POLICING CYBERCRIMES: Situating the Public Police in Networks of Security within Cyberspace (Revised Feb. 2011)

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

Abstract [Page 183]

The Internet and the criminal behaviour it transforms (cybercrime) pose considerable challenges for order maintenance and law enforcement because Internet-related offending takes place within a global context while crime tends to be nationally defined. Policing cyber-crime is made all the more complex by the very nature of policing and security being networked and nodal and also because within this framework the public police play only a small part in the policing of the Internet. In this paper it is argued that the future of the public police role in policing the Internet is more than simply acquiring new knowledge and capacity, but it is about forging new relationships with the other nodes within the networks of Internet security. These relationships require a range of transformations to take place in order to enhance the effectiveness and legitimacy of the nodal architecture. It will then be argued that some of the contradictions faced by 'the police' are being reconciled by the gradual reconstitution of a neo-Peelian paradigm across a global span, which brings with it a range of instrumental and normative challenges.

Keywords: Policing; Cybercrime; Cybercrimes; Cyberspace; Internet; Networks of Security; Nodal Governance

Introduction

The relationship between the public police and technology dates back to their origins in the early nineteenth century. Traditionally a responsive organisation designed to **[Page 184]** counter the dangers produced by urban migration caused by eighteenth-century industrial technology, the police had, by the second half of the nineteenth century, situated themselves as an all-purpose emergency service. It is a heritage that gave them consensual public support and a high degree of local police force independence. As a consequence, it has left ingrained within the organisational and occupational cultures of the police the instinct to protect the public and claim ownership over policing. Although the police and their constitutional position has changed considerably since their formation, many of the original Peelian police principles survive, though adapted

This article was published in May 2007 & revised May 2010, Feb 2011. Much of the revision was conducted during a visiting fellowship at the Centre for Excellence in Policing and Security (CEPS) at the ANU in Canberra and at Griffiths University, Australia. I thank Prof. Peter Grabosky and esteemed colleagues for their support. N.B the original page numbers are in brackets. Variations from the early version are in a dark brown font but should print out in black on a monochrome printer. The few endnotes are now footnotes and the original endnote numbers are included.

to modernity: a bureaucratically organised responsive local police that maintains order and enforces law; officers who are identifiable from the rest of the public, professional in conduct, accountable to law and the community for their actions. However, the increasing pervasiveness of the Internet, along with its global, transformative impacts create a range of entirely new demands upon the public police which question their traditional local dominance over the security domain and could in fact marginalise them completely. Not only does the concept of cybercrime produce problems for the police because Internet-related offending takes place within a global context whereas crime tends to be nationally defined, but policing the Internet is also a complex affair by the very nature of policing and security being networked and nodal (Johnson & Shearing, 2003). While the application of concepts of networked and nodal security may be disputed in the 'terrestrial world' (Crawford & Lister, 2004, p. 426), nowhere is it more networked and nodal than in cyberspace.

This paper explores how the public police are situated in the networks of security that contribute to the policing of harmful behaviour in cyberspace. The first part will question our understanding of cybercrime to identify the tensions arising between the globalisation of harmful behaviour and specific jurisdictional definitions of crime. The second part will probe the networked and nodal architecture of Internet policing to locate, and then situate, the role of the police. It will be argued that the future of the public police role in policing the Internet is more than simply acquiring new knowledge and capacity. For the police to have a role in the policing of cyberspace, they will need to forge new relationships with the other nodes that constitute the networks of Internet security. These relationships will require a range of transformations to take place in order to enhance the effectiveness and legitimacy of the nodal architecture. The third part of this paper will identify the challenges that face the police if they are to maintain their role in networked policing. Finally, the fourth part will look at those responses to argue that some of the contradictions faced by 'the police' have been reconciled by the reconstitution of a neo-Peelian paradigm across a global span. Whilst this may (re)situate the police it nevertheless requires a range of fresh instrumental and normative responses.

Cybercrime as the Focus of Policing Cyberspace

Although a topical and newsworthy subject, little is known about 'cybercrime' other than from press and television reportage. Upon reflection, the term 'cyberspace crime' would have been more meaningful because it more clearly signifies the space in which **[Page 185]** the harmful behaviour takes place. However, because the term is principally a media construct it has subsequently obtained its own linguistic agency and it has entered the public parlance and we are stuck with it (Wall, 2005a, p. 79). Cyber-terrorism, information warfare, phishing (an email purporting to be from a legitimate bank, requesting confirmation of personal details (Toyne, 2003)), spams, denial of service attacks, hacktivism, hate crime, identity thefts, online gambling, plus the criminal exploitation of a new generation of pornographic peccadilloes, it is alleged, conspire to threaten public safety and temper governmental and commercial ambitions for the growth of an information society. Although there is a fairly widespread consensus that cybercrimes exist, there is much confusion as to what they actually are and what risks they pose (Wall, 2005a, p. 77; see Brenner, 2001; Walden, 2003).

To add to the confusion over what constitutes a cybercrime is the frequent practice of media, practitioner and some academic commentators to refer to just about any offence involving a computer as a 'cybercrime'. This practice tends to be accompanied by the tendency to mix, sometimes deliberately so, the debates relating to personal internet security with those relating to corporate or national security. Making matters even worse is the discussion of online offending and deviant behaviours in global terms when in fact their definitions and solutions might be found locally (see McKenzie, 2006). All this has shaped public understanding about cybercrimes and has, arguably, led to a difference between the level of cybercrimes experienced by individuals (which is quite low) and the level of cybercrimes they feel exist (which is quite high). This disparity given rise to a 'reassurance gap' (see Innes, 2004, p. 151) between public demands for policing cybercrime and the level of service that the police can realistically provide. It is therefore important to look first at what is being understood as cybercrime because it contributes to setting the policing agenda. Furthermore, without reliable sources of knowledge, misinformation cannot be countered, misunderstandings are perpetuated and there is no firm platform to establish a responsive criminal justice policy.

Since cybercrimes are the product of networked computers, they must be defined in terms of the informational, networked, and globalised transformation of deviant or criminal behaviour by networked technologies. These transformations give Internet users a global reach, new capacities for distributed peer to peer networking and a panoptic gaze that creates an asymmetric ability to enable one person to simultaneously reach many. These characteristics also contribute to the reorganisation of the division of criminal labour, on the one hand automating and deskilling it (Braverman, 1976), while on the other hand 'reskilling' and empowering the 'single agent' who can single-handedly control a complete and complex criminal activity (Pease, 2001, p. 24; Savona & Mignone, 2004, p. 4; Wall, 2005a, p. 80). The implications of this are profound because the overall set-up and running costs are low and because so few individuals are involved in each incidence of offending, intelligence about the perpetrator is unlikely to leak out.

If Internet transformations are the key to understanding cybercrime, then in order to understand their impact it is necessary to consider what happens if the Internet is removed from the equation. By applying a simple 'transformation test,' three different groups of cyber-criminal opportunity can be identified as points on a spectrum (Wall, 2007). At the near end lie behaviours which are commonly referred to as cybercrimes, but are in fact first generation ‘traditional’ crimes in which computers have been used for information gathering or communication to assist with the organisation of a crime. Remove the computer and the criminal behaviour persists because the offenders will revert to using other information sources or types of **[Page 186]** communication. Towards the middle of the spectrum lie the second generation ‘hybrid’ cybercrimes. These are ‘traditional’ crimes for which entirely new global opportunities have emerged (e.g., globalised frauds and deceptions, also the global trade in pornographic materials including child pornography). Take away the Internet and the behaviour will continue by other means, but not by the same volume or across such a wide span.

At the far end of the spectrum, however, are the third generation ‘true’ cybercrimes which are solely the product of opportunities created by the Internet and which can only be perpetrated within cyberspace (online intellectual property thefts, spams). These are the spawn of the Internet and therefore embody all of its transformative characteristics. Spamming is a good example of a true cybercrime. It is an illegal behaviour in its own right in the laws of the USA, EU, and many other jurisdictions, but it also facilitates secondary offending by enabling engagement with potential victims (Wall, 2005b). Many of the offences that result are small-impact bulk victimisations—de minimis offences. Take away the Internet and spamming and true cybercrimes vanish. These distinctions are important because the first two types tend to be subject to existing laws and existing professional experience can be applied to law enforcement regarding these offences. Any legal problems arising tend to relate more to legal procedures than substantive law. The final group, however, are solely the product of the Internet and pose the greater regulatory challenges.

It is also important, of course, to look for any common features in the substantive behaviours. In this way they can be linked to existing bodies of substantive law and associated experience within the criminal justice processes.

Crimes against the machine or ‘Computer integrity’ crimes are offending behaviours that assault the integrity of network access mechanisms. They include hacking and cracking, vandalism, spying, denial of service, and the planting and use of viruses and Trojans. Many jurisdictions now have legislation such as the Computer Misuse Act 1990 (UK), the Computer Fraud and Abuse Act 1986 (USA) (18 U.S.C. 1030), internationally harmonised by conventions such as the Council of Europe’s Convention on Cybercrime (ETS No. 185; ETS No. 189), to protect against unauthorised access to computer material; unauthorised access with intent to commit further offences; and unauthorised modification of computer material. Computer integrity cybercrimes also pave the way for further offending. For example, unauthorised access can also be the precursor to more serious crimes. Identity theft from computers becomes serious when the information is subsequently used against the owner. Similarly, crackers may use Trojans to install ‘back doors’ which are later used to facilitate other crimes, possibly by spammers who have bought lists of IP addresses of infected computers (BBC, 2003).

Crimes using machines or 'Computer-related' crimes are committed using networked computers to engage with victims in order to dishonestly acquire cash, goods, or services. In addition are socially engineered variants such as 'phishing', advanced fee frauds and the manipulation of new online sales environments, particularly auction sites. Most jurisdictions have legislation concerning thefts and provide legal measures for the recovery of lost assets, as well as intellectual property laws to protect against the unauthorised exploitation of intellectual property.

[Page 187] *Crimes in the machine* or 'Computer content' crimes relate to the content of computers—materials held on networked computer systems. They include the trade and distribution of pornographic materials, the dissemination of hate crime materials, and more recently, the publication of video nasties of the murders of kidnapped foreign nationals. Most jurisdictions have variants of the obscenity laws and laws that prohibit incitement, although their legislative strength can vary where Internet content is also protected by laws of free speech. In common with the other two crime groups, legislation does nevertheless vary across jurisdictions in terms of judicial seriousness (see below).

This mental map or 'matrix' (see further Wall, 2002a, p. 192), illustrates that true cybercrimes are criminal behaviours transformed or mediated by the Internet and distinguishes them from more traditional forms of criminal behaviour. They are, to all intents and purposes, new wines in no bottles! (Wall, 1999) Of the wide range of deviant and criminal behaviours that fall under the rubric of cybercrime, many—both traditional and hybrid—are already covered by existing areas of law. However, while they can be found in the police crime diet, they are not a particularly large part of it and tend to fall within the scope of specialist rather than everyday police work while other behaviours, those referred to as true cybercrimes, are entirely alien to the police. This raises questions not only about whether it is the police who should deal with these offences, but also, in the light of the contrast between the high levels of incidence reported by some statistical sources and very low levels of computer misuse prosecutions, who should be policing cyberspace if the police are not? In the UK, for example, during the first decade following the introduction of the Computer Misuse Act 1990 there were only about 100 or so prosecutions against hackers and even fewer convictions (*Hansard*, 26/3/02, Col. WA35), and this trend is also found outside the UK (see Smith, Grabosky & Urbas, 2004).

