Fair play? Fair game?

Keith Lyons suggests that criminology and sport may be more closely linked than previously assumed.

Most of us have some access to sport. We are often invited to acknowledge the cultural significance of sporting forms and behaviour. We are deluged with a 'documentary reality' of sport. Until the appearance of a radical critique of sport in the late 1970s there was a taken- for-grantedness about sporting behaviour that accepted pervasive myths. Just as criminology has had to address "the 'spectre' of the question of sex" (Collier, 1998) so too has sport had to contemplate gendered behaviour. The social and cultural construction of sporting opportunities cannot be understood without addressing the over-determination of sporting opportunities by men. Sheila Wigmore (1999) has recently re-visited some of the hegemonic issues involved in sport and the 'maleness' of its definition.

Fair play

The challenge to gendered sport is part of a widespread critique of sporting values and behaviour. Modern sport is highly regulated but an essential feature of such regulation is the concept of 'fair play'. For example, the International Olympic Committee (IOC) dedicates its efforts 'to ensure that in sports the spirit of fair play prevails and violence is banned'. Given the recent disclosures about the process of the awarding of the Winter Games to Salt Lake City and the Summer Games to Sydney there is some reason to reflect on the aphorism that rules do not bring about conformity, only a different kind of non-conformity.

Sport offers numerous opportunities for the empirical specification of issues of fundamental interest to criminologists. The Olympic Movement alone provides a rich source of data. The 'graft' controversy surrounding the award of the quadrennial Summer and Winter Games resonates with substantive issues in 'white collar crime'. That graft occurred should be no surprise to anyone vaguely *in touch with the human condition*. The sense of shock expressed by the IOC at disclosures of dishonesty within its ranks is located within a legitimising ideology of the fairness of sporting behaviour.

Drug usage

This putative 'fairness' is also challenged by the desire within competition to win at any cost. The IOC has had a system for drug testing since 1964 and in 1967 became the first sports organisation to have a Medical Commission. Since 1968, the Medical Commission has undertaken 3,715 random tests at the Winter Games and has found evidence of five athletes taking banned substances. The Nagano Games in 1998 provided an interesting opportunity to visit the debate about the status of cannabis. A snowboard gold medallist tested positive for traces of cannabis but retained his medal because the IOC had not formally banned it! In the Summer Games there have been 11,073 tests which have identified 48 athletes taking banned substances.

By coincidence the second sports governing body to establish a Medical Commission was the International Cycling Union (UCI). Last year UCI became involved in the Tour de France 'drugs scandal'. A manager, a doctor and a masseur of one of the leading teams were charged with supplying drugs such as erythropoietin (a blood booster) and human growth hormone. Subsequently a team director and doctor of another team were charged with 'transporting poisonous substances and the possession of dangerous merchandise'. Each year governing bodies for cycling spend approximately £1,500,000 on drug testing and anti-doping controls. As a result of the moral panic about drugs in cycling, UCI (1998) decided 'to perform physiological studies with a view to establishing if, in physical terms, the professional obligations of road cyclists are too great. In other words, we wish to determine whether the physical burden corresponds to what may be expected of a well-trained cyclist in terms of duration of competitions and length of races'.

Match fixing

Sport, like other cultural forms, has a problem in reconciling its ethical precepts with the lived experience of its participants. Most governing bodies of sport would subscribe to the IOC's aspiration that 'the equality of opportunity between players, the impartial refereeing of competitions and the fair play of winners and losers alike are elements which encourage the practice of the virtue of justice'. The codification of sport with elaborate rules and laws is a manifestation of the desire to regulate for equity, impartiality and fair play. Criminologists will intuitively appreciate the problems generated by this approach. In fact the whole edifice of sport is subject to what some have characterised as the 'prisoner's dilemma'. If all sports' participants defer to the rhetoric of equity then sport could enact its rhetoric. If one participant consciously chooses to take advantage of this deference then cheating has enormous rewards.

Match fixing challenges the very essence of sport as do performance-enhancing drugs. In the last year there have been a number of high profile allegations and charges about fixing outcomes. Boxing, cricket, horse racing and soccer are just four sports that have

David Kidd-Hewitt

"A snowboard gold medallist tested positive for traces of cannabis but retained his medal because the IOC had not formally banned it.."

