11
INFORMATION TECHNOLOGY

11.1 Information technology (IT) is fundamental to modern policing. Without timely, well analysed, accurate information, patrol officers cannot hope to do the job described in preceding chapters. Historically the development of IT in the Northern Ireland police was hampered by pressing demands for funding to support security policing, resulting in transfers of funds from IT budgets to other purposes. By the early 1990s they had fallen well behind other police services in the United Kingdom.

11.2 In 1993 consultants devised a long-term strategy to bring the police up to modern standards. Implementation began in 1994, and included the protection of the IT budget from other policing demands. An outside review in 1996 found that significant progress was being made, but highlighted significant understaffing in the IT department, which was failing to maximise the benefits of improved capital funding.

11.3 In our own review we found that, at the strategic level, the police clearly recognised the importance of a coordinated and properly funded IT strategy but accepted that there was still much to do. A particular concern was that the protection of IT funding, which had allowed progress to be made since 1994, has now been abandoned. At the operational level, officers and civilians also recognised the potential of IT to help them do their job much more effectively, but expressed frustration on a number of key issues. The recent report by Her Majesty's Inspector[1] reflected similar concerns about information technology to those described in this chapter.

Access

11.4 There are approximately 3,500 computer terminals in a police organization of 16,000 officers and civilians, which is seriously inadequate for operational needs. Characteristically of a hierarchical organization, priority has been given to senior officers and support functions before operational officers and their supervisors. Operational officers have very limited or no direct access to IT systems. We found CID officers completely devoid of any direct computer access. Detectives wishing to research crimes and criminal intelligence must instead seek access through administrative support or intelligence officers, some of whom operate only eight hours a day. Uniformed officers have no direct access to IT systems. Operational supervisors have no direct access to the command and control system which logs incidents and holds information on how their officers are deployed. The problem is particularly acute in rural stations, where we found an example of 36 officers having to share a single terminal; and that terminal gave them access only to the command and control system but not to any of the other IT systems in use in the police organization. This lack of access affects not only efficiency but also police morale. We recognize that access to information has to be restricted to those who genuinely need it and that the restricted access available now may be a legacy of the police response to recommendations made in the past to protect information. The current position, however, is that access to computer databases is too restricted not only by policy but also by the absence of computer hardware where it is needed.

[1] **1998/99 Inspection, op.cit.**

Interoperability

11.5 Another key feature of effective information systems is that databases are linked together and can be accessed through a single inquiry. At present many of the key databases held by the police are on separate systems that are not linked together. This is inefficient. For example, an officer wishing to conduct crime and criminal pattern analysis in order to help solve a policing problem has to make several inquiries of several different systems. The police have recently begun to introduce a new criminal intelligence system designed to assist officers analyse crimes and spot patterns. However, this is not linked to the crime recording system, so staff must enter details of crimes twice in order to use the system. A comprehensive information system is needed so that information from relevant databases can be accessed through a single search. This will involve a major reappraisal of strategy and investment for the future. Another area of concern is the absence of linkages with the databases of other criminal justice agencies in Northern Ireland. A project to remedy the situation is now under way and we welcome this.

Training

11.6 Police officers and civilians at both senior and operational levels were critical of IT training. We found examples of staff not being trained in the full capabilities of the systems they are using – for example, administration staff who were unaware that the administration IT system contained an e-mail facility. In the same office only two out of four staff had received any formal training. Training should be an integral part of IT strategy and IT projects should incorporate provision for effective and timely training.

Quality and Suitability of Systems

11.7 Some of the IT systems in use by the police are well regarded by the users, but some are clearly not meeting customers' needs. The office automation system is universally disliked. The absence of industry-standard 'Windows'-based software on this system is a problem; we were told that this was being rectified. We note that, as was mentioned in the 1996 review, there has been a tendency to develop systems in-house, at considerable expense and effort, even when there are good systems available commercially, which are specifically tailored for, or can be customised to police needs.

