Information Technology leads the way

Information and Communications Technology has transformed the way the AFP does business.

Today, computing and communication systems underpin all the organisation's activities, and enable real time communication across the globe.

The AFP had no computers when it began operations in 1979. Electric typewriters were seen as technologically advanced, printed forms were used for data collection and records were maintained in large, leather-bound ledgers. Searching for records could take hours, days or even weeks.

Chief Information Officer Rudi Lammers said it is almost impossible to imagine the difficulties involved in typing up reports on a daily basis.

"We had to manipulate sheets of carbon paper and coloured paper to make our reports in triplicate or quadruplicate, or up to six copies for some reports," Assistant Commissioner Lammers said.

"Typing documents took hours, and any mistakes had to be painstakingly corrected on each individual copy using erasers or coloured whiteout. On the first three copies the letter 'o' was generally a hole in the paper, as you had to hit the typewriter keys really hard to make all the copies legible."

Information Technology (IT), or Automated Data Processing as it was called at the time, first came to the AFP in 1980 in the form of a mainframe computer. In 1984 the AFP's computer centre began operations at the Weston Police Services Complex in the ACT. It's still there, although the mainframes are long gone.

At first the only terminals linked to the AFP's central system were in the ACT, and only one terminal was available in an office. Later, mini-computers were introduced in specialist areas, and it became possible to store, compare and identify fingerprints using computer systems. This led to the establishment of the National Automated Fingerprint Identification System, now managed by CrimTrac.

02

By the beginning of the 1990s there was a clear need for greater connectivity within the AFP. Local Area Networks (LANs) and Wide Area Networks (WANs) were established, but they were not always compatible. A major project to standardise the LAN/WAN environment began, and AFPNET became the backbone of AFP Information and Communications Technology (ICT).

A new era of desktop computing had begun. It improved AFP communications and provided secure connections with stakeholders and partner agencies. It also gave members access to the internet and the overseas network.

But rapid advances in computer technology created new problems. Investigators realised they needed a system to share and manage information more efficiently. In 1997 work began on the Police Real-time Online Management Information System, which we now know as PROMIS.

PROMIS allows police to record and assess incidents, events and complaints. It creates a record of all information and actions relating to an investigation, and allows anyone on the system to enter or search information from any location. PROMIS also gives police instant access to information such as a suspect's criminal history. It is regarded as a world-leader in police computing systems.

Despite the success of bringing AFP networks together, liaison officers posted overseas were still not connected to the AFP's core systems, including PROMIS. Initially a secure dial-in system was established, and over time permanent connections were

01: Members of the first AFP computer investigation course in 1988 **02:** The aftermath of the 2003 Canberra bushfire at the front of the AFP Museum at the Weston Police Complex **03:** A modern computer

installed so that now the AFP's computer systems stretch across the globe.

The success of this approach was demonstrated in 2002, when within three days of the Bali bombings an operations centre connected to AFPNET was established at the scene, providing secure access to all core ICT applications and services, including PROMIS, email and video conferencing.

During 2002 and 2003, the AFP's ICT research and development section worked with a New Zealand company to create a case management and intelligence system (CMIS) as part of the Law Enforcement Cooperation Program (LECP). Initially CMIS was used by the AFP in countries including Indonesia, the Philippines, Fiji, Tonga, Samoa, Cambodia and China.

LECP aims to equip police officers with the skills, knowledge and awareness to better respond to transnational crime.

CMIS is part of the AFP's capacity building program, and has provided overseas policing agencies with a system similar to PROMIS. CMIS allows each country to collect information, to exercise ownership of their information, and to share that information with other agencies that use CMIS.

Another crucial stage of the AFP's technological development was to build systems that allowed AFPNET to be used in the Solomon Islands. This allowed members of the Regional Assistance Mission to Solomon Islands (RAMSI) to access vital information during their deployment. Services to support RAMSI such as RAMSINet have also been implemented as part of the AFP's capacity building program.

While the AFP has experienced some major successes in bringing new technology into the organisation, our reliance on computer systems can sometimes create difficulties. In 2003 the AFP's computer centre at the Weston complex was threatened during the Canberra bushfires.

There was a danger that fire could destroy vital equipment that was helping police to manage the emergency situation. ICT staff had to move essential items while putting out spot-fires around the computer complex.

John Ryles was working in ICT at Weston during the bushfire emergency.

"The impact on the AFP's IT capabilities could have been serious if the fire or the water bombing damaged the systems or the emergency power supply," Mr Ryles said.

"Fortunately the work we did, with help from other AFP members, ensured that the systems were kept running."

As a result of the bushfires, a secondary data centre was established to safeguard against data loss in the event of another catastrophe.

The AFP is continually updating the systems it has in place to meet the needs of a constantly evolving criminal environment. A network for the transmission of national security classified data has been developed, and obtained provisional accreditation this year. This capability will soon be extended through the use of existing networks in other government agencies.

ICT has also developed a number of rapid deployment units to provide satellite communications to the AFP during future International Deployment Group and counter-terrorism operations. ICT has also developed a response capacity that can deliver crucial services within hours of deployment.

And as the march of technology continues, the AFP will continue to develop and implement state-of-the-art systems and processes that enhance capability in the areas of national and international law enforcement.