Situating the Public Police in the Networks and Nodes of Security in Cyberspace

The public police role has to be understood within the broader and largely informal architecture of Internet policing, which not only enforces norms and laws but also maintains order in very different ways. Understanding this position enables more realistic expectations and understanding of the police role. It also helps to identify a broader range of cross-jurisdictional and cross-sectoral issues that the police have to attend to in order to participate fully in policing the Internet, by embracing the concept of networking. This growing networking of sources of security during recent decades (Dupont, 2004; Johnston & Shearing, 2003) has emerged as one part of the shift towards the networked society (Castells, 2000).

Below are outlined the principal interest groups that constitute the nodes of networked Internet governance and, without making any specific empirical claims, a brief distinction is made between the ‘auspices’ (entities that authorise governance) and the providers of governance (Shearing, 2004, p. 6), thus encompassing the strategies that shape Internet behaviour (see further Wall, 2005a, 2007).

Internet users and user groups

Internet users and user groups exert a very potent influence upon online behaviour through censure, usually after the occurrence of ‘signal events,’ which are behaviours that may not necessarily constitute a major infraction of criminal law, but ‘nonetheless **[Page 188]** disrupt the sense of social order’ (Innes, 2004, p. 151). Cases of more extreme behaviour may also be reported to relevant authorities, such as the Internet Watch Foundation, Trading Standards/Consumer Direct, Action Fraud (the UK national reporting centre from December 2009), or directly to the police, either in person or through one of the many crime reporting websites (Wall, 2010). Furthermore, the establishment of additional new (official) reporting sites for different types of harmful behaviour will increase the relative power of the internet users and user groups.

In addition, individual Internet users can take direct action themselves either to seek justice against cybercrime or cyber-harms they have become victim of, such as online defamation (as in *Keith-Smith v. Williams* (2006), Sturcke, 2006; Gibson, 2006). Else they can take preventative action by employing a range of software solutions. Solutions available include the use of firewalls and encryption in order to protect personal space, and the application of spam filters and virus checkers. Working on a self-appointed mandate, the Internet users are curiously both auspices and providers of governance (Wall, 2007: 167-169).

Amongst the legion of Internet users are a number of interest groups formed around specific issues who ‘police’ web sites that threaten or offend them. Largely transnational in terms of their membership and operation, these tend to be self-appointed and possess neither a broad public mandate nor a statutory basis. Consequently, they lack formal mechanisms of accountability for their actions which themselves may be intrusive, illicit or even illegal. Nevertheless, they appear to be fairly potent. A number of examples of virtual community policing already exist. In addition to the various complaint 'hotlines' and the development of software to 'screen out' undesirable communications (Uhlig 1996a), some netizen groups have sought to organise Internet users around particular issues. The names of the following anti-child pornography sites reveal their particular mission. CyberAngels seek generally to protect children online. Other groups seek to directly combat child pornography: 'Ethical Hackers Against Pedophilia', 'Pedowatch', 'Se7en', 'Internet Combat Group' and 'Morkhoven'. The final group, The Association of Sites Advocating Child Protection (ASACP) (originally known as Adult Sites Against Child Pornography) is dedicated to the elimination of child pornography from the Internet through its reporting hotline (AIN, 2005). Other active user-groups exist to combat a range of issues, such as spamming and phishing.

The principle of peer-policing by Internet users is now enshrined in e-commerce through vendor rating systems, of which the most well known is e-bay's online auction trading partners profile rating system. Each e-bay member has his or her own profile determined by customer feedback on past sales performance. The rating system enables prospective purchasers to be able to identify the less trustworthy sellers, thus policing undesirable behaviour within the forum: "[l]earning to trust a member of the community has a lot to do with what their past customers or sellers have to say!" (see further Wall, 2007: 167-169).

Virtual environment managers and security

As virtual environments become more popular, then so does the need to maintain order on them. To this end, most virtual environments now employ moderators or online security managers (often from within the community itself) to 'police' the behaviour of their online community according to the particular norms of that community. The moderators ensure that community members adhere to acceptable behaviour policies and prevent discussions from becoming disruptive, libellous or being hijacked. These moderators/ security managers are collectively emerging as a new stratum of online behaviour governors. A useful example of online moderation is found in the virtual world 'Habbo Hotel' which describes itself as: "a virtual Hotel, where teenagers can hang out and chat". It is constantly monitored by trained, police-vetted, moderators and 'hotel guides' drawn from within the 'Habbo Hotel' online community. The values and norms (auspices) that moderators maintain combine the interests of the particular online community with the legal and corporate responsibilities of the virtual environment 'owner' to the host Internet service provider (ISP) to comply with law and also maintain the stated functions of the forum. The sanctions that moderators can invoke when community norms or rules are broken include 'time-outs', the temporary removal of access rights if the offending is minor, or permanent exclusion and reporting to the police from the environment if it is serious. While these 'policing' practices are generally effective in upholding community norms, they are limited in scope, especially when the offending behaviour 'crosses the line' into more serious offending. Then the concern becomes whether or not the correct action has been taken.

Network infrastructure providers (ISPs)

Another principal interest group consists of the network infrastructure providers or ISPs (Internet service providers). ISPs can influence online behaviour through 'contractual governance' (Crawford, 2003, Vincent-Jones, 2000) which is effected through the terms and conditions (auspices) of their contracts with individual clients – the Internet users. The terms and conditions are largely the product of the market, the law and the ISP's own commercial interests. The Internet service providers are also subject to contractual governance through the terms and conditions laid down in their own contracts with the telecommunications providers who host their Internet services. In addition, ISPs can, because of their strategic position in the communications networks, also employ a range of software solutions to reduce offending online. Most typical of these are robust security systems accompanied by sophisticated professional spam filters.

The Internet Service Providers (ISPs) have a rather fluid status because although they are physically located in a particular jurisdiction, they tend to function transnationally (Walker *et al*. 2000: 6). The liabilities of ISPs vary under different bodies of law and have yet to be fully established (see Edwards and Wealde 2000; Rowland and Macdonald 1997), although cases such as *Godfrey v Demon Internet Ltd* (1999) and the *League Against Racism and anti-Semitism and The Union of French Jewish Students v Yahoo Inc. and Yahoo France* (2000), *In Re: Verizon Internet Services, Inc.* (2003) (Wired, 2003) have exerted a 'chilling' effect upon ISPs actions and have made them very risk averse. The fear of civil sanctions encourages ISP compliance with many of the regulatory demands made of them by the police and other state bodies. Consequently, ISPs tend to tread carefully and are fairly responsive to police requests for co-operation. In addition to being wary of their potential legal liabilities, ISPs are also fearful of any negative publicity that might arise from their failing to be seen to act responsibly. The general rule of thumb that appears to be adopted across many jurisdictions is that liability tends to arise when the ISP fails to respond to requests to remove offensive material, whether obscene or defamatory, once it has been brought to their attention following a complaint (*Felix Somm*, 1998; *Godfrey v Demon Internet Ltd.,* 1999; Leong 1998: 25; Center for Democracy and Technology 1998: 3). ISPs tend to organise themselves within specific jurisdictions, but also across them with a further level of transnational organisation, for example, the Commercial Internet eXchange, the Pan-European Internet Service Providers' Association (EuroISPA) and Internet Service Providers' Consortium (mainly US). These transnational organisations focus primarily upon technical/ practical and commercial issues germane to ISPs. In addition to the Internet service providers are the (regional/ national)

Domain Name Registries which allocate domain names under the oversight of ICANN (The Internet Corporation for Assigned Names and Numbers), an international non-profit corporation formed to assume responsibility for the IP (Internet Protocol) address space allocation, protocol parameter assignment, domain name system management, and root server system management functions. ICANN also resolves disputes over domain name registration (Wall, 2007: 170-171).

Corporate security organisations

Corporate security organisations protect their own corporate interests by exercising contractual governance over their members (both employees and clients) and also any other outsiders. In addition, corporate security organisations may directly employ, or buy in from a specialist cyber-security provider[1], a range of software solutions to protect themselves and also to identify and investigate abnormal patterns of behaviour in their systems and also, in some cases, amongst their clients. Contractual terms and conditions (auspices) threaten the removal of privileges or private or criminal prosecution in the case more serious transgressions.

A poignant example of the corporate exercise of contractual governance is found in the demise of Jennicam.com, one of the original and most popular of the cam-girl sites. Jennicam's collapse was blamed upon a change in the acceptable use policies of the online payment service Paypal which also affected online gambling (see PayPal's acceptable use policy). Similarly, charities and card issuers have lobbied the UK government to change the Data Protection Laws to allow them to cancel the credit cards of those using them to purchase child pornography online on the grounds that it breaches the issuers' terms and conditions of use (BBC, 2006a). Along similar lines, online stores, such as those operated by Yahoo or Hotmail, are ceasing to enter into buyer vendor arrangements where the seller has an easy to set up Webmail account (Leyden, 2006). In March 2006 the 'Financial Coalition Against Child Pornography' was formed to make it impossible to profit from child pornography operations on the Internet. The coalition brought together a range of organisations involved in website service delivery and online payment systems to "share information about websites that sell child porn and stop payments passing to them" (BBC, 2006b). Views vary, however, upon the effectiveness of shaping behaviour through acceptable use strategies and it is therefore likely that they will be more effective for some rather than others. For example, in the case of sites distributing sexual content there is clear evidence of their immediate tactical effectiveness, as with the collapse of Jennicam, however, the sheer market demand for sexual materials on the Internet suggests some resilience against regulation.

[1] Although the specialist cyber-security providers are currently very influential players in policing cybercrime they constitute a sub- sector rather than a separate security network.

Following the widespread mass integration of IT within most organisational structures from the 1980s onwards, and notably since the growth of e-commerce during the late 1990s, the security departments of commercial, telecommunications and other related organisations have been strengthened to protect their interests. As e-commerce grows, it is anticipated that corporate security organisations will become major players in policing the Internet. However, because their primary function is to police their own 'private' interests, it is hard to assess their overall impact on policing because of their low 'public' visibility. Importantly, they tend to pursue a 'private model' of justice because the public criminal justice system does not offer them the model of criminal justice that they want (Wall 2001: 174). Consequently, their relationship with the public police is often minimal. Yet, the latter are organisationally ambivalent about this relationship because they resent the loss of important criminal intelligence, but simultaneously appear happy – from a managerial point of view - not to expend scarce and finite police resources on costly investigations (Wall, 2007: 171-172).

Non-governmental, non-police organisations

Non-governmental, non-police organisations are a hybrid combination of public and private arrangements that contribute directly to the order-maintenance assemblage by acting as gatekeepers to the other levels of governance, but also contributing towards (cyber) crime prevention. The Internet Watch Foundation, for example, provides governance under the **[Page 189]** auspices of a mandate from the UK ISPs, Police, Crown Prosecution Service and Government. One of its principle functions is to bring to the attention of ISPs any illegal materials reported to its hotline, particularly child pornography, the eradication of which is one of the objectives of the Foundation. If deemed actionable following a judgement made against set criteria by a trained operative, the IWF takes appropriate action either by informing the offender's Internet services provider, alerting comparable hotlines in the offender's jurisdictions, else, serious enough and within the UK it may pass on details of a WWW site directly to the police. The IWF also contributes more generally towards cybercrime prevention and public awareness. It was formed in December 1996 with the endorsement of the Metropolitan Police, Department of Trade and Industry (DTI), Home Office and the associations of the ISPs, such as the Internet Service Providers Association and the London Internet Exchange (Uhlig, 1996b; DTI, 1996; Akdeniz, 1997). The standing of the Internet Watch Foundation has increased and it has become the quasi-public face of Internet regulation in the UK, more notably since it re-launch in 2000.

