

Hacking the Undernet: Libertarian limits; commercial containment

Jane Long, University of Western Australia
Matthew Allen, Curtin University of Technology

This is an authors' draft of:

Long, Jane and Matthew Allen. (2001). Hacking the undernet: libertarian limits; commercial containment. *Australian Journal of Communication*. 28.3: 37-54.

Introduction

Internet Relay Chat (IRC) dates back to 1988 and the development by Jarkko Oikarinen of an Internet protocol and associated server and client programs to handle real-time text-based chat between multiple users, going far beyond the original one-to-one 'talk' function used over the Internet up to that time. IRC was the last of the three great pre-Web developments in Internet communication (the others being email and Usenet news – both of which were not real-time) and it grew rapidly in popularity (Mirashi, 1993 provides a good early history; see also Chatserver.org, n.d.) for its tremendous capacity to allow social interaction in new forms, without the need for physical presence.

The heart of IRC are the servers through which the networks come into being and through which user communication passes. Thus the administrators of these servers are highly influential participants in the overall management of IRC networks. Assisted by so-called IRCops (operators), they maintain the networks. Channel operators have very limited powers, relating to the capacity to maintain the channels in which most IRC discussion takes place. There are, relatively speaking, a tiny number of administrators and IRCops. Originally thought of as one network, IRC has become more diffuse. Over a decade, differences of opinion amongst the powerful administrators and IRCops over technical organisation, the degree of control to be exerted over users' actions, and the management of the administrators' own roles and responsibilities have seen networks 'split off'. Equally, the increasing size of IRC made it impossible to provide good services to all of the potential users within one network. Thus, today, there are over 300 distinct networks offering IRC (with four main ones accounting for the majority of users), and millions of users. At any one time, some 500,000 users are simultaneously connected, normally chatting in one or more of over 250,000 channels (what AOL calls 'chat rooms') allowing public discussion while also able to conduct private chats. Some 3000 servers interlink to form these networks (Gelhausen, 2001).

While IRC has inspired many different kinds of chat programs and environments and is now increasingly linked into the World Wide Web, rather than standalone IRC clients, it remains a significant element in everyday Internet use. Yet it is strangely anachronistic in this era of highly graphic, website-driven Internet interactions: textbased, not needing a web-based interface, highly programmable and adaptable and with a decentralisation of capability and action. Furthermore, it remains determinedly chaotic / libertarian / anarchic (depending on one's definitions); it remains almost entirely free of commercial exploitation. No-one pays to access IRC (once connected to the Internet); no-one really profits financially from it (least of all

those who devote significant time to running it or who donate bandwidth or server space to support it).

Yet IRC is not without risks and threats. Regularly the terrain for hacking-style activity, IRC networks have from time to time been the *target* of attempts to hack or deny service. As we will discuss in this paper, one such attack took place in January 2001, aimed principally at the Undernet IRC network. A prolonged and severe denial of service attack put the future viability of Undernet in doubt; it has taken some months for service quality to be restored. The circumstances of the attack and the responses, both technical and social, within Undernet are enlightening in themselves. But, they also allow us to explore, contrast and match up the *limits* of the libertarianism which seems embedded in the socio-technics of the Internet and the possible and actual *containment* of 'free' services in a 'free' market, through the operation of commercial transactions.

Understanding IRC as an object of study

The IRC environment has, of course, been a significant focus of research study for a decade or more. Since Reid's ground-breaking and much-cited work in 1991, many researchers of the Internet have looked to IRC for evidence and examples of 'virtual community' and the dynamics of Internet culture. This research has mainly concerned social interaction, through language and represented action, and the groups and textual spaces in which it occurs.

In this later IRC research, what is sometimes ignored is that, in Reid's original formulation, community was associated with a broader concept of culture. For example she asserted that

The measures which users of the IRC system have devised to meet their common problems, posed by the medium's lack of regulating feedback and social context cues, its dramaturgical weakness, and the factor of anonymity, are the *markers of their community, their common culture* [emphasis added] (1991).

Reid routinely describes the IRC collectivity as either or both 'community' and 'culture' in quick succession (1991: see particularly, the conclusion).