11.8 The capabilities of many of the systems currently being used in Northern Ireland are limited and disappointing. The crime intelligence system is capable of only rudimentary crime pattern analysis and is not automatically overlaid on a map to make the information easy to understand. In a visit to officers overseeing a murder inquiry we were advised that some valuable computerised crime analysis tools, which are standard issue in the rest of the United Kingdom, were not available to detectives and had to be specially purchased for this inquiry (Special Branch officers already had access to such systems, but colleagues in CID did not). Although the criminal intelligence system is capable of storing digital photographic images, digital photography is not in use in custody suites. Nor is advantage being taken of developments in digital facial recognition, automated fingerprint scanning and DNA technology. Unlike most other United Kingdom police services, there are no computer systems in custody suites. This technology would save time and improve the accuracy of record keeping in this important area.

11.9 The command and control IT system, which should be at the heart of police operations, was

described to us as slow and prone to regular breakdown. We were surprised to find that handwritten station logs were maintained as well as electronic ones. The administrative system known as the Manpower Administration Registry System is also inadequate. It does not utilise the 'Windows' format; and double entries have to be made, for example to close a file and prepare a letter. Documents are primarily stored and circulated on paper and limited use is made of electronic mail and storage. A rudimentary management information system is in operation, but crime figures are between four and eight weeks old when they reach operational officers and managers. Real time automated data collection systems that are easy to interrogate and interpret are required if police managers are to be able to identify problems in their areas, take effective action and be held to account for their performance.

Project Management

11.10 As with other aspects of management in the police, IT management has been somewhat bureaucratic, with several layers of decision-making. IT projects have tended to run late. There has been confusion over the client/contractor relationship, with the Police Authority regarding itself as a contractor in IT provision while the police have been the client. This makes no sense and the arrangements we have proposed for the new Policing Board (Chapter 6) would do away with this complication. We also found that those using the systems felt that they had no opportunity to comment on the sort of systems that needed to be procured, nor was their feedback sought on the performance of the systems delivered so that modifications and improvements could be made.

Communications

11.11 Variations in NATO radio bands require that all police services in the UK and Ireland revise their radio systems by 2002. This provides the police in Northern Ireland with an opportunity to take advantage of some of the best technology now available. The Garda Siochana recently announced that they would be acquiring the TETRA European Standard radio system. TETRA is a powerful system which can transmit data and pictures as well as speech by way of radio and telephone. The rest of the United Kingdom is expected to adopt the same system, and the police in Northern Ireland should clearly do so, so as to be able to communicate efficiently with police in both the Republic of Ireland and Great Britain. We understand that adequate capital provision for a new radio system has not been made. It is needed urgently. A new system will allow officers to spend more time working in their communities and less time filling in forms and seeking information through third parties. The current communications network, with 22 local control rooms and one regional centre in Belfast, is out of date and inefficient. A report commissioned by the police has recommended a move to two or three regional control centres and we firmly believe this is the way forward. Good use of technology will provide a better service to the public and release police officers for patrol work in the community.

A Vision for the Future

11.12 Police services elsewhere, for example Toronto and Boston, are developing the concept of the 'paperless office'. By means of mobile computers or laptops, officers on patrol can input details of incidents they attend, check databases such as vehicle and criminal records systems while on the way to an incident, and communicate electronically with their control centre in exactly the same way as colleagues in police stations. Officers and civilian staff also have ready access to a range of

integrated systems, including those of other criminal justice agencies such as the probation service, prison service and prosecution agencies. This is the product of not only technical hardware but also of a range of information sharing agreements between the police and other agencies. These systems are supplemented by easy access to Internet and – for internal communication – intranet facilities. The advantages of a properly integrated, well resourced and effectively managed IT strategy are self-evident. This is the vision we have for using IT in policing for Northern Ireland.

11.13 *We recommend an urgent, independent, and in-depth strategic review of the use of IT in policing. It should benchmark the Northern Ireland police against police services in the rest of the world and devise a properly resourced strategy that places them at the forefront of law enforcement technology within 3 to 5 years. It should be validated by independent assessment. The strategy should deliver fully integrated technology systems that are readily accessible to all staff, and should take advantage of the best analytical and communications systems currently available. Users of the technology should play a key part in devising the strategy, and in assessing its implementation.* We recognise that implementing this recommendation will have significant resourcing implications. We are confident, however, that investment of this kind will more than repay itself in terms of increasing the effectiveness of policing and the efficient use of policing resources.