

the electrohippies collective
occasional paper no.1



Client-side Distributed Denial-of-Service:

Valid campaign tactic or terrorist act?

by DJNZ and the action tool development group of *the electrohippies collective*¹, February 2000
For further information:

- see the electrohippies web site at <http://www.gn.apc.org/pmhp/ehippies/>
 - email the electrohippies collective care of ehippies@tesco.net
-

And when he had made a scourge of small cords, he drove them all out of the temple, and the sheep, and the oxen; and poured out the changers' money, and overthrew the tables; And said unto them that sold doves, Take these things hence; make not my Father's house a house of merchandise.

John 2:14

Introduction

Recent actions on the Internet against **e-commerce** sites are not a matter of pleasure-seeking by bored computer nerds. They represent a fundamental disagreement about the purposes of the Internet, and the increasing emphasis on the use of the 'Net as a vehicle for profitable trade rather than of knowledge and discussion. 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 recent development. But, do we label Jesus as a terrorist? Those involved probably have a reverential view of the 'Net. The **public space** that the 'Net represents is being promoted as a marketplace for large corporate interests, and many of those who use the 'Net for other purposes are dissatisfied with this.

In recent weeks, there has been much discussion about 'denial-of-service' (DoS) actions against certain e-commerce web sites. Whilst the Internet was originally a place of discussion and networking, the invasion of corporate interests into this space has changed the perceptions of what the purpose of the Internet is. Some believe that the Internet is no

longer a 'public' space – it has become a domain for the large corporations to peddle their particular brand of unsustainable consumerism. For many this is unacceptable. The increasing emphasis on control, driven by the needs of increasing commerce on the 'Net, is also seen by many as threatening the more philanthropic basis of the 'Nets original use.

Whatever the views of particular people about the development of e-commerce on the 'Net, we must not ignore the fact that as another part of society's public space the Internet will be used by groups and individuals as a means of protests. There is no practical difference between cyberspace and the street in terms of how people use the 'Net. What is disconcerting is the response of governments and e-commerce lobbyists to the recent DoS attacks. They are being viewed as an act of **terrorism**. Now the regulatory agenda in many countries has shifted from expanding the Internet, to controlling the purposes that the 'Net may be used for to restrict certain types of activity. Whilst the Yahoo, eBay and Amazon actions were undoubtedly illegal because of the cracking and modification of other computer systems to launch the action, the backlash against these actions is likely to stifle public debate about the use of the 'Net for protest. It will also criminalise those who seek the use the Internet as a means of extending protest against the corporate forces who now seek to make cyberspace their own.

the electrohippies collective has produced this paper as a means of promoting a debate about denial-of-service actions, and whether or not they can be legitimately undertaken within the public space of the Internet. It has also been produced as a response to the many media inquiries we have received over the last few weeks on this issue. The paper outlines the main issues regarding the development of DoS actions, and the distinctions between server- and client-side DoS actions. It also looks at the *electrohippies* action against the WTO, and considers how *the collective* intends to develop the tools for client-side actions (DoS or otherwise) further.

February 2000 - distributed 'Denial-of-Service' goes public

The initial wave of **Denial-of-Service** (DoS) on February 8th/9th this year have highlighted the issue of the use of the Internet as a means of protest. Originally, the attacks were put down to the use of existing tools, such as *Tribal Floodnet*, to jam web servers². But then it became clear that other computer systems across the globe had been **cracked** and commandeered to launch the action. As time wore on things took on an air of dramatic suspense, especially when the debate turned to the roles of 'black hat' and 'white hat' hackers³.

The important thing is that following the immediate impact of the action there ensued a media panic about hackers hijacking the Internet. But the fact is much of the media and political frenzy that followed, from TV news broadcasts to President Clinton's 'cyber-summit'⁴, were enabled and motivated by one thing... The majority of ordinary people had not a clue what a 'distributed denial-of-service' action was, or how it worked. The public were ripe for exploitation for newspaper column inches and politician's tough-guy moral profiles, and these groups did so to the fullest extent.

In fact there had been a significant DoS action on the Internet only two months before – launched by *the electrohippies collective* against the World trade Organisation's (WTO) web site⁵. But that event received rather less publicity alongside the large numbers of peaceful protestors who were gassed in the streets of Seattle. However, the two actions are starkly

different – which is the subject of this paper.

