Understanding King Punisher and His Order:

Vandalism in an Online Community - Motives, Meanings and Possible Solutions

DR. MATTHEW WILLIAMS[1]

Introduction

Commonly *online vandalism* has been understood to mean the defacement or destruction of commercial, government or personal websites. This is a rather parochial understanding of the phenomenon which marginalises other more esoteric, but nonetheless prevalent, acts of virtual property destruction. Most notably, unique forms of online vandalism exist within graphical *online communities*, where virtual buildings, homes and memorials are often defaced and even destroyed. Findings from an ethnographic study are used to examine the manifestation and regulation of this particular type of *online deviance*. The study examines 'deviance' within a three-dimensional online community named Cyberworlds. The complex social structures within the computer engineered environment are explored, using online participant observation and online group discussions. Work surrounding the aetiology and manifestation of offline vandalism is used in this paper in order to better understand this unique form of online deviance. Primarily the work of Sutton (1987) is utilised in order to rationalise the activities of online vandal 'gangs' within Cyberworlds. The paper also explores the possibility that situational crime prevention methods (Clarke 1983; 1995) are particularly suitable for tackling online vandalism.

[1] Lecturer in Criminology and Criminal Justice, Cardiff University

A multi-layered solution to Internet governance has been identified as a particularly suitable response to cybercrime and deviance (Walker and Akdeniz 1998). Building upon this position by extrapolating from known cases of online vandalism, and the solutions that have worked in cyberspace, there is evidence to suggest that the most effective forms of regulation and prevention may be technology based. The paper concludes that an effective way of reducing and preventing some cybercrimes rests, perhaps, not in changing existing laws, regulations and moral exhortation against either particular deviant or victimisation oriented social practices, but in designing out the opportunity for crime by developing *toughened technology* – that is target hardening the existing technological environment.

Defining Vandalism

It is important to note that there is no statutory offence of vandalism. Within the Welsh and English legal system, acts of vandalism fall within Section 1 of the Criminal Damage Act of 1971 which refers to: "…a person who without lawful excuse destroys or damages property". There are several categories of criminal damage ranging from "criminal damage up to £20" to "criminal damage endangering life" and "arson" (Barker and Bridgeman 1994). The term vandalism has no precise meaning and is an emotive description of behaviours. So called *environmental vandalism*, for example, has been used to describe official town planning policies that include the building of pre-fabricated concrete tower blocks (Ward 1993).

In everyday life, however, the mass media, politicians and the public tend to use the term vandalism to describe criminal damage as the wanton or meaningless destruction of property (Ward 1973). Vandal is a particularly emotive label and acts of vandalism may be done for a variety of reasons that have specific meanings for both participants

and victims. As one example, a vigilante group spray painting paedophile on the walls of a hospital paediatrician's house, because they have misunderstood her job description,[2] is not meaningless act – it is a mistaken act of ideological vandalism. Ideological vandalism was identified by Stanley Cohen (1973) as one sub-type in his six-fold typology of motivations for vandalism. In this typology, Cohen describes first *acquisitive vandalism* (looting and petty theft); second *tactical vandalism* (to advance some end other than acquiring money or property – such as breaking a window to be arrested and get a bed for the night in a police cell); third *ideological vandalism* (carried out to further an explicit ideological cause to deliver a message); fourth *vindictive vandalism* (for revenge); fifth *play vandalism* (damage resulting as by-product of children's games); and sixth – *malicious vandalism* (damage caused by a violent outpouring of diffuse frustration and rage that often occurs in public settings).

The motives for and meanings of illegal property destruction can perhaps be better understood by utilizing the position adopted by Sutton (1987). Sutton points out that it is arguably more useful from a criminological perspective to see vandalism as behaviour that is committed by those who are motivated by a desire to do criminal damage as the primary physical purpose – rather than as a means to another criminal end such as facilitating theft by breaking down doors, or damage occurring during a violent assault. If, for example, property is damaged for reasons of protest, and doing such damage is the primary criminal act, then it is *tactical vandalism* (Cohen 1978). However, Sutton (1987) rejects Cohen's (1973) subtype of *acquisitive vandalism* as nothing more than the necessary means to accomplish theft. This is because our

[2] (see: http://news.bbc.co.uk/1/hi/uk/1713409.stm)

understanding of motivations for vandalism will be blurred if we confuse them with motives for theft. In any event, damage resulting from burglary, 'smash and grabs' or theft from motor vehicles is not normally called vandalism. According to Sutton (1987), vandalism is, therefore: *the deliberate defacement, mutilation or destruction of private or public property by anybody not having the right to do so. Such an act is vandalism, regardless of any instrumental motivation, which might include political protest, where the focus of the perpetrators criminal act is both accomplished and completed by damaging or defacing property.* This definition is concerned only with the motivation of the perpetrators – rather than the reaction of society to various types of property crime or other corporate or municipal eyesore creations.

Building upon earlier research into group delinquency, especially the work of Miller (1967), Sutton (1987) finds evidence in the literature to support the addition of an important sub-type to complement and expand Cohen's (1973) typology, namely: *Peer Status Motivated Vandalism* (PSMV). PSMV is vandalism that is motivated by the desire to acquire or maintain peer status. PSMV might, for example, include spraying graffiti tags on trains, breaking a shop window for a dare or damaging a vehicle. This type of vandalism is more often committed in groups than alone. Further supporting evidence for this sub-type can be found in earlier research that stresses the importance of peer status in group delinquency – along with findings that most vandalism is committed in groups (see Clinard and Wade 1958; Martin 1961; Sveri 1965; Baldwin and Bottoms 1976 and Hindelang, 1976). This sub-type fits well within the definition of vandalism proposed above. PSMV is advocated later in this paper as an explanation as to why a notorious hacker calling himself King Punisher

engaged, along with his Order, in a concerted campaign of virtual property destruction within Cyberworlds.

Defining Online Vandalism

Vandalism is one of the most visible of crimes because, in many cases, vandals intend to draw attention to whatever they have damaged in some way. The altered state of targets often results in a re-signification, indicating that the offender's motivation is based on the desire to communicate a message, be it an expression of emotion, the airing of a grievance, a bid for increased peer status, or the marking of territory. All of these different motivations fit the typology of vandalism outlined above.

The term online vandalism is regularly used by writers and commentators on cybercrime to describe one of an array of activities used by various hacktivists to publicise their own cause. Hacktivists attempt to draw attention to their ideological position by defacing websites, such as those representing commercial or governmental interests. Notable attacks upon UK Government websites occurred in the August of 2000 when a well known hacktivist going under the name 'Herbless' was successful at defacing over ten Government websites with an aim to criticise official policy on smoking. Herbless had already achieved some notoriety, having hacked the UK Cabinet Office website a month previously (see figure 1).

