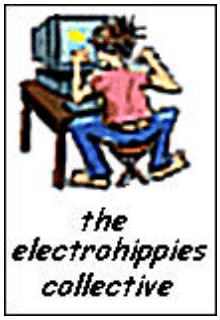
the electrohippies collective's occasional paper no.3:

"*Who does the Internet serve?*"

– "he who pays the piper is only a participant in process; he who makes the pipes controls the tune"

Written to accompany *the electrohippies* presentation to the London Institute of Contemporary Arts meeting, *Hacktivists: Cyberwarriors Or Political Agoraphobics?*, 8th March, 2001



Produced by *the electrohippies collective*, March 2001.
website: http://www.gn.apc.org/pmhp/ehippies/ email: ehippies@gn.apc.org

Hacktivism – a movement without identity?

There is an ancient proverb, "*he who pays the piper calls the tune*". In the world of traditional, real-world media this has been the case for centuries. But today the Internet, the new mass communications media, does not work according to this rule. The Internet is a technology-mediated form of communication. Whoever designs the technical standards, or sets the framework within which those standards are defined, is the person who controls the pipe the piper plays; those who pay the piper merely participate in the process, within the rules of those who control the pipes.

Hacktivism, as a process that people seek to engage in, is a culture searching for an identity. The history of hacktivism is one of computer geeks engaged in earnest programming, pranks or stunts, which are mediated by the open technology of the Internet; perhaps one of the least media comprehensible subcultures. But over the past five years hacktivism has grown to encompass whole new areas, from the free and open source software movements, to localised community pressure campaigns, to global online direct action.

Today, the Internet is under pressure to conform to the model of other mass media – to accept censorship, and some form of political control, "*in the public interest*". Consequently, any use of Internet-mediated communications that seeks to develop an alternative or novel view of the use of the media must internalise these pressures as part of their argument. How hacktivists respond to the calls by the 'status quo' for some form of editorial control over the Internet and Internet-enabled communications will define the future of how hacktivist actions will take place.

The Internet is a tool – *nothing more*. In addressing the future of the Internet we should therefore seek to address it's use as an object of utilitarian function: who does it serve, and hence who defines the form of the medium, who controls the medium, and who defines the constraints of the medium?

Defining the public medium of the Internet

From the point of view of *the electrohippie collective*, the Internet is a Situationists' media. Certainly, that's how we approach our application of 'hacktivism' to Internet-based actions. The Internet was conceived during the period of the Situationists' International, but at that time it was not a mass media. How would the various strands of the Situationists movement, such as Guy Debord, Asger Jorn and Raoul Vaneigem, have addressed the Internet? How would *The Society of the Spectacle* read if the Internet had been present as a viable mass media in the 1950s? The form of the Internet, and its ability to represent abstraction's of human consciousness, in many ways represent a Situationists' dream.

The Internet can be broadly summed up as a totally conceptual medium, devoid of any meaningful human geography, personal stereotypes and real-world cultural or normative etiquette? The barriers to its use are only technical. In terms of a movement seeking to democratise arts and expression, it is possible to have many entertaining hours considering how the Situationists would have used the media created through the Internet – the ultimate psychogeographical landscape. But the analysis of the leading Situationists, especially how they defined the interaction of people, of modern technology and of personal expression, has great relevance to how we can define an identify for hacktivism today.

In society, when describing groups or persons, we are traditionally encouraged to frame that description in terms of ethnic, social, national or political allegiances – the very cultural keys the Situationists sought to challenge. These traditional anchors become weakened or blurred when we look at groups who use the Internet, in turn creating misunderstanding or uncertainty within the medium

itself.

This new identity created within the Internet is not wholly heterogeneous; it is dependent upon the framework in which the individual or group addresses the 'Net. Many of those who came to the Internet from real-world groups merely project an extension of that group's real-world persona. But those wholly virtual 'interest groups' that are today arising on the Internet are developing a new individually based identity. This identity expresses a far more diverse expression of personal opinions rather than a group identity, and reflects the nature of the Internet itself – an alliance of decentralised interests rather than centralised power. It is this underlying transference of the associative structure that gives an individual equal access to a transnational corporation; it this also this transference that many in the corporate and political world perceive as threatening.

Defining the form of the Internet

The Internet is part of society, but it exists only conceptually. However, any conceptual entity is open to external redefinition. For example, in the UK the Internet was promoted as a tremendous platform for e-commerce, bringing 'point and click' consumerism to the masses. But when that e-commerce platform was used to buy babies from the USA, it was soundly condemned by much the same group of people. How we define the value, the threat or the perversity of the 'Net is therefore directly related to the context, the perceptions and prejudices of the beholder (yet another Situationist construct).