To interpret the events of early February it is necessary to look through the media hype surrounding the actions against e-commerce sites. It is important that people consider the clear and qualitative difference between the use of the 'Net for democratically based protest-related DoS action, and the use of the 'Net for individual actions.

First and foremost, it's a matter of terminology. Throughout the period of the 8th to the 14th February there were consistent references to 'hackers'. This is, in terms of the formal meaning of the word in the computer world, completely incorrect.

A **hacker**, in terms of it's computer jargon usage, is someone who has a deep understanding of computers to the point where they undertake experimentation with their own systems themselves. Quite clearly, this makes some of the members of *the electrohippies collective* 'hackers'. But the actions against Yahoo and others were launched by **crackers** – experienced hackers who are intent on breaching the security of computers systems they do not have legitimate access to in order to achieve other ends (the origin of the term being that they 'crack' the security of systems).

The events of early February involved crackers breaking into a number of computer systems across the world and installing software on them that generated tens of thousands of hits an hour to the targeted sites. The technical term for these modified systems is 'zombies' – they perform the illicit task they were programmed to do without the knowledge of their system operators. Conceivably, only one or two people may have caused all the problems at all the sites hit. These were **server-side distributed DoS actions** because they are created by abusing the routers of web servers to generate huge numbers of incomplete requests. Effective, but the manner of the action, and it's covert nature, mean that it does not have any particular democratic legitimacy.

What *the electrohippies* did for the WTO action was a **client-side distributed DoS action**. The electrohippies method of operation is also truly distributed since instead of a few servers, there tens of thousands of **individual computer users** involved in the action. The requests sent to the target servers are generated by ordinary Internet users using their own desktop computer and (usually) a slow dial-up link. That means client-side distributed actions require the efforts of real people, taking part in their thousands simultaneously, to make the action effective. If there are not enough people supporting then the action it doesn't work. The fact that service on the WTO's servers was interrupted on the 30th November and the and 1st of December, and significantly slowed on the 2nd and 3rd of December, demonstrated that there was significant support for the *electrohippies* action.

So, the difference between the two actions is one of popular legitimacy versus individual will. The structure of the client-side distributed actions developed by *the electrohippies* means that there must be widespread support across a country, or continent in order to make the system work. **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.**

Fundamentally, it's the mode of the protest on the Internet that is important when evaluating the legitimacy of the action. This is the important factor that was absent from the debate over DoS actions during early February. The power that computer technology, linked via the Internet, gives to the individual is an important factor in levelling

the traditional imbalance between the individual and government or large corporations.

As a result of the WTO action *the electrohippies collective* were labelled as terrorists⁶. However, the e-commerce industry lobby group that did so failed to provide any meaningful analysis of the object of our action – they just didn't like our message. It is of course a standard tactic of the PR lobbyist to depict anyone who is a threat to their client as aberrant.

It would appear that there are many vested interests involved in e-commerce who are hell-bent on destroying any non-profit use of the 'Net, particularly if it's directed at the social, environmental or employment practices of corporate interests. The problem with the knee-jerk response of politicians and e-commerce gurus is that we run the risk of losing legitimate electronic action as governments use the excuse of 'hackers' to criminalise certain activities. ***We must make sure that both the positive and negative aspects of Internet activism are clearly debated, and that cyberspace is not excised from the everyday realm of constitutional rights and freedoms.***

Javascript – enabling the client-side revolution

JavaScript is a type of object-oriented programming language, developed from the Java programming language, that is used in web browsers to control the processing of forms and other special functions. Javascript was devised by Netscape, and first appeared in its basic form (Javascript 1.0) in their *Netscape Navigator 2* browser. Its versatility meant that it was soon adopted by Microsoft in their *Internet Explorer 3* browser too.

The development of Javascript has had to keep pace with the increasing demands for greater versatility in page design. In 1997, the various models of the language were standardised as the *ECMA script*, and this has since led to the release of Javascript 1.2. There have always been compatibility problems between Netscape and Microsoft versions of Javascript, and this can be a problem when generating broad-based actions over the Internet. But the issue is not so much the detail of the language itself – it's what the incorporation of a programming language into web browser's does for ability of the web to be used as a campaign tool.

