CYBERCRIME AND THE CULTURE OF FEAR: Social science fiction(s) and the production of knowledge about cybercrime (Revised Feb. 2011)[1]

David S. Wall, Criminology, SASS, Durham University, 32 Old Elvet, Durham. DH1 3HN, UK. <d.s.wall@durham.ac.uk>[2]

Abstract [Page 861]

This article maps out the conceptual origins of cybercrime in social science fiction and other 'faction' genres to explore the relationship between rhetoric and reality in the production of knowledge about it. It goes on to illustrate how the reporting of dystopic narratives about life in networked worlds shapes public reactions to technological change. Reactions which heighten the culture of fear about cybercrime, which in turn, shapes public expectations of online risk, the formation of law and the subsequent interpretation of justice. Finally, the article identifies and responds to the various mythologies that are currently circulating about cybercrime before identifying the various tensions in the production of criminological knowledge about it that contribute to sustaining those mythologies.

Keywords cybercrime; cyberpunk; culture of fear; internet myths; reassurance gap; science fiction

Introduction

When politicians, police, interest groups, policymakers and others are pressed for comments about dramatic crimes or events that have captured the public imagination, their immediate response nowadays seems to be to point to the internet as a causal factor. Yet, at the end of the day after the investigations are completed the internet links are very often found to be circumstantial, secondary (say, the result of a knock on effect) but rarely causal. Despite these inconsistencies, the initial reactions never seem to be retracted or for that matter critically challenged, thus causing the internet, cyberspace and the cyber-offender to be further demonized, with adverse effects upon the way that it is viewed and used. If, however, these events are viewed critically, **[Page 862]** then the more they are examined, the more apparent it becomes that conceptualisations of cybercrime, like cyberspace, are riddled with epistemological disparities between 'what is' and 'what aught'. Most notable of these is the startling contradiction between the apparently high levels of public

[1] Please cite as: Wall, D.S. (2008/11) 'Cybercrime and the Culture of Fear: Social science fiction(s) and the production of knowledge about cybercrime (revised Feb. 2011)', *Information, Communication & Society* (11): 861–884. Originally published 1 Sept. 2008. N.B original page numbers are in brackets. Variations from the early version are in brown font but should print in black. Endnotes are now footnotes and the original endnote numbers are included.

[2] Formerly at the University of Leeds until August 2010

Electronic copy available at: http://ssrn.com/abstract=1155155

fear about cybercrimes (fuelled by reports of high prevalence) and the rather sober reality of very few prosecutions (Wall 2008).

Drilling down for an explanation of the contradictions between what people say (reporting) and what is happening (such as prosecutions) reveals the presence of a mythology, or series of myths about cyberspace and cybercrime. This mythology arises from a combination of distortions in the ways that knowledge about cybercrime is produced and cybercrime's powerful cultural antecedents in social science fiction. Social science fiction is the branch of science fiction that explores those forms of society that are the product of technological change and its narratives tend to be informed by facts relating to technical scientific possibilities – see for example, the works of Bruce Stirling, William Gibson, Neal Stephenson and Bruce Bethke. The mythology emerges when fictional ideas subsequently that frame concepts and become presented as truths that reinforce existing public anxieties and apprehensions. This is not to say that 'Cyberpunk writers made it all up', as Bruce Sterling accused me of arguing in his *Wired Magazine* blog (Stirling, 2008). Rather, the problem is that social science fiction continues to be one of a number of cultural reference points that are relied upon when knowledge production lacks both objectivity (actual facts about events and trends) and critique. Thus, as the line between reality and social science fiction becomes blurred then 'what we already fear can now thrive in the new space provided by the internet' (Furedi 2002, p. 34). This fear becomes a central part of the struggle to control cyberspace. Whether it is through an intentional policy or as a knock on effect of other processes, fear becomes normalized in contemporary debates about cybercrime (as it does with crime in general). Not only does fear become a normal part of everyday life, but it also becomes anticipated and even missed when it is not there. '[T]he belief that humanity is confronted by powerful destructive forces that threaten our every day existence' has become deeply embedded in our psyche (Furedi 2002, p. vii). Which is quite startling when the unprecedented high levels of personal security that now exist in Western societies are taken into consideration. This 'culture of fear', as it is has become known, is, according to many commentators (Furedi, 1887; 2002; Simon, 2007), readily exploited by modern governments and used as a tool of governance - a political tool that justifies increased governmental power and control over society.

It is argued in this article that social science fiction contributes to the framing of the cultural frameworks and mythologies that configure our discussions about cybercrime, and in so doing structures our expectations of it in terms of what we expect it to look like. The subsequent text therefore explores the curious relationship between new technologies and social science fiction to map out their influence upon the production of knowledge about cybercrime. The first part looks at the conceptual origins of cyberspace and cybercrime in social science fiction print and audio-visual media. It illustrates how dystopic and utopic simulated realities represented in networked worlds not only shape broad public reactions to technological change (the Futureshock and the emergence of a

Electronic copy available at: http://ssrn.com/abstract=1155155

culture of fear) but also public expectations about online risk. The second part maps out and responds to the resulting myths and mythologies about cybercrime. The third and concluding part of the article briefly discusses the tensions in knowledge production that need to be overcome to demythologise cybercrime.

The conceptual origins of cybercrime

The term 'cybercrime' symbolises online insecurity and risk and it is widely used today to describe the crimes or harms that are committed using networked technologies. 'Cybercrime' is relatively meaningless by itself because it is mainly a fictional construction that has no original reference point in law, science or **[Page 863]** social action. It also tends to be used metaphorically and emotively, rather than rationally, to express ambivalent and general concerns about hacking. The term is, however, gradually entering formal legal terminology due to the harmonising influence of the 2001 COE Cybercrime Convention (ETS No. 185), to describe computer misuse legislation. For example, in Australia (Cybercrime Act 2001), Nigeria (Draft Cybercrime Act), the United States (proposed Cybercrime Act 2007) and the UK (the Home Office introduced its 'Cyber Crime' Strategy in March 2010). The key issue here is that many of the so-called cybercrimes are not necessarily crimes in criminal law, nor are they variations of traditional forms of offending. If we could turn the clock back in time then perhaps the term 'cyberspace crime' would have been a more accurate descriptor. However, merits and demerits aside, the term 'cybercrime' prevails as the accepted term (Wall 2007, p. 10).

Cyberpunk literature – from meatspace to cyberspace and meatcrime to cybercrime

Much of the conceptual baggage that 'cybercrime' carries can be traced back to the cyberpunk social science fiction literature of the 1970s and 1980s. Cyberpunk authors combined cybernetics with the sensibilities of the contemporary punk movement to form a genre of science fiction that thematically joined ideas about dystopic advances in science and information technology with their potential capability to breakdown the social order. As Person (1998) observes

> "Classic cyberpunk characters were marginalized, alienated loners who lived on the edge of society in generally dystopic futures where daily life was impacted by rapid technological change, an ubiquitous datasphere of computerized information, and invasive modification of the human body". (Person 1988)

The cyberpunk leitmotif was essentially a 'hi-tech but low-life' aesthetic and the 'Classic cyberpunk characters' described by Person became a social blueprint for the hacker stereotype.

The term 'cyberspace' appears to originate in William Gibson's 1982 highly influential short story 'Burning Chrome' about the hacker group 'Cyberspace Seven' (Gibson 1982).[3] The short story was published in *Omni Magazine*, a science fiction meets hard science forum that existed between 1978 and 1998[4] and which promoted explorations into cyberpunk. Along with other science fiction forums, novels and films during the 1980s, *Omni*, contributed to the progressive definition of virtual 'cyberspace' as a contrast to the physical environment or 'meatspace' (Gibson 1984) and the linkage between cyberspace and crime was just another short step. Having said this, the linkage has been somewhat confused by the evolution of two quite different visions of cyberspace that are usefully delineated by Jordan (1999, pp. 23–58). Gibson's original symbolic **[Page 863]** vision of cyberspace sees individuals shift their consciousness from their 'meatspace' into 'cyberspace' as in *The Matrix*, leaving their physical bodies or 'meat' behind. Whereas, the John Perry Barlow's hybrid (Barlovian) vision combined Gibson's concept with real-world experience to join the imaginary with reality (Jordan 1999, p. 56; Bell 2001, p. 21). The product was an environment that could be constitutionalised (Barlow 1996). This alternative vision of cyberspace is, after Sterling (1994, p. xi), a place that is not inside the computer or inside the technology of communication, but in the imaginations of those individuals who are being connected. Although imaginary, it is nevertheless real in the sense that the things that happen in that space have real consequences for those who are participating.

The actual point of origin of the term 'cybercrime' is unclear, but it seems to have emerged in the late 1980s or even early 1990s in the later cyberpunk print and audiovisual media.[5] However, the linkage between cyberspace and crime was implicit in the early cyberpunk short stories by William Gibson, Bruce Sterling and Bruce Bethke[6] and many others. The cyberspace-crime theme was subsequently taken to a wider audience in popular contemporary novels such as Gibson's 'Sprawl' trilogy of *Neuromancer* (1984), *Count Zero* (1986) and *Mona Lisa*

---

[3] Not to be confused with Gibson's 1986 book of his short stories called *Burning Chrome*, though the short story is reproduced at p. 176 (originally e/n 1).

[4] There are many competing claims over the origination of the various cyber-concepts, which is not surprising since there was much discussion about them during the 1980s and 1990s because they excited authors, readers and other participants in the discourse. Regardless of the actual attribution, the main point here is to identify the cultural formations and the conceptual links that were made between them (originally e/n 2).

[5] The examples of books and films listed here are intended to be illustrative and not exhaustive, and neither is the choice of media. Print media includes [Originally cited on page 878] novels, short story anthologies, poetry, graphic novels or comics, conceptual design, non-fiction or critical studies. Audiovisual media includes cyberpunk films, films with cyberpunk elements, documentary films, TV series, Japanese anime, rock bands, computer and video games, online computer games. Choices of particular media can become very personal and tastes will vary. The object of the exercise is to draw conclusions of types that illustrate change. For a very handy index of science fiction books and magazines see *The Locus Index to Science Fiction*. Available at: http://www.locusmag.com/ index/ (30 January 2008) (originally e/n 3).

[6] Writer Bruce Bethke is accredited with coining the word 'Cyberpunk' in his 1980 story 'Cyberpunk', see Bethke (1997) (originally e/n 4).