Another example of a non-governmental, non-police organisation is the (US) Computer Emergency Response Team (CERT) based at Carnegie Mellon University in Pittsburgh since its establishment in 1988. It was created in the aftermath of a devastating attack by the Morris Worm which illustrated the Internet's vulnerability by bringing much of it down. Located at the Software Engineering Institute, a federally funded research and development centre of Carnegie Mellon University, the purpose of CERT was to combat unauthorised access to the Internet. Its programmers would log reported hacks and carry out the initial investigations. Where security breaches were found to be too complicated to deal with in-house, they were farmed out to an unofficial 'brain trust' (Adams 1996) and to the relevant public police organisations when an offence was serious and could lead to prosecution. In 2003 CERT joined the Arlington based US-CERT team created by the Department of Homeland Security as part of the national infrastructure protection programme. Prior to the partnership, CERT (Carnegie Mellon) had become the model for many similar computer security organisations throughout the world. CERT was based within a non-governmental public institution, yet, initially funded by a combination of private and governmental resources.

Although the non-governmental, non-police organisations are mainly private bodies, they often perform public functions and a growing concern is that they, as such, lack the formal structures of accountability normally associated with public organisations. (Wall, 2007: 172-174).

Governmental non-police organisations

Governmental non-police organisations provide governance under the auspices of regulations, rules and law through charges (levies), fines and the threat of prosecution. Not normally perceived as 'police', they are nevertheless actively involved in investigating, resolving and even prosecuting cybercrime. They include agencies such as Customs, the Postal Service, and Trading Standards organisations etc. These agencies may employ a range of hi-tech software solutions to protect themselves and also assist them when in conducting investigations.

They also include a higher tier of agencies that set cyber security policy and also oversee the implementation and enforcement of national Internet infrastructure protection policies. Some governments, such as Singapore, China, Korea, Vietnam and Pakistan (in 2010), have at one time or another, and with varying degrees of success, explicitly sought to control their citizen's use of the Internet though such agencies. They have either required users to register with governmental monitoring organisations, or they have sought to directly control Internet traffic in their jurisdictions through government-controlled ISPs (Center for Democracy and Technology, 1996; Caden and Lucas, 1996; BBC 2010). The majority of nations tend to take a more liberal (or pragmatic) approach towards cyber security. Consequently, at the national level in many of the more liberal jurisdictions there exist various higher tier governmental multi-sector cross-sector organisations, agencies or forums with a remit to protect the electronic infrastructure either through active interventions or through the co-ordination of the activities of bodies at an international level. Such arrangements can be complex as the UK example illustrates.

Multi-sector co-ordination is at the heart of the UK Cyber Security Strategy (Cabinet Office, 2009a), which is part of the UK National Security Strategy set by the Cabinet Office (Cabinet Office, 2009b). To help implement and administer the Cyber Security Strategy are two new agencies. The Office of Cyber Security (OCS) in the Cabinet Office provides overall strategic leadership and coherence across government. Because cyber security also impacts upon the Critical National Infrastructure the Office of Cyber Security works with the Centre for the Protection of National Infrastructure (formed in 2007 out of NISCC, the National Infrastructure Security Co-ordination Centre and NSAC the National Security Advice Centre - a part of the UK security service). CPNI is an interdepartmental organisation which draws upon participants from industry, academia and various government departments and agencies to protect national security by reducing the vulnerability of the national infrastructure to terrorism and other threats, including electronic attack.

In support of the Office of Cyber Security is the Cyber Security Operations Centre (CSOC), based at GCHQ in Cheltenham, which has a more tactical remit. CSOC will try to understand the nature of attacks, provide advice, monitor the health of cyberspace and co-ordinate responses to such incidents. A major part of CSOC's remit is to identify national cybercrime threats. Within the Cyber Security Strategy lies the Home Office Cyber Crime Strategy, published in March 2010 to outline the government's approach towards cybercrime (Home Office, 2010a). It is the latest part of a complex jigsaw of national security policy that has gradually been introduced since 2008 to increase the cohesiveness of the UK's National Security Strategy (see further Wall, 2010).

Most EU member countries have similar infrastructure protection and cyber security strategies and agencies with similar functions to OCS and CPNI. There are also emerging a number of EU wide agencies, such as ENISA (European Network and Information Security Agency) whose role it is to support the internal market by 'facilitating and promoting increased co-operation and information exchange on issues of network and information security.'

The UK experience in multi-sector coordination is similar in principle to that of the US. The US Department of Homeland Security (DHS) was created in the aftermath of September 11, 2001. The DHS brought together 22 previously disparate domestic agencies into one department to protect the nation against threats to the US homeland. Amongst the agencies the DHS incorporated under Information Analysis and Infrastructure Protection (IAIP), was the National Infrastructure Protection Center (NIPC) which since 1998, articulated the National Infrastructure Protection Plan of which the Internet was part. The NIPC brought "together representatives from U.S. government agencies, state and local governments, and the private sector in a partnership to protect our nation's critical infrastructures" (NIPC 1998). In 2009 it became the National Infrastructure Coordinating Center (NICC) to serve as the Office of Infrastructure Protection's focal point for coordination and information sharing with the 18 national critical infrastructure and key resources sectors during normal operations and during incident management activities' (NICC page at www.dhs.gov). Under NICC coordination umbrella are many US state-funded non-police organisations that are also involved in policing the Internet to resolve specific problems. For example, the United States Postal Service has a responsibility for the cross-border trading of pornography and the US Securities and Exchange Commission a responsibility for dealing with fraud.

There is a final level of very important and influential governmental non-police organisations which set regulatory policy (often secondary legislation). They are the departments of government that are responsible for trade, and therefore tend to carry the e-commerce portfolios: in the UK this is BIS (Department of Business, Innovation and Skills, formerly BERR and DTI); in the US it is the FTC, (Federal Trade Commission).

Public police organisations

Public police organisations draw upon the democratic mandate of government to impose governance by maintaining order and enforcing national law. Surprising to many, the public police play a comparatively small role in enforcing criminal sanctions upon wrongdoers online, however, whilst small it is an important role because of the public's reliance upon the police in times of emergency. The role played by the police in policing cybercrimes can vary from force-to-force and investigative tactics usually combine traditional policing methods with the use of computers to investigate wrongdoers and collect evidence, they may also use software based techniques to proactively police some priority concerns (Sommer, 2004).

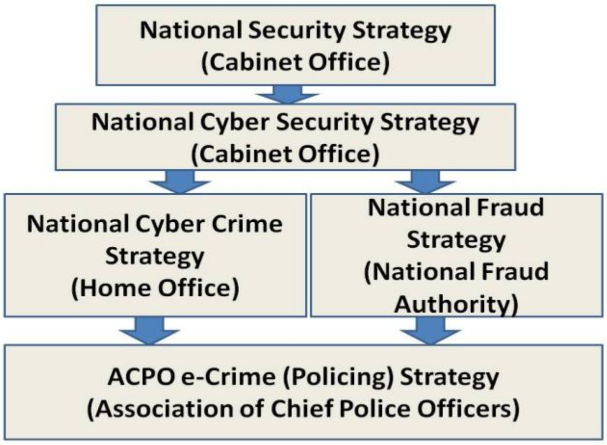
Although the public police are located within nation states and work under national laws, they are nevertheless networked by transnational policing organisations, such as Europol and Interpol, whose membership requires formal status as a police force (see Sheptycki, 2002). In most Western countries, the public police are organised regionally, and within most local police services there usually exist specialist individuals or groups of police officers who can respond to Internet related complaints from the public. Some police forces set up their own cybercrime units, whilst others enter into strategic alliances with neighbouring police forces to provide such services. In addition, there also usually exist national police organisations which deal with the collection of intelligence and the investigation of organised crime. The US and UK experiences sum up the complexities of mapping cybercrime onto 'traditional' policing structures and illustrate the need for specific arrangements for policing cybercrime.

In the USA, the policing of its population of 250 million is carried out by upwards of 17,000 independent local police forces (the actual number varies according to definition of police used). The smaller forces tend to outsource the investigation of cybercrimes to larger forces that possess the expertise. At a national and cross-state level, jurisdiction for cybercrime lies with the Federal Bureau of Investigation. Although the US Secret Service, once a bureau of the Treasury, but since March 2003 part of the Department of Homeland Security, carries a responsibility for investigating crimes “involving U.S. securities, coinage, other government issues, credit and debit card fraud, and electronic funds transfer fraud” (US Secret Service, Duties and Functions).

Policing the UK’s population of 60+million is delivered by about 55 main local police forces (the number varies slightly depending upon how they are defined). Most forces have a cybercrime investigation capability themselves or with a neighbouring force. The types of cybercrime dealt with are traditional crimes that use computers or hybrids, those traditional cybercrimes for which the internet has created globalised opportunities for victimisation. The main problem area for the public police in the UK - as in the US - are the ‘true’ cybercrimes, those which are the spawn of the internet, such as spamming, spam driven frauds and scareware.

Policing cybercrime in the UK is now shaped by a series of strategies (Fig. 1). The Cyber Crime Strategy (Home Office, 2010a) mentioned earlier, specifically deals with online criminal activity, and sits alongside the National Fraud Strategy (NFA, 2009) and the Association of Chief Police Officers’ E-crime [Policing] Strategy (ACPO, 2009). In theory, this combination provides a co-ordinated policing response to the different types of potential harm found online.

Fig. 1 The UK Cybersecurity structure


National Security Strategy (Cabinet Office)
National Cyber Security Strategy (Cabinet Office)
National Cyber Crime Strategy (Home Office)
National Fraud Strategy (National Fraud Authority)
ACPO e-Crime (Policing) Strategy (Association of Chief Police Officers)

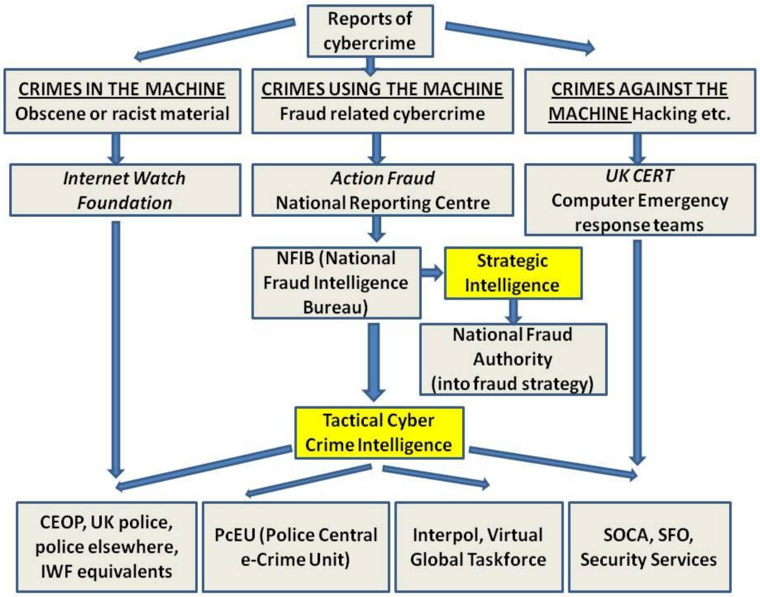
Central to the UK’s cybercrime policing response is a combination of a new national policing capability and new internet crime reporting facilities. The new Action Fraud reporting centre was established in late 2009 as a central point of contact for the public. Supported by the National Fraud Authority it receives reports of frauds and related forms of cybercrime such as phishing (id theft) which are currently the main type of cybercrime affecting individuals and businesses. Action Fraud also offers news and information on fraudsters' activities to alert the public of the dangers facing them.