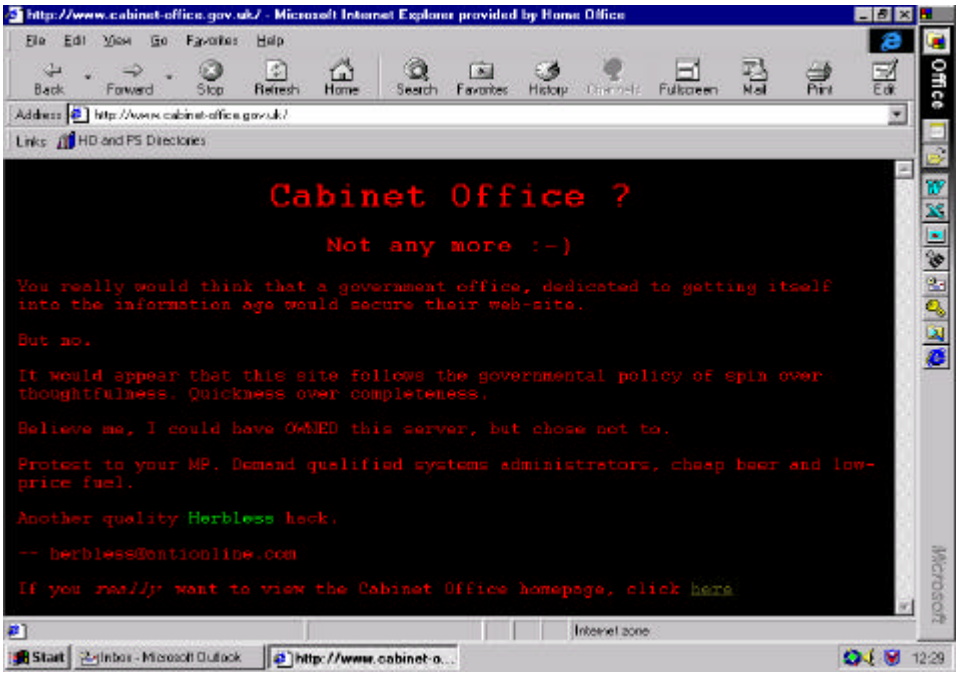

Figure 1: The Government Cabinet Office website hacked in August 2000.

Terrestrial forms of vandalism are material crimes because they have a physical presence. Conversely acts of online vandalism have no tangible element, making them immaterial. Although the defacement inflicted by a hacker on a website is visual, there is actually no physical damage – and repairing the damage done usually involves nothing more than downloading the original file of computer code to replace the corrupted one. The effects of online vandalism, however, are said to be disproportionate because the damage to either corporate or political reputation can be substantial.

The most common type of e-commerce hack is the defacement or alteration of website content. This type of online vandalism accounted for 64 percent of on-line security breaches in 2000 according to the Computer Security Institute (CSI) and the FBI (Richardson 2000). Subsequent surveys reveal that 25 percent of commercial and

government respondents reported website hacks in 2003, with over 23 percent of these victims having been hacked over ten times within a 12 month period. Website defacement was the most prevalent type of hack, accounting for 36 percent of all unauthorised access and misuse incidents. It is reported that these, and associated hacks in the USA, accounted for a loss of over seventy million dollars in 2003[3] (Richardson 2003). However, this type of deviant online activity has received little attention by either the media or regulatory authorities. At the time of writing, the main concerns of the UK Government and criminal justice system were the online distribution of child pornography and fraudulent online transactions. Because of the prioritisation of these other seemingly more 'serious' cybercrimes, online vandalism has many of the same rewards and limited risks as its offline equivalent. As Cohen (1971) reminds us of offline property destruction, a serious reprimand from engaging in vandalism is not likely to occur as there is seldom an immediate victim to complain or retaliate, and targets are often easy to access. For the online vandal these risks and opportunities are respectively attenuated and exacerbated due to the anonymous and ephemeral nature of the Internet.

In tandem with the lack of attention from official bodies towards online vandalism, the academic community has also strangely neglected to adequately broach the subject. Consequently, we have only a paucity of understanding surrounding definitional and motivational issues. Primarily, there is still a lack of knowledge regarding the manifestation and dynamics of online vandalism. Computer security surveys only highlight website defacement, identifying it as a common form of online vandalism. However, there exists a variety of other more esoteric types of online

[3] Calculating financial loss from any type of hi-tech crime and business fraud is complex and caution should be taken when interpreting assessments. Further, financial losses are only one measurement of harm inflicted. Loss of reputation, a diminishing client base and the like are also measures of harm.

vandalism that are worthy of academic attention. In particular, the vandalism of virtual property within established online communities.

Instead of two dimensional web-pages being re-written to misrepresent their creators, vandalism within three-dimensional graphical online communities involves the hacking of its computer code, or bypassing of password security systems, for the purpose of destroying or defacing members homes, public buildings or memorials. The virtual built environment is subjected to unauthorised graffiti and even demolition – deviance that requires considerably more technical knowledge than offline vandalism. Identifying and acknowledging these alternative forms of online vandalism undoubtedly complicates any attempt to understand the motivations behind this types of online deviance.

Directly applying terrestrial definitions, such as those suggested by Cohen (1973), may prove partially fruitful in understanding motivations behind more conventional website vandalism. For example, Cohen's (1973) ideological, vindictive and malicious categories can be adapted to account for website defacement. Herbless' defacement of Government websites could be understood as ideologically motivated. Other types of defacement, such as commercial website vandalism by disgruntled employees – accounting for over 10 percent of hacks in the US in 2003 (Richardson 2003) – or attacks upon multinational corporations by outsiders – accounting for 53 percent of all hacks in the US in 2003 (Richardson 2003) – can be understood respectively as being vindictively and maliciously motivated, as well as potentially ideological. Several of Cohen's (1973) categorisations could also be used to explain the motivation behind virtual property destruction within online communities.

However, in the case study that follows, Sutton's (1987) **PSMV** seems to better fit the behaviour and expressed motives of the vandals in Cyberworlds.

Cyberworlds, Online Community and Architecture

Cyberworlds is just one of many three-dimensional virtual communities that differ in several ways from the conventional text based Multi-User Domains (see fig 2), or MUDs, that have been awarded much attention over the past decade by other writers (Rheingold 1993; Baym 1995; Turkle 1995; Dietrich 1997; Shaw 1997; Danet 1998; Markham 1998; Reid 1999). While still utilising Internet Relay Chat (IRC) style textual communication, new broadband technologies allow new communities to be explicitly represented by a three-dimensional graphical component (see fig 3). Within their 3D environments, community members actually see themselves represented as *avatars* – a graphical depiction of a digital persona. Members navigate their own avatar around digitally represented built environments, in the same way players move the principal character in a computer game. Members can also influence the appearance of the landscape they inhabit by painstakingly creating their own virtual buildings and other 'spaces' such as monuments, gardens and cemeteries.