Overdrive (1988) and Stephenson's *Snowcrash* (1992).[7] Cyberpunk effectively defined cybercrime as a harmful activity that takes place in virtual environments and made the 'hi-tech low-life' hacker narrative a norm in the entertainment industry. It is interesting to note at this point, that whilst social theorists were adopting the Barlovian model of cyberspace, it was the Gibsonian model that shaped the public imagination through the visual media.

Haxploitation movies

Cyberpunk was very popular within the social science fiction community during the 1980s, but its audience was nevertheless relatively small and cliquish. The cultural fusion of cyberspace and crime into mainstream popular culture was largely due to the second and third, of three generations of hacker movies into which some of the cyberpunk ideas dripped. The first generation - defined by original mainframe computer technology and committed within discrete computing systems (Wall 2007, p. 44) - conceptually predated cyberpunk, but demonstrated to a wider audience the power of the computer 'hack'. The first generation of movies featuring hacks included the *Billion Dollar Brain* (1967), Hot Millions (1968), *The* (Original) *Italian Job* (1969), *Superman III* (1983) and *Bellman and True* (1988). In these movies the 'hackers' tended to be portrayed as male, fairly old and usually somewhat comical or eccentric, see, for example, Benny Hill as Professor Peach in *The Italian Job*; Richard Pryor as Gus Gorman in *Superman III*; Peter Ustinov as Marcus Pendleton in *Hot Millions*.

The second generation of hacker films – defined by early network technology (typically using dial-up modems) and committed across networks (Wall 2007, p. 45) – were clearly influenced by cyberpunk ideas, in contrast to the first generation. They focused on the hacker rather than the hack. The earlier second generation films romanticised the guile of the hacker as a penetrator of inter-connected computer systems. These films consolidated the 'hacker' stereotype which endures to this day of a disenfranchised, misunderstood **[Page 864]** genius teenage male who uses technology to put wrongs right whilst having a 'coming of age' experience and possibly some fun in the process. These films included *War Games* (1983), *Electric Dreams* (1984), *Real Genius* (1985), *Weird Science* (1985) and *Ferris Bueller's Day Off* (1986). The later second generation films were a little more sophisticated in that the hackers they depicted tended to use the Internet, or an imaginative sci-fi equivalent. The focus also shifted from portraying hacks across communication networks to hacks in different types of new virtualised environments. Hackers were still young(ish), but not always male. Gordon (2010) found that 7 of the 60 film hackers studied in his analysis were female (see Bradley 2010). They were also less likely to adopt the moral high ground than they did in earlier films and the ends tended to justify the 'technological' means in their *modus operandi*. The films included *Die Hard* (1988), *Sneakers* (1992), *Goldeneye* (1995), *Hackers* (1995), *The Net* (1995),

[7] Stephenson (1992) refers to the virtual environment as the Metaverse (originally e/n 5).

Johnny Mnemonic (1995), *Independence Day* (1996), *Enemy of the State* (1998), *Takedown* (2000), *AntiTrust* (2001) *Swordfish* (2001) and *The (*new) *Italian Job* (2003).

The third generation of haxploitation films, defined by networked technology delivered by broadband (Wall 2007, p. 47), depict both hacker and the hack within a virtual environment and are epitomised by *The Matrix* (1999) and its later derivatives. Underlying *The Matrix* narrative is an articulation of the Gibsonian linkage between cyberspace and meatspace via the avatar, through the conceptual framework of French social philosophy. Jean Baudrillard's ideas about 'hyper-reality' – the impossibility of differentiating fantasy from reality – greatly inspired the Wachowski brothers who wrote and produced the film. Indeed, so strongly did the idea of hyper-reality shape the construction of *The Matrix* narrative that Baudrillard's *Simulacra and Simulation* (Baudrillard 1994) was (allegedly) set as required reading for the film's principal cast and crew. However, true to his form, when asked for his view on this use of his work Baudrillard is reported to have curmudgeonly retorted that he thought the producers and writers had misunderstood it (see Hanley 2003). Observant viewers of the 'follow the white rabbit' scene in *The Matrix* will have noticed that Neo stores his computer disks in a hollowed out hardback copy of *Simulacra and Simulation*.

The dystopic conceptual linkage between crime and cyberspace has been further exploited in 'haxploitation' print and audio-visual media. Coined by internet journalist John Leyden (2001 2007), 'haxploitation' defines a genre that deliberately exploits the public fear of hackers for entertainment (my definition). However, in recent years there has been a noticeable shift away from, what had become, the traditional hack narrative that emphasised the hacker's power over the state and society along with the humiliating public exposure of the state's impotence in the face of the hacker. Instead, the new haxploitation narrative erodes the boundaries between the individual hacker and the state to re-express its dominant norms and effectively redress the perceived power imbalance found in the earlier movies. Moreover, in the new narrative there is a clear reversal of the roles so that the state itself effectively takes over the prime hacker role in order to suppress it's more deviant and dangerous subjects. See, for example, movies such as *Die Hard 4.0*, where the state hits back, along with some help from an ethical, or white-hat hacker, or *Enemy of the State* where the state hacks the individual when driven by rogue elements. The upshot is that these 'factional' images skilfully combine fact with fiction and have crystallised the 'super-hacker' offender stereotype as the archetypal 'cybercriminal' (Wall 2007, p. 16). But also as an outsider, because the combination of the image of the independent 'outsider' with an expression of the power they can yield sets up the hacker as a potential folk devil, which is precisely what the image of the hacker became (Nissenbaum 2004). **[Page 865]**

What makes these various 'hack'-related sources of visual and textual imagery significant is that 'contemporary movie and media imagery subconsciously orders the line between fact and fiction' (Furedi, cited in Wall 2007, p. 16). So much so that Roger Burrows (1997) argued in his ground-breaking article on 'Cyberpunk as Social Theory' that not only has the Gibsonian concept of cyberspace transmuted into a tangible reality, but his (Gibson's) technological vision has also fed back into the theory and design of computer and information systems. Furthermore, despite the contradictions between the different visions of cyberspace, Gibson's fictional perspectives on cultural, economic and social phenomena have also begun to find their way into social and cultural analyses as viable characterisations of our contemporary world (Burrows 1997). Yet, as outlined earlier it was the hybrid Barlovian model of cyberspace, rather than the pure Gibsonian vision, that has actually found the greater purchase with social theorists, especially in thinking about cybercrime. Because if cyberspace is also a space in which criminal intent can be expressed as action, then the extent to which harmful acts are mediated by networked technologies therefore becomes a useful measure of whether or not an act is a true cybercrime or not. When the range of harmful activities tagged as cybercrimes are explored (see Wall 2007), some are found to be familiar forms of offending, but others are not. However, when they are assembled in terms of the extent of mediation by networked technology then three distinct generations of cybercrimes can be identified that can exist simultaneously – which may explain some of the apparent differences of opinion in definition (see Wall 2007, pp. 44–48). The first generation are traditional crimes where a computer has been used peripherally in the offending. If you take away the internet then the same crimes will still take place. The second generation are hybrids which are traditional forms of offending for which new global opportunities have emerged. Take away the internet and they simply reduce in number and become more localised. The third generation are those patterns of offending that have been created by networked technologies and disappear when the internet is taken away.[8]

Dystopias and future shocks

The contemporary, though now traditional, science fiction hacker narrative is, surprisingly, neither unique nor innovatory. Quite the opposite, in fact, because it tends to conform to a character type that originated in Victorian science fiction, namely, a person who constructs or appropriates technological inventions in order to give them extra-human power to wield control over others. It is as popular now as a core theme of science fiction as it was a century or more ago. See, for example, the science fiction novels of H. G. Wells[9] and others, which

[8] Central to this theory is the contention that the same technologies which create the crimes can also be used to mediate them in policing and prevention (see further Wall 2007, Chapters 8 and 9) (originally e/n 6).

[9] H. G. Wells' better known science fiction novels are *The Time Machine* (1895), *The Island of Dr Moreau* (1896), *The Invisible Man* (1897), *The War of the Worlds* (1898), *The First Men in the Moon* (1901) (originally e/n 7).

were written during a time of great social upheaval caused by technological innovation, and which described worlds that had been transformed, but also threatened by new and potentially oppressive technologies. This tradition continued through **[Page 866]** to the cyberpunk of the present day via the works of Brian Aldiss, Aldous Huxley and contemporaries. Indeed, at the centre of most of these works was the 'savant', a learned person of profound knowledge who could utilise technology to his or her (usually his) advantage for good or bad. However, it is the potentially dystopic power that the savant can wield through technology that makes them so much more interesting as a science fictional character. The 'savant' was, in many ways, the Victorian equivalent of the hacker.

The different science fiction genres not only strengthened the modern 'hacker' narrative by emphasising the technological power binary (powerful versus non-powerful), but more generally they also helped to strengthen existing post-war cultural reactions to techno-social change. Interleaved with science fiction, for example, was the social science fiction novel, of which the most well-known example was probably Orwell's now, classic work *Nineteen Eighty Four* first published in 1949 (Orwell 1990). Orwell captured the post-war zeitgeist by combining ideas about technological change with contemporary political events and social theory in order to describe a dystopic future in which state power was augmented by technological innovation.