The lack of a traditional framework within which we can pigeonhole certain groups or campaigns makes it difficult to grapple for those wishing to elucidate or disparage the use of the Internet for campaigns and direct action. But the prejudices of those who oppose, within their 'interpretation' of, what hacktivism is, also make open debate difficult to achieve. To date hacktivists have been very bad at communicating a positive message about the potential of the Internet as a vehicle for public education, participation and debate. Those who have promoted such ideas have themselves, often as members of right wing and the libertarian organisations in the USA, had a quixotic relationship with the 'Net (*they love it, but if they ever had power would they tolerate it?*). One of the early principles evolved within *the electrohippie collective* was that the debate created by Internet action was more important than the action itself. Hacktivism needs to openly promote alternative perceptions of the Internet in order to challenge the authoritarian views of the corporate IT sector and governments.

The problem is, much like the perceptions of the ICA in calling for this debate on the nature of hacktivism, to define what hacktivists represent. This cannot take place within the limited and overly pejorative definitions that the term 'hacktivist' evokes. When deciding a name for the group whom later became known as *the electrohippies* we had this debate on 'identity'. In our view hacktivism, because of the skewed perceptions of the media and politicians on what 'hacktivism' is, doesn't convey the true meaning of what many of those engaged in hacktivism are striving for. It doesn't encompass the concept of free software, it doesn't encompass equality of access, and it doesn't encompass Internet exercisable civil rights.

The lexicon of the IT industry is currently dominated by the IT security goons who want to stamp out any kind of non-corporate independent thought on electronic networks. From recent experience [1], the electrohippies have been able to demonstrate that these groups not only talk-up the threat from hacktivism, but they positively manufacture fictitious threats for the consumption of the broadcast media. What hacktivists must do, to break this confining definition of their philosophy, is to break the status quo's control over the lexicon by subverting that control, using terms that make the IT authoritarians contradict or ridicule their own position. Curiously, this is the same type of thought process as Guy Debord engaged in when undertaking a decomposition of the then prevalent social structures of post-war Europe.

Today, there are three conceptual views of the Internet that are challenging the real-world status quo for domination of this new virtual space:

- **Governments** – who see the Internet as a means to streamline many functions of society, perhaps to reduce costs, but with a longer term objective of reinforcing the political status quo through some sort of 'qualitative' control of the medium's content.
- **E-commerce** – who see the Internet as a low-cost trading environment and, in the longer term, a business medium that can be used to trade without the usual public pressures associated with commerce (labour standards, environmental standards, consumer protection, etc.).
- **The Utopians** (for want of a better label) – who see the Internet as a means to create a seamless, barrier-less medium of human

interaction and consciousness, and therefore a means to greater understanding and human unity.

All these groups will continue to work and coexist on the 'Net. But, in terms of which philosophy will prevail, the conflicts over the nature of the Internet, it's regulation, and the terms on which people have access to it, will be fought over the next five to ten years as the medium matures within the public consciousness.

Who controls the medium

Many hacktivists have talked of the 'un-governability' of the Internet. This is a fallacy, wrapped up within the more libertarian elements of hacker culture that have emerged from the USA. The fact that the American constitution protects free speech is no guarantee for the citizens of other states. You may be free to host controversial material on a US web server, but access it from your own country and you will commit a criminal offence. Is the Internet, and so the practice of hacktivism, immune to real-world control? – NO.

As has been demonstrated in the UK recently, through the new provisions of the Terrorism Act 2000 [2], and the Regulation of Investigatory Powers (RIP) Act 2000, the Internet as a whole system is not governable, but the people accessing it at the end of the pipe are. It makes no difference how free the Internet is if ordinary people are blocked, surveilled or filtered, without any prior evidence of wrongdoing, in their accessing of it's content. This is what the combination of the Terrorism Act, the RIP Act, and the Police Act 1997 enables in the UK. Recent proposals [3], drawn up under the sweeping discretion under the RIP Act creates, also enable all data communications to be centrally stored for four or seven years for later accessing or study by the authorities.

More worryingly, these repressive new laws developed in the UK are now being exported – both South Korea and Australia have expressed intent to enact similar laws soon, and The Netherlands is on the way to doing so.

It is important that hacktivism seeks to move beyond the "we're unstoppable" ethos that dominates it's American origins. The Internet is vulnerable – not as a system, but at the end of the pipe where the individual accesses it. Such hacktivist bravado really stems from a lack of political awareness by many hacktivists, and perhaps a utopian naivety about the forces that have made, and may ultimately break, the open nature of the 'Net. Across the globe, in response to the public's enthusiastic adoption of the Internet, states and security forces are adopting new procedures and laws that seek to make the Internet as something separate, something unique, and something so fundamentally dangerous that it must be defined as apart from other communications media. More importantly, through this double standard, states are seeking to justify the application of highly restrictive laws that offend the very basis of our hard-won civil rights, and which would not be tolerated for other mass media.

It is essential that states are not permitted to seek the same demarcation of standards in the exercise of the public's civil rights in the use the Internet. As the Internet becomes and ever-more pervasive mass medium within society, the exercise of civil rights will increasingly depend upon the ease of access and use of the 'Net. In this situation, where the exercise of civil rights is dependent upon access to the 'Net, uncensored and unfiltered Internet access itself must become a civil right.