"The codification of sport with elaborate rules and laws is a manifestation of the desire to regulate for equity, impartiality and fair play. Criminologists will intuitively appreciate the problems generated by this approach."

had to address the possibility that fair play may not be occurring. Why this should be surprising to sport indicates that a historical consciousness leads to selective perception. What is interesting, I believe, is that each of these sports has been involved in a globalisation process not only of performance but also of structured betting. Like other cultural forms, a world economy of labour and service industries generates a range of pressures that may be antithetical to the ethos of fair play.

Officiating

The problems for sport do not end with players. There are some intriguing issues associated with officiating at sporting events. Referees, umpires and judges have a fundamental role to play in distributive justice. In most instances they are 'witnesses' and 'judges' and are charged with neutrality and objectivity. Some sports' researchers are now exploring the mechanisms of inter-actional justice and the perceptions of fairness. Stimulated by studies of judges' behaviour in the legal system, these researchers are investigating the role of expectancy in sport. A good example of the empirical specification of this problematic is the impact of 'home advantage' on officials' behaviour. Despite the availability of a *de jure* framework for the application of the laws of the game, there is a growing amount of research evidence about the de facto interpretation of law. In games like rugby union and soccer, for example it is not surprising to find instances of home teams receiving minimal sanctions, particularly if the home team is losing. Once officials use their interpretative frameworks then players have no certainty about how their actions will be judged. This lack of certainty again challenges the fair play ethos of sport.

At the start of this article I mentioned the gender issue that has to be addressed in sport. As a cultural form, sport generates constant examples of wider social processes (how could it be otherwise?). Recently, the result of a world heavyweight boxing contest between Evander Holyfield and Lennox Lewis provided another juxtaposition of the maleness of sport and the place of women. One of the three judges at the fight was an American, Eugenia Williams. She scored the fight as a win for Evander Holyfield. Amongst the emotive responses to her decision was one by an 'experienced referee' who suggested that 'women are not fight people. There are two sports where women should not be allowed - rugby and boxing' (BBC News, 14 March 1998). Whilst there was some debate about Eugenia Williams's observational skills in the weeks that followed, her suitability as a judge was questioned solely because of her gender.

Fair game?

The private troubles and public issues of sport resonate with issues addressed by criminologists. The visibility of male sport provides numerous opportunities to problematise fairness and equity. Doping, match fixing and officiating bias invite a critical analysis of sporting institutions and behaviour. Just like 'criminal' behaviour, there are easy things to say about sporting behaviour. Does this make it fair game for our attention?

■

***Keith Lyons** is Reader in Performance Analysis, Centre for Performance Analysis, University of Wales Institute, Cardiff.*

References:

Collier, R. (1998) 'Masculinities and Crime'. *Criminal Justice Matters*, 34, Winter: 21-23

UCI. (1998) *Summary of the Decisions Taken at the Various Meetings between the UCI, Riders, Sports Directors and Race Organizers*. Lausanne, Switzerland. 13 August.

Wigmore, S. (1999) 'Well it just is, isn't it? An examination of the masculine hegemony of sport', in *The Bulletin of Physical Education*, 35(1): 14-22.

Drug use & workplace testing

Peter Francis and **Peter Wynarczyk** look at the development of workplace drug testing and questions the assumed link between drug use and risk.

One, two, three: testing, testing, testing

Under the somewhat crude headline banner 'Tinker, Tailor, Soldier, Smackhead: Doctors on Heroin, Nurses on Pills, Executives on Coke' the homeless weekly magazine The Big Issue ran a two-page article in early 1998 questioning 'how serious is drug taking at work?'. The general thrust of the article was that data on the size of the problem was inconclusive; 'opinions come easy but facts are harder to find' (Williams, 1998: 14). But the underlying theme was not, namely that drug testing is becoming more commonplace across industry and commerce in the UK and is likely to follow the US experience.

In the US, workplace drug testing is big business, and has been since it appeared in the 1960s. Konovsky and Cropanzano (1993) report that in 1986 approximately 25 per cent of all Fortune 500 companies had some drug testing programme in operation, while Macdonald (1995: 703) cites evidence for 1993 that approximately 85 per cent of major firms have some form of testing in place. Drug testing varies between industry type and characteristic, size of organization, nature of work conducted, and geographical location. Williams (1998: 15) in a recent review suggests that the US figure

"Statistical and other data on the nature and extent of workplace illicit drug misuse is at best partial and at worst unreliable."