Equally, Reid's primary concern was with the overall collective of users in IRC as a whole, rather than any specific group of users within it. This aggregation of users formed a qualitatively different kind of community than the specific-interest groups on which most later writers have tended to concentrate. The specific interactions between users, textual and representational, did not of themselves create community: rather, the shared commitment to imagine a world and act within it in certain ways. Further, while later writers have regularly referred to the objects of their research as 'virtual communities', this appellation is not always helpful. Reid's central concern is worth remembering. For Reid, IRC was not about virtual community directly since the creation of a virtual reality – a reality of interactional space in this case – was the *process* of community formation, and *not* a comment on the nature of that community. Effectively, the 'virtualness' of the community was part of its coming-into-being, rather than its central defining quality (See also Wellman and Gulia 1999: esp. 169-171).

The shift in most research about IRC away from the system-wide concerns of Reid towards an emphasis on individual elements within it is a corollary of the increasing emphasis on the communicative and conversational aspects of IRC. Rheingold, in his highly influential *Virtual Community* monograph (1993: Chapter 6), posed the question: “For a student of virtual communities, IRC is an opportunity to observe a critical experiment-in-progress: What are the minimum elements of communication necessary for a group of people to cocreate a sense of community?” Except where Rheingold drew upon Reid, he tended to exclude the other, significant elements that structure the IRC experience – the technical work involved in managing and maintaining and expanding the IRC network. Since the conversations, the interactions that enable this technical maintenance are largely hidden, researchers instead picked up the communication question and have produced excellent but, therefore, incomplete accounts of the nature of IRC (see for example, several excellent papers in the *Journal of Computer-Mediated Communication*: <http://www.ascusc.org/jcmc>). In doing so, the word ‘community’ became associated primarily – even *exclusively* – with online groups that played, debated, exchanged information, and generally performed via IRC (and other avenues) to constitute a shared social space around particular topics, interests, and so on.

This narrowing of meaning and association for the term community was also influenced by a concurrent thread in Internet research concerning Usenet newsgroups. As with initial forays into IRC research, earlier, ground-breaking research (principally by Michael and Ronda Hauben, ???) into Usenet had identified the totality of newsgroup users as a form of community, “a world town meeting” or “the Wonderful World of Usenet News”; the Haubens also emphasised the technical architectures through which the overall Usenet system was maintained. Later research tended to concentrate on the specific social groups within and around particular newsgroups as examples of ‘community’ identity (???). Research into both IRC and Usenet has mainly emphasised the quality, meaning and process of human communication, mediated by computer, involving substantial exchanges of information both as a process for community-building but, increasingly, as the *result* of a community that is already assumed to exist. The communities that exist, in the background so to speak, sustaining and running the structures which permit channels and newsgroups to serve as the places of social interaction are occluded.

To understand the difference, it is worth returning to the mythos of the ‘frontier’, so regularly used in the 1990s, principally in America, to try and write the politics and meaning of cyberspace. Many problems have been identified with the individualist, libertarian and colonising ideologies inherent in the frontier myth (Barbrook and Cameron, ???; see also Werry 1999). An additional one, not normally considered, is that describing cyberspace as a frontier *presumes* the existence of the space into which the community developers and settlers such as Howard Rheingold, John Perry Barlow, Ester Dyson, George Gilder and the multitude of anonymous others were to move. However, these self-styled settlers were preceded by another community, or set of interlinked communities, comprising the engineers and scientists, hackers and coders, sysadmins and operators who – effectively – created the virtual terrain later labelled as ‘the frontier’. Some who utilise the frontier mythology regard these creators as the ‘natives’ to be colonised or even driven off the frontier, (Werry, 1999) but, in effect, that still leaves open the question of who created the cyber frontier in the first place.