Nineteen Eighty Four and its literary offspring served to heighten cold-war anxieties about the potentially dystopic power of technological invention and also fed these ideas back into social theory. Toffler's *Futureshock* (1970), for example, draws upon the dystopic themes to describe how fear of the future tends to rear its head whenever there is a significant period of technological transformation. More recently, Furedi (2002) and others have described the prevailing culture of fear which is a sort of ideological fear of fear which leads to exaggerated public expectations of, amongst other things, crime and danger, which is felt regardless of whether any actually exist. Such process is not far from Garland's 'crime complex' whereby public anxiety about crime has become the norm and now frames our everyday lives (Garland 2001, p. 367) so that we expect crime to exist regardless of whether it actually does, and we are shocked, and even panic, when we do not find it! Garland (2001) and Simon (2007) have suggested that governments and policymakers tactically use prevailing fears of crime to control a broad range of risks.[10] That this tactic should also be used with cybercrime is of no surprise. Taipale has argued that the fear of technology, what he calls 'Franken-Tech', now exists because the 'public debate on complex policy issues is often dominated by information entrepreneurs (including activists and the media) who attempt to engender information cascades to further their own particular agenda' (Taipale 2006, p. 153). Because the resolution of 'issues' takes place 'in situations where the manageable risks are inflated or

[10] 'Governance through crime' is a criminological discourse that locks into the work of Jonathan Simon (2007) and David Garland (2001) (originally e/n 8).

misunderstood' (Taipale 2006, p. 153), then unnecessary levels of public anxiety can result in resource managers being pressurised into misallocating (usually public) resources. The gap that inevitably emerges between the expected threat and the provision of security, displayed, for example, by the disparity between reporting and prosecution as illustrated earlier, is a *reassurance gap* (Innes 2004) that **[Page 867]** clearly needs to be closed. The need for reassurance typically becomes expressed in the form of public demands for more law and 'police' action which, of course, the police find hard to provide because not only is the factual basis of the demands flawed, but police funding models are usually determined by responsive routine activities based upon the 170-year-old Peelian model of policing dangerousness (Wall 2007, p. 161).[11] Policing today remains remarkably similar in principle to its original form when set up in the late 1820s, even though it now operates in more complex late modern societies. As a consequence, the uncritical coupling of the social science fiction driven hacker narrative with the ambiguous scientific conceptualisation of networked virtual space, viewed in terms of a traditional Peelian crime and policing perspective, against a dystopic social science fiction backdrop distorts perceptions of the reality of cybercrime. The conceptualisation of cybercrime in social science fiction as dramatic, futuristic and potentially dystopic proscribes public expectations of cybercrime as above the capabilities of normal folk, as sensational, disempowering victims and being beyond the scope of state protection (e.g. policing). When these perspectives are placed against a backdrop of contemporary cultural reactions to technological change, then they create the circumstances right for the creation and maintenance of mythologies.

Myths and the construction of cyberfear – rhetoric versus reality

The distortions described earlier are reflections of, and also reflect upon, the ways that incidents of cybercrime are reported in the news, which has the knock-on-effect of reinforcing existing (cyber) fears. News reporting tends to simultaneously feed the public's lust for 'shocking' information, but also feeds off it – the relationship is dynamic rather than causal. This endless demand for sensationalism sustains the confusion of rhetoric with reality to create, what Baudrillard described as 'le vertige de la realite´' or 'dizzying whirl of reality' (1998, p. 34). By blurring predictions about 'what could happen' with 'what is actually happening' the message is given by various media that novel events are far more prevalent than they really are. Once a 'signal event', such as a novel form of cybercrime, captures media attention and heightens existing public anxiety then other news sources will feed off the original news story and spread virally across cyberspace. In such manner, relatively minor events can have significant impacts upon public beliefs compared with their actual consequences, especially when they result in panics and moral panics (Garland 2008).

[11] Sir Robert Peel was the founder of the British Police. The British Police were essentially a bureaucratically organised agency formed locally but partly funded by government to keep the dangerous classes off the streets, maintain order and enforce law. The structure and principles of the British Police were subsequently adopted by many countries around the world.

Furthermore, although signal events may not necessarily constitute a major infraction of criminal law, or necessarily a minor one, their outcome is that they 'nonetheless disrupt the sense of social order' (Innes 2004, p. 151). By capturing the public and media's attention they exert 'a disproportionate impact upon beliefs **[Page 868]** and attitudes when compared with their "objective" consequences' (Innes 2005, p. 5), raising levels of (cyber) fear and sustaining internet mythology. For a simple and practical illustration of the way that one news item can spread across the internet, the reader should type the term 'haxploitation' (mentioned earlier) into the Google search engine. Whilst 'haxploitation' is not a crime signal event, it is a unique word with a distinct origin and is therefore easy to follow on the internet in order to illustrate the point being made here. Leyden mentioned the term in his August 2001 article and then again in another in December 2007, and seemingly no where else. On the 30 January 2008, 45 of the first 100 hits were direct reproductions of Leyden's 2007 news item.[12] Consequently, many (possibly hundreds) of news outlets have subsequently fed off these few sources, and judging from the large incidence of direct copying of the original text it would seem that in some cases this process may even be automated. In this way, information begins to flow virally across the internet. What tends to happen with the more dramatic incidents is that they subsequently get transmitted across blog sites as comment, which is then responded, or rather reacted to, thus creating new sources of news on the same topic.

Over the past two decades a number of internet-related urban myths have established themselves as common wisdoms with the effect of not only distorting our understanding the present, but also a new range of emerging issues, even though any factual basis that contributed to their initial creation may long since have disappeared. A paragraph from the abstract of the House Of Lords Science and Technology select committee report conveniently encapsulates much of this dramatic mythology.

> 'But the Internet is now increasingly the playground of criminals. Where a decade ago the public perception of the e-criminal was of a lonely hacker searching for attention, today's 'bad guys' belong to organised crime groups, are highly skilful, specialised, and focused on profit. They want to stay invisible, and so far they have largely succeeded. While the incidence and cost of e-crime are known to be huge, no accurate data exist'. (House of Lords 2007, p. 6)[13]

An otherwise informative report, the phrasing of this one paragraph embodies a range of assumptions and prevailing myths: that cybercrime is dramatic; the internet is pathologically unsafe and criminogenic; hackers are all powerful 'bad-guys'; hackers have become part of organised crime; hackers are anonymous,

[12] I did not look beyond the first 100 hits. Most of the remaining 55 were also reproductions of only a few sources that used the term (originally e/n 9).

[13] Of course, such clusters of phrasing subsequently tend to find their way into press releases and then tend to focus the media coverage of the report and other similar examples (see the later discussion of the disintermediation of media).

they cannot be tracked, they go unpunished; there is no reliable data. And almost unsaid, is the implicit assumption that individual users cannot be trusted and need to be protected from themselves and others. With the exception of the point about reliable data which is dealt with later, they are unpicked and explored below, along with responses and also some of the new issues which they obfuscate. **[Page 869]**

Cybercrime is dramatic, futuristic and dystopic

The term 'Cybercrime' immediately conjures up dramatic, futuristic, technologically dystopic crime imagery in the public's mind's eye, yet the reality of cybercrime is quite the opposite. The three distinct groups of cybercrime, outlined in Wall, 2007, pp. 52–159; 2005/2010: 82-85) – *crimes against the machine* (such as hacking), *crimes that use machines* to commit them (e.g. fraud), *crimes in the machine* (e.g. extreme pornography or racist content) for example, each tend to be mainly small impact, bulk victimisations. They individually lack the drama of conventional crime, but only become significant when the impacts of the bulk-victimisations are aggregated. This is a major challenge for those charged with resolving them. If there is drama in cybercrime, then, it is therefore to be found in their aggregate (global) impact and in the cultural reaction to them.

Cyberspace is pathologically unsafe and criminogenic.

The sheer volume of millions upon millions of person to person, person to business, business to business, government to person and business transactions that take place simultaneously is testament to the fact that the internet is currently working. Against these numbers, even the wilder estimates of levels of cybercrime would still be relatively minor. Plus, for the most part, a good quality regularly updated security product combined with discretionary usage will drastically reduce levels of risk to the user. Despite this, there remains an underlying public concern, propagated by media reportage and adverse commentary, that the internet is not only criminogenic, but also downright dangerous and culpable. On the day of writing these sentences (in 2008), for example, a mini internet panic occurred over whether or not social networking sites romanticised suicide. This panic had been sparked following the heartbreaking suicides of seven (13 in total) young people in South Wales (BBC 2008a). The local MP and others quickly and publicly blamed the internet, and the police announced that they were conducting an investigation. Without any concrete evidence demands were made for inquiries into social networking sites, police investigations and legislation to make internet service providers and host sites more legally responsible. Interestingly, the BBC asked for comments on the question of whether or not social networking sites romanticised suicide and of the 100 published comments most disagreed and did not think that the internet was to blame; only a small handful were in agreement (BBC 2008b). The coroner who subsequently investigated the deaths said that he did not believe them to be

linked (BBC 2008e). The same day 'virtual worlds' such as Second Life took over as the *concern du jour* after US intelligence analysts identified them as potential recruiting grounds for terrorists (O'Harrow 2008, p. D01).

A hacking prosecution in 2008 also usefully reveals the extent to which cyberspace is considered to be pathologically vulnerable to attack. An Estonian man was prosecuted in January 2008 for conducting a 'cyberwar'. Between April and May 2007 he had blocked the website of the Reform Party Prime Minister as one of a series of hacks on Estonian institutions and businesses (BBC 2008c). **[Page 870]** The immediate political and media response was to assume that something more sinister and organised was afoot. In this case, the Russian government was blamed for hacking into the websites, without any supporting evidence (BBC 2007f). The Russians strongly denied involvement, which, of course, until the facts were presented in court also served to strengthen the myth.

Perhaps the greater risk is not so much direct purposeful threats, but accidental damage; for example, in January 2008 many internet connections throughout the Middle East were severely disrupted when a submerged cable was allegedly damaged by a ship's anchor (BBC 2008d). Another area of risk to networked systems is its management and the ability to securely manage the large amounts of critical information that are contained within it, especially when concentrated within one source, such as a database. Again, purposeful attacks are only one aspect of the overall risk. The issue of information management came into the spotlight in November 2007 when CD-ROM disks containing personal information of 25 million child benefit claimants were lost in postal (not electronic) transit from one public agency to another (BBC 2007b). The resulting panic not only brought to light other losses (BBC 2007d; 2007e), but it has also illustrated how potentially vulnerable such concentrations of data are and how important security policies are to the politics of personal security. At the time of writing no evidence has yet been presented to suggest that any of the missing data has caused loss through fraud – although there could be a long delay before any frauds are detected and there exist reasons why they may not be reported. In addition to outlining potential vulnerabilities, the data losses also emphasise the importance of maintaining existing security policies when critical functions are increasingly being outsourced, especially the security of public data when it is shared across the public and private sectors. Yet, these possibilities should also be part of information management plans. What these incidents highlight most of all is that all informational activities within cyberspace will carry risks, as they do in the terrestrial world, and such risks have to be identified and remedied, however, as the events in the United Kingdom have illustrated, the risk lies more in human failings than in the virtual environment.

