What are Cybercrimes?

David Wall describes the importance of accurate new terminology for a new type of crime.

'Cyber-terrorism', 'information warfare', 'phishing', 'spams', 'denial of service attacks', 'hacktivism', 'hate crime', 'identity thefts', 'online gambling', plus the criminal exploitation of a new generation of pornographic peccadilloes, comprise the new language which describes the criminal and harmful behaviours that are conspiring to degrade the overall quality of life online and beyond. In so doing they pose significant threats to public safety and are tempering significantly broader commercial and governmental ambitions to develop the information society.

Particularly confusing is the tendency to regard almost any offence that involves a computer as a 'cybercrime'.

Although 'cybercrime' is a vastly topical and newsworthy subject, little information is known about it other than through news reportage. Although few would deny that cybercrimes exist, there is no overall consensus as to what they actually are. Without reliable sources of knowledge, misinformation cannot be countered, misunderstanding is perpetuated and a firm platform for responsive criminal justice policy is lacking. Particularly confusing is the tendency to regard almost any offence that involves a computer as a 'cybercrime'. This is not helped by the series of contradictory messages in media reportage, which demonise the internet as a place where youngsters are groomed by paedophiles and upstanding citizens robbed of their identity, while simultaneously depicting it as a wonderland of personal, commercial and governmental opportunity. Furthermore, this malaise is not assisted by various academic and government endeavours to alternatively conceptualise similar issues either as 'virtual crime' (Brenner, 2001), 'cybercrime' (Wall, 2005a), 'net-crime' (Morris, 2004), 'hi-tech crime' (NCIS, 2002:s. 8) or 'computer crime' (Walden, 2003), often using different yardsticks.

Whatever its merits and demerits, the term 'cybercrime' has entered the public parlance and we are more or less stuck with it. However, it is argued here that the term has a greater meaning if it is understood in terms of the transformations of criminal or harmful acts by networked computing technologies rather than the acts themselves (see further Wall, 2005a). So, by applying a simple 'elimination test' (in other words, thinking about what happens if the internet is removed from the equation) three different types of 'transformed' cyber-criminal opportunity emerge as points on a spectrum that accommodates many of the previous attempts at conceptualisation.

At the near end lie behaviours often called cybercrimes that are in fact 'traditional' crimes in which a computer has been used – usually as a method of networked communication or source of information to assist with the organisation of a crime (e.g., to find information about potential victims or even about how to harm, defraud, embarrass someone, or alternatively by paedophile groups). Remove the internet and the criminal behaviour persists because the offenders will simply revert to other forms of easily available communication.

Towards the middle are to be found the 'hybrid' cybercrimes – 'traditional' crimes for which network technology has created entirely new global opportunities (e.g., global frauds and deceptions, also the global trade in pornographic materials including child pornography). Take away the internet in this case and the behaviour continues by other means, but not with such great prevalence or across such a wide span of jurisdictions and cultures.

At the far end, however, lie the 'true' cybercrimes which are solely the product of opportunities created by the Internet and which can only be perpetrated within cyberspace (they include intellectual property thefts, spams, phishing and other forms of 'social engineering'). Take away the internet and they vanish – the problem goes away.

These distinctions are important because the first two tend already to be the subject of existing laws and existing professional experience can be applied to law enforcement practice. Any legal problems arising therefore tend to relate more to legal procedures than substantive law. The final group, however, are solely the product of the internet and methods of resolving the problems that they give rise to may not be so easily found.

It is also important of course to look at common features in the substantive behaviours. In this way they can be linked to existing bodies of law and associated experience in the justice processes (Wall, 2005a):

- *Computer integrity crimes* that assault the integrity of network access mechanisms (hacking and cracking, cyber-vandalism, spying, denial of service, viruses etc.).
- *Computer related crimes* use networked computers to engage with victims with the intention of dishonestly acquiring cash, goods or services ('phishing', advanced fee frauds etc.).
- *Computer content crimes* relate to the illegal content on networked computer systems and include the trade and distribution of pornographic materials as well as the dissemination of hate crime materials.

Despite the existence of applicable bodies of law backed up by international harmonisation and police co-ordination treaties such as the Council of Europe's *Convention on Cybercrimes* (ETS. 185) the specific characteristics of cybercrimes often conspire to impede the traditional investigative process. Particularly significant is the observation that the dangers posed by them are not always immediately evident to potential (or actual) victims. Either they are not regarded as serious, or they are genuinely not serious, but possess a latent danger in their being precursors to more serious crimes.