IRC has, for a long time, been understood by researchers (and, indeed, most of its users) principally in terms of what is visible: the wide choice of available networks, some very large, a few almost too small to be considered a 'network'; each with an array of channels reflecting, mostly, the size of the total 'population' of that chat network; the individual users; and, of course, the product of these users' interactions – a constant scroll of conversations public and private. Some, interested in the technologies that enable this long-established Internet activity, see behind the surface, the scroll, the human interface, to the computing processes on which computer-mediated communication like IRC depends. Many of these are interested in the damage which they can cause through greater mastery of technologies than the average user; they seek to promote technologised interaction to the level of social interaction. Only a few, who work to maintain the networks and their segmented channels, understand IRC quite differently: seeing its infrastructure and design as their principal responsibility. These few form a community of administrators. The primary purpose that binds individuals together in this community is the provision of the *opportunity* for social interaction by others. This opportunity is, on the net, all but identical to the interaction itself, formed from packets of data flung far and near through a patchwork of routers and networks, servers and client. But, in social and economic terms, the difference is wide and the story of the attack on Undernet provides a way for this *difference* within the 'meta-community' of IRC to be re-instated.

The Undernet hacked

In January 2001, the Undernet, one of the four largest of many Internet Relay Chat (IRC) networks across the world, came under sustained, damaging attack. The attack took the form of a 'distributed-denial-of-service' (DDOS) attack against some of the forty-five individual servers that, when interlinked, provide the Undernet's technical infrastructure through which individual users maintain channels in which real-time textual conversations occur. The attack consisted of sending enormous quantities of information to the servers concerned, thereby overwhelming them. As the Undernet notice to users stated:

These recent attacks on individual IRC servers have been intense, often in excess of 100 mbps [megabytes/second]. To demonstrate a frame of reference...many of the ISP's hosting IRC servers are utilizing resources of at least a multi-homed DS3 data pipe (45 mbps), costing \$18,000 - \$35,000 per month (Undernet, 2001)

The offensive originated from a single source but, as the name of the attack makes clear, this hack was conducted (like most effective Internet applications) in a distributed manner. A single source, using simple scripts (small snippets of code) took control of many other systems through their own security weaknesses and then used these otherwise innocent sources to launch simultaneous attacks from many places at once (see Farrow, 2000 for a detailed, accessible description). Since these systems were high-bandwidth, they were then more effective in the distributed attack (Undernet, 2001). Higher-bandwidth internet connections, as provided by ADSL and cable modems, are normally more vulnerable to hacking because they are assigned a single, stable IP address and are 'always connected'.

The effectiveness of such destructive action had already been shown in February 2000, when DDOS attacks brought down, temporarily, premier ecommerce websites

such as amazon.com, eBay and Yahoo (Knight, 2001). Moreover, during 2000, hackers developed more sophisticated tools such as the Trinity script which could exploit the particular openness of IRC, installing itself quietly within cyberspace and awaiting activation before deluging target servers with meaningless data and requests for response (Hansen, 2000). Such attacks proved hard to trace and hard to stop, despite the collaborative efforts of the many Internet service companies involved. An earlier effort to attack the Undernet in January 1997, known to be Romanian in origin, had involved a more traditional flooding effort, from one machine which, while damaging, had been easily traced and stopped (Coale, 1997).¹

Undernet was not, by any means, singled out for special treatment. While Undernet was the primary target, statistical analysis of IRC traffic at the time shows that Dalnet and Efnet were also affected (see also Delio, 2001 and Gelhausen, 2001). Nor has IRC itself presented a unique target. A report in June 2001 (Lemnos) indicated that as many as 4,000 DoS attacks (not always distributed) occur weekly and, embarrassingly, a recent victim included the Computer Emergency Response Team Coordination Center (CERT/CC) website – the public face of an organisation dedicated to maintaining Internet security. Since the attacks are basically unstoppable, denial of service risks have prompted much alarm. Initial security, especially within IRC, tends to rely on individual users. As the CERT/CC itself advises, “The result [of IRC’s architecture] is a broader base of exposure to risk across a network with less central control, making security policies that allow chat client usage difficult to implement and enforce” (Houle, 2000). And, equally, “Responding to a denial-of-service attack may require the cooperation of multiple parties” which can severely limit the rapidity of response (CERT/CC & FEDCIRC, 2000).

However, while the quantity and extent of the attacks may be a cause for concern, we should also note that the CERT/CC is, intrinsically, required to be concerned about such attacks and news reporting of the incidents tends to be excessively alarmist (an exception, which also indicated some scepticism about CERT, can be seen in Delio, 2000). In most of the myriad attacks that, it seems, regularly occur on the net, individual websites are the target and, in most cases, the sites attacked are prominent enough to be equipped to respond rapidly, if not always as soon as would be preferred. The consequences for the Undernet (and, in future, for other IRC networks should they be the primary target) were however, more severe and significant for a number of reasons that we will now outline.

