Centre for International and Public Law
Faculty of Law
Australian National University

OCCASIONAL PAPER
THE ELECTRONIC REVOLUTION: IS THE NATION STATE REDUNDANT?

John Broome

Paper presented to the Public Law Discussion Group,
Faculty of Law, Australian National University
23 November 2000

THE ELECTRONIC REVOLUTION: IS THE NATION STATE REDUNDANT?

Today much of our daily business involves the use of the Internet and, through it, electronic commerce or e-commerce. We buy products and pay bills over the net. We access information for work, pleasure or to satisfy our curiosity. We have the ability to communicate with friends and colleagues across the city or across the world instantaneously. We have the ability to conduct research without ever visiting a library.

But the revolution in life-style and work for each of us as individuals has been matched or exceeded by the changes this electronic revolution has brought to every sector of the business community. Massive changes in areas such as health, education and entertainment are also occurring.

But what if it all suddenly stopped?

What if the Australian Stock Exchange went off line for a day or even longer? What if the banks, most of whose business customers and a growing number of individual customers use and rely on line services, were shut down by a denial of service attack? What if the credit card systems were shut down and ATMs unable to function for a significant period? The result would be chaotic and the cost immense. A denial of service attack involves the sending of many messages to a site at the same time with the effect that the system is effectively 'jammed'. If the perpetrator of what is a premeditated 'terrorist' attack on the target site decided to repeat the attack at various intervals (and from different locations) the disruption could be maintained for a significant period. Because of the nature of e-commerce the site must be accessible to the public and other businesses so a change of site name is no solution. Business would come to a standstill.

In February this year a denial of service attack was made on a number of high profile US sites including Yahoo. Estimates of the cost vary widely but all run into tens of millions of dollars. And these estimates involve real, US dollars! The Melissa virus is estimated to have cost at least $10 billion in lost business and disruption, including a number of government sites in Australia. The new economy is very vulnerable to attack. And the attack can be initiated from anywhere around the globe.

In Australia the ASX is susceptible to a denial of service attack now that both brokers and individual traders rely on the net to do business. Such an attack would not only cost millions in lost business it may seriously affect the value of the dollar. If a number of financial institutions were targeted at once it would further exacerbate the apparent perception that the Australian economy is old world rather than new. That perception is often cited as the reason for the continued fall in the value of the Australian dollar. In short we would face an economic catastrophe. It is ironic that the extent to which Australia has adopted electronic commerce makes it so vulnerable.

Such an attack would, of course, involve a serious and deliberate act with huge financial consequences. Yet such an attack is not a criminal offence in Australia. At least not as a matter of federal law unless, perhaps, the target of the attack is a Commonwealth-owned facility. The difficulty arises because the sending of messages to such sites is exactly what the operators of such sites want to happen. It is the frequency and volume that causes the problem. However, the UK made such conduct a criminal offence more than a decade ago. While the Commonwealth has still not acted, some Australian states are contemplating legislation to deal with this problem and related criminal activity that could create widespread interruption to our business activities. Why has the Commonwealth been so slow to react? What are the consequences of this inactivity? Can we deal with the issues at this stage or is it too late? These are some of the issues I want to explore. We are at a critical stage. A number of very significant opportunities have already been lost. For reasons that are not apparent the Federal Government has ignored warning signs and advice. The Australian business community, always antagonistic to government action, has been its own worst enemy in not pressing the Government for action.

This failure to act has been made worse because of the continued inability of Australian law enforcement to have the legal capacity, resources and skills to combat such criminal behaviour.

How are we placed at present?

In a word badly. The present position is that we have inadequate laws to deal with computer-related crime. We have little technical capacity within government to investigate such conduct, even if it were criminal. Our major law enforcement agencies, state and federal do not place sufficient emphasis on or deploy sufficient resources to the identification and combating of such activity. In many areas law enforcement is being privatised by both design and inadvertence. Private sector organisations that might be or become the victims of such activity are reluctant to report it for fear of damaging their reputation and because shareholders might ask what preventative strategies were in place, if any.

A great deal of attention is being given to the vulnerabilities of computer-driven systems to sustained attack in what is known as 'information warfare'. In the defence and intelligence communities these issues are being treated very seriously. Yet, as is often the case, technology and capacities that have both military and civilian applications are often given prominence and resources only in the military context. This paper does not address the information warfare issue but its relevance should be noted.

Why is this so?

How did we get into this position, notwithstanding all of the material that told us of the impending arrival of the new economy? Why are we so ill-prepared?

To answer this question we must look at a number of factors:

- the traditional nature of crime and the way crime is investigated;
- the Constitutional and legislative systems under which we operate;
- the need for effective national and international cooperation;
- the privatisation of law enforcement and business resistance to prosecution of offenders;
- the failure to create an effective legal framework for electronic commerce;
- the failure to create appropriate offences to deal with 'new economy crimes' and to ensure existing legal procedures continue to operate; and
- the failure of government, law enforcement agencies and commercial institutions to understand the threat, the urgency for action and to give the issues priority.

