Mapping Hacktivism

Mass Virtual Direct Action (MVDA), Individual Virtual Direct Action (IVDA) And Cyber-wars

Tim Jordan, Open University

Hackers have been present in computer networks from the moment networks began to exist. Beginning as a term to describe those who wanted to find novel uses for computers and other technologies, by the early 1990s 'hacker' had come to refer in popular use to those who break into computers over networks.

Until the mid-1990s, despite a 20-year history of hacking, there was little evidence of sustained political engagement by hackers. Rather, hackers were overwhelmingly focused on the manipulation and analysis of computers and networks. However, with the 1994 publication of the Critical Arts Ensemble's manifesto *The Electronic Disturbance* and the emergence of pro-Zapatista mass denial-of-service attacks in 1998, a politically motivated hacking movement has emerged. It has been christened 'hacktivism'.

In 2001, this movement has become the focus of mass-media attention and moral panic, often desperately ill-informed.

This article will briefly introduce and outline hacktivism's main components, in keeping with the spatial understanding of the Internet as cyberspace, what follows is a mapping of hacktivism.

Mapping

Hacktivists have found two uses for the Internet: Mass Virtual Direct Action (MVDA) and Individual Virtual Direct Action (IVDA). These uses also need to be distinguished from the use of the Internet for communication by political activists and the ill-defined area of cyber-war and cyber-terrorism.

I will first outline hacktivism's two main areas and then briefly distinguish them from communication and cyber-war.

The distinctions I am about to make are also somewhat less clear in reality than they may appear to be in my definitions. Hacktivism is a fast-evolving movement, which easily crosses boundaries into hacking, cyber-war, Net communication and so on.

The value of what follows is to abstract out from cyberspace the main features of hacktivism, while simultaneously recognizing that the world is a messier place than abstractions usually allow for.

> *"the world is a messier place than abstractions usually allow for"*

MVDA

Mass Virtual Direct Action involves the simultaneous use, by many people, of the Internet to create electronic civil disobedience. It is named partly in homage to the dominant form of offline protest during the 1990s, non-violent direct action or NVDA.

Floodnet

MVDA emerged in 1998 with the call by the Electronic Disturbance Theatre (EDT) for mass participation in a denial-of-service assault on Mexican Government networks in protest against attacks on the Zapatistas, using a tool called Floodnet.

Technically, Floodnet was a Java applet that, once the launching Web page had been called up, repeatedly loaded pages from targeted networks. If enough people participated, the targeted computer would be brought to a halt — bombarded by too many messages for it to handle.

As EDT admitted, they rarely achieved their goal of bringing a network to a halt. Their main achievements were, first, a slowing down of the targeted network and, second, the enrolment of a world-wide constituency of protest in support of the Zapatistas.

Electrohippies

The ideas behind Floodnet have been developed in recent years, particularly by the Electrohippies. The Electrohippies have developed distributed MVDA.

This allows the downloading of a tool that ensures that each participant in a mass denial-of-service attack does not have to remain connected to the one website (sometimes resulting in the collapse of the MVDA-launching website), but simply passes through the MVDA site to download the software, and then automatically launches, multiple requests for the targeted network from each individual browser.

These techniques were developed particularly in relation to an MVDA action against the 1999 WTO conference in Seattle.

The Electrohippies claim the participation of over 400 000 in this MVDA, and success in significantly slowing the WTO's network, as well as, at times, completely halting it.

Echelon bashing

Other MVDA protests utilize less technical support. For example, the Global Jam Echelon day targeted the USA's world-wide surveillance network, known as Echelon. Participants were asked to send as many E-mails as possible on the one day, including in each E-mail up to 50 keywords.

It is believed that Echelon records telecommunications and Internet traffic and subjects its recordings to keyword searches. It was hoped that enough E-mails, with enough keywords, would ensure that Echelon would fail under the sudden extra load.

There is little technical infrastructure provided here, except for the thoughtful provision of 50 likely keywords of interest to Echelon — yet it is clearly an MVDA action.

Action and Enrolment: two-sides to MVDA

MVDA should be understood as working on two levels. First, it attempts to take direct action that is the virtual equivalent of civil disobedience.

These actions try to halt targeted networks, just as protesters using sit-in techniques try to halt a targeted organization.

Unlike civil disobedience, there is rarely an attempt to halt a network completely and forever. In contrast, such protests as Greenham Common's peace camp or anti-roads eco-camps involved repeated actions to try and halt their target completely.

MVDA has, so far, rarely pushed direct action this far, but has sought short interventions that close a site for, at most, a short period of time.

Second, MVDA has symbolic dimensions.

On the one hand, MVDA functions like a street demonstration by creating a mass protest and, on the other hand, in creating a mass protest it draws conscious political commitments from individuals.

MVDA engages participants, through their need to choose whether to participate or not, in discussions about actions and touches on their willingness, or not, to become politicized.

The combination of NVDA and popular protest, distinguishes MVDA actions from more typical hacks, such as breaking into networks or launching individual denial-of-service attacks, like those on eBay, Yahoo and others in 1999.