For the most part, Javascript is used to make pretty graphical effects inside web pages. The other elements of the language, particularly the ability to process data, have not come to the fore because of the use of **server-side** scripting languages such as Perl (Javascript is also available to work server-side). 'Server-side' means that the program code is kept and processed on the web server. The computer holding the web site – the server – processes the data for everyone using the site. Whilst this is fine in terms of accomplishing many data manipulation tasks for web sites, it does not lend itself to effective campaigning. This is because the DoS action is **centralised** on the one server. The server is itself is vulnerable to DoS attack, thus rendering the campaign ineffective. But, more particularly, the owner of the server is traceable, and therefore liable for any legal measures taken by the targets of DoS campaigns.

What the most recent versions of Javascript have enabled, particularly *Netscape Navigator 3.04* and *Internet Explorer 4*, is the development of **client-side actions**. 'Client-side' means the processing of data takes place within the computer that receives information *from* the server. Once the web page containing the Javascript has been downloaded, no input from

the server is required in order to make the program operate. Pages can even be emailed from point-to-point, so cutting out the need for a server altogether. Therefore, rather than one origin for the action, the action is **distributed** over many clients, making countermeasures by the target of the action harder to implement. For example, the **router** at the front end of the server can be configured to refuse or 'bounce' requests from specified servers. If the requests are coming from hundreds of servers then this is extremely difficult to configure.

The most basic type of client-side Javascript DoS actions involve reloading a web pages repeatedly every few seconds. This can be done if a person just keeps pressing the 'reload' or 'refresh' button of their browser. What Javascript does is automate the process so making it easier to accomplish. With modern multiprocessing operating systems such as Windows 95/98, this process can also take place whilst someone is doing another task on the computer. It is even possible to browse the web (albeit slowly) and still run a DoS action).

As noted above, whilst the Yahoo and other DoS actions were automated on the server-side by just one or a few individuals, distributed client-side actions require that thousands or tens of thousands of people take part. Therein lies the strength of the action. Distributed client-side DoS action is only effective if it has mass support, and hence a democratic mandate from a large number of people on the Net to permit the action to take place. These type of actions are directly analogous to the type of demonstrations that take place across the world. One or two people do not make a valid demonstration – *100,000 people do*.

The most basic type of client-side DoS action must utilise some form of framed web page. This is because the page must be able to run the client-side script whilst loading remote pages into other frames in the page. Whilst is possible to have elaborate systems to achieve the loading of multiple pages, the simplest client-side distributed DoS web page is only around 350 bytes long!:

```
<!-- Simple DoS tool (by DJNZ and the electrohippies collective Jan. '00) -->
<HTML><HEAD><TITLE>Basic, standalone denial of service tool</TITLE></HEAD>

<FRAMESET COLS="50%,50%" FRAMESPACING=0 BORDER=3
    ONLOAD="setTimeout('self.location.reload(true)',4000);">

    <FRAME SRC="http://www.target1.com" NAME="site1" NORESIZE SCROLLING="no">
    <FRAME SRC="http://www.target2.com" NAME="site2" NORESIZE SCROLLING="no">

</FRAMESET></HTML>
```

In this case the page displays two frames, each targeted at a different web site (or even the same web site). The page then reloads itself back into the browser every 4 seconds, so reloading the two target pages. The effect of this constant reloading is to queue requests to the web servers, so holding up other traffic. This is a very minimal type of DoS action, and is not that effective unless tens of thousands of people undertake the action simultaneously. Modern web servers and routers can also defeat this type of attack fairly simply if there is not a lot of support for it.

The **virtual sit-in** tools developed by *the electrohippies* are more complex than this. The tool developed for the WTO action enabled users to select the number of frames and the hit rate to suit their connection speed, as well as providing feedback on the progress to date. The next-generation of our sit-in tool will select targets, according to date and international time zone, to direct traffic to where it is most effective. What we are seeking to do is push Javascript as far as it will go whilst making sure that as many people as possible are able to use the systems without the need to resort to upgrading their browser.