Reports of websites containing obscene imagery are still received, evaluated and acted upon by the Internet Watch Organisation (IWF). The IWF is an independent organisation created in 1996 by internet service providers to combat obscene imagery, and broadened in 2000 to include to racist material in its remit. It operates with special ACPO/ Crown Prosecution Service (CPS) immunity under Section 46 of the Sexual Offences Act 2003 which allows staff to view obscene images including child pornography without risk of prosecution. The IWF refers 'actionable' cases to the Child Exploitation Online Protection Centre (CEOP), part of the Serious Organised Crime Agency (SOCA). Originally destined to become an independent agency in April 2011, it is now (following a July 2010 announcement) due to join SOCA, the NPIA (National Police Improvement Agency) and other policing agencies with a national remit become part of the new integrated UK National Crime Agency (Home Office 2010b, 23-30). Reports of hacking (crimes against the machine) are currently received from systems security officers by UKCERT (UK Computer Emergency Response Team). Paragraph 86 of the Cyber Crime Strategy states that the Action Fraud reporting model may be extended to the other types of cybercrime in the future.

The reports of cybercrime received by Action Fraud are passed on to the National Fraud Intelligence Bureau (NFIB) which analyses them and decides how they are to be acted upon through its national tasking system. Located within the City of London Police, the NFIB also builds up a national picture of particular types of fraud that would otherwise be regarded as local problems of which the true scale would never be known. The NFIB works alongside the National Police Central e-Crime Unit (PCeU) which is based within the Metropolitan Police and investigates cybercrimes that have national impact. Alongside these arrangements are a range of other anti-e-crime initiatives, such as an Office of Fair Trading (OFT) facility that enables the public to report bogus websites.

Whenever reported cybercrimes are found to be serious, then other agencies such as SOCA (Serious Organised Crime Agency), the Serious Fraud Office (SFO), CEOP or even the security services may become involved. When the crimes transcend borders – as many do – then Interpol may become involved. If the reports of crimes specifically refer to child abuse on a global scale then the Virtual Global Taskforce (VGTF) becomes involved. Set up in 2003, the VGTF is an international working partnership between different police forces and other law enforcement agencies such as Interpol. The following table summarises the seven networks of security (adapted from Wall, 2007: 168). See Fig. 2.

Fig. 2 The current UK reporting mechanisms for cybercrime

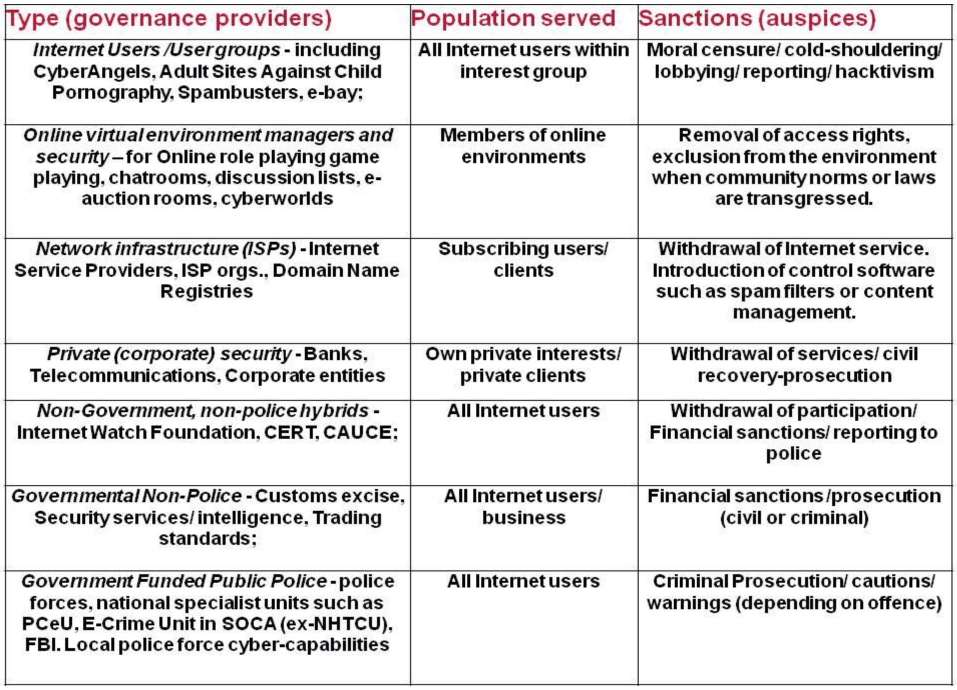

Reports of cybercrime
CRIMES IN THE MACHINE
Obscene or racist material
CRIMES USING THE MACHINE
Fraud related cybercrime
CRIMES AGAINST THE MACHINE Hacking etc.
Internet Watch Foundation
Action Fraud
National Reporting Centre
UK CERT
Computer Emergency response teams
NFIB (National Fraud Intelligence Bureau)
Strategic Intelligence
National Fraud Authority
(into fraud strategy)
Tactical Cyber Crime Intelligence
CEOP, UK police, police elsewhere, IWF equivalents
PcEU (Police Central e-Crime Unit)
Interpol, Virtual Global Taskforce
SOCA, SFO, Security Services

(Source: Wall, 2010: 13)

The answer to the earlier questions posed about the effectiveness of the role of the public police in cyberspace become clearer when understood in terms of the various networks of security which operate to police the internet. Yes, there are low levels of police performance indicators against high levels of policing technology but what the security networks to show is that the police actually only play a very small part in governing the Internet and even then it tends to be jurisdictionally based. This is not however, to say that cyberspace goes un-policed, rather, as Reiner once observed with regard to terrestrial policing more generally: ‘not all policing lies in the police’ (Reiner, 2000, p. xi) (see Fig 3).

The broader governance of the Internet is, then, characterised by a sense of order resulting from a complex ‘assemblage’ of networked nodes of security that continually shape virtual behaviour (Walker & Akdeniz, 1998, p. 8; Wall, 1997, 2001, p. 171, 2002a, p. 192), transcend the ‘state/non-state binary’ (Dupont, 2004, p. 76), and also state sovereignty (Shearing, 2004, p. 6) (see Fig 3). The term ‘assemblage’ is particularly useful in this context when considering the relationships between nodes and also within them. Without attributing causality, ‘assemblage’ describes the relationship between heterogeneous contributors to governance that work together as a ‘networked’ and functional entity, but do not necessarily have any other unity (see Haggerty & Ericson, 2000, p. 605; Miller & Rose, 1990).

Fig 3: Different policing bodies, populations served and sanctions



Type (governance providers)	Population served	Sanctions (auspices)
Internet Users /User groups - including CyberAngels, Adult Sites Against Child Pornography, Spambusters, e-bay;	All Internet users within interest group	Moral censure/ cold-shouldering/ lobbying/ reporting/ hacktivism
Online virtual environment managers and security – for Online role playing game playing, chatrooms, discussion lists, e-auction rooms, cyberworlds	Members of online environments	Removal of access rights, exclusion from the environment when community norms or laws are transgressed.
Network infrastructure (ISPs) - Internet Service Providers, ISP orgs., Domain Name Registries	Subscribing users/ clients	Withdrawal of Internet service. Introduction of control software such as spam filters or content management.
Private (corporate) security - Banks, Telecommunications, Corporate entities	Own private interests/ private clients	Withdrawal of services/ civil recovery-prosecution
Non-Government, non-police hybrids - Internet Watch Foundation, CERT, CAUCE;	All Internet users	Withdrawal of participation/ Financial sanctions/ reporting to police
Governmental Non-Police - Customs excise, Security services/ intelligence, Trading standards;	All Internet users/ business	Financial sanctions /prosecution (civil or criminal)
Government Funded Public Police - police forces, national specialist units such as PCeU, E-Crime Unit in SOCA (ex-NHTCU), FBI. Local police force cyber-capabilities	All Internet users	Criminal Prosecution/ cautions/ warnings (depending on offence)

In some of these networked relationships there may be a consensus of interest in approach, while in others the consensus may be in the outcomes or goals achieved. Consequently, a replication is found in the bifurcation of broader functions in terrestrial policing between the maintenance of order through the assemblage and the enforcement of law to deal with more serious offending behaviour. By separating the two, some sense can be made of the rather conflicting messages that are emerging in debates over policing the Internet. Networked security, for example, **[Page 190]** exploits the ‘natural surveillance’ (see earlier) that networked technologies enable and allows both primary and secondary social control functions to operate. Furthermore, it also tends to mediate, to some extent, global disparities arising from national or jurisdictional legal differences in definition.

The observation made earlier that many cybercrimes fall outside the traditional police agenda would seem to render them unproblematic from a police resourcing point of view—they simply do not get resourced. On the other hand, the public police not only tend to lay claim culturally (organisational and occupational) to a greater ownership of policing the Internet than ‘they actually own,’ but more importantly, they are also expected to do so by the public because of their traditional consensual relationship with the state and their symbolic duty to protect the public from danger.

We see in the debates over the policing of the Internet a replication of the reassurance policing debate (Crawford & Lister, 2004), though with a slight twist. The reassurance policing debate is borne out of the 'increasing recognition that the police alone cannot win the fight against crime and disorder nor meet the public's seemingly insatiable demand for a visible policing presence' (Crawford & Lister, 2004, p. 413). The debate, when shifted to cyberspace, takes for granted that the police alone cannot win the fight against crime, but nevertheless demands a more visible policing presence. This begs two questions: what challenges do cybercrimes pose for the public police? And how do the police deal with them?

The Challenge of Cybercrime for the Public Police

The relationship between the police and technology is long-standing and complex, and a brief reflection explains much about the situation of the public police today. On the one hand, the police were created to deal with the social disorder caused by the technologies of the industrial revolution. On the other hand their responsive and localised nature always meant that they fell behind in their access to, and use of, technology. A long-standing complaint made by members of police and law enforcement agencies is that they do not have the facilities to keep up with criminals, especially with regard to offences that require, what Brodeur has termed, a 'high policing' response (Brodeur, 1983; Sheptycki, 2000, p. 11). Indeed, for over a century readers of the *Police Review* and other contemporary police journals were regularly told by police correspondents that they lacked the resources to obtain the latest technologies that would help them to respond to criminals. More recently, the complaints have focused upon obtaining modern IT equipment and high specification broadband links. Of course, such complaints inevitably backfire as they result in (often unfounded) allegations about police ineffectiveness, which ultimately reinforce the police-originated myth that criminals are ahead of the game. However, while historical themes can be drawn out, what distinguishes the modern debates from their predecessors is not just access to latest technology and skill sets, but access to technology to facilitate networking and networked policing, including access to relevant networks of security.

[Page 191] But, it is one thing to possess the technological capabilities and another to be able to utilise them, and there are a number of institutional obstacles to this task. The public police, like the other criminal justice agencies are deeply conservative institutions that have been moulded by time-honoured traditions, and therefore do not respond readily to rapid change. Furthermore, much of this innate conservatism originates in the police also being symbolic expressions of state sovereignty. Therefore, one way that the police forces generally respond to new issues, whilst preserving their symbolic and organisational conservatism is through the origination of specialist units into which officers with appropriate specialisms are absorbed. While this tactic constitutes an actual and visible response, it nevertheless tends to marginalise the problem it sets out to solve, and runs the risk of preventing the broader accumulation of organisational and professional experience across the force in dealing with the issue at hand. Ultimately, it is the presence of a relevant body of specialist knowledge and expertise within a police force (and whether the other officers know about it) that can determine whether or not the organisational and occupational response of the police to a new public concern is effective or not.