The omnipotent super-hacker

The super-hacker stereotype is found just about everywhere from cyberpunk to haxploitation and features prominently in policy debates about cybercrime. Hackers have long been renowned and even feared for their expert knowledge of the workings of communications systems and many folk would still believe that they can make planes fall from the sky and interfere catastrophically with aspects of the critical infrastructure. Nissenbaum (2004) has argued that the reconstruction of the public image of the ethical hacker from one-time folk hero to miscreant, vandal, criminal and more recently, terrorist, has occurred not as the result of a direct and rational public debate about conflicting ideals and **[Page 871]** interests, but through 'an ontological shift mediated by supportive agents of key societal institutions: legislative bodies, the courts, and the popular media' (Nissenbaum 2004, p. 195). The mythology surrounding the super-hacker not only assumes that their expert knowledge and cunning skills give them 'access to all areas', but once their moral bind has eroded and they go over to the 'dark side' then they become a danger to society. Ohm (2007) has observed that the cybercrime expert discourse is replete with the construction of super-hackers (he calls them 'superusers'). These 'mythical' super-hackers are assumed to be immune from technical constraints and aware of legal loopholes, and are therefore greatly feared by policymakers. Policymakers, whom, Ohm argues, exaggerate their power and too often, overreact by 'passing overbroad, ambiguous laws intended to ensnare the Superuser, but which are used instead against in culpable, ordinary users' (Ohm 2007, p. 1). So, how robust is the myth of the super-hacker?

For many years, the face of the super-hacker was Kevin Mitnick until he was eventually caught and jailed. His own account (Mitnick & Simon 2002) usefully deconstructs his own myth. His account reminds us that at the height of hacker mystique in the 1980s and 1990s overall levels of security were much lower than today. It was not uncommon at the time, for example, to find systems with a default user identity of 'Admin' being accompanied by the password 'Admin'. Where security was tighter, the majority of deep level penetration was and still is the result of 'social engineering' – persuading those in low-level occupations within an organisation to reveal their access codes (Mitnick & Simon 2002). The evidence from such accounts suggests that hackers tend to focus their efforts upon easy victims or 'low hanging fruit' (Ortega 2006, p. 6).

Further evidence of the extent to which the super-hacker/ super-user has become a 21st century mythical folk devil comes from Erickson and Howards's analysis of 589 incidents of compromised data between 1980 and 2006. They found that the proportion of reported incidents involving hackers was about half that of those involving organisational actions (or inaction). "While 31% of the incidents reported clearly identify a hacker as the culprit, 60% of the incidents involve missing or stolen hardware, insider abuse or theft, administrative error, or accidentally exposing data online" (Erickson and Howard 2007, pp. 1242-1243). The implication of this and previous observations is that 'insider', whether

disgruntled, devious or just plain malicious, is arguably as problematic (if not more so) than the 'outsider' - the hacker (the constructed criminal 'other').

Sommer argues that the (super)hacker myth today is little more than 'an amusing diversion and [no longer] an opportunity to dust down 20-year old clichés about teenage geniuses' (Sommer 2004, p. 10). Ironically, although still present, the super-hacker myth contrasts with a new style of automated hacking (Wall 2007, p. 150) that is potentially more potent in the way that it casts a wide net for victims by using malicious software such as viruses, worms that install remote administration software, key-stroke loggers, spyware and so on. These tools are unwittingly downloaded onto computers through spam, deceptive emails or from fake www sites (drive-by downloads). Once activated, the software enables others to obtain access codes, and even use the computers remotely via botnets (networks of infected computers [Wall 2007, p. 150]). Furthermore, there has been a shift away from the use of spam as the primary means for delivering crimeware or malware, towards the use of 'drive-by-downloads' from legitimate, but infected, www sites (see Wall, 2010). New types of crimeware are now 'intelligent' enough to evade 'capture' by proprietary security software and then uninstall itself once its mission has been accomplished. Consequently, identity theft and account take-over is now of great concern, though it is mostly related to collecting information as a precursor to fraud rather than what we conventionally understand as hacking. It is not the result of a direct hack attack, but an electronic trawl or 'phishing' expedition. In terms of news values, the new style 'hack' has neither dramatic impact nor is it carried out by a troubled genius. However, once the impact of ID theft is felt beyond the credit card and its attendant bank guarantees then the intrusion into one's life can become extremely invasive – a spectre that has the hallmarks for spawning a new series of myths.

These developments in hacking will likely result in the emergence of a new unethical-hacker mythology, particularly as the increase in potential ill-gotten gains from online criminal activity now means that online offenders are no longer so eager to be visible as they once were. Whereas online offenders used to want to be known, be recognised, be revered and even be feared for their malign achievements - often advertising their expert services in the process - their modern counterparts are increasingly seeking precisely the opposite, total anonymity. It pays to be invisible today and virtual stealth is becoming the name of the game. Furthermore, attacks are becoming increasingly personalised, as information about occupation, gender, age and or area of residence is sorted using analytical software to profile individuals into potential victim groups. So it is very arguable that hackers in the future will no longer play up to the hacker stereotype and reinforce it, or if they do it would be to purposefully confuse law enforcement investigators rather than to aggrandise their own actions.

We are on the brink of a cyberwar and will fall prey to cyber-terrorists

Nowhere does the super-hacker/superuser myth continue to prevail and distract attention from major issues of concern than in the cyberwar/ cyberarmageddon discourse. It is a discourse that has shaped policy and resource allocation for many years by raising levels of concern to the point that resources are released (more so with military than police) (See Singel 2010 et al.). The threat of an imminent 'Electronic Pearl Harbour' in one form or another has been regularly prophesised by some commentators since the popularisation of the internet in the early 1990s (Smith 1998). It is a convenient metaphor that emotionally invokes the humiliation of the US in WWII and warns that society can be brought to its knees by forces beyond its control unless pre-emptive action is taken. Although the 'Electronic Pearl Harbour' has not yet materialised, its spirit still permeates most contemporary cybercrime debates.

In January 2008, for example, a former intelligence analyst claimed, in a paper that could have come straight from the pages of a science fiction, novel, that crackers had caused major power blackouts in order to blackmail foreign governments (Leyden 2008). As is often the case, responses are divided between those who believe such statements and the growing army of sceptics and 'Proof of concept' relating to the potential for offending is so often mixed up with its reality.

Rosenberger, one of the more vociferous cyber-war sceptics, critically questions the evidence for this and other similar statements (Rosenberger 2008). Furthermore, Leyden (2008) argued that evidence for similar attacks on utilities are thin on the ground and cited as examples three cases of attacks against utilities running Supervisory Control and Data Acquisition (SCADA) systems which work on (usually corporate) networks (though often intranets) and are therefore potentially 'hackable' from within those systems. They include an Australian case in early 2000 where a disgruntled ex-employee hacked into a water control system to wreak revenge by flooding the grounds of a hotel with a million of gallons of sewage. In 1999, malicious Russian hackers took control of a Gazprom[14] gas pipeline for a day, and finally there was a case in early 2003 where a Slammer worm interfered with the running of the corporate network at an inactive nuclear plant in Ohio and in so doing disabled a safety monitoring system for some hours (Leyden 2008). Although potentially serious, **[Page 872]** none of these examples were thankfully catastrophic and were seemingly not intended to be. There is also a question over whether they could be catastrophic if the intent were there because of the widespread existence of national infrastructure protection plans. Such plans include air gaps between the internet and critical systems and most nations now have them in place, precisely to reduce their risk of falling victim to attack.

[14] Gazprom is the largest Russian business and also the main extractor of natural gas in the world (originally e/n 10).

Another group of cyberwar sceptics writing for *WIRED* magazine[15] have stated that the cyberwar (cyberarmageddon) rhetoric is profoundly dangerous because its practitioners seem to think that promoting fear about cyberwar is "the only way to make bureaucracies move in the right direction" (Singel 2010). Using the term and all it invokes as a tactic to release resources is one thing, but it is not without its consequences. In a review of Richard Clarke's *Cyberwar* (Clarke and Knake 2010), Singel argues that not only does the term cyberwar promote unnecessary fear, but:

> "… it feeds the forces of parochial nationalism and militarism — undermining a communications system that has arguably done more to connect the world's citizens than the last 50 years of diplomacy. And, let's be honest, your photocopier will never, ever catch on fire due to a hacker, like it does in Cyberwar. Except, of course, in the movie version of this book, which undoubtedly, will star Bruce Willis or Keifer Sutherland" (Singel 2010).

The last comment in Singel's quote is particularly poignant because the 'cyberwar'/ cybercrime discourse provides a dramatic narrative for the movie industry, and one which ultimately strengthens the culture of fear about cybercrime.

The problem, as Schneier has argued, is that the emotive rhetoric of cyberwar simply does not match the reality of the event and using sensationalised phrases such as "cyber armageddon" [and cyber warfare] only inflames the situation (Shiels, 2011). He argues that a power struggle is currently going on, involving a "battle of metaphors", metaphors that invoke fear, uncertainty and distress. In fact, the problem as Schneier sees it is that: "[w]hat we are seeing is not cyber war, but an increasing use of war-like tactics and that is what is confusing us … We don't have good definitions of what cyber war is, what it looks like and how to fight it" (quoted in Shiels, 2011). Schneier is not alone in thinking thus because Howard Schmidt, the White House cyber security co-ordinator has similarly opined that "[w]e really need to define this word because words do matter". Schmidt describes "Cyber war [as] a turbo metaphor that does not address the issues we are looking at like cyber espionage, cyber crime, identity theft, credit card fraud … When you look at the conflict environment - military to military - command and control is always part of the thing. "Don't make it something that it is not" (Schmidt quoted in Shiels, 2011).

Similar points to those of Schneier and Schmidt were raised by the OECD *Future Global Shocks* report (Sommer and Brown, 2011). The report concluded that very few single cyber-related events would have the capacity to cause a global shock. Rather, the authors argue that while pandemics and financial instability

---

[15] See the various Cyberarmageddon entries in WIRED's Threat Level blog - http://www.wired.com/threatlevel/category/cybarmageddon/

could cause problems, cyber attacks are unlikely to. Trouble caused by cyber attacks is more likely to be localised and short-lived (BBC, 2011).

The need to separate the reality from the cyber-war rhetoric has become all the more important as ongoing state investments in cyberwarfare are expected to develop a full capability around 2015 onwards when full maturity of skill sets occurs - despite PR claims that it will be sooner. There is the (quite serious) danger of a self-fulfilling prophecy taking place with the rhetoric becoming the reality. The intensity and potential severity of the Stuxnet scare of 2010 brought this sharply into focus as the media and other commentators immediately described it in terms of warfare. One commentator even described it as 'a precision, military-grade cyber missile aimed at Iran' (Economist, 2010).