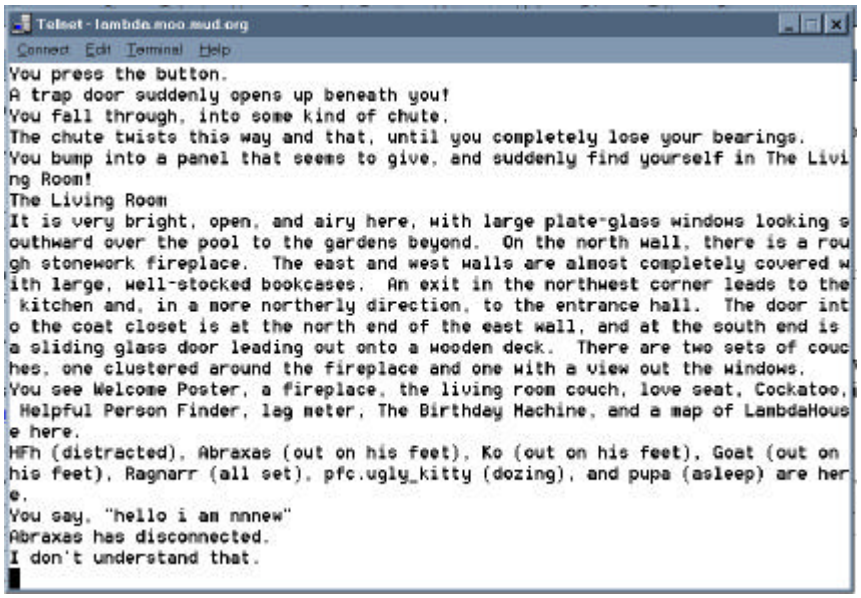

Figure 2: A conventional text-based MUD

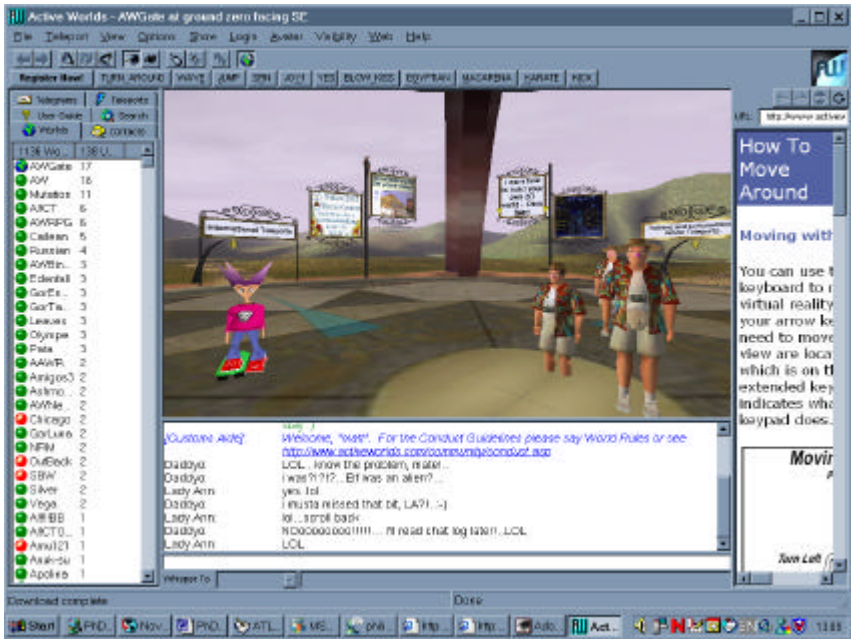

Figure 3: A three-dimensional virtual world such as Cyberworlds

An Established Online Community

The increased *social* use of the Internet in the mid 1990's coincided with general concerns at the time over the demise of community in the 'real' world (Rheingold

1993). Social commentators rushed to substantiate their claims heralding the 'virtual' as a the new homestead. While some of the claims were considered premature, what did emerge towards the end of the twentieth century was a definable online population, some of whom belonged to social groups, much like Cyberworlds, that bore characteristics similar to those of Gemeinschaft communities. These online communities manifest in different ways. Some are purely text based and mediate discussion asynchronously, such as newsgroups and discussion boards. Others utilise newer broadband technologies, such as Cyberworlds, to enrich social interaction, including graphics to compliment the text and allow for synchronous exchanges.

Cyberworlds is considered to be a *legitimate* 'community' both by its creators and, more importantly, its citizens. Previous research conducted in Cyberworlds (Williams 2003) has challenged current claims that meaningful immersed online interactivity is fettered by mediating technologies associated with the Internet (Beniger 1987, Healy 1997, Lash 2001, Lockard 1997, Peck 1987). Cyberworlds, in contradiction to these claims, exhibits many of the characteristics used to qualify offline community. Further, both the presence of avatars (which simulate corporeal immediacy) and the ability to build and claim ownership over space within Cyberworlds proved to increase levels of social immersion, and enrich interactivity between interlocutors online. It was also found that buildings help maintain community by embedding memory, culture and history within online artefacts (Williams 2003). Realising the non-permanence of their online existence, members build to be remembered when offline, creating a permanent attachment to the community. These attachments served to deepen their connection with the community and other members. Finally, claims that relations mediated by technology become 'linear' and 'lifted out' (Lash 2001)

were refuted in light of the entrenched and rich relations that characterise Cyberworlds (Williams 2003).

However, it is clear that these arguments establishing the 'validity' and 'realness' of the community within Cyberworlds may still meet suspicion from more traditional social scientists. In this light it may be more appropriate to argue that the validation of online community need not rest on 'traditional' conceptions of the phenomenon. When attempting to establish if online community exists one may first consider what constitutes a community in the offline world. This is very unclear. Sociological accounts conflict, and are in constant flux. We can talk of traditional community ideals, the kind of community Governments want to encourage within their towns and cities, but it is unfair to use these as a bench mark against which to evaluate online social formations. To a similar extent it is unsuitable to evaluate online social formations against current manifestations of community offline (if community still exists). The characteristics of Cyberspace are quite different and unique from 'meat space'. The expectation that online social spaces need to meet the requirements of offline community to be considered equivalents is the product of one-dimensional thinking. In the same way in which Jones (1997) questions the validity or primacy of face-to-face communication in relation to Computer-Mediated Communication, its is equally viable to question the primacy of offline community in the face of new emergent online social formations. The central point to be made is that those who spend significant amounts of time within online communities, who live a large part of their lives online, and who recognise that actions online have *real* consequences, much like in the offline world, consider Cyberworlds to be a community.

The Virtual Built Environment, Vandalism and the Threat to Community

The ability to build within Cyberworlds has a profound influence upon the ways in which community members interact with their surroundings. Thoughts, messages and histories are imbued within artefacts manufactured by community members that are significant and meaningful to individuals and the Cyberworlds community. For instance, the building of memorials and cemeteries within Cyberworlds indicates the importance of history and memory for the online community. Narratives from community members detail how buildings encapsulate individual identities, a constant reminder to others that there was someone there before their time. The following extract, taken from an online group discussion, provides a rich account of a Cyberworlds member's use and interpretation of the online built environment.

> **1. Brainiac**:
>
> If I turn my computer off tomorrow, two weeks from now, people will stop thinking about where I am. When my citizenship expires, my name will mean nothing to no one. But when someone I know discovers my building all over again, they'll remember me. An image of ourselves is forever engulfed in what we can see. Like tiny trinkets collected over years of road trips, a time capsule, or even just a childhood diary, our buildings are a stone-engraving of our lives at that time.

There is a realisation that online encounters are often fleeting and non-linear (Lash 2001), which results in the desire, among those living in online three-dimensional communities, to build permanent structures that help embed meaning into online

interactions and identity. The speed at which interactions take place within Cyberworlds (often forgoing the convention of an introduction, and the immediate posting of 'ASL' information - Age, Sex and Location) means members are increasingly distancing themselves from the exchange of in-depth narrative. Instead, members exchange units of information as there is little time to sit back and reflect upon detailed life histories. While many members may boast a long contacts list, they sacrifice depth in interaction for quantity. Using Lash's (2001) expression, many Cyberworlds member's relations are 'stretched out' along thin and brittle social networks. As a result many have a desire to entrench what meaning their online identities do have in buildings and memorials – artefacts that transcend the speed of online social interaction – maintaining stability along with significant bonds to the Cyberworlds community. Similarly, due to the ephemerality and speed of encounters and the non-permanence of avatars, members also feel 'lifted-out' of the community. As networked communication can disembody social relationships (Castells 1998) members of Cyberworlds go to extremes to embody their identities in online artefacts. As Brainiac explains above, buildings provide a kind of immortality that is recognised to its fullest extent when individuals leave the community. The feeling that ones presence is not permanent within the online environment urges individuals to leave behind reminders of themselves – as the following online group discussion extract from Buxton explains:

2. Buxton:

In the physical world, friendship may also be short lived due to relocation or moving on in some other way, but this seems accelerated in virtual space. Maybe the lesson of the virtual world is in coming to terms with moving

> on. Yet we build structures to leave behind our virtual 'Kilroy was here' statement. It seems in some way the very speed of the virtual world demands that we, like fairy tale children, leave our trail of breadcrumbs behind. Perhaps we are not yet quite accustomed to the speed.

The ephemeral nature of life within Cyberworlds, and virtual communities in general, results in turbulent and shifting populations. Individuals build so that they can be remembered by others while they are not online. Unlike life offline, once the computer is turned off simulated corporeal immediacy is discontinued within the virtual arena. Connection to virtual social space is purely optional. However, this tenuous link to online life, which for some is as meaningful as life offline, leads individuals to engrave themselves, their personalities into the landscape. Yet the permanence of these artefacts is under constant threat. Vandalism is a constant concern for those who wish to maintain the integrity of their artefacts, both semantically and aesthetically.