Firstly, Undernet is, unlike most other targets of DDOS, a network. As a result, actions against one element (one or other servers) can severely disrupt others in a variety of ways. The data traffic through remaining servers increases, slowing them down, reducing their capacity to host all users; as a result, lag-time (the time between the sending of a text message and its arrival) increases also; further, ‘splits’ (where a server that links one segment of the network to another ‘delinks’) become more frequent, throwing added pressure onto servers that remain linked. Under these conditions, the very strength of IRC (that it involves interaction and communication amongst diverse users in, effectively, a peer-to-peer network) becomes a weakness.

¹ It is likely that the rumour stating that the source of the 2001 hack was Romania came from confusion with this original attack: see discussion at slashdot.com, 2001.

Too many users, too much data, too small a network capacity and IRC becomes unworkable, both technically *and* socially.

Secondly, Undernet is not a commercial operation but, instead, depends upon two forms of donation. Firstly, as Beth Healy, formerly an Undernet administrator said, “The vast majority of Undernet volunteers, including IRC operators and administrators, are people who have real jobs and families and concerns and yet make the time to help maintain the network and continue to provide a totally free service to its users” (cited in Delio, 2001). Secondly, the servers which form the Undernet are primarily provided free-of-charge by Internet service providers or companies that host websites (see Evers, 2001). Therefore, the Undernet was not only vulnerable because the attacks significantly increased the time commitment and workload of the unpaid administrators, but also threatened the financial viability of the Internet businesses whose entire operations were affected: “While providers are currently paying for the resources to provide a free IRC environment, they cannot do so if they suffer substantial losses of business revenue” (Undernet 2001).

There was a significant consequential effect of the attacks on Undernet. The network continued to function, albeit with slowness, interruption and unreliability, and users responded as best they could. However, in the DDOS, key automated services that regulated Undernet (the X and W service bots that maintained channel and operator status integrity) were now missing, unable to run because of the attacks. These services normally functioned to prevent registered channels from being taken over, or otherwise interfered with, by unauthorised operators. This particular effect of the attacks also reveals something of the motivation for them. Undernet publically announced that the attacks were primarily designed to affect some Internet business operations, probably to ensure that the attacks were treated seriously and to insulate Undernet from criticism that it was somehow responsible (Undernet, 2001). But the general chaos caused on Undernet, especially in the absence of the service bots, caused a massive increase in the lower-level disruptive hacking-style activities routinely plague the network.

These activities are not directed at the network’s existence, but at the social fabric built through it. They involve flooding individual users, or channels, trying to take control of channels, running scripts that break down the capacity of people to use IRC. The perpetrators, usually called ‘script kiddies’ (derogatory of their ‘real’ hacking abilities and age), have no specific intent in mind, it would seem, except vandalism. As one Internet user commented:

Efnet, undernet, chatnet, all the big nets. the PFY's known as scriptkiddies (some of them not even youthful pimple faced youths anymore) go to IRC because it's somewhere that magically makes their penis extend two or three whole inches, just because they can find some person or some group of persons, cause them a great deal of displeasure, and say "Look what i did!" to their buddies. (see Slashdot.com, 2001)

It’s a game, effectively, and administrators, and IRC operators, as well as automated channel and similar service bots play a part in controlling these activities. Always a part of IRC, these attacks became an equally dangerous threat to the functioning of Undernet under the adverse conditions of the external hack, suggesting that the two were not unrelated. Indeed, one administrator was reported as saying “the attacks were likely to be the result of some IRC channel feud” (Knight, 2001)

The responses to the DDOS attacks varied and reveal much about the pattern of 'libertarian limits and commercial containment' which forms the concluding section of this paper. Effectively, there were three main groups responding: the Undernet administrators and operators (IRCops); the providers (usually commercial) of server space; and the multitude of Undernet users. The Undernet administration's response remains, in most respects, hidden. Its public statement indicated that Undernet administrators were seeking to locate the source of the attack but cautioned that "the cooperation and assistance of Internet backbone providers is required", suggesting they did not imagine an early end to the attacks. (Undernet, 2001). Since the attacks continued for some months and then ended without any apparent success in tracing them, Undernet's response was, in the end, unable to affect the situation.

