLuhan & Fiore, 1967) that the introduction of a new form of communications technology into a society will directly affect and alter a country and/or culture both socially, cognitively, economically, and politically. Innis was concerned with the interaction between the interests of those who controlled the flow of knowledge and the vehicle for the dissemination of information. Innis (1951) argued that communications technologies are used to exert influence over time and space, and that they are subject to the interests of a particular group who, in his words, represent a ‘monopoly of knowledge’. Primarily, Innis (1951) was concerned with the impact and challenges that new forms of communications had on existing power relationships. The use of this framework also allows for a centre margin analysis of the interaction between different groups and their use of the Internet as a means of challenging network security.

CULTURE JAMMING

Hacking is one form of culture jamming (Klein, 2000, p.281). Culture jamming is defined as “the manipulation of the mass media by artists and activists. The intent, in most cases, is to critique the medias manipulation of reality, lampoon consumerism, or question corporate power” ("Fontana Dictionary of Modern Thought," 2000). Culture jamming has involved “billboard banditry” by the defacing of billboards to produce a new meaning that undermines the advertisers’ intention (Cammaerts, 2007, p.71). This action constitutes political activism in its intention, rather than vandalism, though it may be viewed as vandalism. Adbusters is a good example of culture jamming as their website demonstrates the way in which culture jamming can be used to create alternative meanings or counter hegemony. Some may view all kinds of vandalism as a form of activism, even if the act was not intentionally political.

The main target of culture jamming has been multinational corporations which have targeted their practices in globalisation. The intention is to subvert and challenge the power of these corporations and in a sense exposes what the corporations subject the general population to. Hacking, or hactivism, is used to disrupt services and is also a tool in raising awareness. Hactivists may also use malicious software to spread their message. Depending on one’s perspective, hacking can be viewed as vandalism, whether or not the reasons for doing so are justified. In this sense hacking is always considered to be illegal and unethical. Hacking can be referred to as digital activism, electronic civil disobedience, hactivism, or cyber terrorism, depending on who is doing the hacking and to whom.

Firstly though, it is useful to discuss the individuals involved in the hacking. The Texan, USA based Cult of the Dead Cow (CDC) (Cult of the Dead Cow, 1984) is a predominant media website which is similar in some ways to Adbusters although their focus is based upon privacy and access to information as a basic human right. Access to Information empowers people to make informed decisions. Philosophically, the two organisations have a lot in common with Electronic Frontier Foundation and John Perry Barlow (1996), who wrote a “Declaration of Independence for Cyberspace” and is based on libertarian notions of free access to information and the idea that governments have no right to stifle free speech on the Internet. The CDC is also a leading developer of privacy and security tools, which are offered free to the public (Cult of the Dead Cow, 1984). The CDC participates in several other groups including the Ninja Strike Force and Hactivismo.

Hacktivismo is an international group of hackers, human rights workers, lawyers and artists that have evolved out of the CDC. Hactivismo assumes as an ethical point of departure the principles enshrined in the universal declaration on human rights and the international convention on civil and political rights (ref). They also support the free

software and open-source movements. Through CDC, Hactivismo has distributed Hactivismo, and the CDC has targeted Islamic states. The CDC, Etoy and Electric Hippies are to name a few organisations of many who similarly participate in hactivism. There is debate internally within these groups regarding what is considered to be acceptable ethical behaviour with regard to hacking activities.

CDC has launched a number of campaigns aimed at exposing censorship of the Internet in the Peoples Republic of China. It is often noted that China has the most restricted Internet service in the world (Deibert, Palfrey, Rohozinski, & Zittrain, 2008, p.263). The case studies presented in this paper represent a small number of incidents and activist groups that are active in the area of hactivism.

REAL WORLD EXAMPLES

Iranian Protests

During the Iranian protests in June 2009, the Internet and specifically Facebook, Twitter and You Tube were critical in communicating messages to organise the protests. The riots were in response to the official election result, where the incumbent conservative prime minister was re-elected. The result was disputed by many Iranians and international observers. Iran has one of the most extensive Internet filtering systems in the world and is marked by aggressive online censorship policies (Deibert et al., 2008, p.292). An estimated 7.2 million people were connected to the Internet in Iran in 2006 (Deibert et al., 2008, p.293). Facebook was used extensively by the opposition and was unblocked in February 2009 only to be shut down again by May 2009 during the run up to the elections ("Iran's Facebook access restored," 2009; Iran blocks Facebook," 2009). Facebook was used by activists and anti-government voices to organise massive political rallies and used to debate political opinion ("Iran's Facebook access restored," 2009).