Héloïse Hayman

is now approaching an annual 15 million employees being tested for drug misuse.

The size, extent and cost of drug testing programmes in the UK is much less well documented. Nevertheless, it is suggested that the percentage number of UK firms who test employees for illicit drug misuse is approximately ten per cent and rising. Certainly provision under the *Transport and Works Act 1992* has ensured that drug screening is central to safety-critical industries, while recent high profile media exposés of medical professionals and the work of the national drugs co-ordinator have ensured that it has remained on the political agenda.

In support of workplace drug testing

Yet the question arises, why is the workplace coming under increasing pressure to develop regulatory mechanisms for drug use? Three reasons most frequently cited in support of workplace drug testing are that drug use is a prevalent problem in the workplace; that drug use increases risk of employee accident, injury and death; and that drug use decreases employee productivity.

However, despite these arguments supporting the necessity of workplace drug testing a critical review of the literature raises more questions than confirmation of its worth at the present time (Francis and Wynarczyk 1999). First, statistical and other data on the nature and extent of workplace illicit drug misuse is at best partial and at worst unreliable. Despite the attention given to the general use of drugs in society today, there have been few systematic attempts to document these behaviours empirically among employed persons, not least in the UK, and those that do either focus upon alcohol rather than illicit drug use and/or suffer from serious conceptual and methodological weaknesses. In consequence, although supporters of testing assert that illicit drug use is a major workplace problem, it is far more difficult empirically to demonstrate this.

Second, although there is a body of research which has sought to demonstrate the association of employees' illicit drug use with increased risk, be it to the employees or employer, a critical reading of the research indicates that while correlations may have been established, establishing causality is much more problematic. For example, with regard to the argument that workplace drug use leads to increased employee risk in the form of accidents and injuries, Macdonald (1995: 705) concludes his review of the research by stating that since the relationship between workplace illicit drug misuse and accidents and injuries has not been empirically established, and since few studies have explored the role of drugs in work injuries 'definitive conclusions cannot be drawn'. Criticisms that can be directed at the research conducted include combining drugs into one category by simply comparing users with non-users; failing to differentiate moderate from heavy use, or current from past use. Moreover, too little weight or attention is given to non-drug predictors such as job conditions, demographic variables or other lifestyle characteristics explaining the increased risk.

"The drug testing industry may be partly engaged in perpetuating its own industry and generating an artificially high demand for its product by constructing a social problem myth of employee drug consumption being significantly detrimental to the workplace environment."

Regarding employer risk, three areas are usually identified: that drug use increases worker absenteeism and associated costs; that it increases the costs associated with employee turnover; and that it increases the costs associated with impaired employee performance. Again, in reviewing the research on these three areas, its inconclusive and sometimes contradictory nature is once more an overriding feature (Francis and Wynarczyk 1999).

Is testing effective in reducing risk?

Usually, the effectiveness of any given testing programme is measured against its stated primary objective(s). Such goals include the reduction of workplace accident, injury and death, and an increase in workforce productivity and performance. Because testing can be implemented in a variety of ways, its effectiveness partly depends upon the type of programme, its implementation, its aims and objectives and the particular risk involved. For example, if we take the suggestion that random drug testing reduces the risk of accident and injury, the starting point for any assessment of effectiveness would be that drug use is causally related to increased risk. However, the problem is that there is little conclusive evidence that drug use is causally related to poor performance through accident or injury. As a result, it follows that the effectiveness of drug testing programmes in reducing possible illicit drug related consequences is also 'scientifically unproven' (Macdonald and Wells, 1994: 130-131). Similar inconclusive findings can be suggested for studies into pre-employment testing programmes. Finally, Macdonald and Wells (1994: 137-139) also stress caution in measuring the 'outcome effects' of testing as measured in the percentage reduction of accidents, injuries and performance problems, because such programmes fail to take account of the possible and actual effect of non drug testing factors (such as increased employee training and superior capital equipment) in reducing risk. Indeed, it is the case that such measures may account for the majority of the reduction in risk, thus further problematising the effectiveness of workplace testing mechanisms themselves.

We would stress the need for caution when arguing the case for drug testing programmes in the workplace. First, prevalence rates remain inconclusive and methodologies problematic. Second, the causal link between illicit drug use and increases in employee or employer risk is for the most part largely unsubstantiated. Third, the effectiveness of testing mechanisms is questionable. This raises the question of whether we have been sold the drug testing myth.

