High Tech, High Art, High Crime

by Brian Minards

GIVEN the eccentricity of the art world it may come as somewhat of a surprise to some, and indeed unforgivable in the minds of the purists, that a number of today's artists use computers, as well as canvas, to express themselves. Recently Australian artist Lawrence Daws, who has been described as one of the leading figures of his generation, held an exhibition of his work in Brisbane. Daws, who began painting in 1943, has taken a new direction and become an enthusiast of the latest high technology.

His exhibition featured not only oil paintings but computer prints. He used a computer system to produce prints which represent the conceptual stages of his work.

Discarding his brush and easel he turned to an Amiga 1000 computer, an Okimate–20 thermal printer, a Panasonic W.V. 1410 camera with R.B.G. filter and a digitiser. Pity the art connoisseur of the 21st century who has to determine whether or not that prize piece is a genuine Macintosh, IBM or Amiga!

However, travelling the world in search of that objet d'art will become a lot easier and less taxing for the same connoisseur, thanks in no small way to the computer.

In the United States recently NASA commissioned the most powerful artificial intelligence on earth, a \$150 million 'Rolls Royce' of computers called NAS (Numerical Aerodynamical Simulator). It will enable NASA aeronautical engineers to simulate the effects of hypersonic airflow on potential designs and eliminate many years of model building and wind tunnel testing. NAS is capable of making 250 billion computations each second. It performs three-dimensional simulations of airflow and thermodynamic effects at airspeeds from zero to orbital against any variety of materials and in whatever shape.

NAS will predict also what would happen to a real spaceplane in environments which cannot be duplicated in a wind tunnel.

It is playing a major role in the development of an aircraft that will slash the flying time between Sydney and London from 23 hours to six hours. Computers are playing an ever increasing role in our lives; in our work, our leisuretime, education, in health care,



Mr August Bequai

travel, in the food we eat, the clothes we wear.

Their benefit to society now and in the future is immeasurable.

Not surprisingly, criminals also use computers. They use them to cheat society for their own gains and, paradoxically, the police use computers to catch them doing it.

Computer crime and manipulation comes in many forms, and for many reasons. Through a network of Soviet spies and business fronts, the KGB's infamous Section T has been stealing over \$1.5 billion worth of America's computer technology annually.

Computer chips, disc packs and valuable software find their way to the Soviet bloc where their use poses a threat to America's security and high tech industry. The US administration, through the FBI and its other agencies, fights a constant cat-and-mouse game to counter the activities of these Soviet agents.

A James Bond sound alike who probably knows most about these kinds of activities is Washington lawyer and former chairman of two US government committees on white collar crime, Mr August Bequai, who was in Australia recently on a lecture tour. Mr Bequai has written eight books and 100 articles on computer crime and says this is just the tip of the iceberg in the burgeoning field of computer technology. He claims that the Mafia in the US is marching into the 21st Century with a growing armoury of mainframes, high speed printers and disc drives. In fact, he says, some lawenforcement officials are warning that the 'mob' is turning to computers to maintain its vast commercial empire.

'There is growing evidence that organised crime is using computers to keep track of its gambling, loansharking, prostitution, fencing and narcotics operations,' he said. 'Likewise, electronic computer EFTS (Electronic Funds Transfer Systems) crimes are a serious and growing problem for the business sector. The Chamber of Commerce of the United States places these losses at over \$100 million annually. Some law enforcement sources place them as high as \$1 billion.'

In spite of whatever safeguards are built into the system, the fact remains abuse still takes place and it is left to the law-enforcement agencies to pick up the pieces once the crime has been committed.

August Bequai said Australia, as a sophisticated commercial country, should be aware of the cost that computer crime represents to the community.

'I don't think your laws are adequate, I would venture to say, and I believe it's a view shared by many, that the Australian mentality has been of an ostrich type, stick your head in the sand and the problem will go away,' he said.

'Legislators should provide police with all the necessary powers so as to effectively enforce the law. With more than 330,000 computers in use in Australia already, there is ample opportunity to cheat the system and the authorities should be looking at introducing sufficient legislative clout to give law enforcement agencies the necessary means to counter computer crime.'