The traditional nature of crime and how we investigate crime

Essentially all crime involves physical acts that occur at a place where the law makes such conduct criminal. There has to be a jurisdictional nexus between the activity and the person who undertakes the activity. This is usually a simple matter. A burglary involves the theft of goods and the location of the theft will give rise to the jurisdiction of both the investigative agency and the courts and prosecutors who conduct the prosecution. The same situation occurs for a sexual assault or murder. Crimes such as fraud require that a false representation be communicated to and acted upon by a recipient. Where both criminal and victim are in the same jurisdiction it is relatively easy to identify them and prosecute. Even where they are physically located in different jurisdictions the law has developed rules to determine where jurisdiction to prosecute may lie. Investigation becomes harder because the criminal may not be in the same jurisdiction as the victim. It will be the victim who seeks redress and therefore the police in his or her location that will commence the investigation. They may need to seek assistance

from other law enforcement agencies. But at least there will be identifiable people involved. The same elements are found in drug offences, people smuggling and so on. Even transnational crime, as it is now usually known, has the same familiar elements.

In Australia we have defined organised crime as involving a number of elements such as ongoing activity, a degree of sophistication, the involvement of two or more people and particular types of criminal behaviour such as drug distribution. A different approach is adopted by academics such as Louise L. Shelley in her analysis of the threat of transnational crime. She advocates a description that does not focus on particular offences but rather on the way the crime group operates. Shelly says transnational crime groups are those that:

(a) are based in one state;

(b) commit their crimes in not one but usually several host countries, whose market conditions are favourable; and

(c) conduct illicit activities affording low risk of apprehension.

Crimes that fit this latter characteristic include smuggling, money laundering and drug trafficking. However, in my experience it is often the degree of sophistication that is overstated.

However we define organised or transnational crime, most of us would accept that the kind of criminal offences involved range over:

- Customs offences — smuggling of all sorts of goods, both licit and illicit;
- excise fraud;
- wildlife exports and imports;
- intellectual property offences involving both the theft of intellectual property itself and an attempt to avoid duty or taxes payable in relation to products which have significant intellectual property components;
- corruption of international banking and financial activities;
- people smuggling, which seems to be treated as a single phenomenon but we need to clearly distinguish between those who seek to enter countries illegally as a means of overcoming migration laws and those who enter the country for the purpose of prostitution or to be involved in illegal activities, often under coercion;
- cyber crime and information warfare;
- maritime crime;
- money laundering (although, of course, we need to be careful to distinguish between a money laundering offence itself and the predicate offences which are still an essential element of establishing the money laundering offence in Australia). Whether that continues to be the case will depend upon the Government's response to the Australian Law Reform Commission report on proceeds of crime: *Confiscation that Counts*;
- links with international terrorism (where it has often been suggested that transnational crime takes place to provide funding for terrorist activities); and
- last, but by no means least, is the whole topic of ethnically based organised crime. One example is the Russian mafia. But the generic reference seems inconsistent with the diversity of activities that fall within that general description. Some have argued that there are up to 6000 separate groups

involved in organised crime within Russia or outside its boundaries but with clear connections to Russian criminals. Yet we continue to refer to Russian organised crime as if it were a monolithic (and apparently well-organised) activity. While many of these groups may have contact with each other there is little evidence to suggest that these groups are under common control.

If we look in a little more detail at the criminal activity that is characterised as organised or transnational crime, a number of observations can be made. At this stage I am leaving to one side what I would describe as the computer-related offences (to which I will return later). The following generalisations are true of most, if not all, of the transnational crime which now occupies so much time and effort in law enforcement agencies around the world.

- There is no inherent difference between drug trafficking across country borders and within those borders. It always involves the physical movement of the product from point A to point B with the involvement of a number of participants whose role is to facilitate the movement and avoid detection. Particularly where the borders are arbitrary rather than natural (such as most of western Europe), then the cross-border nature of the offence is merely a man-made element that makes investigation and prosecution more difficult.

- Revenue fraud, which may rely on different taxation regimes in different countries, is no different from the way in which lower rates of state duty within Australia gave rise to the cigarette frauds in the mid 1990s or commercial transactions were contrived (often artificially) to take place in the state or territory with the lowest stamp duty.

- In the case of firearms, there is no difference between the importation of such products into Australia and their movement around Australia. The illegal importation of such products is similar to the movement of unlicensed or prohibited guns within Australia. Yet arms movements are seen as a major transnational crime activity. The essence of the offence is the illicit movement of arms not the fact that it happens to occur across a nation's state border.

- Drug manufacture (for example, Ecstasy) in The Netherlands, and its importation and distribution in Australia, is no different from the manufacture of the same drug in a Brisbane laboratory and its distribution throughout Australia.

