Computer hacking can compromise political process

by Dr Amy McGrath - 26 September 2001

Voting results can be corrupted in transit

"As the data file is shifted from the local to the central area I can put in a Trojan Horse program that says I am the central agency and you shift it to me. I take that file and modify it however I wish and put it back in and send it off. There is perhaps a three or four second dely in the process. But nobody is going to know that the file which arrives at the other end is not the file that was put in at the begining. It is very common and easy to do and well understood technology for computer people."

"Truthfully, any system can be hacked. So insider and outside hackers are possible but actually 90% of the computer crime is done by insiders."

Quotes from Professor Mary Micco, University of Pennsylvania, USA
Lecturer graduate program on electronic fraud

Robbers once, computer hackers now, in our politics

. . . A merry-go-round of break-ins

What a merry-go-round of 'break-ins' politics has been in Australia - into premises of MPs or Senators, into police station cells (by collusion) or parliamentary stores where marked-up rolls are kept, into electorate and Electoral Commission offices, into packages of ballot papers or ballot boxes, even into garages to firebomb cars. Until recently these were physical break-ins.

Such was the rare bombing of bags of votes in the electorate offices of Badgery's Creek and Gladesville just before declaration of the poll in these marginal seats that the ALP won by 107 and 260 votes in the close-run 1995 NSW State election. In Badgery's Creek a plate glass window at street level was smashed and a firebomb thrown in. In Gladesville, the arsonist climbed onto the roof by a ladder he brought with him, jemmied open an upstairs window then threw the firebomb down into the office. Security guards damped the fires in both cases but an unknown number of Legislative Council and referendum papers were destroyed or damaged.

Concern? Outrage? Media headlines? Nothing anywhere but in the local press. Official inquiries? None. Only the NSW Electoral Commissioner, Mr L Dickson, protested but his protest only reached the *Illawarra Mercury (April 8, 1995):*

"It is a bit serious when you get a petrol bomb thrown through an office window at 3:00 am. They must have known what they were after. It is unprecedented to have attacks on electoral offices. I am not aware of any in Australia in the past 20 years and it should be a matter of concern."

Such also was the theft in 1988 of computers and software found later in a vacant house in an adjoining lane, from the NSW Electoral Commission headquarters in Darlinghurst, Sydney. The official view was there was no electoral data of value on these computers, but others have questioned this. They were not reassured by the fact detectives were strangely brought in from distant Liverpool and later lost their notebooks, or the fact the computers were in Australia Post mailbags.

But these break-ins were physical, leaving a trail like the notorious intrusion into Watergate, the Democratic Party headquarters in the US, more important for the 'cover-up' that followed than the offence itself. Now we are experiencing invisible electronic break-ins in Australia, two of them stumbled on by chance, that must also be judged by the 'cover-up' they have provoked than the enormity of the offences involved.

The first from December 17, 1992 - January 10, 1993 was an intrusion into the computer network of the Australian Electoral Commission (AEC) at the highest level, by a Brisbane IT student at the University of Technology, Tim Cooper.

The AEC's own 'Statement of Facts', when Cooper pleaded guilty and was sentenced in a Brisbane District court almost **four** years later, was that his hacking "had resulted in the AEC network being seriously disrupted, and the computer systems and communications facilities attached to it having to be disconnected and shut down. This further meant that members of the AEC were unable to carry out their lawful duties and required diversion of AEC staff to attend to the investigation of the incidents and ratification of the problems."

Not a word of Cooper's hacking had been heard from the AEC over the intervening four years. Not even by their own Divisional Returning Officers, who had a chaotic time trying to enter late enrolments and ballot counts in the weeks after during the 1½ hours ration permitted. Nor by the ABC analyst, Anthony Green, who protested vehemently at the two hour long, and lesser breakdowns, in transmission to the tally room at critical times during the count on polling night. Nor by the Joint Standing Committee on Electoral Matters (JSCEM) of the Commonwealth Parliament to which it was accountable. *(Details are given in an appendix at the end of this article.)*

Not a word was offered by the AEC either when Cooper was first charged on November 3, 1995 or when he was found guilty and sentenced in a Brisbane District Court on December 20, 1996, not indeed until the Chairman of the JSCEM sought comments from the Australian Electoral Commissioner, Bill Grey, on an article of December 29, 1996 in the Brisbane Sunday Mail saying:

"This is a matter of concern to members of the Committee, especially as it may impact on the issue of electoral integrity. The Chairman is also surprised that this matter had not been brought to the Committee's attention by the AEC."

The AEC offered this extraordinary excuse, which was inexcusable given that transparency should he at the heart of anything touching the democratic process.