Countermeasures to DoS – cat ‘n’ mouse on the ‘Net

The ability of a web server to handle these requests depends on its **bandwidth** – that’s the physical capacity to move data in and out. For most servers bandwidth is split. Usually there is only a small proportion of the bandwidth devoted to data coming into the site compared to data going out (this is because far more data flows out of web servers than flows in). So, constantly requesting information puts pressure on the server at it’s weakest point – it’s incoming bandwidth.

Bandwidth is finite – you can only move so many bits in and out of a system. Therefore, the manufacturer’s of servers have developed ever-more elaborate ways of maximising data throughput within the finite confines of bandwidth. The most basic of these is the use of **compression** (making data take less space) and **multiplexing** (slotting the many different data packets into the first available space on the data stream, irrespective of the order they are sent in) to maximise throughput. But recently web servers have developed new ways of handling requests to maximise the number of requests that can be handled.

The principle of a DoS action is to queue requests to the web server. Requests are queued on a first in/first out basis. As each request is dealt with the server retrieves a file from disk and sets it up for transmission over the ‘Net. Systems like this are easily overwhelmed by too many requests because the system of data retrieval intensively uses system run time.

To get around this problem **caching** was developed. In this system the most popular pages are not held on disk, they are held in memory at the ‘front-end’ of the server. Any request for these pages results in immediate dispatch of the data. Caches come in different sizes – the larger the cache the more data it can hold. The latest adaptation of this system is to have the server monitor traffic to decide what is the most heavily used content of the web site, and cache only that material. Systems that use this approach can handle massive amounts of traffic – for example **Inktomi’s Trafficmaster** system that can **dynamically cache** up to 1 terabyte (1,048,576 megabytes) of site content.

There are three obvious countermeasures to this system:

- Rather than polling the same page of the site, the DoS tool can poll a wide-variety of material across the site. By selecting large files (preferably binary files that are incompressible, such as graphics) that are not well used, any static front-end caching can be circumvented through the loading of irregular data.
- Related to the above point, *the collective* are currently experimenting with varying the target location and hit-rate for the DoS tool so that certain sites are targeted when their baseload traffic – that’s the other ordinary traffic on the site – is at its highest. This means that for the largest sites no so many requests from participants are needed to make the action effective.
- Even dynamic caching can be disrupted if the page content is selected widely enough, since the system would seek to continually update the cache contents. We are currently testing version of the sit-in tool that can randomly call pages from a long list so that the widest number of files are sought from the server. This will disrupting dynamic caching because it is unable to select the ‘best fit’ of files for the cache – the list is continually changing in response to the co-ordinated request sequences of the tool.
- Finally, the most effective, but the most difficult to implement, would be to target page functions that require server time for processing. This completely bypasses any caching

system on the front end because the server must respond and dedicate run time to processing the information. This would be quite simple to achieve by automatically pasting data into forms and submitting the data. But, with clear insight by browser developers, it is not possible to do a remote 'submit' call to a site from a client-side Javascript. We're currently investigating ways around the blocking, but the most promising development is the spread of open-source systems such as Linux. Being open-source, all the functions are available and so *the electrohippies* could develop their own browser with special features specifically tailored to distributed client-side DoS actions.

But whatever measures and countermeasures are employed, the basic approach of the electrohippies, and the use of client-side scripting, means that the 'democratic guarantee' is still there. It will still take tens of thousands (if not hundreds of thousands) of people acting over a short period to make the action effective.

Legitimising DoS – balancing free speech with foul deeds

There is one further issue that must be dealt with regarding any type of DoS action - **legitimacy**. *the electrohippies collective* have evolved a general set of principles that govern not only our action, but also the 'lending' of our activism tools to other groups. Everyone, no matter how foul, has the right to express their views, so long as those views do not intimidate or abuse the rights of others. DoS actions are of course in direct contradiction to this principle because by closing a web site you are in effect preventing freedom of speech, and in a virtual sense, freedom of association. It is important therefore that any DoS action is not undertaken on a whim, but is clearly and openly justified.

the electrohippies collective believe that the acts or views perpetrated by the targets of a DoS action must be reprehensible to many in society at large, and not just to a small group. It is on this basis that the collective undertook the action against the WTO during their conference in Seattle, and it is also the basis upon which we are planning future actions.