- There is no difference between a fraud that occurs where both parties are in Australia and a similar fraud where one of the parties is not.

- Extortion through the threat of product contamination is just as real and just as dangerous whether the contaminated products have been imported or have been manufactured, contaminated and distributed in Australia.

- Finally, money laundering around Australia, using inter-bank transfers, the efficient services of the ASX and the buying and selling of their financial products, is no different than similar transactions taking place between Australia and Hong Kong, Singapore or London.

In short, it seems to me that all the major areas of transnational crime are simply the same serious criminal activities which continue to occur at the national level but where some or most of the participants and elements of the offence will be located outside our borders or the borders of another 'victim' country.

It follows that transnational crime is inherently the same kind of criminal activity that we once called organised crime. And as with organised crime we have tended to accept a perception that such crimes are, because they are transnational, beyond our capacity to detect and prosecute. This absolves us of responsibility if we cannot satisfactorily tackle these tasks. That excuse is used as much by government as it is by law enforcement. In my view it is not the inherent nature of these offences that makes them virtually impossible to investigate and counteract but our failure to develop the skills, legal tools and devote resources necessary to the task.

That said, we need to recognise that the reality of organised crime may be quite different from the perception. Sometimes careers have been made on the basis of perceptions about the nature of a criminal threat, rather than an analysis of it. That can be said of law enforcement agencies across the globe.

So it occurs to me that we may have in fact created an image of organised and transnational crime that is different from the reality. Previously we have been looking, for example, for high-level participants within criminal organisations (or as the politicians insist on referring to them 'The Mr Bigs') that simply do not exist. This is because these groups are not the hierarchical organisations that require a nominal or actual head. They tend to have loose structures and less formality than the commonly perceived model.

And finally, perhaps we have created a problem by suggesting that transnational crime is so sophisticated, so organised, so assisted by corruption that we cannot win and therefore our failure is both inevitable and excusable. This is not to suggest such criminal activity is not very serious. It is. It **is** difficult to investigate and prosecute. It **does** involve levels of sophistication and the use of technology. It **does** have very serious effects on the community. And we **must** continue to vigorously attack this criminal activity. These criminals often possess rat cunning rather than sophistication. They are resilient and prepared to rapidly change their methods of operation. They rely on fear and intimidation. But whether these crimes occur at the national or transnational level, they are, conceptually at least, capable of investigation, prosecution and conviction, provided we are armed with the necessary weapons.

The Constitutional and legislative systems in which we operate

While this is well known to each of you there are a few features which are of particular relevance to the problems of effective handling of electronic commerce. The difficulties of the Constitutional limitations on *effective* Commonwealth/state legislative schemes have been the subject of a great deal of consideration by all three arms of government. These problems have bedevilled the legislative schemes that underpin the National Crime Authority and the Australian Securities and Investment Commission. I do not accept that we have made sufficient effort to address these problems, certainly so far as the NCA is concerned. We simply have to be more creative and effective.

These problems are not insurmountable if the range of Commonwealth Constitutional powers were used. Leaving aside the external affairs power (which I would not do) the corporations and telecommunications powers provide fertile ground for development. This is clearly the case in relation to electronic commerce and its effective regulation and the creation of appropriate offences.

Secondly, the Commonwealth has long seemed loath to enter the area of criminal law whenever it could leave the issue to the states and territories. After all, law enforcement and prosecutions are an expensive business. Yet the present Government is at best inconsistent in its approach. It intervened against the Northern Territory legislation in relation to voluntary euthanasia, but declined to deal similarly with mandatory sentencing. It intervened in relation to on-line gambling but refused to take part in the development of a national regulatory approach to the same subject where its powers to legislate would have greatly assisted the enforcement of such a scheme. It intervened in relation to in vitro fertilisation to enable state law to prevail over the Sex Discrimination Act, with the result that Australians in different states have different rights.

There are many areas where the piecemeal approach of the states precludes effective law enforcement. The Commonwealth refuses to sponsor a cooperative national approach for no apparent reason. The deficiencies faced by law enforcement include:

- No cross-jurisdictional framework for the use of listening devices, controlled deliveries or the use of assumed identities.

- Relatively few resources applied to the investigation of organised or transnational crime when

compared with total law enforcement expenditure. Even in organisations like the AFP (which claims national pre-eminence in this field), a careful analysis of its expenditure will show that much of the AFP's budget is spent on community policing in the ACT, protection of dignitaries (both local and foreign), peace-keeping in other countries, the investigation of various activities such as the leaking of official documents and, decreasingly, fraud against various government programs.

- The structure and procedures of the legal system almost guarantee that very substantial amounts of law enforcement budgets are wasted, while outdated rules remain, defence disclosure is not required and witnesses wait endlessly to give evidence.

- There have been substantial changes in the amount of material that must be provided to the defence with no analysis, of which I am aware, that these changes have made any substantive difference to the quality of the judicial system.

