Cybercrimes and Criminal Justice

David Wall seeks to clarify what is meant by 'cybercrime' and ask if new developments in law are necessary to deal with new types of crime.

A decade or so after the term 'cybercrime' was coined it continues to fill precious column inches with tales of the 'Virtual Apocalypse'. However, whilst there is a broadly common agreement that cybercrimes exist, there is little consensus as to what they are. Upon further reflection, many of the concerns about cybercrimes are the product of media sensitisation and do not necessarily have specific reference points in criminal law. Indeed, the term is frequently used to describe harmful behaviours for which the remedy lies in civil law or elsewhere. Consequently, 'cybercrime' is a fairly meaningless descriptor other than it signifies the occurrence of a harmful activity that is somehow related to a networked computer (NCIS, 1999). Yet it has entered the vernacular to symbolise insecurity within cyberspace and has acquired considerable linguistic agency - to the point that cybercrimes are now widely acknowledged as a danger to society and therefore require a criminal justice response (see further Wall, 2001).

Types of cybercrime

Much of the contemporary debate about cybercrime, as expressed in discussion and literature, describes with great alacrity and considerable detail various types of cybercrimes. Usually these are the more sensational crimes -- sex crimes, massive frauds, ingenious hackings, cunning crackings etc. The same sources also analyse the various policy debates which shape and form societal and governmental responses. Yet, the contemporary literature has three key failings that need to be addressed.

First, it rarely disaggregates between harmful behaviours that already exist and those which are entirely new. At one end of the spectrum lie those behaviours which are often called cybercrimes, but are in fact 'traditional' crimes in the commission of which the Internet was used, typically as a method of communication. Towards the middle of the spectrum are 'hybrid' cybercrimes that are 'traditional' crimes for which entirely new opportunities have emerged. At the other end are the 'true' cybercrimes which are the product of opportunities that are created entirely by the Internet and can be perpetrated solely within cyberspace. It is important to draw these distinctions because understandings of 'traditional' crimes and 'hybrid' cybercrimes can be informed by existing literature, law and practice, whereas the 'true' cybercrimes are more likely to be the result of globalised activity and therefore require new bodies of knowledge and experience to be sought. They also suggest that very different responsive and regulative strategies are required.

At the other end are the 'true' cybercrimes which are the product of opportunities that are created entirely by the Internet and can be perpetrated solely within cyberspace.

Second, these same debates over cybercrime rarely draw lines between the substantially different types of harmful behaviour. Elsewhere, I have reduced these to four main groups (Wall, 2001). Cyber-trespass is the unauthorised access of the boundaries of computer systems into spaces where rights of ownership or title have already been established. Cyber-pornography/obscenity is the trading of sexually expressive materials within cyberspace. Cyber-deceptions and thefts are the different types of acquisitive harm that can take place within cyberspace. Cyber-violence is the violent impact of the actions of one individual or social or political grouping upon another. Responding to each of these different types of criminal behaviour will require different strategic and tactical responses from the law, investigators, prosecutors and defence.

Third, the current literature and research on cybercrimes lacks an empirically informed sense of proportion in terms of the occurrence of the various types of harmful behaviour involved – rarely occurring behaviours tend to carry the same gravity as those which are more prevalent. The same literature also provides little indication as to the scale of the activity, whether it be local, national, international or global.

Drawing the above distinctions will help to facilitate our understanding and knowledge of harmful behaviours on the Internet. This is important for two reasons. Firstly, key players in the criminal justice system currently lack the analytical tools for cybercrime that are used for other types of crime to generate 'reliable data' in the form of statistics, identifiable victims groups, offender profiles, known jurisdictions, shared public values and definitions of crime. This type of data is needed to enable them to make, and introduce, informed policy and practice (Wall, 2002, forthcoming). Secondly, an improved knowledge of cybercrimes (and criminals) will help to break the cycle of self-perpetuated myths that currently make them so media-worthy. These myths shape opinion by generating public concerns about 'electronic Pearl Harbors' (sudden large scale attacks) or 'cyber-tsunamis' (unintended catastrophes) and seek to assault the economic infrastructure (Wall, 2001, Taylor, 2001). Myths also confuse risk assessments with reality and exaggerate the fears of those who do not tend to use the Internet, and whose concerns are subsequently "exploited both by politicians and by the mass media" (Walker and Akdeniz, 1998).

