THE EMPHASIS OF THIS PAPER WILL BE ON THE PROTECTIVE SECURITY OF assets and installations in which the federal or a state government has an interest. This accords with the broad charter of the Australian Protective Service (APS).

It is obviously no revelation to state that the financial screws are being tightened to shear-point, and security and law enforcement agencies could be asked (or told) to show further savings—probably without visibly reducing service levels and risking criticism from the people we serve. However, to be pragmatic about the situation and to get on with the job professionally, all measures which show enhanced cost-effectiveness without prejudice to operational effectiveness have been sought. These measures include the time-honoured reorganisation of security and law enforcement agencies in order to demonstrate savings. However, the reorganisation process is more attuned to activity rather than productivity. There is merit in staff reorganisation but, unless there are dramatic inefficiencies to be overcome, the resultant disruption to operational patterns and the lowering of the morale of members who resist change can have a detrimental effect on cost-effectiveness—at least in the short term.

Historically, human resources were thrown at any problem with the full expectation that the problem would be solved. This type of usage of human resources is no longer affordable and more cost-effective options are required. The age of technology is here, and will probably remain forever. The correct use of technology, the correct mix of technology and people, and the vision to look a very long way 'down the track' to ensure the money expended today will provide the expected and required solutions in the future are vital aspects of any security program.

Having arrived at the conclusion that a crystal ball with adequate software is needed to give expertise in people/technology mixing, security law enforcement agencies are then faced with the plethora of technology available. Most people are not technicians, and indeed, most people—even those with a sound knowledge of available technology—probably cannot decipher the varied and complex responses to the question: 'How does this technology work?'. User-friendly technology is required.
This paper will briefly recount the genesis of Commonwealth protective security leading to the activities of the Australian Protective Service as it operates in public places in 1991 and its use of technology—including a vision of the future.

**Commonwealth Protective Security**

During World War I—probably as a response to the internment of 'aliens' in Australia—the Commonwealth Police was formed and performed protective security duties by rounding up aliens and holding them in internment camps. Additionally, the Commonwealth Police guarded vital establishments. At the end of World War I, the Commonwealth Police Force was disbanded and the Peace Officer Guard was formed to continue the guarding function. The Commonwealth Police Force was eventually reformed, absorbed the Peace Officer Guard, and in the late–1970s became the Australian Federal Police (AFP), having narrowly missed becoming the Australia Police. The AFP had two components: the *general duties* policing component, and the *protective services* component which in 1984 was transferred to the federal Department of Administrative Services to form the nucleus of the newly formed Australian Protective Service (APS).

The APS started life as a budget-funded component of the large Department of Administrative Services and spent its formative years coming to grips with the dichotomy of having a uniformed, armed, and disciplined service composed of public servants employed under the *Public Service Act* and subject to the Public Service Regulations. Teething problems were inevitable as the APS found its feet, generated its culture, and focussed on providing a service to its clients in consultation with them.

For the first time, clients were asked to enter into a form of contract with their security providers. Memorandums of Understanding (MOUs) were prepared for each client and showed the services to be provided, staff levels and other details. In 1991, the APS receives no direct government funding and all revenue is received from clients who, with rare exception, are free to seek alternative service providers.

The history of Commonwealth security forces has, therefore, seen many changes and, in 1991, the APS is in the best-ever position to be an effective service which will rise or fall on its own merit. This commercialisation has been very challenging as it has focussed attention on providing cost-effective services in response to specific client requirements—the APS does not merely fill rosters with little emphasis on accountability or costs. This commercialisation of services is a vital and necessary process which has propelled the public service headlong into the realities of working both for the client and in their interests.
Public Places

There is no easy definition of a public place—it encompasses extremely diverse areas. The onus is on every landlord, employer, and manager to provide a safe and secure workplace. Add to this the specific need for some businesses to protect the assets of the Commonwealth or state, national secrets, information provided by foreign governments in areas of cooperation such as defence research and communications, and Internationally Protected Persons, and the security net widens substantially requiring very flexible and responsive service providers. The security of public places, therefore, covers many requirements.