- Jurisdictional and inter-agency conflicts adversely affect the overall success of law enforcement because, at least for some, who gets the result is more important than getting the result.

- Our proceeds legislation in most states and at the Commonwealth level is inadequate. This has been known for years and was the subject of analysis by the Australian Law Reform Commission (ALRC) in a report that was tabled in 1999. Yet despite the obvious evidence, subsequently accepted by the ALRC, there are still those who argue that the present regime, with its central tenant of post-conviction confiscation, is the appropriate legal regime.

While there have been considerable efforts to enhance cooperation and the collection of evidence, the fact remains that progress has been particularly slow in many areas. The Commonwealth Government has been slow to respond to issues, does not show leadership and when it does act seems disinclined to involve the states and territories, as for example in its National Illicit Drugs Strategy.

The need for effective national and international cooperation

This is self-evident. But at the national level it is simply not occurring to a satisfactory level. Given the jurisdictional problems that arise from our federal system it is essential. But cooperation only occurs when an agency sees a benefit for that agency. Public benefit is not considered. In large part this is due to political pressure for local or agency-specific, rather than national, priorities to be addressed. It is community policing issues that concern voters and therefore politicians, particularly at the state level. On the other hand at the federal level interest has tended to be on border issues.

Internationally, there is now a considerable body of treaties, both multilateral and bilateral, to which Australia is a party, that provide a basis for mutual legal assistance. The procedures are inevitably cumbersome and time consuming. This is necessary to ensure that the evidence that is finally recovered through those processes can satisfy all of the necessary local hurdles for it to be admissible in Australian courts.

Having been personally involved in the negotiation of bilateral and multilateral treaties I understand the difficult issues involved, including the need to work in different legal systems.

The success of transnational crime has more to do with the lack of capacity in law enforcement agencies than the organisational skills of the transnational criminals. I do not mean that those involved in the agencies lack dedication, skill or knowledge. What they do lack is the necessary infrastructure, equipment, resources and legal framework with which they could successfully counteract transnational crime.

Where transnational crimes are involved, the procedures involved in collecting and exchanging evidence are ponderously slow. Some of the difficulties include:

- The entire resources of Interpol in Lyon devoted to organised crime amount to five people, while an additional three are looking at money laundering.

- Whatever the original potential for Interpol, it has been significantly undermined by the creation of regional cooperative arrangements, such as Europol, which members see as having more commonality of interest and providing greater protection for information which is shared through these agencies.

- UN conventions, such as the 1988 Vienna Convention and the current draft convention on organised crime, together with declarations on issues such as money laundering, have illustrated a significant commonality of purpose across the globe. But it has taken ten years to develop a draft convention on organised crime. Even when it is settled it will no doubt be some years before it comes into effective operation.

- Notwithstanding that an international court to deal with criminal matters is self-evident, inevitable and necessary, the fact remains that the court has yet to be established. More than half a century of genocide, war crimes and crimes against humanity, let alone transnational crime, have failed to move the international community to establish an effective regime to deal with cross-jurisdictional crime.

- Multilateral and bilateral treaties providing for mutual legal assistance have been established but any of us with experience in their operation know that notwithstanding some successes, the reality is frustrating delays caused by resource restrictions in both the requesting and requested states. Indeed, there are often concerns expressed by central authorities to reduce the scope of requests for fear that large-scale requests may need to be dealt with on a reciprocal basis.

I recognise that in a number of these areas some action is being taken. But what is being done is too little too late.

Given the enormous publicity about transnational crime during the last decade, it is remarkable that there has been virtually no legislation enacted federally to enable us to deal with these issues better. For reasons outlined above, enhancing our capacity to deal with transnational crime will inevitably assist our capacity to address domestic crime.

In other words, transnational crime is successful because it is hard to investigate and prosecute with our **present** tools. Not because the kind of activity that we have labelled in this way is extremely complex, sophisticated, hard to identify, investigate and prosecute, but because we are ill equipped to do so.

In relation to electronic crime, the Australian Government has not been involved in international fora dealing with this issue. The Council of Europe draft treaty on Cyber Crime is presently being drafted. Australia should seek to be part of these discussions and be prepared to be a party to this and similar treaties. There are precedents for such an approach. It is a party to the European Convention on Mutual Legal Assistance. It has been involved in the negotiation of the various United Nations instruments that are in preparation but devoted too few resources to these activities. The Government's attitude to other UN instruments will not enhance our role or credibility in these discussions.

But we need to think laterally about how we deal with offences which take place in an instant and where the perpetrators may have moved their location a dozen times before the first request from Australia has been drafted and dispatched through the diplomatic channel. Given that we have been largely unsuccessful in dealing with traditional crime, we will be even less successful if we seek to combat electronic crime with the same processes.

The privatisation of law enforcement and business resistance to prosecution of offenders

This is an issue which has received very little comment but which is of fundamental importance in determining the extent to which and the way in which serious crime is investigated.