Undernet also noted that it was "cooperating with U.S. federal law enforcement authorities" but made no further reference to the way in which this cooperation was occurring. Notably, some news reporting (Delio, 2001) of the Undernet hack highlighted the extensive cooperation of other IRC networks, such as Dalnet, with the FBI and the successes in tracing and prosecuting hackers, implying that Undernet was less inclined to work with law enforcement agencies or, at least, did not wish to be too open in its collaboration. The admins and their team of IRC operators had more than enough to do assisting in keeping the social fabric of Undernet together. One channel owner reported:

Someone tried to compromise our channel yesterday (a takeover, for the unschooled) but order was restored. With W (X for other channels; we happened to have W when he was still around) the oplist, auto-kicks, and bans are very easy to store; without W, the guy managed to get ops by pretending to be one of us. Could have done some damage, but thanks to some IRCops (Thank you seti and saralee!) order was restored, new bots put in place, and new channel policies....

Right now there's rumors that W and X will never come back. If they don't Undernet is dead...and where is a channel to go? Some IRC networks have strange ident issues; some are dying out; and some have a structure such that it's hard to even keep hold of a channel because of skript kiddies [sic]. (Slashdot.com, 2001)

For the commercial operators who, effectively, were most at risk from the attacks and suffered the financial loss, there was little that could be done in the short-term if they wished to remain committed to IRC. One said "It is impossible to counteract the attacks. All we can do is sit and wait for the attack to end" (Evers, 2001). Some, however, suspended and then completely ended their IRC server activities. From a high of 45 servers in 1999-2000, dropping to an average of 40 in late 2000, servers linked to Undernet went down below 25 (for a comprehensive time-based survey see Gelhausen, 2001; see also irchelp.org, 2001). Since the attacks have stopped, it is notable that the US servers have declined from approximately 70% to less than 50% of the total servers available to Undernet (see <http://www.undernet.org>), probably because, in Europe, servers are more likely to be located within universities and thus less susceptible to the need to be withdrawn from service for commercial reasons.

One server owner, however, went further. AT&T through its WorldNet ISP business (one of the most commercially oriented owners of an IRC server), took the opportunity of the Undernet crisis to withdraw its link to IRC and, instead, introduced its own, commercially oriented chat and community service. On the AT&T webpage (formerly devoted to assisting Worldnet customers to access IRC), it declared:

On March 15, 2001, the IRC Chat Server donated by AT&T WorldNet Service was closed. Our strategy has refocused on building community through AT&T WorldNet's Community Port Chat. We think you'll like it and encourage you to visit us (at: <http://help.att.net/care/ccforums/chatclients/>).

The final area of response lay with the many users of IRC and those users with limited operator privileges to enable them to run and maintain channels and, as well as the technical work of maintaining channels as described above, these responses were mostly social in their character (this material based on observation and discussion by the authors). Users and channel operators were, first of all, highly anxious about the situation and open channel discussion focused heavily on the likelihood, desirable or otherwise, of having to move to another network or, even, to rely on other forms of real-time chat such as ICQ (I-see-you) or Microsoft Messenger (MSN). In an indication of the deep, strong bonds of identity and collective membership of channels, the 'move' to another network seemed a threatening prospect, even though, in technical terms, little would change. Some of this anxiety was undercut by a dark humour: in response to the rumour that Romania was the source of the attack, some users adopted fake Romanian nicknames (Count_Vlad as one example). Of course many IRC users, perhaps those with less identification with a particular channel and a particular group of regular friends, simply stopped logging on or changed networks, further emphasising the social danger of the attack.

Users, who normally are accorded little, if any, technical status within IRC, also became an important source of strength. In the absence of the channel integrity services normally provided, the only way to prevent a channel being taken over by outsiders intent on vandalism (ie taking over, then preventing regular users from joining) was to allow trusted users emergency status as channel operators (with the power to prevent takeovers). Normally, in the absence of operators, the bots take care of the channel's integrity: in the chaotic conditions of the hack, real users had to stay in channel, ready to defend it, at all times. The global nature of IRC meant that, at least in well-populated channels, with hundreds of regular users, a standing watch could be maintained. This limited and emergency increase in authority helped to build an even stronger social network amongst regular users of specific channels.