Some community members use their programming skills and knowledge of Cyberworlds architecture to vandalise other member's creative efforts. The actual type of damage seen by Cyberworlds members varies. Online vandalism can manifest as graffiti on virtual buildings or monuments. In other cases pornographic images have been attached to architecture. In extreme cases architects can find that where their building once stood all that remains is a scattering of polygons – like rubble at the scene of a bombsite. Research respondents voiced how online vandalism leads to uncertainty and fear that undermines community member's bonds to the Cyberworlds

culture. Interestingly, these effects bare marked similarities to the negative outcomes of vandalism in offline public spaces (Wilson and Kelling 1982; Ekblom, Law and Sutton 1996).

The following extract is taken from the community archives. In this extract Rookie, a disgruntled community member, details the existence of an organised group of vandals in operation when Cyberworlds was in its infancy:

> **3. Rookie's Report – Dec. 12 1995:**
>
> I became increasingly appalled at the reported incidents of vandalism to property in Cyberworlds and rumours of a gang of some sort forming. I have seen the leader of this gang, "King Punisher" as he calls himself, in action trying to promote his "order" and recruiting members from a crowd. If anyone questioned him he would respond with profanities and threaten to put them on "the list" to become a victim of the order's vandalism and destruction of property. I was repulsed by the leader of this gang and his tactics and decided that I would work to undermine his efforts and his attempts to bully my fellow Cyberworld citizens.

During the summer of 1995 a teenager entered the Cyberworlds Gateway and began to demonstrate his advanced technological knowledge by rapidly changing his persona (switching between King Punisher and Pharaoh) demonstrating his ability to hack into Cyberworlds architecture. As his abilities grew King Punisher turned to vandalism, targeting individuals who criticised his activates or who attempted to remove him from

Cyberworlds utilising informal vigilante methods. Gradually an 'Order' of vandals emerged, led by King Punisher. Their activities became more pronounced and frequent, creating an environment that Cyberworlds citizens found unpredictable.

Screen shots of King Punisher's recruiting activities can be seen below. In Figure 4 Atomic Jello is attempting to verify the identity of monster byte, an infiltrator who is posing as a *rookie* to the Order, whose intentions are to expose their illicit activities. During the questioning King Punisher emphasises his superior technical skills by stating his ability to adopt multiple personae allowing him to escape apprehension.

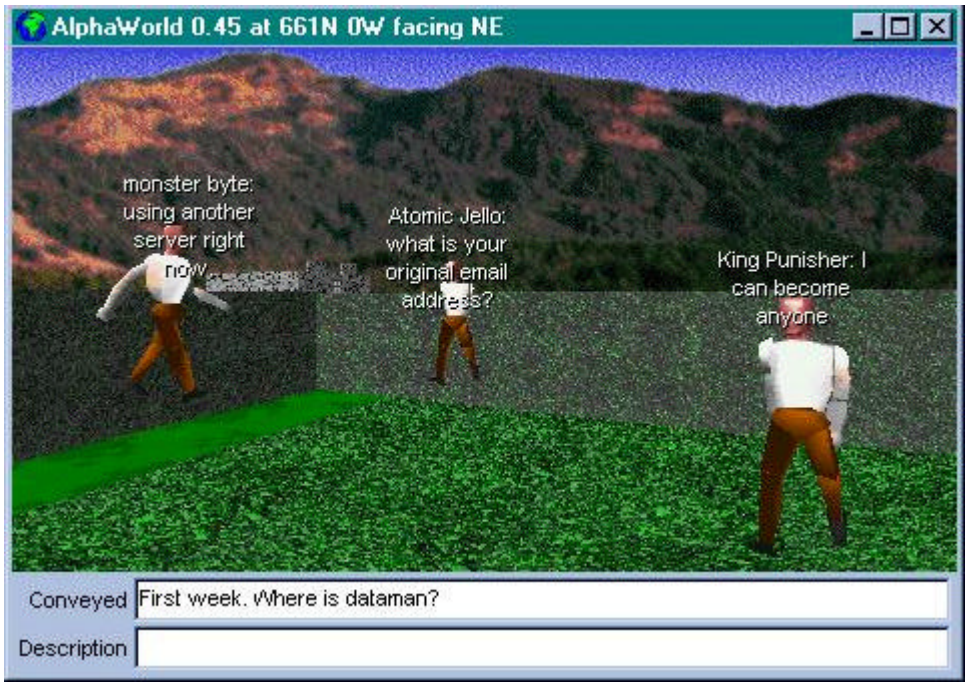

Figure 4

Following the verification of monster byte's pseudo identity he is welcomed into the Order. Figure 5 depicts the inauguration of the new member, and here key aspects of the social structure of the order are also outlined by Atomic Jello, while King Punisher attempts to secure allegiance to himself and the group. A description of the Order's

current activities is shown in Figure 6. Atomic Jello is quick to boast that the Order already attacks properties near Ground Zero, an extremely public and busy environment, while King Punisher gives details as to how the Order maintains its element of terror by delivering threatening messages to local residents.