The reasons for this movement are complex. And they involve both the public and private sectors. Over the last decade the capacity of the Australian Federal Police to investigate federal offences has been diminishing. This is a consequence of reduced real budgets, a failure to publicly and privately (within Government) articulate priorities based on actual capacity and the resultant growth (by default) of capacity within other agencies.

As to the last issue, there is a real chicken and egg situation involved. Agencies have been forced to fill the void created by lost AFP capacity, often by employing former police who have left the AFP. This leaves the AFP increasingly unable to respond to calls for investigative capacity. But at the same time the AFP seems to have accepted this loss of core business without complaint. Partly because it cannot investigate all offences and partly because it sees this move as implicit, if not explicit, Government policy and does not oppose it.

The present position is that frauds of upwards of $400,000 are simply left to agencies to investigate unless there are obvious political imperatives. Agency heads have legal obligations under the Financial Management Act so they are forced to outsource these matters to private companies. These include the 'big five' accountancy firms or other specialist firms. The Government has endorsed standards for training fraud investigators but these are not enforced, so far as I can ascertain. If the investigation proceeds to the preparation of a brief it goes to the DPP. In the event that the brief is deficient it may well be impossible to retrieve the situation. If there are evidentiary problems they may be irrecoverable, evidence may have been lost or destroyed. More importantly, such investigators do not have police powers, access to police equipment or databases and the capacity to liaise with other government agencies. Nor should they. The result may be second-rate investigations and a loss of expertise as the police do not have a range of matters to develop their skills base. There are exceptions such as those involving smaller amounts where there are political factors involved. In fact a great deal of AFP resources are devoted to such sensitive matters as telecard frauds or leaked documents, almost always without success.

We therefore have a less-skilled AFP investigating less offences and less prosecutions, as DPPs cannot accept low-quality briefs. Any discussion with DPPs will confirm the reduced quality of briefs and the reduced number of AFP generated prosecutions.

In the private sector the position is of even more concern. There is substantial evidence that major criminal action is not investigated at all for fear of adverse publicity. This is the case in the banks and other financial institutions. It also occurs in other major companies. Many of the major accountancy firms audit horizontally, not vertically. That is they do not attempt to drill down to confirm that the transactions for which there is a paper trail actually took place. This is a recipe for fraud. Where an investigation does occur, prosecution of major offenders is unlikely. Minor offenders are, of course, prosecuted with enthusiasm. Excluding police from investigating and using private firms achieves this result.

The principal concern seems to be banks where there is resistance to any prosecution that will hurt the public image of and shareholder reaction to the bank by disclosing shoddy or inadequate procedures. Yet rigorous prosecution of fraud should increase public confidence. There is a similar position in relation to credit card fraud. Here fraud is allowed to run rampant through a reluctance to impose procedures which may add some inconvenience but which are paid for by higher interest rates.

Industry prosecution or support for investigators is rare. Macquarie Bank's strong support in relation to the prosecution of one of its staff for insider training is a notable exception.

A similar reaction could be expected where there was an attack on a company's IT system, particularly if this had involved a successful extortion attempt. There is a real risk companies will pay up and leave the problem for someone else to address.

The failure to create an effective legal framework for electronic commerce

It is clear that we do not have the appropriate investigative and legal framework, both domestically and internationally, to tackle traditional transnational crime. That is obviously of great concern. How much more concern should we have about our state of preparedness to deal with transnational computer-related crime? This is the real challenge for law enforcement in the twenty-first century.

This is not a new threat. Some have foreseen its possibilities for a considerable period. The new economy has arrived, but the laws to protect it, the structures to investigate crimes against it and the capacity to prosecute such crimes have not been developed.

Let us look for a moment at the kind of problems we are facing. John Geurts, a federal agent with the AFP, provided some staggering statistics in a speech in September 1999. Geurts claimed that:

> Industry analysts predict that e-commerce, which involved transactions of $7 billion during 1998, is expected to grow to $300 billion globally by 2002. The Australian Government predicts e-commerce will grow by a factor of ten by the year 2000 and keep growing. The current size of e-commerce can be determined through industrial analysis. In an industrial survey involving 55,000 Australian and 27,000 international Internet users, 25% had shopped on-line more than once, with another 13% having shopped once on-line. Australian on-line shoppers spent some $139 million on-line in the 12 months to July 1998. The largest products are books, music as well as software.

If the Government's prediction about e-commerce growth in Australia were correct, then in 2000 almost $1.5 billion would have been spent on-line in Australia. My guess is that that figure will prove to have been significantly understated.

Much of the concern about e-commerce has been related to issues such as security of credit card information used to purchase on-line. That is a genuine concern. But it is not where I believe the major threats will come in relation to transnational computer crime.

Our real vulnerability is that our whole commercial structure now depends on the successful operation of computer networks **all the time**. The same can be said of government. Most government agencies would no longer possess a typewriter! Yet in the event of a power failure or a denial of service they will effectively be unable to communicate with the rest of the world except by long hand and Australia Post! The fax machine will not work and, of course, there will be no e-mail.