Each of the substantive criminal behaviours highlighted earlier illustrate this point. 'Computer integrity' cybercrimes, for example, pave the way for more serious offending - identity theft from computers only becomes serious when the information

is used against the owner. Similarly, hackers or crackers may use Trojan viruses to install 'back doors' which are later used to facilitate other crimes, possibly by spammers who have bought lists of the infected addresses (Wall, 2005b). 'Computer-related' cybercrimes, such as internet scams perpetrated by fraudsters in collusion with spammers, tend to be relatively minor in individual outcome, but serious by nature of their volume. 'Computer content' crimes, on the other hand, mainly tend to be informational and while they are often extremely personal and/or politically offensive, they are not necessarily illegal. But they could contribute subsequently to the incitement of violence or prejudicial actions against others.

This brief deconstruction illustrates that not only does the term 'cybercrime' already have a general linguistic agency, but if understood in terms of the mediating and transformative impacts of networked technology upon the criminal and harmful behaviours it describes, then it can also situate and give relative meaning to the findings of other research done within the area of networked computer technology. Looking to the future, such conceptual preparation is important as we are gradually learning more about the impact that networked technologies are having on criminal behaviour. To assist us in this task more research is being commissioned by the funding councils and government bodies (see Morris, 2004) and the recent inclusion of questions about internet victimisation in the British Crime Survey will yield useful empirical data that will challenge some of the misinformation that has accrued during the past decade. Furthermore, there are proposals to introduce the routine recording of computer crime (Hyde-Bales, *et al.* 2004). Improved conceptual clarity combined with improved quality of data will further assist the analysis. ■

***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

Brenner, S. (2001) 'Is There Such a Thing as "Virtual Crime"?', *California Criminal Law Review*, 4(1): 11.

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.

Morris, S. (2004) *The future of netcrime now: Part 1 – threats and challenges*, Home Office Online Report 62/04 http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr6204.pdf

NCIS (2002) *United Kingdom Threat Assessment of Serious and Organised Crime 2002*, London: NCIS, http://www.ncis.co.uk/ukta/2002/threat08.asp

Walden, I. (2003) 'Computer Crime', in C. Reed and J. Angel (eds) *Computer Law*, Oxford: Oxford University Press.

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

Wall, D.S. (2005b) 'The Email of the Species is More Deadlier than the Mail: Digital Realism and the Governance of Spam as Cybercrime', *European Journal on Criminal Policy and Research* (forthcoming).

THE FUTURE OF NETCRIME NOW (Home Office)

A new two-part report from the Home Office, *The future of netcrime now: Part 1 – threats and challenges*, and *The future of netcrime now: Part 2 – responses* sets out current descriptions of different types of internet crime followed by recommendations to tackle it. The following are some self-descriptive extracts from the report.

"This research coincides with the publishing of e-crime and information assurance initiatives by the Home Office (to which it has contributed) and the Central Sponsor for Information Assurance. In looking to the future, other relevant programmes include the Department for Trade and Industry's (DTI's) Cyber trust and Crime Prevention Project, which is part of the ongoing Foresight futures research programme. The intention of undertaking this research was to play a part in the strategic development of UK information assurance, through its contribution to informing the Home Office e-crime strategy, and to inform policy makers and practitioners, pulling together diverse information assurance measures into a single, if summary, document." (Morris, 2004b)

"Most of the recommendations seek to address fundamental issues or approaches to crime problems, hence the report's call for the tackling of netcrime to be moved from being seen as a specialist capability, to an element of mainstream policing. Discussing the research findings using the whole of the Police Science and Technology Strategy framework has attempted to illustrate this. Similarly, by discussing the findings in established crime prevention terms of the situational model, netcrime seeks to break out from its criminological niche, and be seen as a problem that is permeating mainstream criminal activity. Thus those tackling other offences, through various roles, must accept and indeed explore the implications of netcrime for their own area of accountability, rather than dismiss it as the responsibility of the computer crime or IT security community. Almost all parties involved in tackling crime must recognise that they are now, or will very shortly be, faced with some form of netcrime and it is not going to disappear. Indeed, it is suggested that future efforts in this area should include the development of a 'future scanning' capability. Such activity should not be seen as a one-off exercise, but a permanent and ongoing task, affirming that the challenges of netcrime are not transitory, waiting to be 'solved' with the emergence of yet more new technology. Rather, the day-to-day criminal challenges facing us all have gained another element." (Morris, 2004b)

Morris, S. (2004a) The future of netcrime now: Part 1 – threats and challenges, Home Office Online Report 62/04 <http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr6204.pdf>

Morris, S. (2004b) The future of netcrime now: Part 2 – responses, Home Office Online Report 63/04 <http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr6304.pdf>