Have we been sold the drug testing myth?

Drug testing in the USA has become a several billion dollar a year industry with the potential to grow ever larger. The disadvantages arising from employee drug consumption and the workplace connection have been asserted as significant but, as yet, remain both tentative and inconclusive. The advantages of a drug free workplace, again claimed to be substantial, remain inconclusive. The benefits accruing from drug testing have been effectively hyped and sold to both the private and the public sectors. Expectations are high. We would suggest the need for a more sober approach; the benefits and costs of such testing need to be more carefully assessed and justified alongside alternative strategies. The drug testing industry may be partly engaged in perpetuating its own industry and generating an artificially high demand for its product by constructing a social problem myth of employee drug consumption being significantly detrimental to the workplace environment.

Such developments are, in part, embedded within a wider context of a fear of increasing rates of drug use within society as a

whole, and of how this can effect the workplace. It is also partly a view of the irrational user in need of regulation and partly a conventional wisdom, which has denied any space to debates over decriminalisation and legalisation. Such developments are also in no small degree the result of advancements in testing procedures, and the marketing of them by particular companies. However, in our view, the expansion of workplace drug testing is neither evidence based, nor for the most part suitable for the complexities of late modern society and the post-Fordist workplace. Rather, its continued growth raises a number of issues which remain unsettled and in need of much greater debate and research. These are listed by way of conclusion:

- *Is workplace drug testing necessary?* There is, to date, insufficient evidence that illicit drug consumption is prevalent in the workplace, is responsible for lowering labour productivity and work performance, or that it significantly affects the likelihood of workplace accidents, injuries and death.

- *Is drug testing advantageous?* The benefits of drug testing remain speculative in clearly distinguishing between the drug consuming and non-drug consuming employee and reducing employee and employer risk, as does the belief in the application of the methods of drug testing to distinguish clinically between on-the-job and off-the-job drug consumption, and the occasional from the frequent user.

- *Is workplace drug testing a form of social control?* Whilst drug testing measures tend to be viewed as protecting the collective interests of all (employee, employer and customer alike), they also provide an additional workplace control mechanism that extends beyond workplace activity. Hecker and Kaplan (1989: 701) and Blackwell (1994), for example, present workplace drug testing as a modern form of social control and scientific surveillance. They see this as moving us closer towards the 'Brave New Workplace' and are aware of the dangers posed by a widely adopted practice of workplace drug testing whereby 'one's own bodily fluids can tell tales, not about one's being impaired on the job, but about one's activities last Saturday night, or perhaps a week ago, or about other personal characteristics or medical conditions unrelated to work or to illegal drug use' Workplace testing not only blurs the distinction or boundary between work and non-work activity but places a premium upon the latter not being detrimental to the former.

- *Does drug testing threaten employee rights?* Sensitive civil liberty issues related to such matters as privacy (reduced by the increasingly fuzzy work/non-work distinction) and employee rights may have been undervalued. Within the USA, where such drug testing has been increasingly applied, constitutional issues have been raised and worker rights threatened and possibly violated.

- *Is drug testing fair?* Employees are becoming increasingly concerned about the explicit, especially punitive, sanctions that may be imposed against them due to failure to submit to test or testing positive. They appear to be less worried where rehabilitation and treatment rather than discipline and/or dismissal is the likely outcome. Workers are also concerned with regard to how the drug tests are conducted and the results reached. Doubts remain over just what, in fact, drug testing is supposed to be actually testing.

■

***Peter Francis** is a Lecturer in Criminology and **Peter Wynarczyk** is a Principal Lecturer in Economics, at the University of Northumbria.*

References:

Francis, P. and Wynarczyk, P. (1999) 'Regulating the invisible? The case ofworkplace illicit drugs misuse', in P. Davies, P. Francis and P. Jupp (eds.) *Invisible Crimes, Their Victims and Their Regulation* (Basingstoke: Macmillan)

Hecker, S. and Kaplan, M. 5. (1989) 'Workplace drug testing as social control', *International Journal of Health Services* 19/4: 693-707.

Konovsky, M. A. and Cropanzano, R. (1993) 'Justice considerations in employee drug testing', in R. Cropanzano (ed) Justice in the Workplace: *Approaching Fairness in Human Resource Management* New Jersey: Lawrence Erbaum Associates. Inc.