The denial of service on Undernet was significant and successful for a time and, certainly, raised a very real prospect of the potential collapse of that network. As one former channel operator said:

If we don't do something, IRC will die just like Usenet did. Spammers and idiots have all but killed Usenet. I think IRC is next. It's sad to see...all the conversations between folks about all the important and silly things dry up. (in Delio, 2001).

With hindsight, the fear that this attack meant 'the end' for IRC was ill-founded; but to dismiss it entirely would be to mistake the pervading sense of fragility that surrounds IRC. As our concluding section demonstrates, the Undernet hack does

suggest that there are dangers for IRC; it's just that they do not emanate directly from the hackers, script kiddies and others who are the root cause of the denial of service attack. Rather the danger lies in the political economic conflicts being played out in cyberspace

Libertarian limits, commercial containment

Libertarianism

Libertarianism is the dominant political discourse through the Internet is constructed in contemporary culture. As Winner (1997) wrote, "...a philosophy of sorts has already taken shape in this domain, a widely popular ideology that dominates much of today's discussion". Central to this discourse is a "radical individualism" sustained by a deeply determinist view of the new technologies within which individuals would find a liberty denied to them elsewhere; moreover it embodies and accepts the principles of free-market economics (Winner, 1997). Such libertarianism is not without challenge (for example, see Horvath, 1996). Nevertheless, libertarianism is, in Boyle's words, "the 'default' point of argument, the place from which discussion [about the Internet] begins" (1999), even though much of what passes for discussion amongst the libertarian evangelists is based on a shallow philosophical foundation and built from a motley assortment of empirical evidence.

Barbrook and Cameron (19??), who famously described cyberlibertarianism as the "Californian ideology", identified the marriage between ideals of individual freedom and a particularly vigorous form of New Right economics as a defining feature of the ideology. Libertarianism, when inflected with free-market economics, overstates its positive goals and underestimates its weaknesses and repressive tendencies. However a different inflection to libertarianism, drawing on traditions within anarchism, rather than capitalism can envisage a more redemptive politics of the Internet (see Valauskas, 1996 for an excellent statement of this position). Central to this *different* libertarianism is the gift economy, best analysed in the separate work of Peter Kollock (1999) and Richard Barbrook (1998) (see also Rishab Alyer Ghosh, 1998; Rheingold, 1993).

The gift economy is, for Kollock, an explanation as to why the Internet, in the absence of "central authority" and systems of sanction, is distinguished by the fact that it "is not literally a war of all against all" and is marked by a "great amount of sharing and cooperation" (1999: 220). It leads Barbrook to claim (only slightly provocatively) that the net is "really existing anarcho-communism" owing its character to the origins of the Internet in a scientific community that was already close to a form of communism, even as it was set the task of defeating the 'communism' to which America was opposed in the Cold War.

The gift economy is not selfless: rather, it describes the exchange of free (but valuable) information and products for individual rewards of increased recognition amongst one's peers (especially for software developers), personal prestige, attachment to groups who value such activities (giving identity and a sense of belonging), and also a sense of satisfaction with the efficiency with which the Internet is working (Kollock, 1999; Barbrook, 1998). As Kollock explains, on the Internet, it becomes far easier for valuable goods to become public. The digitisation of information and product massively reduces the costs of distribution; the global

connectivity of the net increases the size of the potential market increase to the point. Thus, those who might otherwise be dissuaded from investing their time and resources into information publication or product development because the returns of prestige and satisfaction would only come at significant personal financial cost, are now able to 'give away' their time and effort because the reward will be much greater, at lower cost.

The gift economy of the Internet has, until now, been analysed primarily in terms of the production and circulation of *information* (ie advice, help, news, collections of knowledge resources) and *products* (principally software, notably the free and open-source Linux operating system but including countless applications for all forms of computing). What IRC reveals, however, is that another aspect of the Internet falls within the gift economy. Those who form the administrative community of Undernet and other networks provide a gift of *service* or opportunity to Internet users. Giving away this service, in return for non-financial, group-mediated rewards of prestige and satisfaction, produces the possibility for freedom on IRC. Moreover this economic system is libertarian since it depends on and champions the individual administrator's skill, commitment and right of refusal to be involved: just as IRC is a network of unique servers that *then* become linked, the community is a social network of individuals who, in their very desire to become a community, embody their own sense of individual authority and responsibility.