Some further explanation of Stuxnet is required to illustrate this point. The Stuxnet worm is a form of malware that can be used to sabotage SCADA (Supervisory Control And Data Acquisition) based industrial control systems ranging from water utilities to gas pipelines to power stations, including some nuclear power plants. A more detailed technical analysis of Stuxnet can be found Falliere et al. (2010). Stuxnet arguably represents a 'paradigm shift' in malware threats and is distinct from other malicious worms because, firstly, its primary method of entry into operating systems is, in addition to entry via the internet, through USB sticks. Secondly, like other worms it establishes a rootkit as well as backdoor connections that allow external control. Thirdly, unlike other worms, it aggressively attacks specific types of SCADA systems produced by particular manufacturers for distinct processes. Fourthly, the July 2010 Stuxnet worm had a kill date and limited scope and sought particular system configurations – indicating that it was intended to hit specific targets.

Although a range of antecedents exist, Stuxnet's most recent iteration, discovered in mid-2010, was found to have infected approximately 100,000 systems worldwide, though the evidence so far suggests that it has not yet found its intended target. Where Stuxnet contrasts with the design and function of preceding malware is that it is a large, multi-faceted 'piece of malware with many different components and functionalities' and therefore poses a particularly complex threat (Falliere et al., 2010). Falliere et al. (2010) estimate that Stuxnet took many months to create and must have been the work of a fairly large and highly skilled team. Of particular significance is the observation that the designers of Stuxnet will have required precise data about the design of the particular systems being attacked, including codes, which could only be obtained through the assistance of an organisational insider (see brief discussion in Wall, 2011: 11). Also significant is the fact that the malware needed to be directly introduced into the target environment by an insider because the most sensitive SCADA systems are usually kept unconnected to the internet. Falliere et al. (2010) go on to show that removable drives, typically USB sticks were the most likely means by which the malware was introduced into the system: it '... may

have occurred by infecting a willing or unknowing third party, such as a contractor who perhaps had access to the facility, or an insider' (2010).

What Stuxnet graphically illustrates is how the risk stakes have been considerably raised in comparison to the past. It also illustrates the different ways that insiders can now become involved as well as the speed at which affirmative action would need to be taken to prevent or serious damage from occurring. However, despite the certainly of the proof of concept, in the absence of conclusive information about the intended target and whether or not it reached it, conspiracy theories quickly evolved that map the Stuxnet threat onto contemporary political divisions, before any supporting evidence. A particular concern, for example, was that the 2010 attack was specifically targeted at Iranian's nuclear processes by Israel. This conclusion was derived from an apparently Biblical reference in a project name buried in the Stuxnet code. As the Economist (2010) [and many others] observe: "We are deep into the realm of speculation here". Although subsequent research by Albright et al (2011) has found strong (but not conclusive) evidence that the targets of Stuxnet were the IR-1 centrifuges at the Fuel Enrichment Plant (FEP) at Natanz in Iran. Albright et al. link the known target of Stuxnet – certain configurations of Siemans SCADA operating systems that run equipment such as centrifuges - with the known destruction of 1,000 of the 9,000 centrifuges at the nuclear plant during the time of the attack (infection) (Albright et al. 2011). Having made a link, Albright et al. then go on to question why only 1,000 of the centrifuges were destroyed (if indeed, that was the case). One conclusion they make is that it may possibly "be harder to destroy centrifuges by use of cyber attacks than often believed" Albright et al (2011) - an observation which concurs with that of the OECD report (Sommer and Brown, 2011).

A significant problem with the debates about cyberwar and cyberterror (emotive enough on their own) is that they tend to bleed into each other to further inflame the public imagination. One useful way of understanding them more clearly is to break them down into more digestible chunks as far as is possible. Firstly, there are acts of protest hacktivism which use hacking to protest in order to achieve a political goal. Secondly, there is electronic Jihad which is the pursuance of a holy war by using computers instead of swords. Thirdly is patriot hacking which is hacking, often country on country, in order to further a national political interest (see examples in Denning, 2010: 171). By separating out these issues, it becomes clear that while there are many tangible examples of protest hactivism, there is less clear blue water between proof of concept and evidence of actual events in support of claims of electronic Jihad and international patriot hacking.

In this section, what has been questioned is not only our assumptions about cyber-terror, but also whether or not we would recognise it if/ when it takes place. Past experience suggests that it is unlikely to take place as often prophesised in security discourse via the malicious hacking – typically of the software that controls key infrastructural hardware. Given that the security of critical national

infrastructures, including cyber-security, are protected today in most countries by national security (and often cyber-security) strategies, then perhaps more attention should be shifted to other sources of potential threat. One such threat (of many) is likely be to spread malicious misinformation virally across the internet in order to ferment public anger beyond the tipping point of social action. The power of this sort of virtual psycops operation is that once the tipping point is reached then it is hard to repair the damage as the truth becomes irrelevant. To emphasise this point, we have already witnessed the almost catastrophic impact that innocent or accidentally formed misinformation can have upon on an economy. In September 2007 an internet fuelled panic almost brought the UK's Northern Rock Building Society to its knees threatening a possible domino effect upon the rest of the British Banking sector. Significant was the fact that the fiscal panic continued for some time after the UK Government had given the public assurances that it would protect saver's deposits. At one point during the panic the police were called to various branches of the bank in order to deal with 'boisterous customers' who aggressively demanded to withdraw their savings (Poulter and Sims, 2007).

Hackers have become part of organised crime

The alleged link between hackers and organised crime has long been made but has always lacked conclusive proof. It is a link that is hindered by differences in legal definitions of organised crime which range from three to four individuals temporarily working together to commit a crime, to massive international 'mafia' organisations with clearly defined lines of command and control – cyberpunk meets *The Godfather*. Predictably, the terminology of internet mafia, digital mafia, or hi-tech crimes gangs is frequently used to invoke imagery of the latter rather than the former (see Lewis 2007; Ward 2008).

In her study of organised criminal activity on the internet, Brenner predicted that it would more likely manifest itself in 'transient, lateral and fluid' forms, as networks of criminals (Brenner 2002, p. 1) rather than replicate the 'gang' and hierarchical American 'Mafia' models of organised criminal activity found offline in the terrestrial world. Mainly because they evolved largely in response to real world opportunities and constraints that **[Page 873]** are largely absent in cyberspace. In support of Brenner's 2002 prediction, there have since been a number of examples of the emergence of new forms of online criminal organisation, but they differ greatly from the mafia model. The first is the finding in 2004 by a German Magazine *C'T*, following the botnet explosion in 2003/04 that virus writers had been selling the IP addresses of computers infected with their remote administration Trojans to spammers (C'T 2004).

The second was in June 2005 when the National Infrastructure Security Coordination Centre (NISCC) warned users about 'a highly sophisticated hightech gang' reputed to be located in the far-East using various means, including botnets, to infect sensitive computer systems to steal government and

business secrets (NISCC 2005; Warren 2005). The final example is 'Operation Firewall' which led to the investigation and prosecution of 'shadowcrew', an international identity theft network which hosted online forums that shared information about stealing, trading and selling personal information that could be used to commit frauds. The various reports of the investigation and prosecution illustrate how different the groups were in terms of their networked organisation. The head of e-crime at the Serious Organised Crime Agency (SOCA)[16] observed that the Shadowcrew worked 'remotely, without ever needing to meet', which is 'typical of how the new e-crime networks operate compared to the old-style "top down" organised crime groups' (Rodgers 2007). These groups have a very detailed division of labour with specific skill sets rather than the 'usual pyramid structure'. One person would provide the documents, 'another would buy credit card details, another would create identities while another would provide the drop address' (Rodgers 2007). The key difference is its networked structure and global reach (see BBC 2007c; Goodin 2007a, b). Together the examples detail the relatively new forms of distributed and flat networked criminal organisation that depart from traditional thinking about hierarchically organised crime (Wall 2010).

The key difference between cybercrime and traditional crime is its networked structure and global reach. The organisation of cybercrime is becoming 'Wikified (for want of a better description) as its organisation increasingly follows a Wiki model of distributed online collaborations (after Tapscott and Williams 2007), rather than the 'command and control' Mafia model that is so often assumed. In many ways cybercrimes, by their very informational, networked and global nature, go against the very grain of the traditional model of organised crime.

> "Indeed, the new networked technologies used are relatively cheap, so there are comparatively few start up costs and little upfront investment, plus they are online and do not need street protection - thus evading two well known hooks of traditional organised crime organisations" (Wall 2010).

Criminals are anonymous and cannot be tracked

Whilst it is true that individuals can use false identities when committing crimes online – as they can also do when committing crimes in the terrestrial world – one of the more stunning and frequently overlooked features about networked technologies is that every move online can be tracked and the 'mouse droppings'

[16] See further, www.soca.gov.uk. 'The Serious Organised Crime Agency (SOCA) is an Executive Non-Departmental Public Body sponsored by, but operationally independent from, the Home Office. The Agency has been formed from the amalgamation of the National Crime Squad (NCS), National Criminal Intelligence Service (NCIS), that part of HM Revenue and Customs (HMRC) dealing with drug trafficking and associated criminal finance and a part of UK Immigration dealing with organised immigration crime (UKIS). SOCA is an intelligence-led agency with law enforcement powers and harm reduction responsibilities. Harm in this context is the damage caused to people and communities by serious organised crime (originally e/n 11).

as they are called, leave a data trail behind. The issue is therefore not so much one of anonymity, but rather one of investigators having the human and technological resources available to follow the digital trail. See for example, the case of the 'Shadowcrew' investigations mentioned earlier. The members of the crime ring had never met in person, thinking that their participation was anonymous. But it had been penetrated by the US secret service and the UK's SOCA who had tracked their activities both electronically and remotely (Wall 2007, p. 80; Rodgers 2007; Parizo 2005). We are actually witnessing the 'disappearance of disappearance' (Haggerty & Ericson 2000, p. 619) because we cannot hide any more, only disguise immediate **[Page 874]** identities and even then our online behaviour patterns leave algorithmic 'signatures' that can allegedly be traced with the right technology and resources.