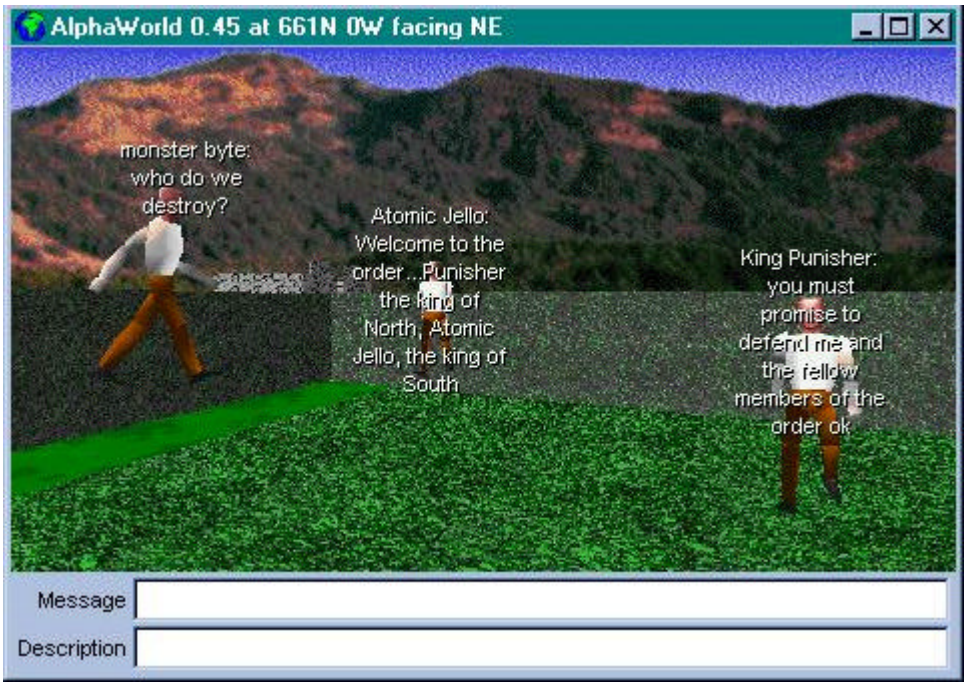

Figure 5

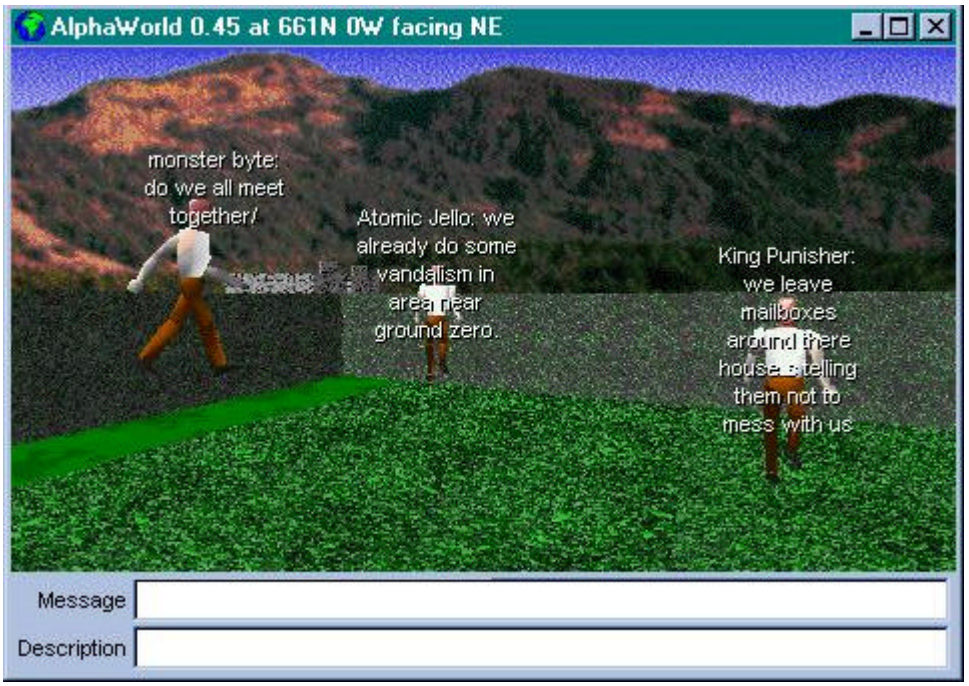

Figure 6

While vandalism was accepted as an already present feature of Cyberworlds, even in its infancy, the evolution of such anti-social behaviour into an organised deviant group was unprecedented. The systematic destruction of virtual buildings and memorials and the defacement of virtual billboards left behind a trail of incivilities that shook the Cyberworlds community. It became evident that virtual communities were not isolated from the kinds of criminal and deviant activities that plague many offline communities. One interview respondent expresses concern over more recent trends in vandalism, highlighting their alarm by comparing the attacks to real world events:

> **4. ReyemNiffirg**
>
> It seems that Cyberworlds has been under attack by terrorism as well as the world. Some of us remember 1998, known as The Summer of Vandalism. Eternal Drifter roamed CW and, until he was finally ridden of, CW was a

> scary unsafe place. Nowadays, its true that things have gotten better, but terrorism and vandalism still affects Cyberworlds as we speak. Radon is the big one right now, and he should be ridden of as soon as possible. It's funny, because I used to know him, in fact I literally grew up in his old world Utopia. Cyberworlds needs to meld together like America has. People need to stop fighting and bickering, and a group of some kind needs to be supported by CWCorp to rid of terrorists/vandals of Cyberworlds. If CWCorp cannot do this, we need to resort to new leadership (program ownership), or someone needs to create a universe independent of Cyberworlds with a supportive leadership. This is the dream of Cyberworlds, and we need to bring it about! Let Cyberworlds unite as one and create a virtual Utopia for all.

The effect that vandalism has on the Cyberworlds community becomes clear when members use expressions such as 'unsafe' and 'scary' places. It is clear that some of the debilitating effects that fear of crime has on community life offline also have the potential to affect the citizens of Cyberworlds. For example, the adoption of avoidance behaviour, similar to that occurring in the offline world, may create hotspots of deviance within the online arena.

Just like in the offline world, a resulting decrease in social interaction means a reduction in social presence, and ultimately the atrophy of bond to the Cyberworlds community. At another level, the defacement of buildings and memorials may harm their architects due to the relevance that these artefacts have to meaning, identity and

belonging within the community. Buildings function as a representation of self, and any attack on them can be considered an attack on the owner's identity. Having been a victim of vandalism Frasier describes the 'real' harm suffered by himself and his friends:

> **5. Frasier**
>
> You don't think it will happen to your place, you think passwords and the peace-keepers are enough. About four of us spent a summer building a place about 100 meters away from Cyberworlds central only for it to be completely decimated in one afternoon. It felt like our home, we spent at least three hours a day around that place, talking, laughing, adding extensions and frills. The place was like us. Bits of us were part of the building. I haven't built anything since, I don't see the point. I don't really visit Cyberworlds much anymore anyway. It's a shame, we had fun times back then.

While the individual physical harm of online vandalism may be negligible, the effect it can have upon the integrity of friendships and the maintenance of online community can be significant. Frasier's statement explains how the building was essential to maintaining their relationships, how it was functional in bringing people together, and how it became symbolic of the group. There are obvious parallels here with the offline world where buildings such as bars and pubs and clubhouses are well known to play traditionally crucial roles in the maintenance of friendship groups and community cohesion (Oldenburg 1999). The destruction of this virtual building by vandals not only symbolically destroyed their friendships, but it also lead to their

actual demise. While the physical harms of these acts may not directly manifest in the offline world, their negative social and psychological consequences cannot go understated. If, for so many within Cyberworlds, online life and relationships are as important to them as offline equivalents, then these online harms should be similarly weighted. Since all the indications suggest that online communities will become central to the lives of a growing number of people, this is an important new avenue for criminological research and crime science – particularly for those concerned with understanding deviance , defining civic responsibility and those seeking solutions to various threats to community safety.

Motives of King Punisher and His Order

Without greater knowledge of King Punisher's history within Cyberworlds, caution should be exercised in any attempt to suggest motives for his or the Order's behaviour. For example, it might be equally persuasive to argue that their motivation was ideological – based on King Punisher's desire to communicate an alternative message to that of Cyberworlds dogma – as it would be to argue it was vindictive or malicious – based on King Punisher's dislike of some online community members. However, there is no documentation in the community archives to suggest that any of these reasons were part of King Punisher's motivation. Further, it is questionable whether King Punisher could have created a loyal order of vandals whose group motivation was based on their leader's personal rancour. The formation of an Order of vandals indicates the presence of complex group relationships. The process of inauguration identified by Rookie's infiltration (Figure 5) indicates that King Punisher's Order operated with a set of alternative internal rules and values akin to that of a subculture. In this context Peer Stated Motivated Vandalism proves useful in exploring motivation. Much of the criminological literature in this area has identified

the importance of acquiring peer status within subcultures (Cloward and Ohlin 1960; Matza 1964; Short and Strodtbeck 1965). In line with the thinking of Matza (1964), it is likely that each member of the Order perceived their peers to be in support of delinquent behaviour, in this case vandalism, and as a result they themselves support it out of anxiety over loosing status within the group. Given the relatively long period of time the Order was able to continue vandalising the community's property it is also likely that its members were considerably immersed within the alternative deviant subculture. This prolonged immersion may have increased their conformity to negative values and the maintenance of a deviant peer status. The destruction of property then becomes a value in itself and provides a vehicle for status acquisition within the subcultural setting (Sutton 1987). It is likely that the actions of King Punisher's Order, rather than being characterised as short run hedonism or motivated by individual resentment, were peer status motivated. From this perspective the Order's members were likely to have cognitively balanced the risks of immediate loss of status in the group against the more remote possibility of punishment by Cyberworlds authorities.

While PSMV helps in understanding the reasons for, process and reinforcement of destructive behaviour within Cyberworlds, little is explained about the motivation to join the Order. Unlike, for example, Cohen's (1955) and Cloward and Ohlin's (1960) class based explanations which focus on a rebellion against hegemonic middle class culture, motivations behind allegiances to subcultures within Cyberworlds prove quite different. Any class based analysis can be ruled out given the existence of a digital divide of Internet use, meaning that those who inhabit Cyberworlds are likely to be middle class young white males (Compaine 2001). Further, evidence of

rebellion against the authorities of Cyberworlds, identifying power indifference as motivation, was also absent in the community archives. From this analysis, classical criminological explanations cannot realistically account for each member's initial motivation to join King Punisher's Order. However, some answers may lie in the unique nature of the online environment. The anonymity granted to every member of Cyberworlds, and the fleeting encounters often experienced via computer-mediated communication, result in turbulent and shifting populations that are often disconnected from any sense of community (Williams 2003). Some individuals feel no allegiance to a wider online social structure, and are possibly therefore free of 'respectable' constraints, disassociating their deviant actions with 'real' consequences.

