Situating the Police in Cyberspace

David Wall argues that the police are not the only agency responsible for controlling cybercrime.

The general public would be forgiven for their inability to square the apparent 'cybercrime' wave portrayed by the news media with the relatively few arrests and prosecutions of so-called cybercriminals (Smith *et. al*, 2004). Particularly striking is that during the first decade of the Computer Misuse Act 1990 (the principle UK computer misuse law) there were only about 100 or so prosecutions and even fewer convictions (Hansard 26/3/02, Col. WA35). Is this shortfall *prima facie* evidence that traditional local police forces working within tightly prescribed budgetary constraints simply cannot cope with demands to investigate the crimes arising from globalised electronic networks? Network technologies appear to leave the police much disadvantaged by enabling individual criminals to control entire criminal processes and reach their victims across infinite spans of time and space.

In the age of the sound-bite, the simple causality of this explanation is appealing – just blame it on conservative police thinking. After all, can we realistically expect an organisation designed to counter the problems of urban migration caused by antique production technology to respond to an entirely new set of virtual policing problems? But counter to this 'conservatism' thesis has been a notable rise in government police investment in recent years and the formation of new local and national police technology crime units. In the UK, the subsequent successes of the National Hi-Tech Crime Unit, Metropolitan Police and provincial police forces (see Sommer, 2004) have been highly publicised as have the successes of similar units in the USA. So, instead of looking for the simple causal explanation, perhaps we should situate and then re-examine our expectations of the police role in this field.

An analysis of cybercrimes (Wall, 2005a & b; and elsewhere in this issue) illustrates that not only do they differ from the regular police crime diet, but they are also quite distinctive in their tendency to be small-impact, multiple-victimisations occurring across a global span. Where once a robber might have had to put together a team of individuals comprising a range of criminal skill sets in order to steal £1million from a bank, new technologies are powerful enough (in principle at least) to enable one individual to rob one million people of £1 each in a number of different ways and across a global span. New networked technologies enable criminal activity to be organised in distinctly different ways to 'traditional' crime (Wall, 2005a; 80).

Combine these changes in criminal organisation with the globalised and cross-jurisdictional span of most cybercrimes and it becomes clear that they fall outside the traditional localised, even national, operational purview of police. Perhaps more importantly, considerable obstacles are thrown up regarding the allocation of police resources for investigation and/or the decision to prosecute. Either it is not deemed to be in the public interest to investigate them individually because of the *de minimis* rule (they are too minor in nature), or they are simply too complex technically or jurisdictionally to make the likelihood of conviction likely. Spams are a very good example in question.

What emerges from this brief analysis is that the police only play a very small part in the overall policing of cyberspace. Although we are now in the 21st Century, the police still continue to work much along the lines of their 170 year old Peelian public mandate to regulate the 'dangerous classes'. Hence the (understandable) focus upon policing paedophiles, child pornographers, fraudsters and those who threaten the infrastructure (including terrorists). However, this is not to say that cyberspace goes unpoliced, as Robert Reiner has observed more generally: "not all policing lies in the police". Nor is it the case that police activity is either inefficient or ineffective. Rather the police role has to be understood within the following broader and largely informal networked and nodal architecture of internet policing, which not only enforces laws, but also maintains order in very different ways (Wall, 2005b).

- *Internet users and user groups* exert a very potent influence upon online behaviour, through moral censure, although cases of more extreme behaviour may be reported to relevant authorities.

- *Network infrastructure providers* exert influence over online behaviour through the terms and conditions of their contracts with clients. They themselves are also subject to the terms and conditions laid down in their contracts with the telecommunications providers who host their services.

- *Corporate security organisations* preserve their corporate interests through contractual terms and conditions; but also use the threat of removal of privileges or the threat of private (or criminal) prosecution.

- *Non-governmental, non-police organisations*, such as the Internet Watch Foundation (www.iwf.org.uk), act as gatekeepers by accepting and processing reports of offending then passing them on (mostly related to obscenities), but IWF also contributes more generally towards (cyber)crime prevention and public awareness.

- *Governmental non-police organisations* use a combination of rules, charges, fines and the threat of prosecution. Not normally perceived as 'police', they include agencies such as Customs, the Postal Service, and Trading Standards etc. But a higher tier of agencies also oversees and enforces national internet infrastructure protection policies (NISCC, DTI etc).

- *Public police organisations*, as stated earlier, play a relatively small but nevertheless significant role in imposing criminal sanctions upon wrongdoers. Whilst located within nation states, the public police are nevertheless joined by a tier of transnational policing organisations, such as Europol and Interpol, whose membership requires such formal status.