Criminals go unpunished and get away with crime

The low reporting to prosecution rate mentioned earlier (also see Wall 2008) could be interpreted to suggest that there is some substance to this statement. But, this is set against expectations of high levels of cybercrime exaggerated by the culture of fear. There are a number of reasons that explain why the prosecution rates for cybercrime may appear low. The first is that, generally speaking, prosecution rates for nearly all aspects of crime, terrestrial or online are low. It is also the case that cybercrimes have some different qualities that set them apart from traditional forms of offending. Research into offences reported to and recorded by the police found that relatively few actually related to the internet and those that did were mostly minor frauds that were passed on directly to the financial sector to deal with (Wall 2007, p. 164). It is also the case that where prosecutions for crimes using computers or computer content are brought, then the 'computer' aspect of the offence may often be dropped in favour of the more substantive offence, e.g., the fraud. This may be due to a lack of evidence or because the prosecution felt that the technical aspects of the computer component of the offence might complicate the issue when presenting the case to the court. Another reason for lower prosecution rates is simply that although there appear to be massive numbers of threats, there are actually few offenders because the networked technologies involved give criminals such a wider and globalised reach. This possibility was certainly highlighted during the prosecutions following 'Operation Bot Roast' (BBC 2007c) which brought down a massive botnet.

Users are weak and therefore need to be protected from themselves

There seems to be an implicit assumption within the various statements and reports issued by computer security community that users have to be protected from themselves in order to prevent them from becoming either victims or offenders. This is a view that appears to run counter to the findings of the British Crime Survey and Offending, Crime and Justice Surveys (Allen *et al*.

2005;Wilson *et al*. 2006) which found relatively little personal victimisation and offending reported by respondents. The prospect of active third-party intervention to protect users from themselves (and to protect society) also runs against the original end-to-end principles of the internet which favoured open communications with end users making the choices as to what to send and receive (Saltzer *et al*. 1984). Having said this, however, there are some vulnerable groups in society who certainly need to be protected, namely new users, cognitively impaired and others, and that novel forms of victimisation also catch users out. The point being made here is that most users tend to be aware of the risks that they face.

Intertwined with the innate distrust of internet users by the security community is the fairly widespread view that not only does the internet place individuals at risk, but it can also corrupt normally law-abiding individuals who go on a moral holiday when on the internet. The internet certainly broadens internet users' life experience and exposes them to a range of social activity that may be outside the confines of their everyday life. But the evidence from research into the moral usage of the internet (Walker & Bakopoulos 2005, and also others) suggests that the greater majority of individuals tend to take their social values with them online. Virtual environments, for example, are increasingly becoming places where all kinds of social relations are being simulated or tried out before participants venture into 'meatspace' (see Wall & Williams 2007). The findings of **[Page 875]** research into online dating suggest that such relationship building can be positive and not as risk prone as pundits have suggested. In 2005, a University of Bath-led survey by Gibbs *et al*. (2006) studied 229 people aged 18 to 65 who used UK internet dating sites to find that 94 per cent of them went on to see each other again (University of Bath 2005). Yet, this sort of positive interaction tends to be treated with much suspicion, even derision, and the negatives, such as the potential for online grooming never seem to be far away from the surface of the discussion. We really must not lose sight of the fact that individual users should and do take responsibility for their actions and, rather controversially in light of some of the security reports, the internet is remarkably ordered if you consider the sheer number of users and the immense volume of transactions that take place on it.

This critical appraisal of prevailing assumptions is important in an information age in which technological development and its associated thinking changes very rapidly. We have to continually subject our conventional wisdoms to critical appraisal, because an acceptable position, say, even two or three years ago may have changed by the current time. Such appraisal is an important tool in the dispelling of myths, because they are at their most destructive when they triumph over reason (Trevor-Roper 1972, p. 259). Worse still, once embedded in local culture they become self-perpetuating. Understanding change as it happens around us requires new types of methodological thinking and is a challenge to be faced. After all, the last sentence of the paragraph cited earlier from the House of Lords select committee report does imply that the statements are not based upon

'accurate data'. As long as these internet myths remain intact and unchallenged, then so does the potential for misshapen public demands for security, distortions in the formation of policy and ultimately the mis-allocation of resources.

Demythologising cybercrime

One of the principal reasons why internet myths can persist is that major tensions currently exist in the ways that knowledge about cybercrimes is produced and which need to be resolved in knowledge-producing cybercrime research strategies (see further Wall 2007, p. 13; 2008). We find, for example, that there are a number of independent and often conflicting discourses simultaneously talking about cybercrime. Lawyers, administrators, police, criminologists, the many academic disciplines, security experts, computer scientists, information officers and the lay person each have a slightly different take on the subject and each tell their own stories. Furthermore, the way that news is generally disseminated has changed because of networked technologies. There are now so many different networked news sources that it has become disintermediated (see Sambrook 2006). Editors do not exercise the overall level of editorial control over the news process that they once did so that information sources are arguably no longer subjected to the same balances and checks.[17]

Drawing upon the findings of specially commissioned research to analyse the content of two weeks' news output from 'the quality newspapers' and comprising of over 2000 stories, *Guardian* Journalist Nick Davies has argued that only about 12 per cent of newspapers stories are the product of journalists' own initiative and are thoroughly checked for integrity (HOC, 2009: Ev126, Q402; Davies, 2008). The purpose of Davies' research, also reported in detail by the researchers in Lewis et al., 2008, was to identify how many stories were based upon a central factual statement and whether or not the evidence for that statement had been thoroughly checked. Rather disturbingly, the bulk (72 per cent) of the remaining 88 per cent were found either to have been directly copied or adapted from wire copy mainly drawn from PA (Press Association) or other news agencies, or directly from PR outputs and press releases. Yet, in nearly all cases (99 per cent) these stories were attributed to a by-lined reporter or 'independent journalist' with little acknowledgement of the original sources (Lewis et al., 2008: 29).

BBC journalist Waseem Zakir has described this new type of journalism as 'Churnalism', arguing that it is a form of modern instant journalism that results from the impact of the twin pressures of time and money and which does not follow the traditional journalistic practice of confirming the integrity of a news story by seeking two or more independent sources of information.

[17] It must be noted, however, that pre-disintermediated news sources were the subject of criticism for the opposite reasons – that the editors exercised too much control and in so doing applied their own value systems! (originally e/n 12).

> "Ten or 15 years ago you would go out and find your own stories and it was proactive journalism," he explained. "It's become reactive now. You get copy coming in on the wires and reporters churn it out, processing stuff and maybe adding the odd local quote. It's affecting every newsroom in the country and reporters are becoming churnalists." (Waseem Zakir interview in Harcup, 2008).

The core function of Churnalists is, then, to utilise 'information subsidies' in the form of press releases, wire stories and other forms of pre-packaged material (see Gandy, 1982) to create articles in newspapers and other news media without undertaking further research or checking. When this 'churnalism' combines with blogging it becomes a central component of viral information flows, further disintermediating news sources.

A poignant example of the disintermediation of news sources, though not in a criminal context, took place in February 2008, when the UK news editors agreed not to cover Prince Harry's (the Queen's Grandson) tour of duty in Afghanistan in order to ensure his safety. In return they were promised access to the prince for publication once his tour was over. The story was leaked by an Australian news source, but it only became a major issue when it was distributed by the self-styled US internet journalist Matt Drudge in his *Drudge Report*. The *Drudge Report* came to prominence in the mid-1990s when it broke news of the Monica Lewinsky affair and Drudge himself has been described as "the most powerful journalist in the world" (Harnden 2008).

In much the same way, but for different reasons, statistics about cybercrime are also disintermediated. Because there are no **[Page 876]** longer any central and formalised points of collection (e.g. police), then fewer commonly applied standards with fewer checks on information quality – which can result in misinformation. The primary source of statistical information tends to be specifically produced by the cybercrime security industry for its own purposes and subsequently generalised or simply misinterpreted in the reporting process (see e.g. BBC 2007a; Symantec 2007).

So, there arises the curious phenomenon of, on the one hand, the over-reporting (and over-problematisation) of cybercrime statistics that represent breaches of scientific rules on individual computers that have been identified by proprietary commercial software that returns the data to its central server. Whilst on the other hand there is the simultaneous under-reporting by victims of offences that should ordinarily be reported to police, but are not because of the unique informational, networked and globalised qualities of cybercrimes. The loss of personal information through identity theft, for example, may only be considered a victimisation when an actual financial loss later occurs. Alternatively individuals may be embarrassed to report their victimisation, their loss may be small, the dangers posed may not be immediately evident may not be regarded as serious by the victim, or the loss may genuinely not be serious. Alternatively, as indicated earlier, it may be the case that police refer victims of online credit card fraud back to their banks who are regarded as the real victims (Wall 2007). Where the

victims are corporate entities, such as banks, reporting losses may expose a commercial weakness and threaten their business model, which raises clear conflicts between the private versus public justice interest with regard to cybercrimes.

Conclusions

Social science fiction has, within the space of a few years, excited an information generation, aggressively embraced networked technologies and made them its own. The information generation's resonance with the various 'factional' depictions of cyberspace, cyberpunk and cybercrime has enabled them to define their identity in late-modern society. The internet's global reach, combined with its easy accessibility, made the information generation feel different – as though they were all hackers. It made them feel free to explore, to roam freely, see and experience new things in what seemed to be a new public commons.

The price of that freedom is not cheap, because there has been an inevitable increase in risks to the individual, but also the increasing need for individuals to be more responsible in their dealings with co-users. Another 'cost' of maintaining those freedoms is the need to engage with the various myths outlined earlier that impede progress. The online policing job, for example, is made that much harder by the conceptual flaws outlined earlier, because cybercrimes do certainly exist, but not in the forms that conventional wisdoms about crime dictate. If the myths and distortions currently shaping internet policing and reform debates are **[Page 877]** not arrested soon, then the benefits of cyberspace will be lost to us all. The need to correct these distortions is made all the more urgent because of the worrying possibility that the networked technologies which create freedoms might turn into a dystopic super-panopticon that might work against us. Especially as the networked technologies that create virtual worlds are increasingly permeating our physical world. Wireless, ambient (AMI) technologies, for example, are increasingly linking domestic household, business and leisure devices to assist the individual and improve their quality of life by automating many routine chores (Wall 2007, p. 219). These also provide potential new crime opportunities – a fourth generation of cybercrime perhaps?