Nevertheless, the global reach of new forms of technological crime organisation, such as cybercrimes, are markedly different to the daily public police crime portfolio. The public police were originally introduced to 'keep the dangerous classes off the streets' by maintaining local order and enforcing law (mostly the former) (Critchley, 1978; Manning, 1998; Reiner, 2000, chap. 2; Wall, 1998, p. 23), and modern police agencies remain largely responsive to public complaints. The routinised responses to these complaints determine police funding and leave the police subject to tight budgetary constraints which restrict the immediate allocation of major resources to emerging matters and therefore their responsive capability.

The limitations of the Peelian policing paradigm[2] have long been understood and there have been employed a number of strategies to resolve the contradictions. At a procedural level, there has been the establishment of international harmonisation and police coordination treaties, such as the Council of Europe's Convention on Cybercrime. A range of national/federal and even international police organisations (for example, Interpol, Europol), have been introduced to complement locally organised police in their investigation of crimes occurring across police jurisdictions. However, despite these procedural and organisational responses, cybercrimes still pose a range of challenges to the police, which are outlined below.

De Minimism

The first is the de minimis trap—the 'law does not deal with trifles' (*de minimis non curat lex*). Characteristic of many cybercrimes is that they are small-impact bulk victimisations with a large aggregated loss, but spread out globally across a range of jurisdictions. Since local policing strategies are often reduced to decisions that are made at a very local level over the most efficient expenditure of finite resources (Goodman, 1997, p. 686), the 'public interest,' a key criterion in releasing police resources for an investigation, is often hard to justify in individual cases of cybercrime victimisation.**[Page 192]**

[2].'Peelian Paradigm' refers to the structure, values and principles of the British Police which were subsequently adopted by many countries around the world and which formed a basis for modern policing standards. Set up by Sir Robert Peel in the late 1820s, 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.

Nullum Crimen Disparities

The second is the problem of *nullum crimen* legal disparities in inter-jurisdictional cases (*nullum crimen sine lege* — no crime without law). Recent protocols, including the cybercrime convention and the establishment of multi-agency partnerships and fora (see later), assist in facilitating inter-force cooperation, but they rely upon the offence in question to have similar priority in each jurisdiction. If, for example, a case is clearly a criminal offence for which the investigation carries a strong mandate from the public, such as the investigation of child pornography, then resourcing its investigation is usually fairly unproblematic from a police point of view. However, where there is not such a mandate, resourcing becomes all the more problematic, especially if the deviant behaviour in question is an offence in one jurisdiction and not in another. Of course, there may also be cultural differences in seriousness attached to specific forms of offending. Some offences may fall under civil laws in one jurisdiction and criminal law in another, such as in the case of the theft of trade secrets which is a criminal offence in the USA, but civil in the UK (see Law Commission, 1997).

Jurisdictional Disparities

Faced with a jurisdictional or evidential disparity, police or prosecutors use their resourcefulness to forum-shop (Braithwaite & Drahos, 2000) to increase the prospect of obtaining a conviction (Wall, 2002b). This process was very evident in United States of America v. Robert A. Thomas and Carleen Thomas (1996) where the prosecutors chose Tennessee because they felt a conviction would best be secured. In R v. Arnold and R v. Fellows (1997) the US investigation was passed to the UK police because they were more likely to secure a conviction. However, these were successful examples of cooperation because they were relatively un-problematic in that they concerned extreme pornography. Inter-jurisdictional cooperation is less likely to be successful with the more contentious types of non-routine offending.

Non-routine Activity and Police Culture

The fourth challenge is the *solitus* or routinisation issue which affects the ability of the police to respond to 'non-routine' criminal activity in terms of their possession of relevant skill sets and experience. Since most public policing tends to be based upon local and 'routinised' practices that define occupational cultures, working patterns and ultimately professional policing, investigative difficulties can arise when non-routine events occur (Reiner, 2000; Wall, 1997, p. 223). In this case, non-routine events include those created by the Internet, such as cross-border investigations, or types of deviant behaviour not normally regarded as criminal by police officers.

Routine events are important to the construction of police occupational culture because they generate stories that are told to others which, through 'figurative action,' can eventually structure the way that police officers interpret events (Shearing & Ericson, 1991, p. 481). Police occupational culture is the accumulation of collective **[Page 193]** 'routine' experience of police officers and it is an important component of police work, because with appropriate safeguards in place to prevent corruption and unfairness in the application of law, it enables officers to make sense of the world they have to police and enables them to apply the law (McBarnet, 1979). Since cybercrimes are rather unique events for most officers, the culture does not assist them. In fact, it can lead to the opposite. Police officers, as a number of research findings show, tend to draw upon the ‘cynical’ application of conventional wisdoms (Reiner, 2000)—recall the earlier vignette about the recurring century-old call for more technological resources to fight crime. So, it is understandable that street police officers are unlikely to see the Internet in terms of its potential for the democratisation of knowledge and growth in active citizenship (Walker & Akdeniz, 1998) or the levelling of ethnic, social, or cultural boundaries. Rather, they are more likely to see it as a site characterised by risk (Shearing & Ericson, 1991, p. 500), as a place where criminals, notably paedophiles, Russian gangsters, fraudsters, and other wrongdoers ply their trade. Although great advances in police officer awareness of technology have taken place over the past decade, a cultural dissonance between traditional occupational police culture and the demands created by the Internet pervades which allows the view to persist amongst many officers that ‘cyberspace is like a neighbourhood without a police department’ (Sussman, 1995, p. 59).

Under-reporting

The fifth and most revealing challenge is the under-reporting of cybercrimes to the police. The (assumed) problem of under-reporting to the police has long been argued and the small amount of research into reporting practices, police recording procedures, and prosecutions reveals some startling information shortfalls. The various cybercrime surveys published by Experian, CSI/FBI, the (UK) DTI, and many others all indicate a large volume of victimisations numbering tens of thousands each year. This contrasts sharply with the findings of empirical research conducted for the UK Home Office in 2002 which found that relatively few Internet-related offences were reported to the police (Wall, 2002b, 2007). A detailed study of various police databases in one police force, followed up by interviews with reporting centre staff, revealed that only about 120–150 Internet-related offences per 1 million had been reported to the police during one year and most of these were minor frauds over which no further action was taken. When extrapolated to the national figures (taking into account relative police force sizes), a statistic was obtained of about 2,000 Internet-related offences per year throughout England and Wales being reported by the public to the police (Wall, 2002b, p. 132). Even if these figures were five- or tenfold, there would still be an apparent shortfall in reporting. This apparent under-reporting could be interpreted as evidence of low public expectations of the ability of the local police to resolve Internet-related crimes. Alternatively, in recent years, catalysed by—though not wholly attributable to—the hardened security following the events of 9/11 (Levi & Wall, 2004, p. 196) there now exist a range of national and international police organisations that address cybercrimes.

[Page 194] There are also national intelligence models, for example, in the UK the National Intelligence Model (NIM) (NCIS, 2000, p. 8) which structures the collection of intelligence about all crimes, including low level losses, in order to construct a national or international picture of specific criminal activity. Whether or not they would pick up the very minor de minimis cybercrimes is debateable, but a criminal intelligence model now exists in the UK to link the local with the national and international, whereas five years ago none existed. In addition, many of the larger local police forces/services possess a capability to respond to Internet-related complaints from the public and also have local facilities to investigate computer crimes and conduct the forensic examination of computers. The latter have also been introduced because the investigation of traditional criminal code offences increasingly involves seeking electronic evidence to establish offenders' motives or whereabouts and much of this information is located in computers, Internet traffic data, and also mobile phone records. Finally, there are a growing number of online public portals in both the UK and USA through which to report victimisations.1 In the UK, each of the various local police forces have web sites and facilities that enable the public to contact them about a range of non-emergency minor crimes, Internet related or not. Action Fraud (mentioned earlier) receives all fraud complaints, and the IWF and UK Cert receive reports about offensive content and intrusions respectively. In time, the Action Fraud model may be extended to cover other areas of cybercrime as is the case in the USA. The US Internet Crime Complaint Centre (IC3) was set up as a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA).

One could argue that many of the above reporting facilities are fairly recent interventions and it will take some time for the public to become aware of them and to use them. While there may be some truth to this observation, there also currently exist the many systematic disincentives to reporting cybercrime arising from the challenges that were mentioned earlier, especially de minimis crimes or where an offence is not regarded as a crime. Many victims of cybercrime, be they primary or secondary victims, individuals or organisations, may be unwilling to acknowledge that they have been victimised, or, at least, it may take some time for them to realise it. At a personal level, reluctance to report offences could arise because of embarrassment, ignorance of what to do, or by just simply 'putting it down to experience.' Alternatively, where victimisation has been imputed by a third party upon the basis of an ideological, political, moral, or commercial assessment of risk, the victim or victim group may simply be unaware that they have been victimised or may even believe that they have not been victimised, as is the case in some debates over pornography on the Internet. In the commercial sector, fear of the negative impact of adverse publicity greatly reduces their willingness to report their victimisation to the police, preferring to pursue a 'private' rather than 'public' model of justice which furthers the corporate, rather than the public, interest. One way that law enforcement agencies have addressed the issue of under-reporting by businesses has been through the introduction of confidentiality charters, for example, run by the UK National Hi-tech Crime Unit between 2002 and April 2006, when it was absorbed into the Serious Organised Crime Agency (SOCA). The charter assured businesses that communications would be kept confidential. The story with regard to individuals is somewhat complex. The 2002 study (Wall, 2005a) found that relatively few Internet offences were reported directly to the police as primary responder. Where **[Page 195]** they were related to credit card fraud, complainants were, as a matter of policy, usually referred back to their banks, who were regarded as the actual victims. The banks then tended to 'charge back' the loss to the merchants and retailers.

What we have here is a combination of different factors at play that can explain under-reporting, most of which are clear evidence of the influence of the Peelian paradigm driving public expectations of the police and suggest that cybercrimes simply do not fit into the broader public perception of what the police do. This contrast in perceptions is exacerbated by the reassurance gap between what the police and the media perceive as the problem and the 'signal events' (mentioned earlier) (Innes, 2004, p. 151) that actually shape public perceptions and increase levels of fear of cybercrime. These signal events are in fact often spam-driven small-impact bulk victimisations, or other attempts to victimise online, which increase perceptions of high levels of cyber-.crime and the dangerousness of the Internet. The police gaze, therefore, tends to focus their attention upon crimes committed online where offenders are 'dangerous,' such as paedophiles and also the more notorious hackers. The dangerousness of the former is undisputed; however, it is more contestable with regard to the latter. Indeed there exists some anecdotal evidence of the deliberate demonization of hackers as a 'dangerous other' to play up public fears in order to obtain public funding. Former hacker Bevan (aka Kuji) argues that it is no coincidence 'that requests for increased funding [for an Information Warfare programme] coincide with news headlines of "dangerous hackers" or computer viruses' (Bevan, 2001). Bevan himself was once described in overly dramatic terms by a Pentagon official as 'possibly the single biggest threat to world peace since Adolf Hitler' (Wall, 2001, p. 9; see also Bevan, 2001; Campbell, 1997; Power, 2000, chap. 6).

It is increasingly apparent that the under-reporting of cybercrimes to the police is a reflection of the diverse nature of the provenance of the individual acts of cybercrime as described earlier. Simply put, relatively few Internet-related crimes are reported to the police because most are dealt with and resolved elsewhere by the individual victims or by the panoply of other types of organisations and social groups involved in the regulation of behaviour in cyberspace.