Macdonald, S. (1995) 'The role of drugs in workplace injuries: is drug testing appropriate', *Journal of Drug Issues* 25/4: 703-722.

Macdonald, S. and Wells, 5(1994) 'The impact and effectiveness of drug testing programs in the workplace', in S. Macdonald and P. Roman (eds) *Drug Testing in the Workplace Research Advances in Alcohol and Drug Problems* Volume II (New York: Plenum Press).

Williams, J. (1998) 'Tinker, tailor, soldier, smackhead: doctors on heroin, nurses on pills, executives on coke. How serious is drug taking at work?', *The Big Issue* February 9-15: 14-15.

Getting to grips with cybercrime

David Wall suggests that the law lags some distance behind cyber criminals.

Love or hate it, the internet is here to stay and for better or for worse, it will continue to shape our future, so we must seek to understand it, particularly the 'worse' aspect. This article will explore the key issues that currently concern cybercrime and the governance of cyberspace. It will identify the main areas of harmful activity that concern us, it will outline the pluralist/multi-tiered policing/governance model that has already developed and it will explore how definitions of cybercrimes are being shaped by the fight for control over the environment of cyberspace.

The internet has had three different levels of impact upon criminal, or harmful activity. Firstly, the internet has become a vehicle for existing patterns of harmful activity, such as hate speech, bomb-talk and stalking. Secondly, it has created an environment which provides new opportunities for harmful activities that are currently covered by existing criminal or civil law; examples would include paedophile activity, but also fraud. Thirdly, the nature of the environment, particularly with regard to the way that it accelerates the 'distanciation' of time and space (Giddens, 1990: 6), has engendered entirely new forms of (unbounded) harmful activity such as the unauthorised appropriation of imagery, software tools and music

"Whilst the dark side of cyberspace is probably not as large as originally anticipated, it is nevertheless formidable and will continue to be explored as a site for opportunities; consequently, the concerns over this dark side are driving the debate over regulation."

"The definitions of acceptable and unacceptable cyber-behaviour are themselves being shaped by the ongoing power play or 'intellectual land grab' that is currently taking place for market control."

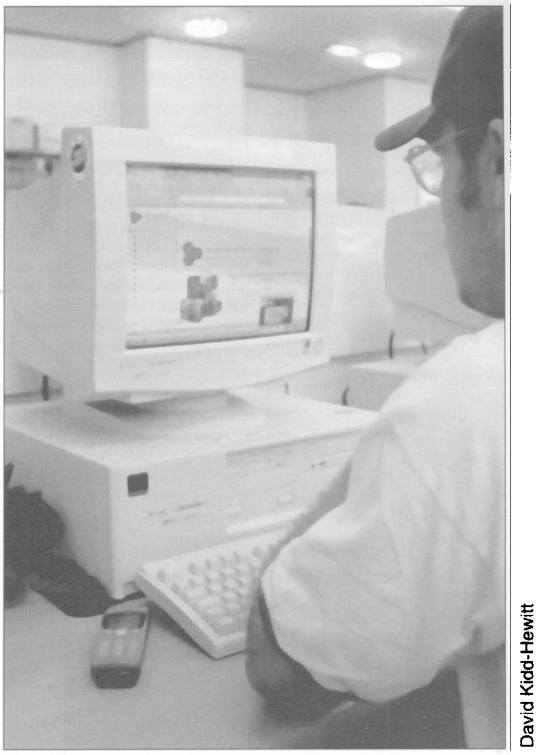
products. Each is linked to the increasing commercial potential of cyberspace and in turn, is part and parcel of the emerging political economy of information capital (see later). It is clear that across these three levels of impact lie four broad areas of harmful activity which are raising concerns. They are cyber-trespass (hacking which ranges from ethical hacking to information warfare), cyber-thefts (fraud, appropriation of intellectual property), cyber-obscenities (pornography, sex-trade), and cyber-violence (stalking, hate-speech).