The degree to which individuals feel connected to the online community, and how behavioural constraints vary with connectedness can be usefully examined by applying Hirschi's (1969) social bonding theory to the online setting. Examining Cyberworlds through Hirschi's (1969) elements of *bond* (attachment, commitment, involvement and belief), it becomes clear that not all members are behaviourally constrained by the community. Bonds to other individuals, organisations and rules facilitate the internalisation of group norms and values that heighten consciousness of other member's opinions and expectations. Conversely, those with weak bonds have a tenuous attachment to wider group norms and values and may be ignorant of community evaluation. Although somewhat tautological, it follows that those who deviate from rules and regulations are likely to have a weak bond to the Cyberworlds community. Those with little commitment to achieving or maintaining a 'respectable' reputation online are more likely to deviate from wider Cyberworlds group norms and

values. Because commitments online are less constraining than those in the offline world, less is jeopardised by being deviant. For example, there are less material belongings in an environment made up of purely social relations. A lack of legitimate online avocations also increases the propensity for an individual to drift into deviance. Those not involved in building, maintaining friendships or running community organisations are more likely to have time on their hands to break rules and regulations. This is especially the case within online environments where some deviant acts, such as vandalism and other forms of hacking, require a great deal of time and concentration. Variations in the extent to which members believe they should follow the rules of the wider Cyberworlds community impact on levels of deviant activity. Those who consider the 'law' of Cyberworlds to be culturally biased, sexist, ageist or racist are less likely to accept aspects of the 'respectable' belief system, allowing harmful acts to be neutralised. Finally, lacking attachment to significant others, peers and friends in Cyberworlds might be the most significant indication of a weak bond to the community.

Those who are less 'bonded' to the Cyberworlds community attach little significance to online encounters. The 'act' becomes important, while the significance of its effect goes unrecognised. Individuals begin to identify a disassociation between action and consequence, allowing for the neutralisation of deviant activity. Mitigating comments such as 'online life isn't real' and 'it's only words' allow individuals to justify their deviant acts. It is likely that those individuals with weak bonds to the Cyberworlds community were attracted to King Punisher's Order. Those with strong bonds formed part of the wider community while all others were left in abjection. It is feasible that

the Order provided a social structure and a sense of belonging for those with little attachment, involvement, commitment or belief in the wider Cyberworlds culture.

Regulating Online Vandalism within Cyberworlds

It seems reasonable to assume that the emergence of an organised deviant group roaming through Cyberworlds causing havoc was never anticipated by the environment designers or the various world owners. Since it appears that the designers did not "think crime" (Foresight 2000) there were no adequate technological or other regulatory mechanisms in place to deal with deviance on such a systematic and organised scale. As the Order rapidly expanded and its pattern of victimisation spread to other areas, senior community members, world owners and the corporate arm to Cyberworlds began to consider a response that was equally as organised as the criminal activity they were facing. As a direct response to the threat King Punisher's Order posed to Cyberworlds citizens and the community, a formal policing body was established and new methods of *technology toughening* were developed to upgrade the architecture of Cyberworlds.

In effect, the defacement of virtual homes, memorials and other artefacts within a community centred environment has seen the introduction of novel prevention methods that may prove beneficial to the wider Internet community. These forms of anti-vandalism prevention methods will form the focus for the remainder of this paper

Patterns of Policing

The patterns of policing vandalism, amongst other deviant activities, within Cyberworlds can be neatly rationalised using Gill's (1994) model of societal policing. Before King Punisher's organised attack on the community in 1995 social control was

organised around a *Community Involvement* model, in that the community took responsibility for the policing and introduction of crime prevention measures on a non-structured basis (Gill 1994). World creators within Cyberworlds would monitor behaviour when they were online, forming regulations that were specific to their environment. If and when an 'incident' occurred, community members could log a complaint with the appropriate world creator who would then decide how to deal with the offender. Implementation of these regulations was ad hoc, and there was no formalised method for dealing with troublesome individuals.

In a response to the organised vandal attacks engineered by King Punisher, it was recognised that an equivalent organised response had to be developed for the community to maintain social integrity. As a result, the Peacekeepers were established – a voluntary organisation of community members trained to patrol the various Cyberworlds worlds to identify, report, record and punish instances of deviant activity. This, among other events, was an important mark in the increasing 'civilisation' of Cyberworlds, and served to increase the belief, commitment, involvement and attachment of citizens to the community. These developments can be considered a progression to Gill's *Volunteer Community Policing* model, where the community provides some limited structure to policing. The Peacekeepers are essentially an organisation of volunteers who are formally trained to deal with rule breakers within Cyberworlds. They are a structured organisation with an online Peacekeeper Academy for training new recruits, and teams of Peacekeepers working on a shift basis. A Special Response Team is dedicated to the investigation of complex and serious cases of vandalism and harassment.

Online Crime Prevention

Tertiary Crime Prevention

The ability of Peacekeepers as *capable guardians* (Felson 1994) to punish 'on the spot' exemplifies how tertiary crime prevention developed under a structured model of policing in Cyberworlds. Ejecting offenders from the environment, locking-down and removing accounts are several methods employed to deter and prevent recidivism. However, these efforts to formalise social control are only marginally effective at reducing instances of vandalism. While the Peacekeepers were effective at policing and reducing organised forms of vandalism, sporadic acts continued. This is because groups of vandals are easier to identify reactively in the online environment, especially if they develop a group identity. King Punisher's Order was recognisable by their overtly public presence (that was necessary in order to 'recruit' new members) and their marking (the use of mailboxes) left behind on all vandalised properties. This left the Order open to disruption as it was easily penetrable by subversive agents (see Figure 4), allowing it to be exposed and finally disbanded. Acts of vandalism by individuals working alone are, however, more difficult to detect. Reasons for this are two fold. Firstly, vandals working alone may be one-time offenders – so no pattern of offending can be identified. Secondly, individual vandals may not have an established bond to the online community and so, for them, anonymity is easily maintained.

Primary Crime Prevention

Vandals in Cyberworlds damage the online built environment by exploiting technical computer programming knowledge in order to gain illegitimate access to other community member's building rights. To be an effective vandal within Cyberworlds

you have to be a good hacker. Hackers, such as these, look for weak points or loopholes in computer code, in order to gain access to secured areas. This behaviour is akin to Walls' NetCrime categorisation of Cyber Trespass (2001). It follows that changing code to make it more complex, and therefore more secure, would reduce the ability for hackers to gain access to private areas. Cyberworlds code goes through this *technology-toughening* process several times a year – following advances in system architecture. While this proactive process is not primarily a response to the need to reduce vandalism, it does create a *diffusion of benefits* (Pease 1997) in a routine and a systematic way.

Advances in system technology can be considered as a form of primary crime prevention in Cyberworlds. More secure technologies increase the perceived effort for individuals to commit acts of online vandalism through a process of target hardening (Clarke 1997). Increasing the complexity and security of the code reduces the opportunity for vandalism, especially amongst opportunistic, or one-time, offenders. The situation within which virtual vandalism is committed is altered. It is this form of online crime prevention that allows for a systematic eradication of vandalism and other forms of online deviance. A similar but deliberate systematic approach of *technology-toughening* effectively reduced the ease by which a group of online hackers could break the encrypted code of satellite TV services (Mann and Sutton 1998). Within the realm of technology mediated and dependent environments tertiary forms of prevention are reactive, labour intensive, and have limited potential for crime reduction. Primary forms, however, are proactive, relatively non-labour intensive, take immediate effect, are implemented system-wide, and hence have greater scope for crime reduction.