Twitter was also used extensively by pro-democracy activists to spread information on how to bypass proxy server restrictions. The response to the Iranian protests by activists and hactivists was spontaneous and the use of Twitter was extensive. A “Cyberwar Guide for Beginners” (Doctorow, 2009) emerged to provide more detailed information on how to further protect the identities of Iranian protestors using the service and to make people aware of the tactics used by Iranian authorities to curb the use of the Internet by dissidents. The flexibility and adaptability of citizen-based intelligence networks (Diebert & Stein, 2003).

Hacking also became part of the tactics used by protestors to disrupt the government. The call to hack, news outlets and government web sites was posted to Twitter ("Internet brings events in Iran to life," 2009). Further links were posted to websites detailing instructions on how to disable or disrupt official government websites (Shachtman, 2009). The American President Obama requested after the election that scheduled maintenance shutdown of the Twitter site be postponed ("US asked Twitter to stay online after Iran vote," 2009). Research conducted indicated that most of these messages and links to hacking tools and proxy server exploits came from the western countries and in particular the United States of America. Hactivists found a way to turn their “collective power and outrage into a serious weapon that could be used at will, without ever having to feel the consequences” (Shachtman, 2009). The hactivists had found a way to practice distributed citizen-based warfare (Burton, 2009).

There was however ethical debate amongst supporters on Twitter in regards to the use of DDoS attacks and that it inhibited freedom of speech (Shachtman, 2009). According to *Wired* others were concerned that the DDoS strikes could consume the limited amount of bandwidth available inside Iran (Shachtman, 2009). One poster claimed that “quit with the DDoS attacks - they’re just slowing down Iranian traffic and making it more difficult for the protesters to tweet,” (Shachtman, 2009).

Individuals such as a technologist in San Francisco who writes under the name of Austin Heap, posted instructions on how to access hacking tools and set up proxy servers to allow people to circumvent government firewalls (Stannard, 2009).

There is no evidence to suggest US government involvement in supporting this illegal activity as individuals posting to these social networking sites had no obvious association with the government. However in terms of hegemony, the Twitter posts analysed all supported democracy and freedom of information which may be considered to be

consistent with western hegemony. Therefore, whilst local Iranian protesters actively participated on the social networking sites, a significant proportion of the English based posts appeared to be external international posts.

Melbourne International Film Festival

In the prelude to the Melbourne International Film Festival the Chinese Consulate in Australia requested that festival organisers remove a documentary, *Ten Conditions of Love*, based on the Uighur leader, Rebya Kadeer (Levin, 2009). The festival organisers refused citing that they were an independent organisation (Toy, 2009). In July 2009 the international press reported that there had been a number of hack attacks on the festival website (Levin, 2009). The attacks were in response to the screening of the documentary. In addition, seven Chinese film makers withdrew their work also in protest of the Kadeer documentary, and a Hong Kong sponsor also withdrew from the festival. The Australian ambassador in Beijing was also summoned to discussions ("China summons Australia over Uighur leader visit," 2009).

The hacks involved embedding the Chinese flag onto the festivals website and email attacks. The *China Daily* ("Kadeer film prompts hacker attack on website," 2009) reported the hack attacks along with a denial that the Chinese government had anything to do with the attacks. A calling card from a hacker, Old Jun, was also left on the website. A second attack took place in the second week of the festival; this attack flooded the festivals booking system with bogus ticket requests ("Kadeer film prompts hacker attack on website," 2009).

APPROPRIATE RESPONSES

The saying that 'one man's terrorist is another man's freedom fighter' can also be applied to hactivists in that, what they do may well serve the interests of governments. So while the efforts of hactivists in the west during the Iranian protests maybe regarded as the promoters of free speech by their governments, their actions are regarded by the Iranian government as interference in the countries internal politics. The same principal can be applied to the Chinese hackers as they had tacit support from their government. The tactics of many of these groups are the same; they aim to disrupt communications using Internet tools. To date there is no evidence that any of the hactivists involved in the Iranian protests and the attacks on the Melbourne International Film Festival have been arrested. Most countries, including China, the USA, Australia and Iran, have laws against hacking. The USA's hacking laws are in fact harsher than China's hacking laws.

CONCLUSION

The consequences of the development of the Internet and globalisation in many ways are increasingly challenging international relations. The hackers are in a sense really hacking to support the hegemonic practices of their respective countries. These kinds of hack attacks represent a new form of civic participation in international relations.

REFERENCES

Arquilla, J., & Ronfeldt, D. (2001). The advent of netwar (revisited) *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Retrieved Oct 19, 2009, 2009, from www.tsa.gov/assets/pdf/NetWar.pdf

Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Retrieved Oct, 21 2009, 2009, from http://homes.eff.org/~barlow/Declaration-Final.html

Burton, M. (2009, June 16, 2009 - 10:43am). On The Weaponization of the Collaborative Web. Retrieved Oct, 21 2009, 2009, from http://personaldemocracy.com/blog-entry/weaponization-collaborative-web

Cammaerts, B. (2007). Jamming the Political: Beyond Counter-hegemonic Practices. *Continuum, 21*(1), 71-90.