As we develop an understanding of the virtual environment of cyberspace, an interesting, but paradoxical situation is emerging. On the one hand, it is now quite clear that in its various capacities, the internet really does have the capability to transcend economic, political, geographical, social and even racial and gendered boundaries as the early commentators had predicted. On the other hand, although the mass media would have us believe otherwise, the anarchy and widespread criminality which was predicted by those who favoured early regulation has not yet materialised. By comparison, cyberspace is remarkably ordered considering the large numbers of individuals who inhabit it and also the breadth of their involvement(s) with it. However, whilst the dark side of cyberspace is probably not as large as originally anticipated, it is nevertheless formidable and will continue to be explored as a site for opportunities; consequently, the concerns over this dark side are driving the debate over regulation

So why is it the case that all 'netizens' have clearly not become pornographers, cyberterrorists, paedophiles or embezzlers? The answer lies in the propensity for individuals, for the most part, to act responsibly without statutory supervision. Furthermore, a system of governance has already started to develop, which combines this factor with existing legal norms as enshrined in law. Putting aside here concerns about the accountability(ies) of the organisations and groups involved, there are currently four main levels at which this 'policing' activity takes place within cyberspace to effect governance. Respectively, they are: the internet users themselves, including internet user-groups; the internet service providers; state-funded non-public police organisations; state-funded public police organisations. This development reflects the 'organisational bifurcation' (Reiner, 1992) or 'spatial polarisation' (Johnston, 1993) that is also taking place within the sphere of terrestrial policing.

Underlying the above are a series of tensions that are actively shaping definitions of (cyber) behaviour, the victims of that behaviour, and also who the perpetrators are. The definitions of acceptable and unacceptable cyber-behaviour are themselves being shaped by the ongoing power play that is currently taking place for market control (see Boyle, 1996). Of concern is the increasing level of intolerance that is now being demonstrated by the new powerful towards certain 'risk groups' whom they perceive to be a threat to their interests. Such intolerance tends to mould broader definitions of deviance, but they are not simply so one-sided, because definitions of crime and deviance arise, not only from the social activity of elite or power groups, but also from that of 'common members' of society and offenders themselves; 'the struggle around the definition of crime and deviance is located within the field of action that is constituted by plural and even conflicting efforts at producing control' (Melossi, 1994: 205).

An important (shaping) factor here is the current 'media sensitization' towards internet related issues which has, in turn, heightened their overall newsworthiness, especially with regard to the dark side of the internet. Such sensitisation is gradually moulding the legal and regulatory responses to these harms by inflating public concerns and therefore providing the regulatory bodies with a (sometimes implied) mandate for taking action. Moreover, public awareness is further heightened by the common failure of journalists, pressure groups, policy makers and others, to discern between 'potential' and 'actual' harms, an act that is made easy by the virtual impossibility of making any systematic calculation of the extent of cybercrimes.



David Kidd-Hewitt

Two observable cautionary tales exist to demonstrate the need to focus upon actual rather than potential harms. In the mid-1990s, the moral panic over pornography available on the internet was fuelled by bogus empirical research claims (Wallace and Mangan, 1997) and resulted in the United States Government introducing formal regulation without a complete analysis of the problem (since partially overturned by litigation). The other example, again from the USA, relates to the overstating of the extent of cybercrimes in order to secure state funding for security and policing organisations (see Campbell, 1997).

Such fluidity of definition creates a degree of confusion over who are the victims and how they are being victimised. Not only can victims vary from individuals to social groupings, but the harms done to them can range from the actual to the perceived. In cases such as cyberstalking or the theft of cybercash, the victimisation is very much directed towards the individual. However, in other cases the victimisation is more indirect, such as with cases of cyberpiracy or cyberspying/ terrorism. Moreover, as has been found to be the case with the reporting of white-collar crimes, it is likely that many victims of cybercrimes, be they primary or secondary victims, may be unwilling to acknowledge that they have been a victim, or it may take them some time to realise it. Alternatively, where the victimisation has been imputed by a third party upon the basis of an ideological, political, moral, or commercial assessment of risk, the victim or

"The issue of cybercrime is creating a series of interesting challenges for twenty-first century criminology."

victim group may simply be unaware that they have been victimised or may even believe that they have not, such as in the case of some of the debates over pornography on the internet. To complicate matters further for the victim, the public nature of the cyberspace medium also provides a constitutional defence (typically in the USA) as freedom of expression with regard to a number of the perceivably harmful activities.

The issue of cybercrime is creating a series of interesting challenges for twenty-first century criminology. Clearly, the early research into the subject is suggesting that the debate over cybercrimes falls outside the realm of traditional criminological understanding, with its focus upon the analysis of working class subcultures or the underclass. But that same research is also suggesting that it also falls outside much of the literature on white-collar crime as well. So, whilst both bodies of literature inform our understandings of cybercrimes, we have nevertheless got to develop a specific criminological knowledge base relating to the internet.