The limit, of course, is that when attacked, the personal cost of IRC service promise increases dramatically (both for those commercial operators who also participate in the gift economy) and for the many volunteers who have to respond with their time and effort to a seemingly lost cause (and, in the process, lose some of the prestige which normally attaches to them for offering an 'efficient' service). The real threat, then, that the Undernet hack (and all similar attacks) posed was in challenging the possibility for the continuation of the gift economy of service that defines IRC.

Commercial containment

Those seeking commercial exploitation of the Internet have had mixed views of the way that they might profit from the development of virtual communities such as are to be found within the networked social interactions of IRC. Communities were at first dismissed as emblematic of what was *wrong* (from a commercial view) with the Internet, then seen as a target for marketing, but have, in many current business models for Internet commerce, now become central, providing corporations not only with an audience for its own products and the advertisements of others' products but also with a ready supply of community-generated content, activity and events, thus meaning that community "is being rapidly integrated into existing networks of corporate commodification" (Werry, 1999). To achieve this end, the principle policy is one of *containment*. If a community and its membership is contained within those parts of cyberspace controlled by the corporation sponsoring the community, then it can be more effectively exploited for profit and sustained against the competing attractions and demands for attention elsewhere on the 'net.

An example can be seen in the only substantially successful commercialisation of IRC yet seen. TalkCity (<http://www.talkcity.com>), one of the examples used by Werry, began life as an IRC network before moving to a single server and a web-based chat experience that owes more to the approach to online community of

Yahoo.com than to its origins in IRC. Users of TalkCity are, effectively, contained within the boundaries established by Talkcity and offered the promise that all their requirements for information and Internet activity, community and interaction can be met from that single place. Since TalkCity is no longer a network, this containment is reflected in technology: all user interactions focus through a single server, controlled by the corporation. No doubt WorldNet's new chat community will operate in a similar manner; and, when some members of Dalnet feared its impending commercialisation, a central concern was that one of the most influential administrators of Dalnet would exploit his technical control of Dalnet servers to contain and then exploit the Dalnet user-base (see <http://dalnet.org>).

In dealing with the challenge of the denial of service attack, Undernet had to face the threat that users and producers of IRC chat experiences would recognise that commercial operations could also provide a more effective response to this kind of hacking activity by containing the technological openness and social freedom from responsibility which, at base, led to Undernet's vulnerability. Liberty is deeply engrained within IRC (for example, on ircnet, server operators and administrators do almost nothing to restrict script warfare or offer channel maintenance functions and, indeed, most of the social splits in IRC networking have been caused by arguments about the resolution of individual freedoms and group needs). But, in exposing its social and technological limits, the Undernet hack provided an opportunity for containment to seem a worthy alternative (again, it is notable that Dalnet has been, at times, a highly regulated network, a kind of proto-containment indicating a possible move to commercialisation).

Reversing the polarity: containment contained; limiting the hack

But, in the end, there are no easy justifications for commercialism, nor is it possible to dismiss libertarianism. For, the Undernet hack also shows how commercial exploitation is itself contained...contained within broader, more expansive internetworked spaces. The boundaries that commercial containment places around communities to organise their members for exploitation, also help define, perhaps more clearly, the freedoms and possibilities that lie outside those containing walls. The libertarian commitment to open code, limited regulation and individual achievement that makes IRC vulnerable to attack, also helps to *limit* the dangers of cyberattack because there are no static targets. When the service that produces the spaces of community interaction is itself distributed, denial of service attacks are less capable of long-term success. The contained spaces of the commercial world may have more stout defences, may have more to lose if they succumb, but they present targets which are also more easily identified and threatened.

References

- AT&T. 2001. *AT&T Worldnet Service* website. Available at: <http://help.att.net/>.
Barbrook, Richard and Andy Cameron. ????. *The Californian Ideology*. ???
Boyle, James. 1999. *Libertarianism, Property and Harm*. ???