Historically, human resources were used to cover all requirements. The more sensitive the area, the more human resources were deployed to protect it. This is still germane in 1991, but to a far lesser extent as cost pressures force the need to exploit other options and to reassess the basic need for security at every installation. The ‘old’ days of ‘meeters and greeters’—convenience gates opened for staff who did not accept the additional walking or driving, or the perceived importance of an establishment deciding the high numbers of security personnel on duty—have either gone forever or are about to be removed from the last of the establishments now coming to grips with the realities of their reducing budgets. To give examples of these areas the following illustrates the client base of the APS:

- category ‘one’ and ‘two’ airports, where the APS provides a counter-terrorist first-response force;
- joint defence facilities at Pine Gap, Exmouth, and Nurungar;
- immigration detention centres;
- defence research establishments;
- diplomatic and consular protection;
- the new Commonwealth Parliament House;
- access control of ‘sensitive’ Commonwealth agencies;
- any other areas demonstrating a ‘Commonwealth interest’. These can be state government or commercial clients; and
- security advice and training services.

The clients cited vary in type from comfortable offices in Australian capital cities to the desert of Central Australia, and the remoteness of north-west Australia. The duties vary from being very authoritarian to being very understanding of other peoples’ problems and demonstrating very high interpersonal skills—as is essential at immigration detention centres, where people of most nationalities (males, females, and children) are held pending a court decision on their status as an Australian citizen. Thus, the definition of a ‘public place’, in this context, is extremely broad. The unchanging element is APS accountability for providing quality services.
The effect of commercialisation has seen some APS clients put their requirements to open tender and the APS not regain their business. Some areas, particularly areas where access and egress control in basic office areas was the sole requirement, accepted the services of the lowest priced tender and switched to commercial services. The APS did not see this as an indication of a lack of faith in its abilities, but rather as a natural concomitant of financial constraints in the 1990s. The managements of these public places practised risk management by reducing the quality, and hence the cost, of their security and accept this reduced service as ‘adequate’. The APS offered only one level of service—the highest. Not all clients need an expensive service level. The benefit to the APS of this experience is that it now has a ‘second tier’ service to offer clients. The APS has officers who are not trained to the original, all-encompassing high standards, are not paid to the same levels, and, consequently, their services are commercially competitive in price. The APS does, of course, maintain its original service tier for those areas which require it. As a result of recent client losses, the APS offered voluntary redundancy to 150 officers nationally. Although the APS is not striving for maximised staff numbers, it is likely that the second tier service will more than recover the 150 staff losses.

To summarise, public places covers such a wide variety of security requirements that each threat and risk assessment sees a mix of solutions (both human and technological) being used. The quality and cost of these solutions is determined by the perceived importance of the particular public place.

**Technology**

Technology can save money and be more cost-effective, OR, technology can be expensive, complicated, unreliable, and put one at the financial mercy of technicians. Both these statements can be true depending on the wisdom of the technology selector or the quality of the advice given to that person.

There is an absolute plethora of technological devices on the security market in 1991. One can buy devices to open safes, close safes, delay safes from opening. One can buy biometric devices which read eyes, palms, and fingerprints. The Japanese have a computerised device which can read the shape of one’s facial features to a very high accuracy in spite of attempts to mask one’s appearance. Intruder alarms can do nearly everything, including make the coffee at the appointed time. Access controls use a wide variety of technology, most involving a plastic card or key (which does not necessarily belong to the user). The only guidance for technology selection the APS has is that the technology must do the job for which it is selected, must do that job reliably, and must be cost-effective. The starting point for determining which technology to purchase, therefore, is always to carry out a thorough threat and risk assessment and only select technology which satisfies the set requirements. Risk management by adequate insurance cover may alleviate the need for security in some areas and this option is not always available to government areas—choosing technology can be a confusing and sometimes frustrating experience.