In February 2000 we saw the consequences of a serious denial of service attack on major US web sites. Unknown individuals, from unknown locations, who may well have worked alone, were able to close down sites such as E-Trade and Yahoo for a number of hours. Press reports have suggested that these attacks are the subject of FBI investigation in the US and of AFP investigation in Australia. According to some press reports smaller-scale versions of the denial of service attack affected unnamed Australian sites. The problem is that there seems to be no offence on the statute books concerning such attack, at least in Australia.

On 12 February 2000, the Minister for Justice and Customs released a discussion paper relating to computer offences. This coincided with the denial of service attacks in the USA. The discussion paper is part of the development of a Model Criminal Code.

In the discussion paper a number of new offences are proposed. According to the Minister 'these new offences address a number of short comings in existing offences. They recognise the fact that the

criminal law cannot remain the same for even a reasonably short period if it is to genuinely reflect a change in society'. Note the Minister spoke approvingly of the content of the 'new offences' as if they reflected either actual offences or at least proposals approved by the Government. Yet the press release went on to say that none of the proposals reflected actual policy. The Government had not, at that time, formulated its policy and was merely asking for public content on the discussion paper. By the end of the year the issues were the subject of consultation with the states and territories. I have no problem with consultation but as these issues fall squarely within Commonwealth legislative competence why delay?

I agree with the Minister's analysis of the proposals but not with her failure to act. The difficulty is that the existing computer crime offences in the Commonwealth Crimes Act are a decade old and have not been reviewed despite enormous changes in technology and the widespread prediction of the potential for disruptive conduct during that time. Indeed, the process by which the Model Criminal Code is being developed and implemented can best be described as thorough and painstaking because it had its origins in reports by Sir Harry Gibbs in the 1980s and the Code is still being developed. Some aspects have been legislated but it has taken almost two decades.

I commend to you the elements of the Discussion Paper concerning computer crimes. It seems to me to provide a very sensible analysis of the need for offence provisions relating to denial of service attacks and other computer crimes but we must expect that it will be some years before we will have such laws enacted, particularly if the recent pace of legislative reform is maintained and legislation is needed in each jurisdiction.

In the second part of the Model Crime Code discussion paper, the issue of geographical jurisdiction is analysed. I found that analysis to be a depressing catalogue of the conspicuous failure of Australia's legal system to address the modern world.

For example, a scheme was developed by the Solicitors-General, endorsed by the Standing Committee of Attorneys-General and implemented in a number of states, to ensure that the antiquated common law rules of jurisdiction were overcome where all of the elements of an offence could be established, albeit that they did not all occur in one jurisdiction. Australian judges, despite the clearest possible statement of legislative intention, have conspicuously ignored it. What courts across Australia have demonstrated is a clear preference to ignore the unequivocal language of the statute and to return to the dark ages of jurisdictional difference between the Australian colonies.

As the discussion paper itself says

> the history of criminal law reform in Australia, including that of the consideration and implementation of the recommendations of this Committee, shows that the goal of uniform criminal laws has been illusive, particularly when dealing with laws which provoke highly emotive debate. Australians can expect disuniformity to continue in relation to such areas as gambling, drug law reform, uniformity, age of consent for sexual behaviour and the like.

Since the Discussion Paper was released there have been further developments. In March the police commissioners at their annual conference 'decided to place the issue of electronic crime firmly on the law enforcement agenda and to urgently develop a strategy to enable timely and effective policing responses to future issues and challenges'. The inevitable steering committee and working party was established. In November a report entitled *The Virtual Horizon: Meeting the Law Enforcement Challenges* was released. In fact it is a scoping paper that identifies the kind of problems and issues we are facing. There is still no strategy. The Australasian Centre for Policing Research paper contains some assessment of the present state of our legislative readiness to address these issues. It demonstrates how far we have to go in dealing with new concepts, adapting old ones and dealing with procedural legal issues. There is still no clear legislative attempt to deal with the need for a proper regime to search computer databases.

If we cannot achieve uniform criminal laws between the Australian states, what chance have we got to combat transnational crime in general and computer crime in particular?

But there is a second area of concern. That is the failure to provide a legal regulatory framework for e-commerce. This involves issues such as the potential loss of a significant part of the taxation base as old economy businesses operate in cyber space where the question of who is entitled to tax profits becomes a very real issue. This is an area being addressed in bodies like the OECD but the simple problem of on-line purchases avoiding the GST illustrates the nature of the problem.