In this post-cyberpunk world where new technologies shape the social and the social shapes new technologies the lines between science fiction and science fact become more and more blurred. Social science fiction has for a long time provided social analysts with an academically coherent 'dystopic vision of a very near future, which is about to collapse on the present' (Burrows 1997). Of current concern is the observation by Burrows that, whether intentional or not, Gibson's cyberpunk fiction is now coming full circle because it is being read as social and cultural theory, rather than simply reflecting it. Although Gibson writes excellent fiction informed by his substantial knowledge of technological developments, it is still fiction, and it is Barlow's hybrid vision that arguably provides the more robust 'factional' basis for theory building. This observation emphasises the need for

good quality information, because it not only makes for informed debate and policy-making, but it arguably feeds back into the literary process which has a close relationship with the formation of science fiction ideas. We are at the beginning of a new chapter of 'the social' in which hypothetical risk and the culture of fear plays a dominant role, a social in which, to paraphrase Furedi (2002, p. 34), what used to pass for science fiction is now becoming a statement about society's anxieties. Only by engaging directly with these fears and myths can this trend be arrested and the benefits of what is to come be realised.

References

Albright, D., Brannan, B., and Walrond. C., (2011) *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*, ISIS, 15 February, http://www.wired.com/images_blogs/threatlevel/2011/02/stuxnet-update-feb-15-2011-final.pdf

Allen, J., Forrest, S., Levi, M., Roy, H. & Sutton, M. (2005) 'Fraud and technology crimes: findings from the 2002/03 British Crime Survey and 2003 Offending, Crime and Justice Survey', *Home Office Online Report 34/05*, [Online] Available at: http://www.homeoffice.gov.uk/rds/pdfs05/rdsolr3405.pdf (30 January 2008).

[Page 879]

Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S. & Zarsky, T. (eds) (2006) *Cybercrime: Digital Cops in a Networked Environment*, New York University Press, New York.

Barlow, J. P. (1996) 'A declaration of the independence of cyberspace', *John Perry Barlow Library*, [Online] Available at: www.eff.org/Misc/Publications/John_Perry_Barlow/barlow_0296.declaration.txt (30 January 2008).

Baudrillard, J. (1994) *Simulacra and Simulation*, University of Michigan Press, Ann Arbor.

Baudrillard, J. (1998) *The Consumer Society: Myths and Structures*, Sage, London.

BBC (2007a) 'Hi-tech crime "is big business"', *BBC News Online*, 17 September, [Online] Available at: http://news.bbc.co.uk/1/hi/technology/6998068.stm (30 January 2008).

BBC (2007b) 'E-mails reveal data check warning', *BBC News Online*, 22 November, [Online] Available at: http://news.bbc.co.uk/1/hi/uk_politics/7106987.stm (30 January 2008).

BBC (2007c) 'Arrests made in botnet crackdown', *BBC News Online*, 30 November, [Online] Available at: http://news.bbc.co.uk/1/hi/technology/7120251.stm (30 January 2008).

BBC (2007d) 'Up to 3,000 patients' data stolen', *BBC News Online*, 14 December, [Online] Available at: http://news.bbc.co.uk/1/hi/wales/7143358.stm (30 January 2008).

BBC (2007e) 'Data of 60,000 on stolen computer', *BBC News Online*, 7 December, [Online] Available at: http://news.bbc.co.uk/1/hi/northern_ireland/ 7133194.stm (30 January 2008).

BBC (2007f) 'Russia accused of "attack on EU"', *BBC News Online*, 2 May, [Online] Available at: http://news.bbc.co.uk/1/hi/world/europe/6614273.stm (30 January 2008).

BBC (2008a) 'Web worries after suicide spate', *BBC News Online*, 23 January, [Online] Available at: http://news.bbc.co.uk/1/hi/wales/7204172.stm (30 January 2008).

BBC (2008b) 'Do social network websites romanticise suicide? Views of 100 respondents', *BBC News Online*, [Online] Available at: http://newsforums.bbc.co.uk/nol/thread.jspa?forumID=4138&edition=1&ttl=20080124213959 (30 January 2008).

BBC (2008c) 'Estonia fines man for "cyber war"', *BBC News Online*, 25 January, Available at: http://news.bbc.co.uk/1/hi/technology/7208511.stm (30 January 2008).

BBC (2008d) 'Web disrupted "across Mid-East"', *BBC News Online*, 30 January, [Online] Available at: http://news.bbc.co.uk/1/hi/technology/7218008.stm (30 January 2008).

BBC (2008e) 'Coroner denies 13 suicides linked', *BBC News Online*, 8 February, [Online] Available at: http://news.bbc.co.uk/1/hi/wales/7234115.stm (8 February 2008).

BBC (2011) 'Risks of cyber war 'over-hyped' says OECD study', *BBC News Online*, 17 January, http://www.bbc.co.uk/news/technology-12205169

[Page 880]

Bell, D. (2001) *An Introduction to Cybercultures*, Routledge, London.
Bethke, B. (1997) 'The Etymology of "Cyberpunk", [Online] Available at: http://www.brucebethke.com/nf_cp.html (30 January 2008)'.
Bradley, D. (2010) 'Forty years of hackers at the movies: review', *Science Text*, 4 February, [Online] Available at: http://www.sciencetext.com/forty-years-of-hackers-at-the-movies.html (3 May 2010).
Brenner, S. (2002) 'Organized cybercrime? How cyberspace may affect the structure of criminal relationships', *North Carolina Journal of Law & Technology*, vol. 4, no. 1, pp. 1–41.
Burrows, R. (1997) 'Cyberpunk as social theory', in *Imagining Cities: Scripts, Signs and Memories*, eds S. Westwood & J. Williams, Routledge, London, pp. 235–248.
Clarke, R. and Knake, R. (2010) *Cyber War: The Next Threat to National Security and What to Do About It*, New York: Harper Collins
Clayton, M. (2010) 'Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant?' *The Christian Science Monitor*, 21 September, http://www.csmonitor.com/layout/set/print/content/view/print/327178
C'T (2004) 'Uncovered: trojans as spam robots', *C'T Magazine*, 23 February, [Online] Available at: www.heise.de/english/newsticker/news/44879 (30 January 2008).
Davies, N. (2010) *Flat Earth News*, London: Chatto
Denning, D. (2010) 'Cyber-conflict as an Emergent Social Phenomenon', pp. 170-186 in T. Holt, T., and B. Schell (eds) *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, Hershey, PA (USA): IGI Global.
Economist (2010) 'A cyber-missile aimed at Iran?' *Economist*, 24 September, http://www.economist.com/blogs/babbage/2010/09/stuxnet_worm
Erickson, K. and Howard, P. (2007) 'A Case of Mistaken Identity? News Accounts of Hacker, Consumer, and Organizational Responsibility for Compromised Digital Records', *Journal of Computer-Mediated Communication*, vol. 12, no. 4, pp. 1229–1247.
Falliere, N., Murchu, L. and Chien, E. (2010) 'W32.Stuxnet Dossier: September 2010, version 1.0', *Symantec White Paper*, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (15 November 2010)
Furedi, F. (1997) *Culture of Fear: Risk Taking and the Morality of Low Expectation*, Continuum: London
Furedi, F. (2002) *Culture of Fear*, Continuum, London.
Gandy, O. (1982) *Beyond Agenda Setting: Information Subsidies and Public Policy*, New York: Ablex Publishers
Garland, D. (2001) *The Culture of Control*, Oxford University Press, Oxford.
Garland, D. (2008) 'On the concept of moral panic', *Crime, Media, Culture*, vol. 4, no. 1, pp. 9–30.
Gibbs, J., Ellison, N. & Heino, R. (2006) 'Self-presentation in online personals: the role of anticipated future interaction, self-disclosure, and perceived success in Internet dating', *Communication Research*, vol. 33, no. 2, pp. 152–177.
Gibson, W. (1982) 'Burning chrome', *Omni Magazine*, July (Also reproduced in Gibson 1986, p. 176).
Gibson, W. (1984) *Neuromancer*, Grafton, London.
Gibson, W. (1986) *Count Zero*, Grafton, London.
Gibson, W. (1986) *Burning Chrome*, Arbor, New York.
Gibson, W. (1988) *Mona Lisa Overdrive*, Grafton, London.

Goodin, D. (2007a) 'Botmaster owns up to 250,000 zombie PCs: He's a security consultant. Jail beckons', *The Register*, 9 November, [Online] Available at: http://www.theregister.co.uk/2007/11/09/botmaster_to_plea_guilty/ (30 January 2008).

Goodin, D. (2007b) 'FBI crackdown on botnets gets results, but damage continues: 2 million zombies and counting', *The Register*, 29 November, [Online] Available at: http://www.theregister.co.uk/2007/11/29/fbi_botnet_progress_ report/ (30 January 2008).

Gordon, D. (2010) 'Forty years of movie hacking: considering the potential implications of the popular media representation of computer hackers from 1968 to 2008', *International Journal of Internet Technology and Secured Transactions*, vol. 2, no. 1-2, pp. 59 – 87.

Haggerty, K. & Ericson, R. (2000) 'The surveillant assemblage', *British Journal of Sociology*, vol. 51, no. 4, pp. 605–622.

Hanley, R. (2003) 'Simulacra and simulation: Baudrillard and the Matrix', *Whatisthematrix*, December, [Online] Available at: http://whatisthematrix.warnerbros.com/rl_cmp/new_phil_fr_hanley2.html (30 January 2008).

Harcup, T. (2008) 'Reporters need to ask what they're not being told', *Press Gazette*, 18 February, http://www.pressgazette.co.uk/story.asp?storycode=40268

Harnden, T. (2008) 'Matt Drudge: world's most powerful journalist', *Telegraph.ac.uk*, 1 March. [Online] Available at http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2008/02/28/wdrudge128.xml (3 May 2010).

HOC (2009) *Press standards, privacy and libel, Second report of session 2009-10, Volume 2*, Unprinted Evidence, House of Commons: Culture, Media and Sport Committee, HC 362-II, April, http://www.publications.parliament.uk/pa/cm200910/cmselect/cmcumeds/362/362ii.pdf - Nick Davies' evidence on Tuesday 21st April 2009, Q402-Q495, pp. 125-149.

Home Office (2010) *Cyber Crime Strategy*, Cm 7842, London: Office of Public Sector Information, March, [Online] Available at http://www.official-documents.gov.uk/document/cm78/7842/7842.pdf [3 May 2010]

House of Lords (2007) 'Personal Internet security, Volume I: report', *House of Lords Science and Technology Committee, 5th Report of Session 2006–07*, HL Paper 165–I, 10 August 2007, London, The Stationery Office Limited, [Online] Available at: http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf (30 January 2008).