Mr. Bequai said that in the US, 40 states had enacted computer crimerelated legislation and the Federal gov-

ernment had passed two major computer crime Bills. The government had also passed legislation that would make it a federal crime to tap into federal digitised communication lines, which was a far cry from tapping into oral communications, he said.

'As a point of interest, one of your prosecutors said if such legislation was passed in Australia we would be putting people in jail for tampering with digital watches,' he added.

'I can safely say we have passed that kind of legislation in the US with appropriate safeguards to protect the innocent.'

Mr Bequai said Australian law enforcement officers also needed specialised training to deal with computer crime.

'When I see Australian police going to the FBI Academy I don't think it's good enough. Sending two or three people to the US, or elsewhere, once or twice a year is not sufficient,' he said.

'You must set up your own broadlybased training programs dealing with specialised methods to combat computer crime. Fifteen years ago in the US we realised that we had to take the initiative and while we still have too many crimes of this nature they would be far greater in number if untrained people were thrown in the deep end of such investigations. I believe that all too often young police officers who show great promise have their confidence shaken by being assigned cases that are far too complex for them to handle,' he said.

'They become bogged down and start doubting their capabilities and look upon themselves as failures. Inexperienced officers should be assigned to routine cases, by way of an apprenticeship, if you like, before being asked to perform much more complex tasks.'

Mr Bequai added a chilling dimension to computer abuse which poses a threat to life and limb.

'There is evidence in America and Western Europe that clearly shows that terrorists groups have used key computer facilities for their own advantage,' he said.

'Don't for one minute think that all terrorists are disillusioned malcontents who run around shooting people and blowing up buildings; some of them maybe, but their ranks also include well educated people such as engineers, scientists and other, some of whom have computer training'!

Mr Bequai said more than five hundred instances have been documented where terrorist organisations have attacked computer facilities and computer vendors. He said the Los Angeles District Attorney's office had released details of a study that clearly indicated that terrorist groups had used computers to further their claims.

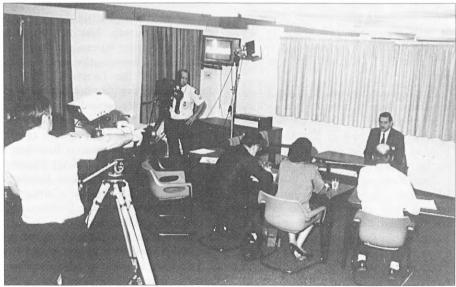
'The Pentagon spends more than \$3 billion of the taxpayers' money each year to secure its computers and is still at risk from the insider,' he said.

'If you pick your target, the drug addict who needs large sums of money to support his habit, the debt-ridden gambler, the womaniser scared of being found out, all can be compromised.'

According to Mr Bequai, in the final analysis it all gets back to basics. 'These systems are only as good as the people who manage and operate them; it is not the computer that commits the crime and causes the havoc, it is the dishonest people who manipulate them,' he said.

On balance the advantages that computers bring to mankind far outweigh the disadvantages and wherever this technological marvel may lead us in the future, who could have guessed that from the humble abacus would evolve technology that would enable artists to expand their horizons, and place the potential for crimes of gigantic proportions at the very finger tips of the unscrupulous.





Detective Superintendent John Mitchell holding a simulated press conference at the AFP College Barton with Sergeant Bill Mackey and Senior Constable Graham Tulk on the cameras



Media Match

Fourteen senior Australian Federal Police officers took part in a three-day media awareness course starting on 5 August at AFP Training College Barton.

The course has been organised to ensure that all AFP officers are better able to deal with the media and respond quickly and effectively to media members' reasonable requests.

The officers, mostly Chief Superintendents and Superintendents, are from the ACT and the regions.

The program emphasised practical 'hands on' training in which for two of the days the officers undertook television and radio interviews organised by media consultants Mr Bill Dowsett and Ms Sue Smith.

The course was organised by the AFP's training staff in liaison with the Director of Information, Mr Philip Castle, who conducted some sections of the instruction.

During the three days, field visits were made to the editorial offices of The Canberra Times and the studios of Capital 7 TV News where the officers saw the final touches being put to news items.

The course is part of a wider program of media training for all AFP officers and recognises the need that to be an effective enforcement body, officers must understand the media and work with it.