eLucidate Vol. 1 Issue 6, November/December 2004
ISSN: 1742-5921

Political Hacktivism: Tool of the Underdog or Scourge of Cyberspace?

We are grateful to the Editor of *Aslib Proceedings* for permission to carry this shortened version of the article which first appeared in Vol 56 Issue 4 2004.
Please note that some of the sites are only available through the wayback machine (http://www.archive.org/)

The inspiration for this article came from the numerous amusing newspaper articles that examined so called “spoof” sites on the internet – notably around the time of the US and French Presidential elections. On closer inspection, some of these sites deserved more recognition than to be termed “spoof” or “fake” as they clearly served higher purposes. Many spoof sites are actually effective vehicles for protesting against a person, political party or unpopular policy; a better term for them would be protest sites. A trawl of protest websites led me to wonder what other forms of online political protest or hacktivism exist and how effective these are. Basically, there are online equivalents for most forms of activism – leafleting (protest websites), graffiti (defacement of websites), blockades (denial of service attacks) and occupations (cybersquatting).

Protest sites can be found covering a whole range of issues across the political spectrum: pension mis-selling (http://www.badpension.com/), poor housing construction (http://bovishomesexposed.com/) and international finance (http://www.whirledbank.org/). Taking the example of congestion charging, dubbed by some the “poll tax on wheels” there are several protest sites. For example, http://www.londoncongestioncharges.com, http://www.sod-u-ken.co.uk and http://www.beatcongestion.co.uk . An examination of their content shows that while some are unprofessional and bordering on libellous, others are a cheap and effective way of publicising campaigns, telling people how to evade the tax, criticising policies/people and provoking debate. Bizarrely, the former of these has itself attracted a protest site hosted at http://www.wiseupandpay.co.uk/.

A related phenomenon and often a vehicle for creating a protest site is cybersquatting. Often squatters leave sites empty purely as an annoyance but they can also used to criticise opponents. A good example of cybersquatting was reported by ABC news covering an election in California:

Saying "the Web is crucial" in today's political campaigns, California Assembly candidate Dan Dow has an official Web site: http://Dandow.com/ . But he's also registered the URLs JohnDutra.com, JohnDutra.net and JohnDutra.org. And incumbent Assemblyman John Dutra — Dan Dow's opponent in the upcoming election for California's 20th District — is none too pleased that his name is being used against him in the campaign. Interested voters happening by JohnDutra.com may expect to see platform positions from the candidate and his record as a state legislator — in other words, key information about the Dutra campaign. Instead, the site, owned and operated by Dutra's opponent, slams him on all sorts of issues. See http://abcnews.go.com/sections/scitech/TechTV/techtv_cybersquattingpols020911.html

The US Presidential elections of 2000 spawned a host of cybersquat protest sites. [see Election Collection 2000 - editor] An excellent example of this is http://www.gwbush.com/ that appears fourth on the list if you type “George Bush” into Google. This is a parody site but describes itself as “the Official Site to Re-elect Bush” and then leads users to a series of anti-Bush statements in questionable language. There is also an online facility to buy stickers with slogans such as “Regime change starts at home”, “Anyone but Bush 2004” and “Vote GOP, Enron’s private party”.

Other protest websites pick and register uncomplimentary domain names as vehicles for mis-information. Examples from 2000 includes www.stopbush2000.com, www.ungore2000.com, www.nogorecom and www.nogore.org. Most of these sites are filled with criticism and unfortunate quotes.

The French Presidential election of 2002 was also subject to a range of protest sites and Cybersquatting. These were covered in an article in the Guardian entitled “Cracker, Jacques” in the Guardian of 4th April 2002. The first site mentioned (www.bilanchirac.net) detailed the many scandals to hit Chirac during his many years in power, carried press reports on these and listed his unkept promises (always a useful element to have on spoof sites). Bilan meaning, in French, evaluation or assessment or even death toll. The portal http://www.presidentielles.net/annuaire/ actually catalogued humorous sites for both Presidential candidates.

