Policing Operation Ore

Caroline Metcalf examines the difficulties British police face in tackling child sexual abuse through the internet.

The growth of the internet in recent years is at the heart of current anxieties about child sexual abuse images, internet chat rooms, and the lack of suitable protection for children using this new-found technology (Kennison and Read, 2003). Concerns about these issues focus broadly on how to police the internet (ibid.) because unlike traditional methods of policing, there is no scene of crime and the methods of investigation are not conducted entirely within the parameters of the physical domain. It represents challenges to traditional methods of policing which 'collapse the notions of time, space and geography' (Wall, 1997). Interest in this phenomenon has expanded, not only with the public and the media but also within the political agenda.

In April 2001, the National High Tech Crime Unit (NHTCU) was introduced as part of a multi-agency organisation to offer resources to local and regional forces to carry out investigations relating to 'cybercrime' (Jewkes, 2003). This includes hacking, virus writing, drugs trafficking and child abuse (ibid.). In July 2002 the US Postal Inspection Service discovered a website providing adult pornography as well as child abuse images. The website was called 'Landslide Productions', and following its detection the matter was handed to the Federal Bureau of Investigation (FBI). The FBI passed on intelligence to the National Criminal Intelligence Service (NCIS) relating to some 7,272 British individuals suspected of downloading images of child abuse on the internet. This was to become known as Operation Ore – the largest ever national investigation. Since Operation Ore the HTCU's operations have been stifled.

According to an internet source, under Operation Ore the UK police carried out 4,283 searches, made 3,744 arrests, (Warren 2005) and 35 suspects/ offenders had committed suicide. And in 2005, there were 800 investigations pending (Warren 2005). It is well documented that the police are limited in resources and, since Operation Ore British forces are being launched into a technological field where computer expertise is becoming a necessity for effective investigation. This clearly presents a problem for the police given that those downloading abusive images of children are often highly computer-literate.

During the initial stages of Operation Ore, there were more than 750,000 British suspects. This figure alone illustrates the enormity of such an investigation. According to my research findings (Metcalf 2006), the enormity of the task relates not only to the vast number of suspects but also to issues regarding the sheer range of evidence seized. It does not involve simply examining the hard drives of the suspects' computers. It also includes a phenomenal number of floppy discs, zip files, CD ROMs, palm top computers, laptop computers, printers, scanners, cameras, game consoles, fax machines, telephones, pagers, answerphones, DVDs, tapes, solid state cards, thumb drives, not to mention the endless hours of examining every VHS tape the suspect owns (personal communication 2003). This only accounts for the multi-media type evidence; there are also credit card bills, bank statements, diaries and personal organisers, which may link to the purchasing of child abuse images.

Staff at the computer units tend to be police officers that are untrained in the area of computer crime, and so money must be spent on upgrading their knowledge and skills (author's unpublished PhD thesis 2006). The HTCU also deal with crimes of fraud, blackmail and extortion, hacking and virus attacks, software piracy and Class A drug trafficking. There is other computer related crime that needs to be investigated at the HTCU, and if something more urgent arises, then it is quite likely that Operation Ore would no longer be their highest priority. Indeed, the success of policing investigations like Operation Ore can depend on the priorities of any given force. For example, if such investigations are not part of a policing plan then it might be that they are low on the list. Certain forces might prioritise burglary, car crime, robbery, and drugs, as part of their policing plan and this will remain their focus. Furthermore, the enormity and ambiguity of Operation Ore left some forces not knowing 'where on earth to start'.

Another issue relates to the tracing of suspects. The Federal Bureau of Investigation (FBI) provided the National Criminal Intelligence Service (NCIS) with the credit card details of British suspects. NCIS gathered intelligence on each suspect and passed the data on to the relevant forces across England and Wales. However, security and surveillance surrounding the internet was not as reliable as it seemed; the information could be somewhat broad and required time-consuming work to establish its accuracy in order to pursue the investigation. At first glance it appears that every person who used their credit card to obtain images of child abuse via the Landslide website got 'caught in the loop'. However, it soon became apparent that despite the so-called financial and security procedures of Landslide Productions, it was not quite as strict as it initially appeared. Because of this generic information, the investigation became a lengthy process for British forces and that was before the operation even got started.

Perhaps the most pressing issue around policing Operation Ore was the problem of resources. The National Steering Group acquired £500,000 from the Home Office to support police forces dealing with Operation Ore. The money, managed by the National Crime Squad, was able to provide training, hardware and software equipment for at least one and up to five police officers in every force across the country (personal communication 2003). The issue of resources is both human and non-human. Indeed, human resources should increase along with financial resources although arguably, viewing such material is an unattractive job. One British police officer emphasised the need for manpower, stating 'you only have manpower if you've got money to buy it. You can't go out and say, we'll take out some temporary staff to come in and do it. The staff are what we've got and if you want more man hours under that number of staff then you've got to pay them to work the man hours so it all comes down to money' (personal communication 2003).

The resourcing of manpower is stretched between the sheer enormity of the task, and the willingness of officers to be involved in such work. 'Cop culture' could be the underlying reason for the unwillingness, given it is not seen as 'real police work'. Jewkes (2003) points out that most UK police forces are still paper-based organisations and refers to a Detective Superintendent at West Yorkshire police who complained that most of his colleagues do not feel computer-based investigation is 'normal' work, and that their ability to respond to internet crime is 'haphazard and based on luck rather than a prepared and researched provision of a service to the public' (Hyde, 1999:7 cited in Jewkes 2003:17). Compounding this is many officers' lack of computer and technical knowledge. Officers that were interviewed were aware that there was a recognition at a national level of the need for police training in computer crime (unpublished PhD thesis).

There is clearly a range of difficulties involved in the policing process of investigations like Operation Ore. As this article has demonstrated, forces might not be effective if such offences are not prioritised. Furthermore, the problem of resources is an ever-present feature in policing, particularly in an investigation that involves tens of dozens of suspects in each force area. This has a significant impact on policing internet sex offenders since it is not only manpower that is required but *specialised* manpower. In other words, Operation Ore and similar investigations require firstly, an officer or civilian willing to work within the HTCU, and secondly, they must be 'technologically trained', which of course requires time and money. It is a case of 'time will tell' about how future similar investigations are managed. Ever-changing social conditions require the police to become more specialised and professionalised through the development of specialist units dealing with specific crimes.

Caroline Metcalf PhD, *is Programme Specific Facilitator for a Community Sex Offender Groupwork Programme.*

References

Hyde, S. (1999) 'A few coppers change', in *Journal of Information, Law and Technology.* Available Online at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1999_2/hyde/

Jewkes, Y. (2003) 'Policing the Net: crime, regulation and surveillance in cyberspace', in Jewkes, Y. ed. (2003) *Dot Cons: Crime Deviance and Identity on the Internet.* Cullompton: Willan Publishing.

Kennison, P. and Read, M. (2003) 'Policing the Internet, part one; The Internet and child protection' in *Community Safety Journal* 2(2), University of Middlesex: Pavillion.

Metcalf, C. M. (2006) *Making Sense of Sex Offenders and the Internet.* Unpublished PhD Thesis: Brunel University.

Wall, D. S. (1997) 'Policing the virtual community: The Internet, cybercrimes and the policing of cyberspace', in Francis, P., Davies, P. and Jupp, V. (1997) *Policing Futures.* London: MacMillan.

Warren, P. (2005) 'UK police tackle mounting internet porn caseload', in *The Register.* Available Online at http://www.theregister.com/2005/04/22/uk_police_internet/print.html.