This is underlined as MVDA activists rarely try to hide their identities through pseudonyms (handles) or to cover their tracks. Like many protesters, MVDA activists seek public debate and discussion and, even when their actions are either illegal or border on the illegal, they argue that there is a right to protest, even in cyberspace.

"there is rarely an attempt to halt a network completely and forever"

However, MVDA does not cover all hacktivist actions, and there is a second, vital area of protest: IVDA.

IVDA

Individual Virtual Direct Action takes up classic hacker/cracker techniques and actions for attacking networks, but uses them for explicitly political purposes. One initial point, is that the name IVDA does not mean the actions are taken alone by hacktivists, but rather that the nature of each action means it could be taken by an individual and in no way relies on a mass protest.

Hackers and hacktivists rarely hack alone. Even if they are physically alone, hackers are often simultaneously communicating online through chat-rooms, E-mail and bulletin boards, and it would be a mistake to take up the popular image of the hacker as an obsessive loner.

The key point is that the actions discussed under IVDA would be impossible to take as mass actions. IVDA refers to the nature of the action, not who takes it. The actions we find here are a range of attacks perhaps best divided into semiotic attacks, computer intrusion and network security.

Semiotics

Semiotic attacks are exemplified by website hacks. For example, the British Labour Party's website was hacked to replace the picture of its leader with a satirical picture and to change its links from titles such as *Road to the Manifesto* to *Road to Nowhere.*

The CIA website was altered from *Central Intelligence Agency* to *Central Stupidity Agency.* Klu Klux Klan and Whitepride sites have been altered to attack their racism and so on.

Like the painting of slogans on bill-boards or the addition of satirical stickers on public advertisements, website hacktivist hacks make a political point by picking out relevant websites and placing protests on them for anyone to see

Of course, website hacks are not exclusively a hacktivist action, with probably the majority of such hacks being undertaken for typical hacker reasons (bragging, demonstration of expertise and the like).

However, political website hacks appear to be a growing phenomenon, and connect to other campaigns such as adbusters and what is more generally known as 'culture jamming'.

"MVDA activists rarely try to hide their identities through pseudonyms"

Attacking Networks

Network attacks are infiltrations of targeted networks, in order to protest. This may involve simply demonstrating the insecurity of a network — which is an important point if the network supports dangerous activities such as nuclear weapons — or damaging the network.

Following the Indian Government's nuclear weapons tests, a hacker infiltrated Indian Government networks claiming to have both acquired secret documents and damaged computers. Threats of repeated and more damaging actions, if more nuclear tests were conducted, were also made.

An attack made prior to the emergence of hacktivism as a movement was the 1988 Worm Against Nuclear Killers (WANK) launched against NASA in protest at its use of nuclear energy in space probes. This worm successfully infiltrated, and brought NASA networks to a widespread halt, claiming to be deleting all files as it froze computer after computer (though the threat of deletion turned out to be only a symbolic one).

IVDA continues many typical hacker actions of computer intrusion to create *"it would be a mistake to take up the popular image of the hacker as an obsessive loner"*

both symbolic protests and to damage targeted computers.

Network Security

Finally, under IVDA there are a range of hacks that draw on long-standing hacker concerns with what can perhaps best be called online security issues.

Here we find a range of hacktivist actions that all explore the political significance of online communications.

The clearest example is Cult of the Dead Cow's (CDC) BackOrifice. This is a software tool, employing a GUI, that allows anyone installing it on a Microsoft based network to hack any other PC attached to the network.

Such surveillance capabilities are obviously of interest to many hackers, but in hacktivist terms, CDC argue that their software uncovers the insecurity of most people's privacy on networks because Microsoft's systems administration software includes the same stealth features as BackOrifice.

This means BackOrifice makes it clear both that networks are insecure, and that administrators have spying capabilities.

CDC's main political aims are expressed in terms of ensuring free flows of information rather than in engaging with anti-corporate or eco-activist protest, and is an example of an important different political focus within hacktivism.

IVDA consists of a range of hacks, and with its concern for network and Internet security, introduces a second range of political ethics, freedom of information flows, alongside the more obvious current activist concerns with globalization, ecological and other protests.

Before concluding by exploring some distinctions within hacktivism, it is important to briefly consider relations between hacktivism and both the use by activists of Internet communications and the emergence of cyber-warfare.

Communication and cyber-war

While hacktivism is currently gaining most publicity and often appears to be the most dramatic grassroots political intervention in cyberspace, we should remember that a globally distributed, many-to-many, cheap (for some) communication system has aided the formation of many recent global protests.

For example, the first uses of the Internet in support of the Zapatistas were in order to disseminate information, and it was only after such communications networks were operating that MVDA was mooted as a possible form of support.

It is possibly even true to say that these communications, of course available to most who use the Internet and not just to hackers and hacktivists, have had the most profound effect on popular political activism.

