editorial

crime and technology

David Wall puts this issue into perspective.

There is just no escaping the fact that technology shapes the architecture of the social and physical world in which we live. The longstanding articulation of desirable values through innovative systems which solve problems and extend our human capabilities have brought immeasurable benefits to overall quality of life. But one of the sad inevitabilities about technological development has been that its benefits always seem to be in close proximity to its potential harms.

Although the hardware which implements technological ideas may have changed across the span of time, many of the basic ideas remain familiar. Our ancestors' motives to use bone hammers and stone axes to beat their enemies into submission to steal their food and grain are not so far removed from those of cyber-criminals who launch automated phishing expeditions to steal money. This long standing, though 'uneasy', relationship between crime and technology also extends to ideas about crime prevention and security – the architects of the Pyramids, for example, employed sophisticated security technologies to thwart tomb raiders — a few wrong moves and the tomb entrance was sealed forever — not so far off in principle to the automated surveillant technologies installed at airports to identify potential terrorists through abnormal patterns of movement.

The technological cat and mouse game between offender and investigator remains much the same. Offenders still exploit new technologies and the investigators catch up quickly and then use those same technologies to form the basis for prevention. What has changed significantly in late modern times has been a significant increase in personal computing power within a globalised communications network. As a consequence, not only are ideas about committing crime, its investigation and prevention being shared on a global scale, but high levels of computing power also enables these ideas to be put into practice across the global networks.

This issue of *Criminal Justice Matters* contains a selection of current work and thinking that highlight (though not exclusively) many of the key debates currently taking place in the field of 'crime and technology'.

One of the main rules of thumb in the crime and technology debate is that as technology permeates the criminalisation process, then once any flaws in the technology are identified they can (increasingly) be reversed to resolve the problem. The cause effectively becomes the policing solution. This premise lies very much at the heart of the crime science debate. As **Ken Pease** observes, the application of scientific principles to the prevention and detection of crime and the reduction of disorder in ethically acceptable ways is something that most citizens desire. As a consequence, what is, and is not, an 'ethically acceptable way', becomes a crucial decision point because the more crimes are mediated by technology, the more ideal they are for the application of the scientific principles of situational crime prevention. This is not a view shared by all, and a concern raised in a number of contributions herein and also elsewhere is that the scientific measures employed in crime science often fall short of their intended goals, possibly with negative implications for privacy and even personal safety.

Yvonne Jewkes shows how high-tech solutions have been applied to deal with the relatively low-tech crimes that constituted the terror attacks of 9/11 and the Madrid train bombing with confusing results. On the one hand, high-tech policing was successfully applied to identify the perpetrators, but the application of high technology in terrorism prevention has had mixed results, exposing a range of practical issues that need to be overcome with regard to the reliability of the technology that reduce the likelihood of it achieving its intended goals. Within a different context, **Toby Seddon** has found that the evidence base to support drug testing in the police station is currently rather weaker than might be supposed given its rapid expansion over the last three years. Concern about 'reliability' was also an observation identified by **Craig Patterson** in his piece on 'technocorrections', in which electronic monitoring is used to govern at a distance by managing "offenders in the community through an intensification of [networked] surveillance".

But even if the technology does work as intended then concerns may still remain about the ethics of its application. **Una Padel** argues that electronic monitoring simply does not achieve its stated goals in diverting offenders from prison, nor does it have a particularly positive outcome. Instead, it erodes the civil liberties of offenders and their families. **Mike Nellis** on the other hand has a slightly more optimistic take, arguing that although the 'commercial' and the 'humanitarian' are uneasy bedfellows in the private provision of electronic monitoring services, the providers are not "deaf to the ethical arguments".

Reminding us that a wide ranging process of change has to take place in the relevant criminal justice agencies in order to make technology achieve its purpose, **Peter Gill** looks at police intelligence systems following the Bichard enquiry. He finds that although progress is being made, major obstacles remain and that the "garbage in, garbage out" principle still threatens the effectiveness of key information systems.

But what if the technology worked, the information was 100% reliable, and all ethical and process change issues were considered! Then, as **Russell Smith, Peter Grabosky** and **Gregor Urbas** conclude in their analysis of cases involving the prosecution of cybercriminals, the technologies that facilitate the commission of modern crimes would also provide the best means for investigation and evidence collection as well as future prevention. **Clive Walker** also argues this for the courts processes. However, this scenario requires complete understanding and correct conceptualisation of the problem. Drawing upon the experience of cybercrime, **David Wall** argues that without conceptual clarity, any flaws in the analysis of the 'problem' will become replicated in policies and practices. And in his analysis of emerging problems in digital evidence, **Peter Sommer** observes that

Continued on page 42