Policing Using Non-traditional Methods (Technological Interventions)

The final challenge for the police is to decide how, and if, to use non-traditional police methods in the policing of cyberspace, particularly those involving powerful technological interventions. The ‘digital’ realism of network technology is that the same characteristics that create new opportunities for crime also create powerful new tools for policing the Internet. As a rule of thumb, the more ‘transformed’ by the Internet a behaviour is, the greater is the potential for that the same technology to be used to police the same behaviour. The globally surveillant and ‘dataveillant’ (Clarke, 1994) panoptic qualities of Internet technology that enable offenders to engage with many victims also facilitate synopticism, thus reversing the direction of the gaze (Mathieson, 1997, p. 215). This asymmetric two-way flow of information provides powerful new tools for policing the Internet: tools that not only enable investigation, but also aid the **[Page 196]** collection of new sources of evidence which can be utilised to secure prosecutions and convictions, and facilitate cybercrime control and prevention.

The root of the ‘disciplinary’ potential of networked technology lies in the routine collection and retention of Internet traffic data that records and traces virtually every Internet transaction and which can subsequently be ‘data-mined’ (Gandy, 2003, p. 26). These ‘… fine-grained distributed systems; through computer chips linked by the Net to every part of social life …’ (Lessig, 1999, p. 1), establish the potential for online monitoring and also for the mining of the various databases of Internet traffic. One of the great public misperceptions about the Internet is the myth of anonymity—in fact networked technology leans in the opposite direction, to the point that we are now in danger of experiencing what has been described as ‘the disappearance of disappearance’ (Haggerty & Ericson, 2000, p. 605). This adds further weight to Ericson and Haggerty’s (1997) arguments that policing of ‘the risk society’ is increasingly information-.driven, and that relations between policing bodies are becoming largely concerned with negotiating the exchange of information (Crawford & Lister, 2004, p. 425; Ericson & Haggerty, 1997). In this case, the exchange of information relates to Internet traffic data which can be used more broadly to gather intelligence about deviant (including terrorist) networks or in relevant cases to establish conclusive evidence of wrongdoing (Walker & Akdeniz, 2003), leading to the emergence of formal and informal relationships that underpin the networks of security.

Crime opportunities can thus be actively designed out of new software products and technologies, and security inserted by the modification of ‘code.’ Katyal (2003) states that cyberspace solutions to cybercrime must try to capture the root benefits of the technology’s potential for natural surveillance, territoriality (stewardship of a virtual area), and capacity for building online communities and protecting targets, without damaging the Internet’s principal design innovation—its openness (Katyal, 2003, p. 2268). They can also be used to generate a range of automated active ‘policing’ tools, such as the ‘honeynets’; fake websites that possess ‘key words’ that offenders search for and have the outward appearance of the ‘real thing’ (Honeynet Project, 2002). Users who access sites containing illegal images wilfully pass through various levels, agreeing at each stage that they are aware of the content and indicating their intent. They eventually find themselves facing a law enforcement message—a ‘gotcha’—a notice that their details will be recorded, and where intent is clear, will become the subject of investigation. Currently, cyberspace solutions are used to exploit the discipline of the panopticon (Foucault, 1983, p. 206), and create a 'chilling effect' on consumers of child pornography, spammers (Sophos, 2004), hackers (Honeynet Project, 2002), and many other forms of undesirable behaviour online. This 'electronic panopticon' (Gordon, 1987, p. 483; Lyon, 1994, p. 69) or 'Super panopticon' (Poster, 2000) also has even broader applications (see Honeynet Project, 2002).

The extreme use of technology takes us to the very edge of what one of the original architects of the Internet has described as 'ubiquitous law enforcement' (Vinge, 2000). So a key consideration for the public police is not only to ensure their own ethical use of these interventions, but also to decide how they keep checks upon appropriate use by others. **[Page 197]**

Renegotiating the Police Role: The Neo-Peelian Agenda

The preceding discussion situates the police as a relatively minor player in the broader network of security that constitutes the policing of cyberspace. By outlining the various challenges faced by local police when policing globalised and transformed offending the preceding analysis suggests that the police are in fact ill-equipped organisationally, occupationally, and culturally. However, that is only part of the story.

As Crawford and Lister (2004) observe, during the past decade or so we have witnessed the increasing pluralisation of policing. The 'public police are becoming part of a more varied and complex assortment of organisations and agencies with different policing functions together with a more diffuse array of processes of control and regulation' (Crawford & Lister, 2004, p. 414). Crawford and Lister argue that while 'much policing is now taking place beyond the auspices' of the public police (2004, p. 426), it would be premature to view the partnerships that form plural policing as facilitating a form of 'networked governance' in the British context: '[t]he reality, at the moment at least, is that crime and disorder partnership remain state-dominated institutions' (ibid.). However, these observations can inform our understanding of the police role in cyberspace because of its networked and nodal architecture. The earlier discussion about situating the police demonstrated a considerable pluralism in the policing of cyberspace that was beyond the auspices of the local public police. However, the twist here is that the increasing role of the police as information brokers (Ericson & Haggerty, 1997) has led to the emergence during the past decade of a new role for the public police in which the original Peelian principles outlined earlier are being promoted within the networks and nodes of multi-agency cross-sector partnerships, fora, and coalitions.

Traditionally, the tensions between the commercial and public sectors arise because the primary function of the former is to police their own 'private' interests. In so doing they pursue a ‘private model’ of justice that does not expose publicly their organisation’s weaknesses and thereby maintains the confidence of the market – it excludes the police (see McKenzie, 2006). The public criminal justice model, on the other hand, is public and the prosecution of offenders is carried out in the public interest and in the public gaze—not a model of criminal justice that many corporate entities want (Wall, 2001, p. 174). Within the public sector are found equally destructive differences between different policing agencies. Not only do ‘turf wars’ take place between national and local police forces for ownership of cases, but there are also distinct contrasts between the organisational and occupational ethos of law enforcement and police agencies that can damage the collective effort. For example, in his analysis of governmental responses to the September 11 terrorist attacks Gorman (2003) argued that the ‘FBI [are] from Mars, and the CIA from Venus … it’s not that [FBI agents and CIA officers] don’t like each other … they’re really different people … they have a hard time communicating.’

The purpose of the multi-agency cross-sector partnerships is, therefore, to build up networked trust relationships through what is effectively a form of ‘peace building’ (Wood, 2004, p. 41) in order to engender a willingness to share information. Although these partnerships tend to be driven by Internet security and law enforcement initiatives, **[Page 198]** it would be wrong simply to assume they are the product of formal policy or that they represent state law enforcement imperatives. The following three North American examples (of similar enterprises) illustrate how the partnerships, fora, and coalitions of interest can vary in terms of their being multi-agency or cross-sector (or both) and also the boundaries between them can overlap. POLCYB (Society for the Policing of Cyberspace) is both multi-agency and cross-sectoral, and exists to share information across networks of trusted individuals and agencies to promote cooperation between sectors, whilst actively inviting international involvement from law enforcement, corporate entities, and interest groups. The High Tech Crime Consortium (HTCC), on the other hand, is more multi-agency than cross-sectoral. Largely Internet-based, it provides a closed forum for law enforcement and security officers—mostly, but not exclusively, from North America—to discuss matters within a secure environment. Whereas POLCYB tends to discuss policy-end issues face to face, HTCC is more about sharing information about problem solving, providing solutions, and identifying emerging problems—mostly on a day-to-day basis. Other fora are much looser coalitions or friendship associations of law enforcement and security experts. The AGORA, for example, encourages cross-sector relationships and provides a face-to-face environment for information exchange between members/associates about Internet-related security matters. In a similar manner to POLCYB, the discussion about information-sharing in AGORA tends to take place at a policy level rather than specifically sharing substantive intelligence data. For example, to develop ideas about security issues and good practice, whilst also identifying, and even agreeing (pre-policy) upon possible acceptable limits for data storage concerning economic transactions and Internet traffic flows. However, the networked trust relationships established within the fora also facilitate the subsequent sharing of intelligence, even criminal intelligence accrued in protecting commercial interests, which includes the reporting of commercial victimisations. Importantly, the personal and occupational interests of the members indicate a substantial crossover of membership between the three organisations.

Alternatively, the partnerships may be driven by specific national policies, or legislation, and be primarily multi-agency in emphasis, drawing together relevant aspects of (governmental and non-governmental) agencies under the auspices of a coordinating body. Appel (2003) provides a very detailed and useful list of the many private–public multi-sector partnerships that operate in the USA with regard to different types of cybercrime associated with the Department of Justice and the Department of Homeland Security. The UK equivalent is the Office of Cyber Security (mentioned earlier) which coordinates key agencies. Within the US context, Appel (2003) argues that public–private collaborations are currently working in many states, counties, regions, and cities, and cites many examples of effective solutions with many different approaches that involve law enforcement, business, private security, government, and academia.

It is difficult to assess how effective these partnerships and fora are in achieving their respective tasks because there are few applicable performance indicators and there exist multiple information flows arising from the networking of nodes of security. However, by creating environments of openness through the establishment of trust, the networks **[Page 199]** created by the partnerships, fora, and coalitions facilitate the flow of essential information to the nodes. At the centre of the establishment of trust appears the ‘police’ bond (this is a hypothesis based upon observations and requires further research). A brief examination of the composition of management boards indicates a mix of law enforcement and other organisations. What comes across very strongly from a cursory examination of their activities is that the police clearly play an important, though not always a leading, role in these multi-agency and cross-sector partnerships. There also remain a number of unanswered questions about the nature of their role because the actual working of the partnership operation tends to lack oversight and transparency—yet discretion of course is one of the main reasons why the partnerships work. Also relatively unknown is the extent to which the non-police contacts in these networks of trust are themselves former police officers. Again, a brief look at the composition of the boards of these agencies and their working parties suggests that the number is fairly high. At the heart of the trust building dynamics appears to be a meeting of minds who possess a similar *weltanshaung*, which is probably the main reason why the networks actually work (this is another research project). Indeed, if this is the case, then the shared occupational values sustain and culturally reproduce the Peelian paradigm so that while the milieu of policing cybercrimes may be different, the perceived public mandate remains much the same.

Cybercrime and the Police–Public Mandate

The future of the public police role in policing the Internet is about more than simply acquiring new expert knowledge and capacity. As is increasingly the case with ‘terrestrial policing’ it is about forging new types of working relationships with other nodes within the networks of Internet security. Relationships that require a range of new transformations to take place in order to enhance the effectiveness and legitimacy of the nodal architecture—a flattening of policing structures, parity of legal definitions across boundaries, broadly accepted frameworks of accountability to the public, shared values, multi-agency and cross-sectoral dialogues, and more. Without these transformations there will always be the danger of a drift away from the ‘disciplinary society’ towards a technology driven ‘control society’ of ‘ubiquitous law enforcement’ and also ‘ubiquitous crime prevention.’ However, this adverse potential is for the time being tempered by the intervention of law, the human condition (through inaccurate data entry), and some theory failure in crime prevention caused by an inadequate conceptualisation and understanding of cybercrime and its associated risks. This will not last indefinitely however.

Some of the contradictions faced by the police have been reconciled by the reconstitution of the Peelian principles of policing and the emergence of a neo-Peelian agenda across a global span. Whilst this resituates the police as an authority within the networks of security it nevertheless demands a range of instrumental and normative responses from them. Whilst one of those responses is to temper the drift towards ubiquity, there is also optimism in the potential for those same technologies also to provide important opportunities for police reform (Chan, Brereton, Legosz, & Doran, **[Page 200]** 2001). The surveillant characteristics that make technology a powerful policing tool, for example, also make it a natural tool for overseeing police practice, and for creating broader organisational and public accountability (see debate in Newburn & Hayman, 2001).