The globally linked protests for such days as J18 (18 June — day of action against global capitalism), which featured many different protests around the world, and the assistance with organization that the Internet has allowed, has formed an increasingly important aid.

This is particularly the case as many protest organizations favour non-hierarchical, networked styles of organization in which virtual communications are particularly effective (though not necessarily effective in maintaining security).

Cyber-war

Cyber-war is a different issue when considering hacktivism. Whereas mentioning communication is a matter of remembering potent virtual issues outside of direct action, cyber-war is an arena of direct action and often of very similar actions to hacktivism.

The clearest recent example is the so-called cyber-war between Israel and Palestine. Over the last year, there have been a series of mutual virtual assaults between Israeli and Palestinian supporting hackers. It is unknown who fired the first virtual shot, but it is clear there have been Israeli hacks closing down Hezbollah sites and Palestinian assaults that closed the Israeli Prime Minister's official site, and the Israeli Foreign Ministry site.

The Israeli army switched some sites to a server connected to US corporation AT&T, which led to threats to re-route telecommunications traffic from AT&T to its competitor Qwest Communications.

The Israeli Government released the well-known hacker The Analyzer, who helped set up a site that offered security information to Israeli corporations, despite clamour in the US for the Analyzer's extradition to the US for hacking Pentagon networks.

Similar, and often similarly vague, reports of attacks on both sides of the Kosovan crisis in the Balkans also exist. What is missing from many such actions is MVDA — these have largely not been mass actions.

However, they are similar IVDA actions and this makes cyber-war or cyber-terrorism difficult, at times, to distinguish from some hacktivist actions.

The distinction may be similar to ones between offline war and protest, with wars occurring between national or nationally aspiring groups, and protests being generated from outside of the consideration of national ideals.

This is, however, a tentative and crude distinction and, while MVDA is quite distinct from cyber-war, it is not so clear on what basis IVDA and cyber-war can always be distinguished.

The many faces of hacktivism

Hacktivism should not be treated as a simple entity. The divisions I have drawn between MVDA, IVDA, communication and cyber-war all help us to grasp hacktivism, but it needs to be kept in mind that these divisions also spill over

"WANK launched against NASA in protest at its use of nuclear energy in space probes"

into each other and that not all hacktivists agree with each other.

In particular, there is a potential split between those hacktivists who are dedicated to long-standing hacking ideals of free flows of information — and who therefore see denial-of-service attacks as wrong in principle — and those who see mass actions as both direct actions and important symbolic moments.

Cult of the Dead Cow objected to the Electrohippies' justification of their distributed denial-of-service (MVDA) attacks in the following way:

> *"Denial-of-service, is denial-of-service, is denial-of-service, period. The only difference between a program like Stacheldraht (a DDoS application written by the Mixter) and the client side javascript programs written by the Electrohippies is the difference between blowing something up and being pecked to death by a duck… 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."*
>
> **Oxblood Ruffin, foreign minister,**
> **Cult of the Dead Cow**

Ruffin expresses here CDC's long standing and vocal commitment to free flows of information, expressed in other places by their attempts to facilitate passing information across the Chinese Government's censoring firewalls.

However, CDC here also misses the broader significance of protest, its symbolic and enrolling aspects. Within hacktivism, like all political movements, there is debate and dissension.

The Hacktivist's Dictionary

CDC

Cult of The Dead Cow: a hacktivist group that espouses free frow of information

Distributed MVDA

More sophisticated than denial-of-service attacks, such as Floodnet, because it is automated and more likely to succeed

Electrohippies

Hacktivist group that popularized the use of Floodnet for politically motivated denial-of-service MVDA

Floodnet

Tool used for denial-of-service

IVDA

Individual Virtual Direct Action: using technology to make a political point. Protest can be symbolic or involve real damage

J18

18 June — day of action against global capitalism

MVDA

Mass Virtual Direct Action: involves many people simultaneously using the Internet for purposes of electronic civil disobedience. The virtual equivalent of a sit-in protest

Semiotics

Defacement of websites to make a political point

Hacktivism, like hacking, is here to stay. There is no guarantee that hacktivism will remain within the political ethics it has so far adopted, but there seems little doubt that the ability to take politicized direct action across cyberspace will continue.

Hacktivists might or might not seek broader change in society by pecking networks to death in MVDA actions, and might or might not continue exposing security and privacy problems, but there seems little doubt that the map offered here outlines the early years of virtual direct action.

About the author

Tim Jordan works in Sociology at the Open University. He is the author of "Cyber-power: the culture and politics of cyberspace and the Internet", London: Routledge and co-editor of "Storming the Millennium: the new politics of change", London: Lawrence and Wishart. He has published work about online social movements, hackers and social theory, as well as working on recent popular protests and social movements. He is currently researching politically motivated hacking, or hacktivism, and relationships between political activism and society's imagined futures.

He is a co-founding editor of the journal "Social Movement Studies", to be launched with Routledge in 2002. To contact him, send E-mail to t.r.jordan@open.ac.uk or send feedback via the editor: c.palmer@elsevier.co.uk.