***David Wall**, Cyberlaw Research Unit, Centre for Criminal Justice Studies, University of Leeds.*

References:
Campbell, D. (1997) 'More Naked Gun than Top Gun', *The Guardian* (OnLine), 27 November, p.2.
Giddens, A. (1990) *The Consequences of Modernity*, Cambridge: Polity Press.
Johnston, L. (1993) 'Privatisation and protection: spatial and sectoral ideologies in British policing and crime prevention', *Modern Law Review*, vol.56, pp.771.
Melossi, D. (1994) 'Normal crimes, elites and social control', in Nelken, D. (ed.), *The Futures of Criminology*, London: Sage.
Reiner, R. (1992) 'Policing a Postmodern Society', *Modern Law Review*, vol.55, p.
761.
Wallace, J. and Mangan, M. (1996) *Sex, Laws and Cyberspace*, New York: Henry Holt.

Ghosts in the machine: computer misuse within the organisation

Zaiton Hamin and **David Wall** consider the vulnerability of organisations to the 'harms' of computer misuse.

The rapid growth of the internet during recent years is now legend, as are its social, educational, organisational and commercial benefits. However, the increasing dependence upon information systems by many major infrastructural organisations has made them more vulnerable to computer-related harms. The term 'harm' is used here because misuse is not necessarily contrary to criminal law. Yet much of the debate over computer related harm has tended to concentrate upon the individual and, where the debate has included organisations, these threats have for the most part tended to be perceived as coming from without, rather than from within. This article draws upon ongoing research into computer related harms within the organisation and it will seek to map out some of the issues relating to cyber-threats from within the organisation.

"Much of the debate over computer related harm has tended to concentrate upon the individual and, where the debate has included organisations, these threats have for the most part tended to be perceived as coming from without, rather than from within."

One of the main obstacles to developing an understanding of misuse within the organisation is obtaining reliable data. On the one hand organisations tend, for a variety of reasons, to be reluctant to admit that they have been the victim of an attack. This could be because of the corporate fear of the negative commercial impact of adverse publicity in terms of lost market share, or that they lack faith in law enforcement capabilities, or that they favour civil, rather than criminal, remedies. Alternatively, organisations might find it easier to claim for losses through insurance, or just simply pass on the costs directly to their customers. Furthermore, misuse is also hard to detect, never mind regulate (Wall, 1998), because individual motivations are very diverse in nature. Computer misuse within the organisation can be motivated by revenge, malice, intellectual challenge, thrills; personal problems such as gambling debt, drug-taking or investment losses, greed/financial gain; frustration, dissatisfaction with, or protest against, their employers. In addition, the organisation's employees, themselves, may have been targeted by outsiders to help in the commission of computer-related crimes or telecommunication offences. In *R v Pearce* (unreported), for example, the defendants were employees of a mobile telephone company who, while working with an outsider, were held to be guilty of gaining unauthorised access, having conspired to obtain data from the employer's customer accounts in order to instigate a phone-cloning scam.

Confusion over harms

On the other hand, reports of misuse tend to confuse potential and actual harms. Indeed, there is some evidence to suggest that this confusion could be a deliberate ploy by the burgeoning cybercrime industry to secure trade and, in some cases, public funding. The little empirical information about misuse that does exist points in one direction, towards a general increase in harms both from outside, but also from inside the organisation (Hamin, 1999). However, whilst most jurisdictions have some form of criminal (anti-

"While most jurisdictions have some form of criminal (anti-hacker) legislation to deal with external threats to the organisation, the law relating to the insider threat within those same jurisdictions is less easily definable."

hacker) legislation to deal with external threats to the organisation, the law relating to the insider threat within those same jurisdictions is less easily definable, often combining criminal, civil and common law with employment regulations. So the insiders present a considerable legal dilemma, particularly, as indicated above, they tend to be persons with legitimate access to the computer system. These persons might include current and former employees, temporary workers, on-site contractors, consultants, partners and suppliers.