"The AEC did not raise the eventual conviction of the offender with the 1996 JSCEM because the events leading up to his conviction did not relate to the 1996 federal election. In addition, the investigation of the matter during 1993 and 1994 by the AFP and the AEC, under tight confidentiality, precluded any reporting of the matter to the 1993 JSCEM. The AEC was advised at the time that any publicity about the investigation could make the AEC a possible target for other intruders. Further it was clear that the 1993 federal election was not in any way affected by this security breach. Nonetheless, the then Minister for Administrative Services and his successor after the 1993 election, were both briefed on the incident (both ALP MPs)."

The *"Yes Minister"* soothing assurances flowed - full testing, no material damage, no access to electoral roll data, counter measures conducted in consultation with the Defence Signals Directorate (DSD) the Australian Federal Police (AFP) Telecom, the Australian National Audit Office (ANA0) and the AEC computer suppliers. All those people in the know. Yet the last people to know were the people most affected - the MPs and Senators who stood to win or lose by any such computer fraud.

Questions remain in the wake of the AEC's uncharacteristically brief apologia.

- Why did Cooper begin his hacking immediately after the ELMS management system had been finalised in December 1995?
- How did he know the secret phone numbers of two of the only three members of the Australian Electoral Office of the AEC in Brisbane, who were not Divisional Returning Officers?
- How did Cooper have passwords changed each fortnight of AEC employees?

- Why did he choose to 'hack' one of the most boring of systems on offer?
- Why did he intrude into the ballot count as the AEC consultant Michael Lightfoot admitted *(Australian National Review October 1997)?*
- Did he hack into the AEC's computer again when caught operating in a very much more sophisticated way through university computer systems in 1995 shortly before the next election?

Has the AEC told us the whole story? Can its assurances, that its systems are 100% secure from hacking fraud, be believed? Experts in the US and our media say no. For example Mr Duggie warned in the New Yorker (November 7, 1988 p.44)

"Computer operators do not leave fingerprints inside a computer; the events that occur inside it cannot be seen, and its records and printouts can be fixed to give no hint of whichever of its operations an operator wants to keep secret. The practical problem of the computer is its invisibility .. whether or not elections have been stolen by computer before, some citizens and some officials are asking if it could happen in the future … Could people acting for political reasons or personal gain, steal House or Senate seats, or even the White House itself?"

Has Timothy Cooper told us the whole story? *The Sunday Mail (29-Dec-1996)* threw out this mysterious hint when reporting on Cooper's case.'"After his court appearance yesterday his mother, Mrs Cooper, said her son had been through a lot and the truth was not all known."

Could the truth he that he was not acting alone but for others? But the thought is not ludicrous. After all Stephen Mills in his book, about *'The New Machine Men',* of the 1970's Wran government, listed computer hackers among them.

“Pollsters, advertising agents, TV time buyers, media consultants, **computer hackers**, psychologists, group discussion leaders, direct mail writers, lobbyists and Party officials. **They are in the business of winning elections**. We have only a slender knowledge of how politics is actually conducted today, and who is conducting it; we know little because these jealously competititive practitioners have told us little."

In any event, Cooper blocked off any chance to find out. He refused to answer questions on legal advice at all times, and, having pleaded guilty, was not cross-examined in court on December 10, 1996 when Judge Skoien released him on bond, with a suspended sentence, praising him for having spared the Crown a long trial.

Could JSCEM members tell if they had not been told the whole story?

“Computer fraud is full of difficulties and technicalities not easy for the layman to understand. A person who had knowledge of the computer system probably has the greatest opportunity for committing fraud. The disgruntled employee is the greatest danger still to his employers. Other categories of workers, by virtue of their knowledge, can post the threat of fraud to the computer-based organisation: ex-employees (who know the organisation’s systems and procedures) former employees re-employed as agents or consultants, contract programmers and outside software experts." *(Fraud and Abuse of IT Systems R. Doswell and GL Simons p.26).*
And there are plenty of the latter in AEC operations.

Can the AEC really guarantee it cannot happen again with all its firewalls and encryption security? Peter Neumann, a US computer expert, warns us:

“Even if you can look at the source code, you can't guarantee that there's not a Trojan horse embedded somewhere in the code. Any self-respecting system programmer can hack the innards of the system to defeat encryption techniques, or any password protection … In the election system the vulnerabilities are enormous. You have to trust the entire staff of the corporation producing your software."

Notes On The Unix System Used By The AEC

- Unix vendors such as IBM, Digital and NCR had been developing clustering technology for years giving their systems very high availability
- They were closely associated with the Internet
- 24 hour Internet demonstrated the reliability of Unix-based servers
- Unix machines were compatible with almost any microprocessor available - Unix was good for large-scale data processing
- Unix vendors had scored well in the market through close association with the Internet

Appendix - Computer Hacking of Timothy Cooper

Timothy Cooper hacked into the AEC computer twice shortly before elections - during December-January 1992-3, and November 1995 - the first a month before the issue of the writs, the second, three months before.