Carey, J. W. (1989). Space Time and Communications: A Tribute to Harold Innis. In Hyams (Ed.), *Communication as Culture: Essays on Media and Society*. London: Unwin.

China summons Australia over Uighur leader visit. (2009, Sat Aug 1, 2009 6:16am AEST). Retrieved August 1 2009, 2009

Comor, E. (2001). Harold Innis and the Bias of Communication. *Information, Communication & Society, 4*(2), 274-294.

Cult of the Dead Cow. (1984). Cult of the Dead Cow: About - Who We Be. 2009, from http://w3.cultdeadcow.com/cms/about.html

Deibert, R. J. (1997). *Parchment, Printing, and Hypermedia Communication in World Order Transformation*. New York: Columbia University Press.

Deibert, R. J., Palfrey, J. G., Rohozinski, R., & Zittrain, J. (Eds.). (2008). *Access Denied:The Practice and Policy of Global Internet Filtering*. Cambridge: The MIT Press.

Deibert, R. J., & Stein, J. G. (2003). Hacking networks of terror. Dialogue IO. Retrieved October 16, 2009, 2009, from http://74.125.155.132/scholar?q=cache:2lx4kMVcfxQJ:scholar.google.com/+distributed+citizen-based+warfare&hl=en

Denning, D. (2001). Activism, hacktivism, and cyberterrorism The internet as a tool for influencing foreign policy In Networks and Netwars: The Future of Terror, Crime, and Militancy. Retrieved May 19, 2008, 2008, from http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf

Doctorow, C. (2009). Cyberwar guide for Iran elections. June 16, 2009. Retrieved Oct, 21 2009, 2009, from http://boingboing.net/2009/06/16/cyberwar-guide-for-i.html

Drache, D., & Beyer, R. (1996). *States Against Markets: The Limits of Globalisation*. London: Routledge.

Fontana Dictionary of Modern Thought. (2000) (3 ed.). London: Haper Collins Publishers.

Innis, H. A. (1951). *The Bias of Communication*. Toronto: University of Toronto Press.

Internet brings events in Iran to life. (2009, 01:48 GMT, Monday, 15 June 2009 02:48 UK). from http://news.bbc.co.uk/2/hi/8099579.stm

Iran's Facebook access restored. (2009, 17:28 GMT, Tuesday, 26 May 2009 18:28 UK). Retrieved Oct, 21 2009, 2009, from http://news.bbc.co.uk/2/hi/middle_east/8069038.stm

Iran blocks Facebook. (2009, Sunday, 24 May 2009, 11:17). Sunday, 24 May 2009, 11:17. Retrieved Oct, 14 2009, 2009, from http://www.theinquirer.net/inquirer/news/1137462/iran-blocks-facebook

Kadeer film prompts hacker attack on website. (2009). Retrieved August 28 2009, 2009, from http://www.chinadaily.com.cn/china/2009-07/28/content_8479251.htm

Klein, N. (2000). *No Logos*. London: Flamingo.

Levin, D. (2009, August 11 2009). Film Festival in the Cross Hairs. *New York Times* August 9, 2009. from http://www.nytimes.com/2009/08/10/movies/10festival.html?_r=1&ref=global-home

MacAskill, E. (2009, Wednesday 17 June 2009 09.03 BST). US confirms it asked Twitter to stay open to help Iran protesters. Retrieved Oct, 21 2009, 2009, from http://www.guardian.co.uk/world/2009/jun/17/obama-iran-twitter

McLuhan, M., & Fiore, Q. (1967). *The medium is the message*. Harmondsworth: Penguin.

Metac0m. (2003). What is Hactivism? 2.0. Retrieved Oct 19, 2009, 2009, from http://www.thehacktivist.com/whatishacktivism.pdf

Samuuel, A. (2004). *Hactivism and the Future of Political Participation.* Harvard University, Cambridge, Massachusetts

Shachtman, N. (2009, June 16, 2009). Web Attacks Expand in Iran's Cyber Battle | Danger Room. from http://www.wired.com/dangerroom/2009/06/web-attacks-expand-in-irans-cyber-battle/

Stannard, M. B. (2009, Wednesday, June 17, 2009). S.F. techie helps stir Iranian protests. Retrieved Oct, 10 2009, 2009, from http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/06/17/MN75188C6K.DTL

Toy, M.-A. (2009, July 26, 2009). Chinese hack film festival site. Retrieved July 26 2009.

US asked Twitter to stay online after Iran vote. (2009). Retrieved June 17 2009, 2009, from http://www.abc.net.au/news/stories/2009/06/17/2600586.htm?section=world

COPYRIGHT