Joining up these 'tiers' are a range of initiatives designed to make their governance function more effective: international coalitions of organisations; multi-agency, cross-sectoral partnerships and coalitions and also international co-ordination policies, such as the COE's Cybercrime Convention. Active public police participation in these partnerships and coalitions performs a number of functions. It enables 'the police' to extend their own reach at a symbolic and normative level by reconstituting the fundamental Peelian principles of policing across a global span and thereby resolve some of the contradictions that they face.

At a more practical level it enables them to perform their emerging function as information brokers (see Haggerty *et al.* in this issue), the information in this sense mainly relating to internet traffic data and its evidential and intelligence value.

Whilst this neo-Peelian agenda enables them to resituate the public police as an authority within the broader networks of security, it nevertheless institutes a range of instrumental and normative challenges. One of the key challenges is to temper the private sector's (presently) unreflective drift towards the routine use of the surveillant technologies to strengthen security by catching offenders and preventing crime by exclusion. Unless checked, the 'ubiquitous policing' (Wall, 2005b) that follows this 'hard wiring of society' (Kevin Haggerty) could contribute to the destruction of the democratic liberal values which currently bind most societies. For the time being this adverse potential is tempered by the intervention of constitutional law, the imperfect human condition (e.g. through inaccurate data entry), and some theory failure in crime prevention caused by an inadequate conceptualisation and understanding of cybercrime and its associated risks - but not forever. However, if this tendency is contained within a supportive socio-legal context, for there is still time, then those same technologies could – optimistically – assist the process of police reform (Chan *et al*, 2001). This is because the same surveillant characteristics that make network technology a powerful policing tool also make it a natural tool for overseeing police practice and also for creating broader organisational and public accountability (see debate in Newburn and Hayman, 2001).

In formulating responsive strategies to cybercrime we need to have realistic expectations of what the police can and cannot do, accepting in the process that not all policing lies in the police, but in other structures of order. Furthermore, the future of the public police role in policing the internet is clearly 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 the other nodes within the many networks of security (Crawford and Lister, 2004; also Shearing, 2004). These relationships require a range of transformations 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 sector dialogues and more (Wall, 2005b). Without these transformations there will always remain the danger that technological ubiquity will displace the values that we hold dear.

■

***David Wall** is Professor of Criminal Justice and Information Technology and Director of the Centre of Criminal Justice Studies at the University of Leeds.*

References

Chan, J., Brereton, D., Legosz, M. and Doran, S. (2001) *E-Policing: The Impact of Information Technology on Police Practices*, Brisbane: Queensland Criminal Justice Commission.

Crawford, A. and 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.

Newburn, T. and Hayman, S. (2001) *Policing, CCTV and Social Control: Police Surveillance of Suspects in Custody*, Cullompton: Willan Publishing.

Shearing, C. (2004) 'Thoughts on Sovereignty', *Policing and Society*, 14(1): 5-12.

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

Smith, R.G., Grabosky, P.N. and Urbas, G. (2004) *Cyber Criminals on Trial*. Cambridge: Cambridge University Press.

Wall, D.S. (2005a) 'The Internet as a Conduit for Criminals', pp. 77-98 in A. Pattavina, *Information Technology and the Criminal Justice System*, Thousand Oaks, CA: Sage

Wall, D.S. (2005b) 'Policing Cybercrime: Situating the public police in networks of security in cyberspace', *Police Practice and Research: An International Journal* (forthcoming).

THE POLICE RECORDING OF COMPUTER CRIME (Home Office)

From Hyde-Bales, K., Morris, S. and Charlton, A. (2004) 'The police recording of computer crime', Home Office Development and Practice Report 40. London: Home Office. www.homeoffice.gov.uk/rds/pdfs04/dpr40.pdf

The research aimed to find out if it was possible to identify computer crime from force information systems through the use of suitable markers and/or the use of free text searches. To do this the survey examined how forces are recording and allocating computer crime incidents.

Findings

Two hundred and twenty-four questionnaires were completed out of a possible 258. Twenty-two forces completed all six questionnaires, with a minimum of three questionnaires received from every force.

Recording computer crime (recommendations)

- Forces should implement a computer crime marker on both their crime recording and force intelligence systems (and consider a similar implementation to incident systems also) to enable the identification and subsequent analysis of computer crime incidents, crimes and offenders.
- Such a marker should be accompanied by documented guidance on its application.
- Individuals, who undertake analysis of incident, crime and intelligence data would benefit from receiving specific training on the key aspects of computer crime.