Such threats have always existed and the literature on the sociology of work is replete with examples. Sociologists will remember Taylor and Walton's (1971: 219) fabled account of industrial sabotage, where a disgruntled worker who, upon being sacked from a confectionery manufacturer, wrote a colourful expletive in half a mile of Blackpool rock. What is different, however, with the insider cyber-threat is not that it is new, but rather the potential scale of both the harm that can be effected and also its implications. Take, for example, the Nick Leeson affair which brought down Barings Bank and, in so doing, ultimately contributed to the downfall of some of the Far-Eastern tiger economies.

Managing change

In addition to the potential scale of harms that can occur there has been an increase in the overall level of motivations that underlie threats to the organisation. In the race to rationalise capital and make organisations more economic, effective and efficient, organisations would appear to have shown little regard for the management of the change that information and communications technologies have upon their employees, particularly with regard to the acceleration of the de-skilling and re-skilling process (Wall and Johnstone, 1997; Braverman, 1976). This 'permanent revolution' has simultaneously decreased job security while diminishing the workers 'bond with their employers' (Ulsch, 1998).

Of course, recent patterns of media reporting have concentrated upon the more sensational examples of insider attack. In practice, however, most examples are more mundane. At this latter end of the spectrum of insider misuse one can see, for example, the cumulative financial impact of employees mis-using the office computer for private work, such as sending personal electronic mails, playing computer games or surfing the Internet. These activities largely result in an overall loss of resources and productivity. Towards the other end of the spectrum, however, lie the more onerous threats, such as input or output data manipulations (data-diddling); theft of confidential information or trade secrets (economic espionage); cyber-fraud (siphoning funds from one account to another); cyber-blackmail (holding data hostage); cyber-vandalism/revenge (Hamin, 1999). These more serious threats can actually damage the organisation and threaten its existence.

The law and the resolution of conflict with regard to insider threats, other than those which clearly fall under the ambit of criminal law, as suggested earlier, can be fairly ambiguous. Even the criminal law is often not so clear. For example in the UK case *DPP v Bignall* [1997] (Crim LR 53, 1998), the Court of Appeal held that accessing the Police National Computer (database) by the police defendants did not constitute an unauthorised access, contrary to the *Computer Misuse Act 1990*. This was because the defendants had a general authority to access the database, even though they had used the database for private and unauthorised purposes. Similarly in *R v Gregory Michael Brown* [1996] (146 NLJ 209), it was held that access into the Police National Computer by the police defendants for purposes other than policing was not an offence under section 5(2) of the *Data Protection Act 1984* (before amendment s.161, *Criminal Justice and Public Order Act 1994*), on the grounds that there was no evidence that the defendants had made any actual or tangible use of the information obtained from the computer. Such decisions send out very mixed messages when it is clearly in the public interest to protect sensitive information from misuse.

"Recent patterns of media reporting have concentrated upon the more sensational examples of insider attack. In practice, however, most examples are more mundane."

"The new information and communications technologies are creating not just new patterns of work, but also new associated patterns of offending which challenge many of our traditional perceptions of crime and crime prevention."

In conclusion, the new information and communications technologies are creating not just new patterns of work, but also new associated patterns of offending which challenge many of our traditional perceptions of crime and crime prevention. Of particular concern is the continued focus upon the external rather than internal threat. Consequently, a shift is required in the way we both seek to understand, but also deal with, internal threats such as computer misuse within the organisation. ■

***Zaiton Hamin**, researcher, and **David Wall**, Deputy Director, both at the Cyberlaw Research Unit, Centre for Criminal Justice Studies, University of Leeds.*

References:

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

Hamin, Z. (1999) 'Computer Misuse in the Workplace: A research note', *International Review of Law, Computers and Technology*, vol.13, no.3 (forthcoming).

Taylor, L. and Walton, P. (1971) "Industrial Sabotage: Motives and Meanings", in Cohen, S. (ed) *Images of Deviance*, Harmondsworth: Penguin.

Ulsch, M. (1998) 'Hold Your Fire' at http:www.infosecuritymag.comlhold.htm

Wall, D. (1998) 'Policing and the Regulation of Cyberspace', pp.79-91 in Walker, C. (ed) Crime, Criminal Justice and the Internet, *Criminal Law Review* special edition, London: Sweet and Maxwell.

Wall, D. and Johnstone, J. (1997) 'The industrialisation of legal practice and the rise of the new electric lawyer: the impact of information technology upon legal practice' *International Journal of the Sociology of Law*, vol.25, pp.95-116.