Innes, M. (2004) 'Reinventing tradition? Reassurance, neighbourhood security and policing', *Criminal Justice*, vol. 4, no. 2, pp. 151–171.

[Page 881]

Innes, M. (2005) 'Why disorder matters? Antisocial behaviour and incivility as signals of risk', Paper given to the *Social Contexts and Responses to Risk (SCARR) Conference*, Kent, UK, 28–30 January, [Online] Available at: http://www.kent.ac.uk/scarr/events/papers/Innes.pdf (30 January 2008).

Jordan, T. (1999) *Cyberpower: The Culture and Politics of Cyberspace and the Internet*, Routledge, London.

Lewis, J., Williams, A. and Franklin, R. (2008) 'Four Rumours and an Explanation: A Political Economic Account of Journalists' Changing Newsgathering and Reporting Practices', Journalism Practice, 2(1): 27 – 45.

Lewis, L. (2007) 'Digital mafia threatens internet integrity', *The Times*, 7 April, [Online] Available at: http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article1624030.ece (30 January 2008).

Leyden, J. (2001) 'Haxploitation: the complete Reg guide to hackers in film', *The Register*, 3 August, [Online] Available at: http://www.theregister.co.uk/2001/08/03/haxploitation_the_complete_reg_guide/ (30 January 2008).

Leyden, J. (2007) 'Tiger team brings haxploitation to TV: Penetration testing telly show up against the Queen', *The Register*, 19 December, [Online] Available at: http://www.theregister.co.uk/2007/12/19/tiger_team/ (30 January 2008).

Leyden, J. (2008) 'CIA claims crackers took out power grids: Future threat or urban myth in the making', *The Register*, 21 January, [Online] Available at: http://www.theregister.co.uk/2008/01/21/scada_threat_warning/ (30 January 2008).

Mitnick, K. & Simon, W. L. (2002) *The Art of Deception: Controlling the Human Element of Security*, John Wiley and Sons, New York.

NISCC (2005) 'Targeted trojan email attacks', NISCC Briefing 08/2005, 16 June, [Online] Available at: http://www.cpni.gov.uk/Docs/ttea.pdf (30 January 2008).

Nissenbaum, H. (2004) 'Hackers and the contested ontology of cyberspace', *New Media & Society,* vol. 6, no. 2, pp. 195–217.

O'Harrow, R. (2008) 'Spies' Battleground turns virtual: intelligence officials See 3-D online worlds as havens for criminals', *Washington Post*, 6 February, p. D01, [Online] Available at: http://www.washingtonpost.com/wp-dyn/content/article/2008/02/05/AR2008020503144.html (8 February 2008).

Ohm, P. (2007) 'The myth of the superuser: fear, risk, and harm online', (May 22, 2007) *University of Colorado Law Legal Studies Research Paper No. 07-14*, [Online] Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=967372 (30 January 2008).

Ortega (2006) 'News', *Security & Privacy Magazine*, vol. 4, no. 6, pp. 6–9.

Orwell, G. (1990 [1949]) *1984 Nineteen Eighty-Four*, Penguin, London.

Parizo, E. (2005) 'Busted: The inside story of 'Operation Firewall, *SearchSecurity.com*, 28 November, [Online] Available at: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1146949,00.html (30 January 2008)'.

Person, L. (1998) 'Notes toward on a postcyberpunk manifesto', *Nova Express*, no. 16, [Online] Available at: http://slachdot.org/features/99/10/08/ 2123255.shtml.

Poulter, S. and Sims, P. (2007) 'Police called to break-up Northern Rock panic queues as customers withdraw millions', *Daily Mail*, 15 September, [Online] Available at http://www.dailymail.co.uk/news/article-481778/Police-called-break-Northern-Rock-panic-queues-customers-withdraw-millions.html (3 May 2010).

Rodgers, L. (2007) 'Smashing the criminals' e-bazaar', *BBC News Online*, 20 December, [Online] Available at: http://news.bbc.co.uk/1/hi/uk/7084592.stm (30 January 2008).

[Page 882]

Rosenberger, R. (2008) 'SANS director confirms the CIA confirmed ... absolutely nothing', *Vmyths*, 20 January, [Online] Available at: http://vmyths.com/column/1/2008/1/20/ (30 January 2008).

Saltzer, J., Reed, D. & Clark, D. (1984) 'End-to-end arguments in system design', *ACM Transactions in Computer Systems*, vol. 2, no. 4, pp. 277–288.

Sambrook, R. (2006) 'How the net is transforming news', *BBC News Online*, 20 January, [Online] Available at: http://news.bbc.co.uk/1/hi/technology/ 4630890.stm (30 January 2008).

Shiels, M. (2011) 'Cyber war threat exaggerated claims security expert', *BBC News Online*, 16 February, http://www.bbc.co.uk/news/technology-12473809

Simon, J. (2007) *Governing through Crime: How the War on Crime Transformed American Democracy and Created a Culture of Fear*, Oxford University Press, New York.

Sommer, P. (2004) 'The future for the policing of cybercrime', *Computer Fraud & Security,* vol. 1, pp. 8–12.

Sommer, P. and Brown, I. (2011) *Reducing Systemic Cybersecurity Risk*, OECD/IFP Project on 'Future Global Shocks', Paris: OECD, January, http://www.oecd.org/dataoecd/57/44/46889922.pdf

Singel, R. (2010) 'Richard Clarke's *Cyberwar*: File Under Fiction', *Wired Threat Level blog*, 22 April, [Online] Available at: http://www.wired.com/threatlevel/2010/04/cyberwar-richard-clarke#ixzz0lto8rNw9 (3 May 2010).

Smith, G. (1998) 'Electronic Pearl Harbor? Not likely', *Issues in Science and Technology*, 15 (3): 68–73, at www.nap.edu/issues/15.1/smith.htm.

Stephenson, N. (1992) *Snowcrash*, ROC/Penguin, London.

Sterling, B. (1994) The Hacker Crackdown: Law and Disorder on the Electronic Frontier, Penguin, London.

Sterling, B. (2008) 'Cybercrime: Cyberpunk writers made it all up', beyond the beyond, Wired, 30 August, http://blog.wired.com/sterling/2008/08/cybercrime-cybe.html

Symantec (2007) *Internet Security Threat Report Trends for January–June 07*, vol. XII, Symantec, September.

Taipale, K. (2006) 'Why can't we all g*et al*ong: how technology, security, and privacy can coexist in the digital age', in *Cybercrime: Digital Cops in a Networked Environment*, eds J. Balkin, J. Grimmelmann, E. Katz, N. Kozlovski, S. Wagman & T. Zarsky, New York University Press, New York, pp. 151–183.

Tapscott, D. and Williams, A. (2007) Wikinomics: How mass collaboration changes everything, London: Atlantic Books.

Toffler, A. (1970) *Future Shock*, Bantam Books, New York.

Trevor-Roper, H. (1972) *The Last Days of Hitler*, Pan Books, London.

University of Bath (2005) 'Internet dating is much more successful than previously thought, study shows', *University of Bath Press Release*, 14 February, [Online] Available at: http://www.bath.ac.uk/news/2005/2/14/internet-dating.html (30 January 2008).

Wall, D. S. (2007) *Cybercrimes: The Transformation of Crime in the Information Age*, Polity, Cambridge.

Wall, D. S. (2008) 'Cybercrime, media and insecurity: the shaping of public perceptions of cybercrime', *International Review of Law, Computers and Technology*, vol. 22, no. 1, pp. 45–66.

Wall, D.S. (2005/10) 'The Internet as a Conduit for Criminals', pp. 77-98 in Pattavina, A. (ed) Information Technology and the Criminal Justice System, Thousand Oaks, CA: Sage (Chapter revised March 2010). [Online] Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=740626 (3 May 2010).

Wall, D.S. (2010) 'The Organisation of Cybercrime', in P. Brunst, M. Bellini and J. Jaenke (eds) *Current Issues in IT Security*, Freiburg: Max Planck Institute (Forthcoming).

Wall, D.S. (2011) *Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders*, White Paper: Data Loss Prevention, Reading, UK: Symantec.

Wall, D. S. & Williams, M. (2007) 'Policing diversity in the digital age: maintaining order in virtual communities', *Criminology and Criminal Justice*, vol. 7, no. 4, pp. 391–415.

Walker, R. & Bakopoulos, B. (2005) 'Conversations in the dark: how young people manage chatroom relationships', *First Monday*, vol. 10, no. 4, [Online] Available at: http://firstmonday.org/issues/issue10_4/walker/index.html (30 January 2008).

Ward, M. (2008) 'Boom times for hi-tech criminals', *BBC News Online*, 2 January, [Online] Available at: http://news.bbc.co.uk/1/hi/technology/7154187.stm (30 January 2008).

[Page 883]

Warren, P. (2005) 'UK trojan siege has been running over a year', *The Register*, 17 June, [Online] Available at: www.theregister.co.uk/2005/06/17/niscc_ warning/ (30 January 2008).

Williams, M. (2006) Virtually Criminal: Crime, Deviance and Regulation Online, Routledge, London.

Wilson, D., Patterson, A., Powell, G. & Hembury, R. (2006) 'Fraud and technology crimes: findings from the 2003/04 British Crime Survey, the 2004 Offending, Crime and Justice Survey and administrative sources', *Home Office Online Report 09/06*, [Online] Available at: www.homeoffice.gov.uk/rds/pdfs06/ rdsolr0906.pdf (30 January 2008).

David S. Wall is Professor of Criminology at Durham University where he conducts research and teaches in the fields of cybercrime, policing and intellectual property crime. He has published a wide range of articles and books on these subjects. His most notable authored book in this field is *Cybercrime: The Transformation of Crime in the Information Age* (Polity, 2007). His edited collections on the topic include *Crime and Deviance in Cyberspace* (ed. Ashgate, 2003), *Cyberspace Crime* (ed. Ashgate/Dartmouth, 2003), *Crime and the Internet* (ed. Routledge, 2001). He also has a number of articles on the subject that are available at http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=376504.
He is an Academician of the Academy of Social Sciences (AcSS) and a member of the ESRC Grants Delivery Panel. He was formerly Head of the School of Law (2005-2007) and Director of the Centre for Criminal Justice (2000-2005) at the University of Leeds.

Address: Criminology, SASS, Durham University, 32 Old Elvet, Durham, DH1 3HN, UK.
[email: d.s.wall@durham.ac.uk]