Events before the March 1993 federal election

Cooper's hacking from two months before issue of the writ 1992-3

- Between December 17-January 15, 1993. Cooper backed into computer systems operated by the AEC and Deakin University
- On January 21 Australian Federal Police executed a search warrant at his Birkdale, Brisbane home. They seized his computer, modem and related items, finding:
  - full host name of the AEC Hope computer, its X.25 and AARNet IP addresses
  - modifications to it, comprising counts 3 and 4 of the subsequent indictment
  - details of the AEC Victorian Tower computer
    - X.25 address, passwords of two user accounts allowing root access to that system
    - all legitimate user accounts of the UNIX system
- On February 3, Cooper attended AFP headquarters at Milton with a solicitor. He answered no questions about his computer hacking activity on legal advice.
- No charges were laid until August 23 1996 in the Brisbane Magistrates Court. No judgement was made until December 1996, exactly four years later.

Effect *of* hacking on computer systems *of* the AEC

Count 1 against Cooper

a) On January 6, 1993, someone rang a computer systems administrator in Canberra, Mr. Kanwal Singh, received a complaint that the AEC's Hope Computer was being used improperly at 7:00 am . He found that the intruder

- logged into the Sequent Hope computer (connected to the public *Telecom AUSTPAC X.25)*
- used the user name of an AEC employee to do so
- further used that name to alter a file to conceal his login identification
- attempted to change the 'bin' account which would have allowed widespread access to the Sequent Hope computer system

b) At 8.30 pm that day Mr Peter Spelman, one of three members of the AEC's Brisbane office with access to a phone number connected to the AEC network, rang Mr. Singh to say his number had been constantly engaged from an unknown source. The next day it was also engaged several times over, three times from 7.30 to 9.30 pm.

c) On January 8, Mr. Singh:

- changed user passwords
- enhanced monitoring software to record events on the two main Sequent systems
- disconnected the X.25 communication network from the Internet
- however he could not disconnect the X.25 network (WA/Tasmania used those links)

Count 2 against Cooper

On January 10, 1993, Mr. Singh noted a log-in at 2:00 am that morning, which had gained access to the Hope system via Austpac.X25 using a different password by another AEC employee. He checked all existing rile systems on Hope, Tennyson and Tower computer systems for alteration. An analysis of the system backup tapes revealed that alterations to the computer system, involving these programs, occurred between 11 December 1992 and January 7,1993.

Count 3 against Cooper

The computer hacker had altered a file known as the **Ipsched.sav** file, which contained routines giving him use of a 'root' access shell, and allowing him to modify the system logs to delete entries in the wtmp file which should have recorded his presence on that system on January 6 and 10.

Count 4 against Cooper

A hacker had inserted a new **Ipsched.sav** file into the system.

a) This was the original Ipsched.sav program stored under another name in a directory in which it did not belong.

b) If a user tried to write the legitimate program using its original name, the illicit program would execute it under the new name and the user would not know.

c) The new Ipsched.sav file was probably used to alter the wtmp file of the Hope Sequent computer as it failed to record the presence of Cooper on that system on January 5 and 10, 1993.

Counts 5 and 6 against Cooper

Two unauthorised files were inserted into the Victorian NCR Tower computer. No legitimate user would have any reason to install them on that system. They severely compromised security on the AEC system.

Count 5 **- Edit.c file**
This program gives a hacker access to the most powerful of all accounts on the Unix computer system (the root account sometimes called the superuser account) which allows the system administrator, and other authorised users:

- to carry out almost any activity on the system
- to conceal his actions from administration staff and legitimate users

Count 6 **- Login.c file**
When the hacker installed and executed this file (a modified version of a UNIX login program), he could login to the system without a password because it captures the login names and passwords of legitimate users, and saves them into another file.

Counts 7 and 8 January 14, 1993 only involved Deakin University

Cooper charged for new offences on October 3/November 3, 1995

Charges on October 3 for 12 offences committed in January 1995 for hacking into the University of Melbourne Computer and Connect.Com.au Pty Ltd using other persons' computer accounts under the Queensland Criminal Code and the Commonwealth Crimes Act 1914

Charges on November 3 for nine offences under the Commonwealth Crimes Act, 1914 over hacking into the computer systems operated by the University of Melbourne and the Collaborative Information Technology Research Institute.

“A Federal Police spokesman said the new charge related to Cooper allegedly accessing the internet using University of Queensland and University of Melbourne accounts.”

Timothy Cooper was charged on all counts. 23 August 1996

Eight indictable charges were brought against him in the Brisbane Magistrates Court, linked to new charges, on August 23, 1996. In the meantime he accumulated fresh charges during 1995.

