AUSTRALIAN INSTITUTE OF CRIMINOLOGY

TECHNOLOGIES OF ELECTRONIC CRIME

Elizabeth Montano
Australian Transaction Reports and Analysis Centre (AUSTRAC)

*Paper presented at the
4th National Outlook Symposium on Crime in Australia,
New Crimes or New Responses
convened by the Australian Institute of Criminology
and held in Canberra 21-22 June 2001*

Thank you for inviting me to speak to you today. I have always found participating in an AIC Conference a very pleasant and stimulating experience and this Symposium is no exception.

I have been asked to speak to you today about "Technologies of Electronic Crime". Before I explore what these technologies might be, I should perhaps explain what AUSTRAC does and why I have been asked to speak on the subject in question.

AUSTRAC is the Australian Transaction Reports and Analysis Centre. We are Australia's specialist anti-money laundering regulator and financial intelligence unit. We follow the money and, after all, except for crimes of passion, money is the motivator. Often the money will provide the trail to follow where more traditional investigative techniques will not.

We also do all this electronically. We collect over 5 million transaction reports a year (mainly from the financial sector), 98% of them are reported electronically and we provide on-line access to our database of 55 million reports to 26 Commonwealth State and Territory agencies. And we give them search tools, both micro and macro to do it.

We also do our own analysis, identifying and profiling to find patterns and networks of interest. The money is often the most visible link – if you can follow it.

Given AUSTRAC' role, it is not surprising that when Commonwealth Agencies identified the need for research on how electronic commerce and its environment would affect the capabilities of law enforcement and revenue agencies, AUSTRAC was asked to lead that work.

I chair the Action Group into the Law Enforcement Implications of Electronic Commerce (AGEC) which comprises representatives from HOCOLEA agencies and the Australasian Centre for Police Research.

And now, to get back to the subject of this presentation, as you can see we've been looking at the technologies of electronic crime for some years now.

And what we've found is that the technologies of electronic crime are, in the main, the technologies of electronic commerce and the wider information economy. When you think about it – why would they be anything else?

The old world adage still applies – crime follows opportunity. And new technologies and the new business models and environments they create provide plenty of opportunities for crime.

I should say that this is not a new phenomenon – in our 1998 Report, the AGEC cited the example of the motor car as a new technology in its day which opened up whole new avenues for criminals.

In the 1920s private cars became widely affordable. This technology embodied the following characteristics:

- affordability – wide spread across socio-economic groups
- speed – cars were much faster than any previously available private transport (ie the horse)
- distance – cars could travel long distances without resting (like a horse would have to)
- carrying capacity – cars could carry much more than a horse
- anonymity – occupants of a car could not be as easily recognised as someone on horse back or foot

The result was significant growth in certain types of crime, including:

- bank robberies and housebreaking;
- abduction;
- smuggling and other transport of illicit goods; and
- theft of cars themselves.

Consequent regulatory and law enforcement countermeasures included:

- introduction of number plates, chassis and engine serial numbers;
- introduction of motorcycle police and patrol and pursuit cars;
- special regulation of goods vehicles;
- improved premises security including burglar alarms and security patrols; and
- improved cross – jurisdictional arrangements.

It is worth noting, that while some of the countermeasures were aimed at specifics new crimes, most were aimed at counteracting old crimes using new technology.

Following this line, our 1998 Report identified that the general characteristics of e-commerce are also the general characteristics of e-crime.

E-commerce is –

global; accessible; automated, immediate; capable of operating without the "collateral info" we have all relied upon in the past; can be hidden from scrutiny through encryption and all these things together create new business models – new ways of doing business.

So why is anyone surprised that electronic crime can be:

- global; criminals can operate around the world literally;
- accessible in ways never before seen and to people who, in the past, may never have led lives of crime;
- automated
  - lots of small crimes can be effected wherein the past that would have been all too hard;
- immediate
  - criminals can move fast!;
- anonymous, or as good as;
- hidden.

And all these things produce variations on old themes – old scams, old crimes done in new ways.

So, just as the motor car became a vehicle for facilitation of crime – so too, all the wonderful new applications, capabilities which we embrace as participants of the information economy, are capable of use by criminals.

But then, that is the risk run everytime a new development occurs. In commercial terms, crime is a risk of doing business and it requires risk management. Not risk elimination, but management.

So, how do we manage the risks associated with the technologies of electronic crime?

If you want a fulsome answer on that one – invite me back to the 10th National Outlook Symposium – but in the meantime – we are looking to the strategies that work now. We are adapting them. Where we find, after analysis that a strategy cannot be translated, we have to abandon it, we move on. New environments will also lead to new opportunities for law enforcement.

And more than ever it is clear that to counter crime, both environmental and law enforcement specific measures must be taken. Our society and its infrastructure need to be hostile to crime.

Getting back to those characteristics of both e-commerce and e-crime;

- they're global; so we get better at working internationally;
- they accessible; so, we engage with the private sector in target hardening
- they're automated; so we encourage better and earlier crime detection and automated anti-crime strategies;
- they're immediate; so we improve the pace at which we can work;
- they're anonymous or as good as - it's in no-one's interests (except the criminals) that this be so, so we build reliable authentication structures;
- they're capable of hiding their contents, so we look for other evidence and clues. We look for the interactions between the physical world and the ether; and
- we develop new business models; new partnerships, alliances and capabilities.

In all this work, we are examining relationships. The relationships between the environments in which crime occurs, the tools available to criminals and the strategies and tactics law enforcement will use.

In simple terms we need: a law enforcement friendly information economy (where public and private sectors play complementary roles); and we need to use the same things that e-criminals use.