CERT/CC & Federal Computer Incident Response Capability (FedCIRC). 2000. *CERT® Advisory CA-2000-01 Denial-of-Service Developments*. Available at: <http://www.cert.org/advisories/CA-2000-01.html>

Chatsserver.org. nd. *IRC History*. Available at: <http://chatsserver.org/history.asp>

Coale, Kristi. 1997. Romanian Cracker Takes Down the Undernet. *Wired News*. January 14. Available at: <http://www.wired.com/news/print/0,1294,1446,00.html>

Evers, Joris. 2001. Attacks on IRC network hurt other Web services. *CNN.Com*.

Delio, Michelle. 2000. The Internet is Falling ... Not! *Wired News*. September 18. Available at: <http://www.wired.com/news/print/0,1294,38844,00.html>

_____. 2001. IRC Attack Linker to DoS threat. *Wired News*. January 12.

Farrow, Rik. 2000. More hype, or a hint of new DoS attacks?. *ZDNet News*. December 7. Available at: <http://www.zdnet.com/zdnn/stories/news/0,4586,2662473,00.html>

Gelhausen, Andreas. 2001. *Networks of the Internet Relay Chat*. (Website). Available at: <http://netsplit.de/networks/>

Hansen, Evan. 2000. New Web attack tools exploit chat technology. *Tech News*. September 5. Available at: <http://news.cnet.com/news/0-1005-200-2701686.html>

Hauben, Michael and Ronda Hauben. ????. *The Netizens And The Wonderful World Of The Net: An Anthology*. Available at: <http://studentweb.tulane.edu/~rwoods/netbook/contents.html>

Horvath, John. Internet Independence and the Mass Mind. *Telepolis*. ????. Available at: <http://www.telepolis.de/english/inhalt/te/1026/1.html>

Houle, Kevin. 2000. *CERT® Incident Note IN-2000-08: Chat Clients and Network Security*. Available at: http://www.cert.org/incident_notes/IN-2000-08.html

irchelp.org. 2001. *Internet Relay Chat (IRC) help archive*. Available at: <http://www.irchelp.org>

Knight, Will. 2001. Hacker hits IRC network Undernet with denial-of-service attack. *Tech News*. January 9. Available at: <http://news.cnet.com/news/0-1005-201-4423794-0.html>

Kollock, Peter. 1999. The Economies of Online Cooperation: Gifts and public goods in cyberspace. In Smith and Kollock, 1999: 220-239.

Lemnos, Robert. 2001. DoS attacks underscore Net's vulnerability. *Tech News*. June 1. Available at: <http://news.cnet.com/news/0-1003-200-6158264.html>

Mirashi, Mandar. 1993. *The History of the Undernet*. Available at: <http://www.user-com.undernet.org/documents/uhistory.html>

Reid, Elizabeth. 1991. *Electropolis: Communication and Community On Internet Relay Chat*. Available at: <http://home.earthlink.net/~aluluei/electropolis.htm>

Rheingold, Howard. 1993. *The Virtual Community: Homesteading on the Electronic Frontier*. Available at: <http://www.rheingold.com/vc/book/>

Slashdot.com. 2001. Undernet in Serious Trouble: Any Suggestions? (Discussion). *Ask Slashdot*. Available at: <http://slashdot.org/askslashdot/01/01/08/2242223.shtml>

Smith, Marc A. and Peter Kollock (eds). 1999. *Communities in Cyberspace*. London: Routledge.

Undernet. 2001. *Notice to Our Users*. 11 January, archived now at *IWS – Information Warfare Site*. Available at: <http://www.iwar.org.uk/news-archive/2001/dos/undernet/user-notice.htm>

Valauskas, Edward J. 1995. *Lex Networkia: Understanding the Internet Community*. *First Monday*. 1.4. Available at: <http://www.firstmonday.dk/issue4/valauskas/indes.html>

Wellman, Barry and Milena Gulia. 1999. *Virtual Communities as Communities: Net surfers don't ride alone*. In Smith and Kollock, 1999: 167-194.

Winner, Langdon. 1997. *Cyberlibertarian Myths and the Prospect for Community*. Available at: <http://www.rpi.edu/~winner/cyberlib2.html>