Nine indictable offences on November 3, 1995 under the Commonwealth Crimes Act 1914 while on bail awaiting sentence on the 12 charges on November 24, 1995, which also involved Cooper.

Twelve indictable offences during January 1996 hacking into University of Melbourne and Connect.Com.au Pty Ltd, five under the Queensland Criminal Code, seven under Commonwealth Crimes Act 1914.

A further six offences on June 21-22, 1996 involving the all-night computer laboratory at the Queensland University of Technology.

Hearing of Charges on December 20, 1996 in District Court

As Judge Skoien pointed out on December 20, 1996 “these offences began in December 1992 and continued through until June of this year. You were sentenced by me on November 24 for similar matters. While you were on bail and awaiting your sentence on those matters you committed further offences. You have breached your bail, you have breached a good behaviour bond, and you have breached probation.”

Cooper's Sentence by Judge Skoien SJ. December 20 1996

Conditions of judgement

- A suspended sentence of imprisonment. A' global' sentence of three years for all charges

  “you have flouted the criminal law. You have treated the criminal law with contempt.”
- immediate release on condition of good behaviour for five years

  “You have saved the taxpayer a great deal of money. Had you wished go plead not guilty to these offences the trials would have been lengthy and very complicated and very expensive."

  “You have caused great expense to the institutions concerned and the taxpayer.”
- provision for the bond to be varied at any point in its duration
- forfeiture of equipment and reparation to specified institutions

Reasons for judgement

The Judge admitted the psychiatrist's report influenced him when he was wavering.

a) youth and his blameless background

b) his computer hacking was of the 'look-see 'type, a mixture of intellectual curiosity and the excitement of being able to do it

c) it was comparable to the behaviour of an obsessional or addicted gambler.

d) it did not involve fraudulent conduct (stealing intellectual property)

e) it was not his primary intention to harm others, although in fact he did so greatly.

f) his 'nasty experience' of custody warned him what to expect if he offended again.

g) he had a steady job lined up in this 'field in which you have a great deal of talent.'

Report of case - Sunday Mall Queensland December 29, 1996

Prosecutor Mr. Frank Walsh said Cooper's invasion of the Australian Electoral Commission's computer system in 1993 had the potential to cause enormous difficulties for the Government.

Cooper had used his skills to invade the AEC's system via the Internet. He had gained access to the system at the highest level, which would have enabled him to install programs and alter existing programs and data in the system

The AEC's system included the electoral roll of 11.5 million Australians. It also enabled fast counting on election nights and was used for payroll details of some 50,000 casuals employed on election night.

His activities were discovered by the Federal Police just before the federal election of March 1993 was announced. A lot of extra work, checking to ensure Cooper's invasion had not compromised the integrity of the AEC's computer system, was caused.

The Chairman of the Joint Standing Committee on Electoral Matters Requests an AEC Response to the Sunday Mall article

According to the above report, two systems were involved, that of the enrolment system and that of the ballot count management

In his response to the JSCEM Mr. Paul Dacey, (then AEC's Assistant Commissioner Election & Enrolment Division, now Assistant Commissioner) Cooper had 'set up trapdoors into the AEC's enrolment system during that period. Procedures were immediately put in place to ensure that in fact that could not happen through the development of stronger firewalls." Elsewhere he said 'a hacker did not get into the AEC;s enrolment system'.

Does Mr Dacey mean us to believe that Cooper had successfully opened a trapdoor gateway into the AEC's enrolment system, but had not been able to use that gateway between December 17, 1992 and January 7, 1993 when Mr Singh first began to act to frustrate his hacking? Action that took much longer than could be defined as 'immediately'.

In his response to the JSCEM Mr Dacey made no mention the hacker had intruded into the ballot count. This emerged in a letter by Michael Lightfoot, a consultant to the AEC involved, commenting on an article in the *Australian National Review* (July 1997) traversing the disruption caused throughout the entire election process to enrolments, ballot counting and management of divisional offices. In Mr. Lightfoot's view Cooper had not intruded into the enrolment system but only into the ballot count

Cover-up by the Australian Electoral Commission

The AEC did not report the affair to the Commonwealth Parliament, its Joint Standing Committee on Electoral Matters, the States, the parties, the members and Senators of the Divisional Returning Officers who were most seriously affected. Their response?

"Many DRO's are hurt and angry that even today they have never been advised of the fact that an unknown number of unknown people could obviously access their Divisional Rolls and manipulate data after hours in their own homes. Why were they given access (in all states but one) by a public telephone line as in the case of Messrs Spelman and Brockman whose modems were usurped? Who gave authorisation for this procedure? What security was in place?"