Clearly, the above matrix of distinctions suggests that the 'reliable data' could actually be generated with regard to the 'traditional', and possibly the 'hybrid' cybercrimes described earlier. But it also suggests that the likelihood of generating 'reliable' data about 'true' cybercrimes diminishes rapidly as you move away from the 'traditional' crime model because of the increasingly hidden nature of the harmful activity, also because of the fact that the remedies may lie outside the criminal justice system and/or because of the globalised nature of the problem. Cybercrimes share these characteristics with white-collar crimes.

Cybercrime as a global phenomenon

Maureen Cain (2002) has argued that globalisation, as a concept and a social process, configures, and reconfigures, 'relationships between multiple entities – from individuals to international agencies – which are widely distributed in space'. These relationships, she observes, are neither innocent nor power free. So, very simple economic drivers can generate criminal opportunities, for example, the prohibition or excessive taxation of goods in one jurisdiction immediately creates criminal business opportunities elsewhere and the Internet provides the global links through which those opportunities can be exploited.

But crime is not just simply about opportunity, it is also about combining imagination, abilities and desires. Add the Internet, a global communication media, to this combination and the result is potent, particularly as value in cyberspace is mainly attached to ideas rather than things. The focus of 'true' cybercrime is therefore upon the ideas to which the values are attached. Therefore cybercrimes are activities that include the illegal acquisition, manipulation or destruction of intellectual property (copyrighted, trademarked or patented materials, information, data). They also include new aspects of pornography, information warfare, economic espionage and many other activities. The 'true' cybercrime is a global phenomenon which transcends cultural as well as geographical boundaries, and it can be committed anywhere on the Internet, from anywhere, at any time.

At some point, however, the 'local' enters into the equation via the offenders' input (commission) and/or output (gains), the victim and the investigation. But, when formulating a criminal justice response, it is important to note that this is a different 'local' to that found in the analysis of 'traditional' crime because the internal linkage between the local and the global has changed. Cain (2002), draws upon Bauman's (1998) conceptualisation of 'glocalisation' in order to explain that "the intrinsic linkages between these global and local processes" are not "trans, or inter national", rather they are 'glocalised'.

Although concepts like 'globalisation' and 'glocalisation' are highly contestable, they nevertheless flag up the directions of future discourses. One certainty is that cybercrimes will become increasingly more global. Visible examples of this trend are already being found in the criminal opportunities that are emerging from the convergence of information technologies, for example, the convergence of communications technologies with linked databases that contain very private information about ourselves (eg., health and finance), our patterns of consumption and our lifestyles. Alternatively the databases might be intrinsic to a corporate operation. Without a research-led debate about the various levels, types and impacts of cybercrimes then criminal justice systems will be unable to make strategic decisions about whether or not to, how to, or when to engage with new forms of criminality. ■

***David S. Wall** is Director of the Centre for Criminal Justice Studies, University of Leeds.*

References:

Bauman, Z. (1998), *Globalization: The Human Consequences.* Cambridge: Polity.

Cain, M. (2002), 'International Crime and Globalisation', *Criminal Justice Matters*, in this issue.

National Crime Intelligence Service (1999), Project Trawler: *Crime on the Information Highways*, London: NCIS.

Taylor, P. (2001), 'Hacktivism: in search of lost ethics?', in D.S. Wall (ed.) *Crime and the Internet*, London: Routledge.

Walker, C. P. and Akdeniz, Y. A. (1998), 'The Governance of the Internet in Europe with Special Reference to Illegal and Harmful Content', in C. P. Walker (ed) 'Crime, Criminal Justice and the Internet', special issue of the *Criminal Law Review.*

Wall, D. S. (2001), 'CyberCrimes and the Internet', in D. S. Wall (ed.) *Crime and the Internet*, London: Routledge.

Wall, D. S. (2002 - forthcoming), 'Insecurity and the Policing of Cyberspace' in A. Crawford (ed) (2002 - forthcoming) *Crime and Insecurity*, Cullompton: Willan Publishing.