At a more fundamental level there is the absence of a simple legal framework for e-commerce sites. We have a well-developed system to regulate corporations. The basic company structure brings with it the need for registered offices, an address to serve documents, legal sanctions for failure to comply with Corporations Law requirements and so on. Yet we have allowed Australian web sites to be issued willy-nilly by a private company (which grew out of a university cottage industry). There is no requirement that commercial sites can only be registered where a registered business is identified. We have lost the capacity to effectively translate a great body of business practice and law into the electronic commercial world. Nor do we have well-developed legal rules relating to the identification of parties who use e-commerce. The recent Electronic Transaction Act 2000 facilitates commercial transactions but leaves many issues such as authentication unresolved.

I appreciate that there are current moves to create new domain names that will be safer and overcome some of the failures to regulate the dot coms. But this is again being done in large part at the private level with Melbourne IT and not the Australian Government primarily involved. The new domains such as '.biz', '.museum', '.pro' (for professionals) will apparently require greater verification of the identity of the operators and their *bona fides*. But this will be left to the market and not a regulator. The ASIC should have taken on for dot coms the role it performs in relation to company registration. The growing problems in this area were the subject of a report to the Attorney-General almost four years ago. It is apparently still on his desk. The National Office of the Information Economy (NOIE) has taken some initiatives to look at issues but these are driven by a desire for systems of self-regulation. The market cannot protect the public interest.

The failure to create appropriate offences to deal with 'new economy crimes' and to ensure existing legal procedures continue to operate

I refuse to accept the excuse that it is all too hard. That compromise (and not at the level of the lowest common denominator) cannot be achieved. That so-called states rights interests override those of the Australian community. The fundamental role of government is to provide for the peace, order and good government of society. By not providing a basis on which we can successfully tackle these problems, our governments have failed at the most fundamental level.

To anyone who says that agreement is impossible, because it is too complex or involves some abrogation of sovereignty, I say that this is rubbish. One simply needs to examine the history of the European Union, particularly over the last ten years. The development of uniform rules within the European Union in a range of areas shows that jurisdictions with vastly different social, cultural and legal histories can reach agreement where the Commonwealth and the Australian states and territories have failed. We cannot expect the world community to deal with these issues while we have such a tardy domestic record.

Sometimes I wonder whether this lack of preparedness for governments to govern in areas as critical as these, is the unforeseen consequence of an unquestioned commitment to 'small government'. Or is it a fundamental failure to understand the issues and the importance of them to our national economic well being? These issues are fundamental to the efficient and profitable operation of our economy, yet this point seems to be lost on those in Government.

In February 1998 the Prime Minister, the Hon John Howard MP, opened the ICPO-Interpol 15th Asian Regional Conference. In specifically addressing the question of transnational crime the Prime Minister said:

> Transnational crime is now a serious security issue which has been recognised by Interpol's new observer status at the United Nations. But there is only so much that governments can do either in isolation or collectively. Treaties may be important but all the agreements in the world cannot replace the indispensability of cooperation between law enforcement professionals. You, as individual police professionals, will always be the most important element in defeating international crime.

It seems to me that the Prime Minister is both right and wrong. There is a limit to what governments can do. It is true that the level of cooperation between law enforcement professionals is essential to the investigation of transnational crime.

But much more can and must be done by governments than has been the case to date. And law enforcement professionals cannot cooperate if the legal systems in which they work are so encumbered by procedural difficulties that it becomes virtually impossible, if not actually impossible, to collect, transmit and use admissible evidence. In his second Inaugural Address Bill Clinton spoke of the need for governments to govern. He pointed out that the problems of discrimination and inequality in American society could only be solved by government taking a leading role. You cannot expect the market to develop policy and implement law. Markets will not regulate behaviour, certainly not in the public interest. Light-handed regulation and self-regulation are the current buzzwords. I have yet to see an example of self-regulation effectively protecting the public interest.

In any event, as things stand at present, the criminals involved in transnational computer crime can do so, far away from the place where the action is felt. A person, who wishes to extort vast sums from the business community, by threatening to disrupt computer transmissions, can do so via satellite, from the open sea, and ensure the disruptive messages pass through a number of jurisdictions before reaching their eventual target. It is a very real possibility indeed that companies, faced with the threat of catastrophic disruption to their business, may well succumb to extortion in circumstances which will be much more difficult to investigate than recent examples of product contamination. We are ill prepared and going backwards.

My concern about the failure of Australian governments to deal with these issues is highlighted by the fact that the Model Criminal Code discussion paper actually proposes a model to deal with computer crime that was developed by the UK Law Commission in the 1980s and is reflected in the Computer Misuse Act 1990 (UK). That is not a criticism of its content, rather a comment on its speed of evolution.

Essentially, the UK legislation seeks to:

- protect data and programs from unauthorised access;
- prevent criminal activity consequently upon unauthorised access; and
- protect the corruption of data.

It will be clear that these principles do not deal with the denial of service problem. That requires a fourth element that prevents the intentional disruption of a computer service. The discussion paper specifically rejects the notion of an offence of sabotage in relation to computer systems (except perhaps in a national security context) but does make strong recommendations in relation to the need for offences relating to the impairment of electronic communication. Whether, however, a maximum penalty of imprisonment for ten years is adequate is debatable.