It is important to note, however, that hackers often have the ability to develop and to adapt to advances in technology. The aptitude of criminals to keep up with advances in target hardening technology is well known. For instance, safe crackers developed new methods to break into safes during a century-long technology war between the *cracksmen* and the manufacturers. This hi-tech war was eventually won by the industry – because it simply became too difficult, time consuming and therefore too risky to break into the newer safes. At the time of writing, however, computer code, no matter how new, complex or secure, can be compromised given time. It remains to be seen whether the hacker will go the same way as the safe cracker. However, given the insider knowledge hackers are able to acquire through their subversive employment within the information security profession, with over one third of US corporations willing to employ hackers as security professionals (Richardson 2003), it seems unlikely that their abilities will fall short in the foreseeable future.

Applying Situational Crime Prevention to the Wider Net Context

The effectiveness of technology as a regulator within Cyberworlds resonates with the current legal scholarship of Greenleaf (1998), Hosein, Tsiavos and Whitley (2003) and Lessig (1999). Regulation was excursed bi-modally with Cyberworlds, through established norms, conventions and regulations and via technology. The first mode, which might be considered social, exercised its regulation *ex post*. An offender would be punished after the deviant act had been committed, either via forms of vigilante justice or Peacekeeper action. The second mode of technological regulation, which may be considered the 'nature' of Cyberworlds, exercised its regulation *ex ante.* For example, alterations in code, akin to that of situational preventative methods, prevent many suitably motivated offenders (Felson 1994) from vandalising property. The

toughening of code – removing loop holes and weak spots – has the systematic effect of increasing the perceived effort, increasing the perceived risks and reducing the anticipated rewards of deviant activity (Clarke 1997). This process within Cyberworlds is also more widely employed within many other technological systems, including those that constitute the whole Internet and its associated technologies.

The idea that technology is a more effective regulator of cyberspace than laws, norms or markets has been advanced by Lessig (1999). It was Lessig's (1999) aim to counter the technological deterministic view that the Internet could not be regulated. Instead, he subscribes to the idea of a 'digital realism' that recognises the disruptive capacity of technology with cyberspace. Rejecting Boyle's (1997) notion of an Internet Holy Trinity – that regulation was impossible due to the *technology of the medium*, the *geographical distribution of its users*, and the *nature of its content* – Lessig (1999) proposes that the thread that links all of the Internet's characteristics together – code or architecture – can be used to control behaviour. In the same way that the architecture of Cyberworlds restricted the behaviour of vandals, Lessig (1999) believes technology performs a similar function on a much wider scale on the Internet.

The effectiveness of technology as regulator can be accounted for in several ways. First, technology can disrupt human action, forcing individuals to renegotiate paths and goals (Latour 2000). Second, technology, code or architecture is malleable; it is easily shaped by actors that have access to its control. In Lessig's (1999) opinion, the law can still be used to regulate cyberspace, due to its ability to officially manipulate the technology. Third, the way in which technology imposes constraints on how people can behave is more pervasive and immediate than other modes of regulation.

Fourth, technology is more readily and rapidly adaptive than laws, norms or markets (Sutton *et al* 2001), to cyber criminal threats, allowing it to control criminal, quasi-criminal and other deviant behaviour. Fifth, changes to system architecture have a preventative approach. It is far more effective to prevent an online offence as opposed to reactively identifying and apprehending an offender. Sixth, it is a native form of regulation making it less contentious. Often the origins of the technology are concealed, and hence its regulatory practice is perceived as less coercive than a state-sponsored regime. Technology is then perceived to be more benign, merely shaping – or even facilitating – individual choices (Boyle 1997). The effectiveness of technology as a regulator then lies in its ability to alter behaviours, its ability to be shaped, its rapid adaptability, its *ex ante* approach, its wide reaching scope, its sensitivity towards criminal and sub-criminal activity, and its less visible approach to social control.

However, not all uses of technology are effective. While system wide architectural upgrades within Cyberworlds prevented the majority of serious acts of online vandalism not all instances were detected or eradicated. The use of bots[4] to monitor graffiti within certain areas caused a degree of contention amongst the members of Cyberworlds. The bots were only programmed to identify certain kinds of graffiti that were already known to the Peacekeepers, leaving a substantial proportion of Cyberworlds population free to create novel forms of defacement unrecognisable to the bots. This shortfall in the technology forms the basis of Hosein *et al's* (2003) argument which aims to complicate the role architecture or code has in regulating cyberspace. Instead of being a self-executing benign regulator, Hosein *et al* (2003)

[4] Computer programs that perform automated tasks and so act as human surrogates.

talk of technology as a biased cultural artefact, which is embedded with subjectivity. For this reason alone, there can be no certainty that technology will produce a particular behaviour. In the case of the bots in Cyberworlds, the objective to systematically reduce graffiti failed because of the technologies reliance upon codewriters. Hosen *et al* (2003) continue to complicate this relationship. Instead of claiming it is the technology that determines freedom and rights, they take a non-technologically deterministic approach, arguing instead that individuals (codewriters) become the alternative sovereign. Concerns are raised about the accountability of these new masked regulators, and the basis or root of their authority is questioned. They conclude by considering technology as one form of regulation that cannot be separated from other modalities. Technology, law, social norms and markets are all intricately connected, and need to remain so to make sense of one and other. Online regulation should then be considered a socio-technical issue, where the nature or roots of regulation are not always made clear and are in constant flux; where its outcome is never certain, and sometimes even autonomous (Hosein *et a* 2003). Clearly, further research is required to map out socio-technical relations - to identify the optimal conditions for actors to successfully regulate technology. It is also important to better understand how technology can be applied so that it can autonomously regulate behaviour.

Conclusion

Things have changed since Cohen (1971) wrote that little technical or expert skill is needed to vandalise. Today, there are new deviant opportunities where computer programming skills are required in order for people to commit acts of online vandalism. With the emergence of NetCrime as an important area for criminological

research (Mann and Sutton 1998), this remarkable evolutionary quantum leap of deviance is worthy of considerably more attention from the research community.

Contentious debates over the definition of vandalism within offline settings are likely to become more complex now that this behaviour has moved into cyberspace. Establishing motives is particularly complex, and in the face of such difficulties it seems appropriate to adopt a solution that focuses its attention on the situation and site of the deviant activity, as opposed to any psychological or social root, since this approach is likely to yield more immediate results. However, root causes remain an important issue and more research is needed to map out and further understand how online deviants neutralise guilt and identify suitable opportunities and targets.

While situational crime prevention has been criticised in its offline application (including its micro approach to crime, its ignorance of underlying causes and its limited impact on overall crime rates), its application online may prove more popular and even more effective in reducing online vandalism[5]. This is because online vandals are dependent upon the exploitation of technology that forges the environment in which they are operating. Hence, online vandals are more susceptible to disruption than many other offline offenders whose terrestrial environment is much more static and harder to manipulate. The very technologies that facilitate online vandalism can also be used to prevent it. More secure computer code and tighter access control may reduce the opportunity for individuals to use technologies to vandalise. The main argument is that developments in technology occur much more regularly and rapidly than changes in law and social practices, and so it is a

[5] Situational crime prevention may prove to be particularly effective at reducing online theft– See: Newman and Clarke (2003).

particularly useful way to reduce certain types of NetCrime before they grow to alarming proportions.

The corporate and community response to King Punisher and his Order ensured the survival and growth of a pioneering online community. This is, therefore, an important early example of *what works* in improving virtual community safety.

References

Baldwin, J. and Bottoms, A. E. (1976) *The Urban Criminal: A Study in Sheffield*, London: Tavistock.

Barker, M. and Bridgeman, C. (1994) *Preventing Vandalism: What Works,* London: HMSO.

Baym, N. (1995) 'The Emergence of Community in Computer-Mediated Communication' in Steven Jones (Ed.) *CyberSociety,* Newbury Park, CA: Sage.