The prognosis is fairly good in one respect: we are gradually learning more about the impact of networked technologies upon criminal behaviour, and therefore learning more effective and acceptable ways of dealing with them. More research about Internet victimisation is being commissioned by funding bodies and the recent inclusion of relevant questions in the Bureau of Justice Statistics’ National Crime Victimization Survey (NCVS) and the British Crime Survey (2003-2004 and again from 2010) will yield useful empirical data about victimisation that will counter some of the misinformation about cybercrime that has accrued during the past decade. Within the UK public policing family, we have in recent years seen the publication of the UK Cyber Crime Strategy, subsequent creation of the Office of Cyber Security, the introduction of the (National) Action Fraud reporting centre and the National Fraud Intelligence Bureau, plus the Police Central E-Crime Unit. When combined with the various regional police units, a corpus of professional policing experience in the field is being established—as is also the case in other jurisdictions. And the laws are still being revised. In the UK, the Computer Misuse Act 1990 has been expanded by s. 35–38 of the Police and Justice Act 2006 to make DDOS attacks and the distribution of hacking tools illegal. In the common law jurisdictions, the laws are, of course, also being clarified by case law.

Another plus is that the actions of police officers are currently framed by legislation and codes of practice, however, it is of concern that many of the other partners in policing the Internet are not, other than within the broader confines of law. Particularly worrying is the lack of checks and balances on the noticeable shift towards the technological determinism of automated policing initiatives, driven largely by the influence of the cyber-security industry in the application of software solutions to cybercrime. There are, for example, a broad range of moral, ethical, and legal concerns about the implications of the high degree of entrapment when employing 'honeypots' and 'honeynets,' not least in the validity and strength of evidence presented to the court— that is if this form of policing is in fact designed to capture offenders or simply deter offending through the technological imposition of panoptic 'discipline' and its 'chilling effect.' Take for example, something as seemingly innocuous as spamming, which is a true cybercrime in more ways than one (Wall, 2005b). Many ISPs have introduced anti-spam software into the delivery process and in so doing contravene the long-standing end-to-end principle of the Internet which is freedom of movement across the network to its nodes while leaving choice and mode of receipt to the end users. No one in their right mind wants to receive spam, except perhaps the spammers, yet there has been little critical discussion about the application of spam filters into the delivery mechanisms. The point here is that true cybercrime is increasingly being regarded as a 'technical problem' and as a consequence, important decisions are being made largely on scientific grounds—simply because a filter can be made possible. In the case of spam there is understandably little objection, but since the technological solutions appear to work, then, why not also apply similar filtering to hash-set analyses of images or to certain words or combinations of words, and filter out everything that is deemed undesirable? The main concern here is that whilst the offending behaviours may be the **[Page 201]** provenance of comparatively few individuals (compared with all Internet users), all users are affected by what effectively become the application of an 'anti-social criminology of everyday life' (Hughes, McLaughlin, & Muncie, 2001). In this matter we may do well here to take heed of the concerns expressed by the Frankfurt School—Horkheimer and Adorno in the *Dialectic of enlightenment*—about using technology to solve problems, because without balances and checks, the technology becomes 'aware of everything but itself and its own blind spots and biases' (Agger, 2004, p. 147).

Conclusions

This paper has explored the challenges that cybercrimes pose for the police and their mandate from the public. It has mapped out the nature of the cybercrime issue, highlighted some of the public misunderstandings about it, before examining the role played by the public police in policing the Internet within the broader architecture of Internet governance. It has illustrated how the Internet and the criminal behaviour it transforms challenge the processes of order maintenance and law enforcement. Not only does Internet-related offending take place within a global context while crime tends to be nationally defined, but the police's public mandate prioritises some offending over others, particularly where there is a perceived dangerous 'other,' as in the production of child pornographic images. Furthermore, policing the Internet is a very complex affair by the very nature of policing and security being networked and nodal. It is also complex because within this framework the public police play only a small part in the overall policing process. Yet the Peelian heritage of the police that has long defined their relationship with the state and the public has caused the police to instinctively assert ownership over the policing function. Cyberspace generates many questions about whether their cultural heritage and traditional constitutional position actually fits them organisationally for a role in policing cyberspace.

In formulating responsive strategies to cybercrime we need realistic expectations of what the police can and cannot do and what are the capacities of the other nodes in the security networks. Accordingly, Internet governance should be configured to assist and strengthen the Internet's natural inclinations to police itself, keeping levels of intervention apposite while installing appropriate structures of accountability. Remember that the same networked technologies that empower criminals also provide a range of highly effective policing tools that are made all the more powerful by the capture of data trails following each Internet transaction and which enable policing to transcend time, place, and space. Indeed, much of the debate in past years about equipping a beleaguered and under-equipped police to cope with technology is rapidly being replaced by increased concerns about over-surveillance through the gradual 'hard-wiring of society' (Levi & Wall, 2004, p. 205). A delicate balance has to be drawn between the need to maintain order and the enforcement of laws in order to provide a balance between the desires of law and the desires of law enforcement. Without such a balance, every infringement of law could easily become automatically identified by using technology and we will begin to descend into a world of strict liability characterised by reverse burden of proof. In **[Page 202]** such a scenario, we are likely to experience an uncontrollable drift from a 'disciplinary society' to a 'control society' where post-event Peelian policing models will be replaced by a 'pre-crime' mentality based upon simulations of crime and behavioural prediction. In such a situation, entire populations could become vulnerable to being evaluated in terms of their individual potential criminality and to technological sorting according to their particular risks to society.

Note: [1] A search using the key words 'reporting crimes to the police online' reveals many police-.driven Internet sites. References

Acknowledgements: This paper draws upon research funded by the Arts and Humanities Research Council (AHRC) Award No. AN10611/APN18143. The author would like to thank Clifford Shearing and Jennifer Wood for their very useful comments on an earlier draft.

Biographical note: 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 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.

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.

References

ACPO (2009) *ACPO e-Crime Strategy, Version 1.0*, Association of Chief Police Officers, <http://www.acpo.police.uk/asp/policies/data/Ecrime%20Strategy%20Website%20Version.pdf>

Adams, J. A. (1996) ‘Controlling cyberspace: applying the computer fraud and abuse act to the internet’, *Santa Clara Computer and High Technology Law Journal*, 12: 403–34.

Agger, B. (2004). *The virtual self: A contemporary sociology*. Oxford: Blackwell.

AIN (2005) ‘ASACP changes name: Association of Sites Advocating Child Protection’, *Adult Industry News*, 2 March, at <www.ainews.com/story/8557/>.

Akdeniz, Y. (1997) ‘The Regulation of Pornography and Child Pornography on the Internet’, *The Journal of Information, Law and Technology* (1), [Online] Available at <http://elj.warwick.ac.uk/jilt/internet/97_1akdz/default.htm>.

Appel, E. (2003, September 23). *US cybercrime: Model solutions.* Paper presented at the Technologies for Public Safety in Critical Incident Response, National Institute of Justice, Office of Science & Technology. Retrieved November 5, 2004, from http://www.nlectc.org/training/nij2003/ Appel.pdf

BBC. (2003, April 30). Spammers and virus writers unite. *BBC News Online*. Retrieved November 5, 2004, from http://news.bbc.co.uk/1/hi/technology/2988209.stm

BBC (2006a) ‘Paedophiles face cancelled cards’, *BBC News Online*, 19 July, at <http://news.bbc.co.uk/1/hi/business/5194150.stm>.

BBC (2006b) ‘Sites selling child porn targeted’, *BBC News Online*, 16 March, at <http://news.bbc.co.uk/1/hi/technology/4812962.stm>.

BBC (2010) ‘Pakistanis divided over internet restrictions’, *BBC News Online*, 20 May, http://news.bbc.co.uk/1/hi/world/south_asia/8693842.stm

Bevan, M. (2001). 4.2.6. Mathew Bevan, infamous hackers and phreaks. Retrieved November 5, 2004, from http://alt.ph.uk.com/node20.html

Braithwaite, J., & Drahos, P. (2000). *Global business regulation*. Cambridge: Cambridge University Press.

Braverman, H. (1976). *Labour and monopoly capital*. New York: Monthly Review Press.

Brenner, S. (2001). Is there such a thing as ‘virtual crime’? *California Criminal Law Review*, 4(1), 11.

Brodeur, J.-P. (1983). High policing and low policing: Remarks about the policing of political activities. *Social Problems*, 30(5), 507–520.

Cabinet Office (2009a*) Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space*, Cm 7642, Cabinet Office, June, <http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf>

Cabinet Office (2009b) *The National Security Strategy of the United Kingdom: Update 2009: Security for the Next Generation*, Cm 7590, Cabinet Office, <http://www.cabinetoffice.gov.uk/media/216734/nss2009v2.pdf>

Caden, M. L. and Lucas, S. E. (1996) ‘Accidents on the information superhighway: on-line liability and regulation’, *Richmond Journal of Law & Technology*, 2: 1.

Campbell, D. (1997, November 27). More naked gun than top gun. *The Guardian (Online)*, 2.

Castells, M. (2000). Materials for an explanatory theory of the network society. *British Journal of Sociology*, 51, 5–24.

Center for Democracy and Technology (1998), *Regardless of Frontiers: Protecting the Human Right to Freedom of Expression on the Global Internet*, Washington: Global Internet Liberty Campaign.

Chan, J., Brereton, D., Legosz, M., & Doran, S. (2001). *E-Policing: The impact of information technology on police practices*. Brisbane: Queensland Criminal Justice Commission.

Clarke, R. (1994). Dataveillance: Delivering 1984. In L. Green & R. Guinery (Eds.), *Framing technology: Society, choice and change* (pp. 117–130). Sydney: Allen & Unwin.

Crawford, A. (2003). Contractual governance of deviant behaviour. *Journal of Law and Society*, 30(4), 479–505.

Crawford, A., & Lister, S. (2004). The patchwork future of reassurance policing in England & Wales: Integrated local security quilts or frayed, fragmented and fragile tangled webs? *Policing: An International Journal of Police Strategies & Management*, 27(3), 413–430.

Critchley, T. A. (1978). *A history of the police in England and Wales*. London: Constable.

[Page 203]

DTI (1996) ‘Ian Taylor Challenges Internet Service Providers: Develop New Software to Come Clean’, *DTI Press Release* P/96/636, 14 August. [Online] Available at <http://www.mit.edu/activities/safe/cases/demon/minister-statement.txt>.

Dupont, B. (2004). Security in the age of networks. *Policing and Society*, 14(1), 76–91.

Edwards, L. and Wealde, C. (eds) (2000) *Law and the Internet:A Framework for Electronic Commerce*, 2nd edn, Oxford: Hart.

Ericson, R., & Haggerty, K. (1997). *Policing the risk society*. Oxford: Oxford University Press.

Foucault, M. (1983). Afterword: The subject and power. In H. Dreyfus & P. Rainbow (Eds.), *Michel Foucault: Beyond structuralism and hermeneutics* (2nd ed., pp. 208–226). Chicago: University of Chicago Press.

Gandy, O. (2003). Data mining and surveillance in the post-9.11 environment. In K. Ball & F. Webster (Eds.), *The intensification of surveillance: Crime terrorism and warfare in the information age* (pp. 26–41). London: Pluto Press.