Who defines the constraints of the medium

The Internet is a technologically mediated mass communications media. As such, the transference of information is circumscribed by the stands that this system of technological apparatus operates to. In the early years of the Internet all standards were open. But the advent of Internet enabled commerce has led to a proprietary annexation of the Internet's governing bodies and technical standards. Two issues stand out here:

- **Internet governance** – There are a number of bodies that control the operation of the Internet. For example, the *Internet Engineering Task Force* (IETF) is an 'expert body' that develops operational standards for the Internet. To date this body has not come to prominence in the debate about the Internet – although they might shortly as their new standard for Internet data packets has serious implications for civil liberties. But the more minor of the governance bodies, the *Internet Corporation for Assigned Names and Numbers* (ICANN) has become very prominent because the names people can use on the Internet represent intellectual property – and therefore carry great financial value. The recent power struggles within ICANN do not directly threaten the technical operation of the Internet, but should the IETF come under the same pressures there would be serious implications for the ability of ordinary people to use the Internet freely, without

proprietary barriers.

- **Technical standards** – As noted above, IETF set standards for the physical hardware of the Internet. But increasingly IT corporations are defining their own proprietary standards that sit on top of the 'network layer' that the Internet represents. Leading these organisations is Microsoft. Microsoft has an identified policy of adopting a technical standard, adding proprietary functions to that standard that no one else can use it, and then using their global dominance in computers to enforce their system over all others. In this way, the substance of which was the core of the recent Microsoft anti-trust trial in the USA, Microsoft are able to enforce their own view of "*what's good for the 'Net*" over everyone else.

Perhaps the best example of the 'hacktivist' movement is the response to the technical constraints imposed by the increasing proprietary domination of IT systems – led by the free software and open source movement, enabled by the freely available GNU/Linux operating system. This is also a good example of where the traditional media and corporate IT definitions of what hacktivism is break down. This is a strand of hacktivism that clearly takes human openness and sharing as it's core philosophy.

Fundamentally, unless the public as a whole are able to become involved within the issue of Internet governance, and in particular the setting of standards, then the Internet as a whole will remain vulnerable to exploitation or control by proprietary interests. This would have an inevitable detrimental impact, compared to the currently 'open' system, in determining to how the public at large is able, or are permitted technologically, to use the 'Net.

What is hacktivism?

This has been left to the end. Why? Because, like the term '*Situationism*', '*Hacktivism*' has no tangible meaning. In 1961, here at a meeting of the Institute for Contemporary Arts, Maurice Wyckaert was asked "*what is Situationism*". Guy Debord, after promptly issuing an insult, then led a walk out of the Situationists' from the room. A similar issue arises with 'hacktivism'. Hacktivism, as a label, has evolved predominantly as a convenient tag for activities which many, particularly within the media, do not understand. But hacktivism cannot encompass, as a term, all those activities that it seeks to containerise.

A hacker is someone who is good with computers – nothing more. This should not be confused with people who are good with computers and who use this expertise to break into computer systems – in computer parlance these people are 'crackers'. The activities of hackers are, to all intent and purposes, far more benign, but in the process may still threaten many vested interests (such as governments wanting to restrict debate on public issues, or IT corporations seeking to restrict the release of free alternatives to their software).

Hacktivism can be anything that the context defines. It can be writing a new utility for the Linux operating system. It can be developing a new web site to promote civil rights or social change. It can also be developing online direct actions against the virtual personas of corporations or governments on the 'Net.

In deciding what the relevance of the Internet is to social movements we have to identify whom the Internet serves and how, and the tensions that these differential perceptions of the Internet create – and so where the 'hackers' fit in. As a filtered reflection of society, understanding how the Internet enables debate or action can provide an insight into how people are using this new medium. But for the online activists, such as *the electrohippies*, understanding how different groups perceive the Internet is the first step in developing, or influencing, a new online consciousness that can create a new environment for realising societal change, locally, and even globally.

At its root, *hacktivism* is seeking to use one's knowledge of IT systems to create a meaningful human use of computer hardware or computer networks. Within that definition, anything is possible. It is, like the conceptual nature of the 'Net, defined within the meanings, influenced by the context, that the individual applies to the action. It is then, ultimately, a Situationist philosophy, and therein lies the paradox that defines its identity.

References:

1. See *the electrohippies communiqué*, April 2000 (in the 'archive' section of our website).
2. A briefing on *The Terrorism Act* is available from the GreenNet *Civil Society Internet Rights Project* web site – http://www.gn.apc.org/action/csir/index.html
3. See *The Observer*, 3rd December 2000 – http://www.observer.co.uk/uk_news/story/0,6903,406191,00.html
   A leaked copy of the ACPO/NCIS discussion document is available at http://cryptome.org/ncis-carnivore.htm