The important issue regarding the justification for a DoS action is **proportionality**. It is not acceptable to disrupt the communications of an organisation on a general basis. The 'event' that justified the use of a DoS tactic must provide a focus on which the debate about the activities of the organisation with a particular set of actions – for example a court case, a conference or product launch. *the collective* undertook the action against the WTO during their Seattle conference because it was clear that the one event would produce a public dialogue about the past conduct and the future course of the organisation. In actuality, *the electrohippies* event provided an opportunity for around 450,000 people (over 5 days) across the globe to express their dissatisfaction with the WTO – and without the risk of being gassed by Seattle's 'robocops'.

The effect of the action must be to **substitute the deficit of speech** by one group by encouraging debate with others. During the period *the electrohippies* WTO action was undertaken our web site provided a large number of links to sites containing information about globalisation, free-trade and it's effects on society and the environment. These pages were selected from those who were both for and against the position of the WTO. In our view this packaging of a resource for people to explore and learn about the issue ensured that they were fully aware of the issues when taking the action. It also ensured that others visiting

our web site could explore both sides of the argument.

Finally, there are two important aspects to the operation of the electrohippies collective that we believe are important to anyone undertaking electronic activism or electronic civil disobedience – **openness** and **accountability**. *the collective* does not use encryption as part of our communications with each other, and with those we associate with, as a matter of principle. We have nothing to hide, as we believe that our purpose is valid, and so we do not seek to hide it from any authorities who seek to surveil us. Likewise, we do not try bury our identities from law enforcement authorities – any authority could, if it chose to, track us down in a few hours. However, because some of us work in the IT industry, we do not make our general membership known because this would endanger our livelihoods. **The right to take action against another entity on the 'Net must be balanced with the principle of accountability.**

The future for electronic activism – definitions and dissent

The mission of *the electrohippies collective* is to assist the process of change towards a more fair and sustainable society using only electrons. **Electronic communications and the new media represent a new space within society that we have to utilise as we would the street or the council chamber.** Our aim is to use our skills to make tools available for ordinary people to do undertake electronic activism themselves. We must reduce the complex to the everyday, and enable people to access technology and use it to further their own causes.

Many of the people responding to electronic activism, such as the *iDefense* group, perceive this point of view as a threat to the democratic order. To put it simply, politicians and the forces of the status quo are not the defenders of democracy – they merely administrate it. The real defenders of democracy are those who dissent from the status quo, for by that dissent they make democracy viable. Therefore, if we wish to defend democracy, and prevent society slipping into the sort of technological nightmare described by many 20th Century sci-fi authors, then it is up to those who lead dissent to take the initiative in developing electronic activism. If we do not then the forces who wish to develop the new electronic media will run rampant – unchecked by the ordinary democratic forces that operate in 'real life' society.

the collective are definitely not **cyber-terrorists**. Anyone who says we are is misrepresenting our position, and is debasing the real meaning of the term 'terrorist'. One of the implicit meanings of the term *terrorist* is the use of violence for political ends. How can you have violence in cyberspace? If so, how do we evolve such a definition? Does **cyber-violence** mean the use of computer systems for purposes they are not programmed to do? Such a definition would not include the act of cracking (since the system would be responding as programmed), but it would include any damage done to systems once a system was successfully cracked. If we accept this definition of cyberviolence then we engage in 'non-violent' action; the use of systems in ways they were programmed to be used, but used in a mode as to convey a message or protest. Such a definition encompasses everything from sending an email to a politician to a full-scale client-side distributed denial-of-service actions.

The Internet is a mechanistic system - hence it is fundamentally dumb, and can only apply terse logical rules. The public can use this characteristic of the 'Net to engage in collective

actions to get their message across – deconstructing the intended message to be broadcast in cyberspace and placing the alternative viewpoint. To adapt the catch phrase from the film *Alien*, ‘In cyberspace everyone can hear you scream - if you want them to’.

What we're all about is bringing community accountability to the Internet. Government's and corporations are setting up stall on the 'Net in the expectation that the space is immune from the normal pressure present in society – like a new frontier.... but it isn't. We have to treat cyberspace as if it were another part of society. Therefore, we must find mechanisms for lobbying and protest in cyberspace to complement those normally used in real life. Without public pressure cyberspace will have no moral or normative controls to control the excesses of politicians, groups or corporations who would seek to dominate that public space.