I understand that a final report will shortly be released. This will reflect consideration by governments of the responses to the discussion paper. We might expect legislation to be introduced next year. It also seems likely that as with other elements of the Model Criminal Code exercise the states and territories will also legislate. Indeed New South Wales has already announced its intention to legislate. Why? There is a clear Constitutional basis for the Commonwealth to legislate. It should do so. We cannot afford the potential difficulties of jurisdictional problems that are unnecessary and preventable.

In the recent denial of service attack, Yahoo is reputed to have lost almost $700,000 in revenue during the few hours that its system was closed down. Imagine the likely penalty for someone who had stolen $700,000 from, say, a bank. I venture to suggest that Australian courts would be unlikely to impose a similar penalty in relation to computer crime. Indeed, the evidence strongly suggests that the larger level of fraud or commercial impact, the lower the period of imprisonment. The Alan Bond case is but one example.

So we need to not only provide an appropriate legal framework, but we need to do something to ensure that the seriousness of these offences is reflected in the sentences that are imposed. Our present domestic legal systems and law enforcement structures and our international treaties and agencies have proved inadequate to deal with transnational crime in the twentieth century. I fear they will prove even less so this century unless significant advances are made and made rapidly.

The lack of urgency

The real challenge is to develop a national and international response to computer crime, which has an element of urgency that reflects the real social and economic threats that we are facing. It is, of course, essential, that we critically and correctly analyse the nature of the problems that we are facing. But we have to be prepared to legislate and, if necessary, amend legislation to respond to emerging threats.

The business community is noticeably missing from this debate. Unless and until they are engaged there will be no appreciation of the urgency of the situation by government. Law enforcement is not good at engaging with the business community at the national level (it does this much better at the community level) but it needs to do more. This must be one part of the proposed strategy. But governments must govern. They must take the lead. The market cannot regulate, legislate, properly investigate or prosecute.

Is the nation state irrelevant?

Is the nation state irrelevant in dealing with computer crime? No. At least not yet. It is still the basic polity that must engage in the international debate and be a party to the necessary international instruments to react to these threats. But there is a growing tendency for the role of governments to be subjugated to the interests of corporations. For the role of government to be outsourced or privatised to the extent that the very advocates of such policies find that the protection they want from government is no longer provided. Do we want private international police services to grow up? Do we want corporations to reach agreements to conduct private investigations outside the knowledge or control of governments because governments cannot or will not provide the necessary capacity?

Our government has to respond to these challenges. If it does not it will be increasingly irrelevant as groups within a community reach global solutions to these problems. We may well see internationally the development of private police forces. Indeed there are many firms which now investigate crime outside of established legal frameworks, often working for governments as well as the private sector. The problem arises when such bodies use techniques and technologies which are not legitimate in the country in which they operate.

What must government do?

The elements of a successful strategy to deal with electronic commerce are really quite obvious. They include:

- Acceptance by all Australian governments that electronic commerce must operate within a satisfactory legal framework and be protected by adequate laws;

- Develop a regulatory structure for registration and operation of e-commerce sites. Make ‘dot au’ a synonym for the safest sites in the world to do business;

- Place regulation of e-commerce squarely within the jurisdiction of ASIC and resource it accordingly;

- Develop and implement, as a matter of national urgency, a comprehensive set of laws to protect consumers and deal with criminal conduct using the Internet;

- Ensure that there are effective offences to deal with damage to data, interference with sites and misuse of data;

- Enable our law enforcement agencies to be equipped with the ancillary legislative tools to facilitate investigations such as effective search warrant laws, cross state powers and adequate interception capacity, including the ability to obtain access to encryption keys;

- Provide law enforcement with the technology, skills and resources to properly investigate computer crime;

- Encourage the business community to be part of the solution not part of the problem by reporting criminal conduct and assisting prosecutions;

- Recognise that we need to develop a system of mutual legal assistance that is set in the twenty-first century not the nineteenth century. This means allowing electronic requests, electronic transfer of material, electronic authentication, and providing the resources to enable requests to be actioned quickly;

- Apply some of the available military technology to deal with the imminent threat to national well being and economic security posed by electronic crime;

- Participate enthusiastically in the various international fora seeking to deal with these issues and become parties to relevant international treaties.

These issues are of fundamental importance to our economy and our capacity to operate effectively as a nation. Governments can no longer ignore the issue, or respond by creating committees. It is time for a serious response. Resources will be needed, but in a country with the capacity of Australia these are simply not an issue if we have the correct priorities. We can commit billions of additional dollars to national defence, fixing rural potholes and developing new tax systems. We must be able to find the millions, and the cost is not that great, to have an effective, skilled and resourced law enforcement capacity able to protect business activity in Australia. That capacity needs to be augmented by a legislative and diplomatic response commensurate with the importance of the problem.

It is now time for action.