Technology in protective security is cost-effective and is the way to go, but technology must be very carefully selected and only after it has been seen to operate effectively in a similar situation to that required. The APS has a stated aim of using technology where it can be demonstrated to be more efficient or more cost-effective. The APS does not intend to advocate technology for technology’s sake and the individual client’s needs will always determine which parameter drives the decision.
The APS has invested substantial time and money in developing its technological awareness and expertise. The APS has, for example:

- in 1990, sent two senior officers to Singapore to study protective security in that country. The officers visited organisations such as the Commercial and Industrial Security Organisation (CISCO), the Singapore Police, the Singapore Air Terminal Services Security Organisation (SATS Security Services), the Singapore Port Authority, and a commercial organisation. This visit was found to be a valuable learning process and it was concluded that Australia is in the forefront of both effective security services and the use of technology;

- held a Certificate of Technology course, through the Latrobe University, where the APS qualified a broad range of its officers to this standard. More officers are currently on a similar course being held for TELECOM;

- sponsored financial reimbursement of fees and purchase of textbooks for APS officers undergoing the Associate Diploma of Security Management course at the Phillip Institute of Technology. In Victoria, four officers have graduated from this course;

- entered into joint agreements with commercial companies who are developing leading-edge technology and has assisted them with marketing and promotion of their products;

- a policy of promoting Australian developed and manufactured technology ventures wherever it can. Obviously the APS is discriminating and believes the products it promotes have sound merit. An example is the use of Zone Technology Digital CCTV systems which transmit television pictures through a dedicated or dialler telephone line to APS Central Stations in Canberra and Melbourne. One technology is 3DIS, a three dimensional interactive-space alarm system which uses CCTV cameras, through a personal computer and dedicated software, to provide active freestanding alarm zones which can be drawn, and redrawn around any object or area by the personal computer’s mouse. A sixteen camera installation is currently successfully guarding stabled trains from graffiti vandals in Melbourne;
developed two Central Stations; one each in Melbourne and Canberra. These stations will be certified to National Grade One standard by the end of 1991 and monitor dialler and direct line alarms; and

a dedicated technology officer in the National Office who maintains focus on technological developments and gives advice to regions.

This level of commitment is felt to be necessary if the APS is to provide quality services to public places.

The Future

The future will see far greater acceptance and use of technology in many areas. One has seen the explosion of technology in the information arena; for example, in our homes with video cassette recorders, compact discs, clocks that 'talk'; and in children's rapid acceptance and need for personal computers. Some of the areas security is likely to enter in the future are:

• fully-automated electronic security systems with no human component at the operating level. These systems would provide the necessary controls—be it access/egress control, building opening or closing, or security of assets. All infringements would be automatically reported to a computer program which, drawing on its various databases, would verify the infringement, identify the person or persons responsible, allocate a penalty, and take the necessary corrective action;

• vehicle tracking systems which will remotely display a vehicle's position on a computerised map. Satellite communications would extend the currently available city-based systems to all areas of Australia;

• biometric systems which use DNA analysis to provide identification of people, with no errors;

• perhaps an 'electronic policeman', fitted to every vehicle, which notes the traffic infringements of the driver, transmits this to a centralised police computer which electronically deducts the appropriate penalty from the vehicle owner's bank account and sends out a Traffic Infringement Notice with a receipt attached; and

• remote electronic tracking of people (children) through micro-chip implants. This system is currently used to identify animals, albeit not remotely.

Conclusion

Technology and its uses are limited only by imagination and finances. In the security of public places arena, technology is consolidating its position as a cost-effective alternative to human resources and is positioned to make further inroads in that direction as reliability and cost factors improve. Given the choice between technology and human security, the human factor would always be preferred. Properly trained, managed, and equipped, the security officer can decide a course of action by logically
assessing factors which have not necessarily been pre-programmed or envisaged, can be relied on to act even if not 100 per cent serviceable, and can offer advice based on experience. In the future, the choice of human resources may not be affordable.