What's next

Within the next two months *the electrohippies collective* will be launching a new week-long action in support of a global campaign by other organisations. This will utilise two new tools:

- A new, improved virtual sit-in tool, developed to tackle some of the challenges created by new caching technology;
- A new tool developed to work with email based actions that enables people to quickly create detailed emails and send them to agencies and decision makers in order to lobby for change; and
- We will also be releasing the first of our ‘do it yourself’ (DIY) electronic action kits based on the above tools.

The first of these tools is complete, and is just undergoing compatibility tests across various browsers and platforms. But the DIY kit is complete – it tools is already ‘out there’ on the ‘Net being beta-tested as this paper is written through people developing new client-side DoS actions with it. The second email tool is currently under development, but will be rolled out for our special action in April. Likewise, there will be a simpler DIY version to accompany it.

However, in distributing these tools the collective are putting conditions on their use:

1. The tool must be used as directed in this manual. The code must not be changed, or the program modified in any way not intended by *the collective*. All identifying features within the program and it's resident web page must be retained.
2. The users of the tool must identify themselves – in a way traceable by law enforcement authorities – in the space provided within the tool page.
3. The users of the tool must include within the tool details about the motives of their group in promoting the action – the tool must not be used for any kind of ‘covert’ DoS action.
4. The targets of the action must be informed of the groups’ intentions to use the tool at least two days before the action starts, and this warning should include the basis of the justification.
5. Most crucially, the use of the tool must be objectively justified by those using the development kit. This justification must be included within the final web page for all to see before they are asked to engage in the action.

6. When planning the action you should seek to contact the electrohippies and inform us.

There are many who criticise our approach of 'openness and accountability'. Some equate it with 'turning yourself in' before the action. We however view it as a basic guarantee of human rights, for both those taking part and those who are the subject of the action. But in our view this essential for two reasons:

- Firstly, it ensures that the tool is only used in justifiable situation. If the group using the tool do not feel they can be open about its use then we consider that their action cannot be considered justifiable. A justifiable action cannot be mounted from behind the mask of anonymity.
- Secondly, the use of openness and accountability is essential to defeat the notion of the 'Net being hijacked by 'terrorists'. If the 'Net is to be used as a valid tool for protest and dissent then we must develop it in a manner that makes it hard for the State and law enforcement authorities to challenge the validity of the tactics. Being open and accountable, and demanding our constitutional rights as part of virtual actions, is crucially important in this respect.

This, really, is THE issue that defines the purpose of our actions. We must make cyberspace another, equal, part of society. We will not achieve this by developing ever-better methods of financial transactions and accounting. We will do it by extending the ordinary legal and moral guarantees of freedom of expression and association to this space, and promoting equal access irrespective of race, class or language. If the state and corporations cannot tolerate dissent in cyberspace, then they will have a widespread, and legitimate, backlash from those already using the media for this purpose before the advent of e-commerce.

For further information visit *the electrohippies* website. Also, to keep abreast of the latest information join the electrohippies mailing list at:

<http://electrohippies.listbot.com>

DJNZ

action tool development group,
the electrohippies collective

February 2000

¹ *the electrohippies collective* are a 'virtual group' in the sense that their activities are organised and carried out solely on the Internet – they do not meet. The aim of the group is to extend the philosophy of activism and direct action into the 'virtual' world of electronic information exchange and communications. Why use the name 'electrohippies'? It's based upon a situationist paradox that seeks to promote a positive message by exploiting it's negative connotations. But it's also a nicely comical label, with plenty of stereotypical overtones, that we can exploit as a means to make our point about the position of ordinary people within the global 'new world order'.

² For example, *Denial of service hackers take on new targets*, CNN Online, February 9th, 2000

³ *Inside the hacker's web*, The Observer, 13th February 2000

⁴ *Netcos to attend Whitehouse security 'Cybersummit'*, The Industry Standard, February 11th, 2000

⁵ This action was launched globally from the 30th November to 3rd December 1999. For a report see the electrohippies web site.

⁶ The *iDefense* group (www.idefense.com) is an e-commerce defence organisation that provides reports on 'cyberterrorism' to journalists. We picked up their report as part of an article in the Christian Science Monitor *Bandwidth* column on 3rd January, 2000.