In terms of UK political players, we seem to be exempt from the trend registering namesucks.com and such. Http://www.williamhague.com/ is owned by a naturist (complete with images). However, British political parties have been subject to spoofing and cybersquatting, as an article in The Register 23rd May 2001 indicated (taken from

http://www.theregister.co.uk/content/52/19142.html).

Other forms of hacktivism exist. Defacement of websites is not a new phenomenon. The Labour Party site was hacked during the 1997 General Election campaign, and more recently when a picture of George Bush's dog was altered to show the head of Tony Blair MP. Likud's website was thoroughly hacked in 2001 when all the content was replaced with copy critical of Ariel Sharon. In 2000 Slovakia's opposition party (the Movement for a Democratic Slovakia), was hacked and the web changed to read Movement for a Devastated Slovakia and Movement for Drastic Feebleness. Slogans from the previous election campaign were also amended. Parties in Sweden and Germany were also defaced during recent election campaigns.

The problem has not been confined to party sites as government departments and even Governments have been hijacked. A useful article on the egovernment Australia site lists examples ranging from the US Department of Justice whose logo was changed to the US Department of Injustice to the Department of Foreign Affairs, Fascist republic of Indonesia. In Australia the issue is aptly referred to as "cybersabotage". Security firm mi2g has calculated that the Israeli domain .il has been the biggest victim of web defacements over the past three years, suffering 548 of the 1,295 attacks in the Middle East.

However, this e-graffiti seems to be the cyber-equivalent of having eggs thrown at you. Although these incidents are embarrassing and inconvenient, little lasting impression is made. Few websites are archived and this type of action only really receives press coverage in amusing diary items, rather than mainstream news pages. Denial of service attacks are another form of hacktivism but are more effective and with longer lasting consequences. In a political context these have been aptly described as "a little like pranksters repeatedly and rapidly calling your office phone number, tying up all the lines so that constituents could not get through". See http://www.cdt.org/security/000229judiciary.shtml. DoS actions are also cheap to organise and put into practice – the Electrohippy website gave clear instructions on how to attack the WTO electronically and its server was soon brought to its knees. This coincided with protests on the ground – activism and hacktivism working together.

In March of this year, Al Jazeera's website was subject to a DoS attack while in this country, Downing Street and other governmental computers were attacked as part of the anti-Iraq war protest. The Whitehouse website was also subject to similar action.

DoS actions are clearly an effective form of online protest and have even received attention in Parliament, being the subject of the Computer (Misuse) Amendment Bill in session 2001/02. Anything that suggests that parties or political institutions are not taking their security seriously smacks of amateurism and this would not be tolerated in any other area of modern political communication (press releases, media interviews, for example).

In conclusion, the key to determining the success of these different forms of hacktivism depends on the following criteria: how much nuisance was caused, how widely was it covered (in the press), and fundamentally – did anything change as a result

Using the internet in any sphere is generally regarded as a cheap option and political hacktivism certainly falls into this category. None of the methods discussed costs much to execute and most require only limited technical expertise. However in the majority of cases, the maximum effect was one of embarrassment rather than long-term policy change. Most of the activities listed received limited press coverage and most of that was in IT supplements or diary columns – not the news pages. Similarly, none of the types of hacktivism listed have fostered long term policy change, at best they've just succeeded in irritating people.

Additionally, there are ethical and legal considerations to be taken into account. Ethically, the differences between hacktivism, electronic civil disobedience, cyber-vandalism, cyber-terrorism could be said to be purely semantic. One mans cyber-freedom fighter is another's cyber-terrorist, so to speak. Unfortunately, unlike true activist protests on the street, many hacktivist activities are considered to be on the wrong side of the legal boundary and people's cyber freedom to protest isn't guaranteed.

Caroline Auty
Ciber, Department of Information Science, City University
carolineauty@hotmail.com