Gibson, O. (2006) 'Warning to chatroom users after libel award for man labelled a Nazi', *Guardian Online*, 23 March, at <www.guardian.co.uk/law/story/0,,1737445,00.html>

Goodman, M. (1997). Why the police don't care about computer crime. *Harvard Journal of Law and Technology*, 10, 645–694.

Gordon, D. (1987). The electronic panopticon: A case-study of the development of the national criminal records system. *Politics and Society*, 15, 483–511.

Gorman, S. (2003, August 1). FBI, CIA remain worlds apart. *The National Journal*. Retrieved November 5, 2004, from http://198.65.138.161/org/news/2003/030801-fbi-cia01.htm

Haggerty, K., & Ericson, R. (2000). The surveillant assemblage. *British Journal of Sociology*, 51(4), 605–622.

Home Office (2010a) *Cyber Crime Strategy*, Cm 7842, Home Office, March, <http://www.official-documents.gov.uk/document/cm78/7842/7842.pdf>

Home Office (2010b) *Policing in the 21st Century: Reconnecting police and the people*, Cm 7925, Home Office, http://www.homeoffice.gov.uk/publications/consultations/policing-21st-century/policing-21st-full-pdf

Honeynet Project. (2002). *Know your enemy: Revealing the security tools, tactics, and motives of the Blackhat Community*. Harlow, Essex: Addison-Wesley.

Hughes, G., McLaughlin, E., & Muncie, J. (2001). Teetering on the edge: The futures of crime control and community safety. In G. Hughes, E. McLaughlin, & J. Muncie (Eds.), *Crime prevention and community safety: Future directions*. London: Sage.

Innes, M. (2004). Reinventing tradition?: Reassurance, neighbourhood security and policing. *Criminal Justice*, 4(2), 151–171.

Johnston, L., & Shearing, C. (2003). *Governing security. Explorations in policing and justice*. London: Routledge.

Katyal, N. K. (2003). Digital architecture as crime control. *Yale Law Journal*, 112, 2261–2289.

Keith-Smith v Williams, Court of Appeal - Queen's Bench Division, March 21, 2006, [2006] *EWHC* 860 (QB)

Law Commission. (1997). *Legislating the criminal code: Misuse of trade secrets*. Consultation Paper 150. Retrieved November 5, 2004, from http://www.lawcom.gov.uk/library/lccp150/ summary.htm

Leong, G. (1998) 'Computer child pornography – the liability of distributors?', special edition: 'Crime, Criminal Justice, and the Internet', *Criminal Law Review* (December) 19–28.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Levi, M., & Wall, D. S. (2004). Technologies, security and privacy in the post-9/11 European information society. *Journal of Law and Society*, 312, 194–220.

Leyden, J. (2006) 'Online fraudsters love webmail – true: easier to block accounts linked to spamming than fraud', *The Register*, 19 July, at <www.theregister.co.uk/2006/07/19/online_fraud_survey/>.

Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. Minneapolis: University of Minnesota Press.

Manning, P. K. (1998). The police: Mandate, strategies, and appearances. In P. Manning & J. Van Maanen (Eds.), *Policing: A view from the street* (pp. 7–32). New York: Random House.

Mathieson, T. (1997). The viewer society: Foucault’s Panopticon revisited. *Theoretical Criminology*, 1, 215–234.

McBarnet, D. (1979). Arrest: The legal context of policing. In S. Holdaway (Ed.), *The British police*. London: Arnold.

McKenzie, S. (2006) *Partnership policing of electronic crime: an evaluation of public and private police investigative relationships*, PhD thesis, University of Melbourne.

Miller, P., & Rose, N. (1990). Governing economic life. *Economy and Society*, 19, 1–31.

NFA (2009) *The National Fraud Strategy: A new approach to combating fraud*, National Fraud Authority, Attorney General’s Office, <http://www.attorneygeneral.gov.uk/NewsCentre/News/Documents/NFSA_STRATEGY_AW_Web%5B1%5D.pdf>

NCIS. (2000). *The National Intelligence Model.* London: NCIS.

Newburn, T., & Hayman, S. (2001). *Policing, CCTV and social control: Police surveillance of suspects in custody*. Cullompton: Willan.

Pease, K. (2001). Crime futures and foresight. In D. S. Wall (Ed.), *Crime and the Internet* (pp. 18–28). London: Routledge.

Poster, M. (2000). *Second media age*. Cambridge: Polity Press.

Power, R. (2000). *Tangled web: Tales of digital crime from the shadows of cyberspace*. Indianapolis: Que.

Reiner, R. (2000). *The politics of the police (3rd ed.)*. Oxford: Oxford University Press.

Rowland, D. and Macdonald, E. (1997) *Information Technology Law,* London: Cavendish.Rowland

Savona, E., & Mignone, M. (2004). The fox and the hunters: How IC technologies change the crime race. *European Journal on Criminal Policy and Research*, 10(1), 3–26.

Shearing, C. (2004). Thoughts on sovereignty. *Policing and Society*, 14(1), 5–12.

[Page 204]

Shearing, C., & Ericson, R. (1991). Culture as figurative action. *British Journal of Sociology*, 42(4), 481–506.

Sheptycki, J. E. (2000). Introduction. In J. E. Sheptycki (Ed.), *Issues in transnational policing* (pp. 1–20). London: Routledge.

Sheptycki, J. (2002) *In Search of Transnational Policing :Towards a Sociology of Global Policing*, Aldershot: Ashgate.

Smith, R. G., Grabosky, P. N., & Urbas, G. (2004). *Cyber criminals on trial*. Cambridge: Cambridge University Press.

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

Sophos. (2004). The threat of the spam economy. *SysAdmin Magazine* (Spam Supplement). Retrieved November 5, 2004, from http://www.sysadminmag.com/articles/2004/0413/

Sturcke, J. (2006) ‘Expert warns of more chatroom libel awards’, *Guardian Online*, 22 March, at <www.guardian.co.uk/uk_news/story/0,,1737000,00.html>.

Sussman, V. (1995, January 23). Policing cyberspace. *U.S. News & World Report*, 54–61.

Toyne, S. (2003, October 24). Scam targets NatWest customers. *BBC News Online*. Retrieved November 5, 2004, from http://news.bbc.co.uk/1/hi/business/3211635.stm

Uhlig, R. (1996a) ‘Hunt is on for Internet dealer in child porn’, *Electronic Telegraph*, issue 518, 23 October, at <www.telegraph.co.uk/htmlContent.jhtml?html_/archive/1996/10/23/nporn23.html>

Uhlig, R. (1996b) ‘Minister’s warning over Internet porn,’ *The Daily Telegraph,* 18 August.

Vincent-Jones, P. (2000). Contractual governance: Institutional and organisational analysis. *Oxford Journal of Legal Studies*, 20, 317–351.

Vinge, V. (2000). The Digital Gaia: As computing power accelerates, the network knows all—and it’s everywhere. *Wired*, 8(1). Retrieved November 5, 2004, from http://www.wired.com/wired/ archive/8.01/forward.html

Walden, I. (2003). Computer crime. In C. Reed & J. Angel (Eds.), *Computer law* (pp. 295–329). Oxford: Oxford University Press.

Walker, C., & Akdeniz, Y. (1998). The governance of the Internet in Europe with special reference to illegal and harmful content [Special issue: Crime, criminal justice and the Internet]. *Criminal Law Review*, 5–18.

Walker, C., & Akdeniz, Y. (2003). Anti-terrorism laws and data retention: War is over? *Northern Ireland Legal Quarterly*, 50(2), 159–182.

Walker, C. P., Wall. D. S. and Akdeniz, Y. (2000) ‘The Internet, law and society’, in Y. Akdeniz, C. P. Walker and D. S. Wall (eds), *The Internet,Law and Society*, London: Longman, 3–24.

Wall, D. S. (1997). Policing the virtual community: The internet, cyber-crimes and the policing of cyberspace. In P. Francis, P. Davies, & V. Jupp (Eds.), *Policing futures* (pp. 208–236). London: Macmillan.

Wall, D. S. (1998). *The Chief Constables of England and Wales: The socio-legal history of a criminal justice elite*. Aldershot: Dartmouth.

Wall, D.S. (1999) “Cybercrimes: New wine, no bottles?”, reprinted at pp. 3-38 in D.S. Wall, (ed) (2003) *Cyberspace Crime*, Aldershot: Dartmouth/ Ashgate.

Wall, D. S. (2001). Maintaining order and law on the internet. In D. S. Wall (Ed.), *Crime and the internet* (pp. 167–183). London: Routledge.

Wall, D. S. (2002a). Insecurity and the policing of cyberspace. In A. Crawford (Ed.), *Crime and insecurity* (pp. 186–209). Cullompton: Willan.

Wall, D. S. (2002b, March). *DOT.CONS: Internet related frauds and deceptions upon individuals within the UK*. Final Report to the Home Office.

Wall, D. S. (2005a). The Internet as a conduit for criminals. In A. Pattavina (Ed.), *Information technology and the criminal justice system* (pp. 77–98). Thousand Oaks, CA: Sage.

Wall, D. S. (2005b). Digital realism and the governance of spam as cybercrime. *European Journal on Criminal Policy and Research*, 10(4), 309–335.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity.

Wall, D.S. (2010) ‘The UK tackles crimes against the machine’, *Jane’s Intelligence Weekly*, 2(15) 28 April, 13.

Wired (2003) ‘Verizon must reveal song swappers’, *Wired News*, 24 April, at <www.wired.com/news/digiwood/0,1412,58620,00.html>.

Wood, J. (2004). Cultural change in the governance of security. *Policing and Society*, 14(1), 31–48.

Cases

Godfrey v. Demon Internet Ltd. (1999) 4 All E.R. 342.
Keith-Smith v.Williams (2006) EWHC 860.

League Against Racism and Anti-Semitism (LICRA) and The Union of French Jewish Students (UEJF) v.Yahoo Inc. and Yahoo France (2000), Interim Court Order, 20 November, The County Court of Paris, No. RG: 00/05308.

In re Verizon Internet Services, Inc. (2003); at <http://news.findlaw.com/hdocs/docs/verizon/inreverizon12103opn.pdf>

People v. Somm (1998), Amtsgericht Munich [Local Court], File No. 8340 Ds 465 Js 173158/95 (F.R.G.) (May), later overturned on appeal (173158/99).

R v. Fellows; R v. Arnold, 2 All ER 548 (1997). United States of America v. Robert A. Thomas and Carleen Thomas, 74 F.3d 701 (6th Cir. 1996).

Internet Sources

Action Fraud <http://www.actionfraud.org.uk/>
Consumer Direct <http://www.consumerdirect.gov.uk/>
CyberAngels <http://www.cyberangels.org/<
High Tech Crime Consortium <http://www.hightechcrimecops.org/>

[Page 205]

Internet Crime Complaint Center (IC3) [formerly the Internet Fraud Complaint Centre] <http://www.ic3.gov/default.aspx>

Centre for the Protection of National Infrastructure (CPNI) [formerly the National Infrastructure Security Co-ordination Centre or NISCC] <http://www.cpni.gov.uk/>

National Crime Victimization Survey (USA) <http://www.ojp.usdoj.gov/bjs/cvict.htm>

National Policing Improvement Agency [replaced Police Information Technology] Organisation PITO] <http://www.npia.police.uk/>

Police.UK Online Services <http://www.police.uk/services> [Is now defunct but the www page still exists]

Society for the Policing of Cyberspace <http://www.polcyb.org>

The Internet Watch Foundation <http://www.iwf.org.uk/>