Boyle, J. (1997) 'Foucault in Cyberspace: Surveillance, Sovereignty and Hard-Wired Censors', *University of Cincinnati Law Review*, 177.

Castells, M. (2001) *The Rise of the Network Society (Second Edition),* Oxford: Backwell.

Clarke, R.V.G. (1983) 'Situational crime prevention: its theoretical basis and practical scope', in M. Tonry, and N. Morris, (Eds.) *Crime and Justice: An Annual Review of Research,* Vol 4. Chicago: University of Chicago Press.

Clarke, R.V.G. (1995) 'Situational crime prevention', in M. Tonry, and D.

Farrington, (Eds) *Building a Safer Society: Strategic Approaches to Crime Prevention.* Vol. 19. Crime and Justice: University of Chicago Press.

Clarke, R.V.G. (1997) *Situational Crime Prevention: Successful Case Studies (Second Edition),* Guilderland NY: Harrow & Heston.

Clinard, M. B. and Wade, A. L. (1958) 'Toward the Delineation of Vandalism as a Sub-Type in Juvenile Delinquency'. *The Journal of Criminal Law, Criminology and Police Science,* 48.

Cloward, R. and Ohlin, L. (1960). *Delinquency and Opportunity: A Theory of Delinquent Gangs*, Glencoe, IL: Free Press.

Cohen, A. (1955) *Delinquent Boys: The Culture of the Gang*, Glencoe, Ill: Free Press.

Cohen, S. (1971) 'Directions for research on adolescent group violence and vandalism', *British Journal of Criminology*, 11 (4) 319-40.

Cohen, S. (1973) 'Property Destruction: Motives and Meanings', in C. Ward (Ed.) *Vandalism*, London: Architectural Press**.**

Compaine, B. M. (ed.) (2001) *The Digital Divide: Facing a Crisis or Creating a Myth*, London: MIT Press

Danet, B. (1998), 'Text as Mask: Gender, Play, and performance on the Internet', in Steven Jones (Ed.) *CyberSociety*, Newbury Park, CA: Sage.

Dibble, J. (1993) 'Rape in cyberspace or how an evil clown, a Haitian trickster spirit, two wizards, and a cast of dozens turned a database into a society', *Village Voice*, 38 (51) 36-42.

Dietrich, D. (1997) '(Re)-fashioning the Techno-Erotic Woman: Gender and Textuality in the Cybercultural Matrix', in Steven Jones (Ed.) *Virtual Culture: Identity and Communication in Cybersociety*, London: Sage.

Downes, D. (1966) *The Delinquent Solution*, London: Routledge

Ekblom, P. Law. H. and Sutton, M. (1996). 'Domestic Burglary Schemes in the Safer Cities Programme' *Home Office Research Study No 164*, London: Home Office.

Felson, M. (1994) *Crime and Everyday Life*, Thousand Oakes CA: Pine Forge Press

Foresight (2000) *Turning the Corner: Report of the Office of Science and Technology Crime Prevention Panel*, London. HMSO.

Gill, M. (1994) *Crime at Work: Studies in Security and Crime Prevention*, Leicester: Perpetuity Press.

Greenleaf, G. (1998), 'An Endnote on Regulating Cyberspace: Architecture vs Law?' *University of New South Wales Law Journal*, 21.

Hindelang, M. J. (1976) 'With a Little Help From Their Friends: Group Participation in Reported Delinquent Behaviour', *British Journal of Criminology*, 16, 109-125.

Hirschi, T. (1969). *Causes of Delinquency,* Los Angeles: University of California Press.

Hosein, G. Tsavios, P. and Whitley, E. (2003) 'Regulating Architecture and Architectures of Regulation: Contributions from Information Systems' *International Review of Law, Computers and Technology*, 17:1.

Lash, S. (2001) Technological Forms of Life, *Theory, Culture and Society*, 18:1.

Latour, B. (2000) 'When things strike back: A possible contribution of science studies to the social sciences' *British Journal of Sociology*, 51:1.

Lessig, L. (1999) *Code : And Other Laws of Cyberspace,* New York: Basic Books.

Mann, D. and Sutton, M. (1998) '>>NetCrime: More change in the organisation of thieving', *British Journal of Criminology,* 38: 210-229

Mann, D. Sutton, M. and Tuffin, R. (2003) .'The Evolution of Hate: Social Dynamics in White Racist Newsgroups', *Internet Journal of Criminology*. [Available online at: www.flashmousepublishing.com]

Markham, A. (1998) *Life Online: Researching Real Experience in Virtual Space* Walnut Creek, California: AltaMira.

Martin, J.M. (1961) *Juvenile Vandalism*, Illinois: Springfield.

Matza, D. (1964) *Becoming Deviant*, Englewood Cliffs New Jersey: Prentice Hall

Newman, G. and Clarke, R.V. (2003) *Superhighway Robbery: Preventing e-commerce crime,* Cullompton: Willan Publishing

Oldenburg, R. (1999) *The Great Good Place*, New York: Marlowe and Company.

Pease, K. (1997) 'Crime Prevention.' In M. Maguire, R. Morgan, and R. Reiner (Eds.) *The Oxford Handbook of Criminology*, Oxford: Oxford University Press.

Pease, K. (2001) 'Crime Futures and Foresight: Challenging criminal behaviour in the information age', in David S. Wall (Ed.) *Crime and the Internet*, London: Oxford University Press.

Reid, E. (1999), 'Hierarchy & Power: Social Control in Cyberspace', in P. Kollock & A. Smith (Eds), *Communities in Cyberspace*, London: Routledge.

Rheingold, H. (1993) *The Virtual Community Homesteading on the Electronic Frontier,* New York: Harper Collins.

Richardson, R. (2000), *CSI/FBI Computer Crime and Security Survey*, California: Computer Security Institute

Richardson, R. (2003), *CSI/FBI Computer Crime and Security Survey*, California: Computer Security Institute

Shaw, D. F. (1997), 'Gay Men and Computer Mediated Communication: A Case Study of the Phish.Net Fan Community' in Steven Jones (Ed.) *Virtual Culture: Identity and Communication in Cybersociety*, London: Sage.

Short, J. F. and Strodtbeck, F. (1965) *Group Processes and Gang Delinquency*, Chicago: University of Chicago Press.

Sutton (1987) *Differential Rates of Vandalism in a New Town: Towards a Theory of Relative Place,* Unpublished PhD Thesis: Lancaster.

Sutton, M. Schneider, J. and Hetherington, S. (2001) 'Tackling Theft with the Market Reduction Approach', *Crime Reduction Research Series paper 8,* London: Home Office. [Available online at www.homeoffice.gov.uk]

Sveri, K. (1965) 'Group Activity', in K. O. Christiansen (Ed.) *Scandinavian Studies in Criminology,* Vol. I. London. Tavistock.

Turkle, S. (1995), *Life on Screen: Identity in the Age of the Internet*, London: Weidenfield and Nicolson.

Wade, A. L. (1967) 'Social Processes in the Act of Juvenile Vandalism' in R. Clinard and R. Quinney (Eds.) *Criminal Behaviour Systems,* New York: Holt, Rhinehart and Winston.

Walker, C. and Akdeniz, Y. (1998) 'The Governance of the Internet in Europe With Special Reference to Illegal and Harmful Content', *The Criminal Law Review Special Edition on Crime, Criminal Justice and the Internet.*

Wall, D. (2001) 'Maintaining order and law on the Internet'. In D. Wall (Ed.) *Crime and the Internet*, London: Routledge.

Ward, C. (1973) *Vandalism*, London: Architectural Press.

Williams, M. (2003) *Virtually Criminal: Deviance, Harm and Regulation Within an Online Community,* Unpublished PhD Thesis: Cardiff.

Wilson, J. Q. and Kelling, G. L. (1982) Broken Windows: the police and neighbourhood safety, *The Atlantic Monthly*, March. pp 29-38.