



## National Information Infrastructure Protection (NIIP) and the Role of IDS.

**Professor William J (Bill) Caelli, AO**  
 Professor Emeritus – Information Security Institute  
 Queensland University of Technology  
 &  
 Senior Consultant in Information Assurance,  
 International Information Security Consultants Pty Ltd (IISEC)

**RAID-2007 Conference**  
**5-7 Sept 2007**  
**Gold Coast, Queensland**  
**Australia.**



7 Sept 2007
(c) W. Caelli
1

### **National Information Infrastructure Protection (NIIP) and the Role of IDS.**

Professor William J (Bill) Caelli, AO  
 Professor Emeritus – Information Security Institute  
 Queensland University of Technology, and  
 Senior Consultant in Information Assurance,  
 International Information Security Consultants Pty Ltd (IISEC)

Phone: +61-7-55782255 Fax: +61-7-55273255 Email: w.caelli@iisec.com.au

IDS has taken on major significance in relation to critical infrastructure protection (CIP) particularly when enterprise information systems are interconnected with data acquisition and control systems (DACS), such as SCADA based sub-systems, used to manage major utilities such as power, water etc. Compounding the information security problem is the fact that at the same time those enterprise information systems are facing two new and specific information assurance challenges imposed by an increasingly mobile workforce, using enterprise information systems from mobile phones, PDAs, laptop computers and the like through unprotected wireless access points, and the development of those enterprise systems around service oriented architectures (SOA) based on a web services ("Web 2.0") structure. Placement, management, control and monitoring of IDS/IDP systems thus takes on new importance along with the policy, regulatory and legal environments under which they operate, particularly where the majority of a nation's critical infrastructure and its associated national information infrastructure are privately owned and operated. Questions arise as to best usage of IDS/IDP systems in this environment along with the ethical and legal obligations placed upon enterprise management. This paper builds upon almost 5 years of experience in Australia's Trusted Information Sharing Network (TISN) through its Information Technology Security Expert Advisory Group (ITSEAG) to analyse the technical and policy/legal aspects of IDS in the CIP/NIIP environment.

## National Information Infrastructure Protection (NIIP) and the Role of IDS.

1. TISN – Australia
2. The Threats
3. Fear of information warfare rising ?
4. Some Developing Themes
5. The Challenges to NIIP
6. Conclusions - Policy Changes



7 Sept 2007

(c) W. Caelli

2

### Professor Emeritus William J (Bill) Caelli, AO

BSc (Hons) N'cle, PhD (ANU), FACS, FTICA, Fellow of (ISC)2, CISM (Hon), Sen. MIEEE

Prof Bill Caelli is a **Senior Consultant** and **Director** of **International Information Security Consultants (IISec)** (See: <http://www.iisec.com.au>) and **Professor Emeritus / Adjunct Professor** in the **Information Security Institute (ISI)** at the **Queensland University of Technology (QUT)**, Brisbane, Queensland, Australia (See: <http://www.isi.qut.edu.au>). In 2005 the ISI incorporated QUT's **Information Security Research Centre (ISRC)**, a research centre of which he was the **Founding Director** in 1988. He is a member of the **"IT Security"**, and chairs the **"Futures"**, Expert Advisory Groups (EAG) of Australia's **Critical Infrastructure Advisory Council (CIAC)** established under the Australian Government sponsored **Trusted Information Sharing Network (TISN)** (See: <http://www.tisn.gov.au>). He also serves on the advisory board to Australia's **AISEP** (Australian Information Security Evaluation Program) which involves the security accreditation of information technology products and systems under the international **"Common Criteria"** (IS 15408). He has been a member of IFIP's Technical Committee 11 (Information Security) since 1984 and is a Board Member of the USA's **Colloquium for Information Systems Security Education (CISSE)** and a co-director of its Asia-Pacific affiliate (**CISSE-AP**).

He has over 44 years of experience in the ICT industry, with over 33 years involvement in information security and cryptography, including the provision of extensive consultancy services to both the public and private sectors in Australia and internationally. He co-founded **ERACOM Pty Ltd** in 1979, a company that developed and marketed advanced, integrated cryptographic systems and information security products around the world. These products and systems particularly addressed the information security needs of the banking and finance industry. The company was purchased by SafeNet Inc of the USA in 2005.

In 2007 he was made the **world's first Fellow of (ISC)2**, and also received the **"William Hugh Murray Founders' Award"** from the CISSE **"for his outstanding contribution to information assurance education"**. He is a **Fellow of the Australian Computer Society (ACS)** and the **Institute for Combinatorics** as well as being a **Senior Member of the IEEE**. He is an **Honorary CISM** of ISACA. In 2002 he was presented with the **Kristian Beckman Award** by IFIP's Technical Committee 11 for his international work in information security. He received the **Pearcey Medal** in September 2002 for his lifelong work in and contributions to the ICT industry. Computerworld Australia has designated him as a **"Computer Pioneer"** and Business Review Weekly (BRW) has nominated him as one of Australia's **"Top 100 Smart"** people.. In Queensland, he received **"The Queensland Premier's Individual Contribution Award"** in 2000.

He was made an **Officer in the Order of Australia (AO)** in the January 2003 Australia Day honours list for his services to the ICT industry and education/research in information security.

He received his PhD from the **Australian National University (ANU)** in Nuclear Physics in 1972. Professor Caelli's research and education interests lie in trusted computer systems and networks, cryptography and its integration into systems as well as in the legal, social, historical, policy and political aspects of information security and, in general, development of the ICT industry and related matters. He has had a long entrepreneurial interest, and real experience, in the development of the ICT industry, particularly in Australia as well as acting as a technical due diligence consultant in business acquisition and development activities internationally.



# TISN

## TRUSTED INFORMATION SHARING NETWORK



7 Sept 2007

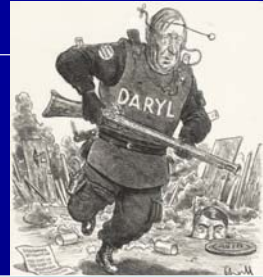
(c) W. Caelli

4

The Trusted Information Sharing Network (TISN) is a forum in which the owners and operators of critical infrastructure work together by sharing information on security issues which affect critical infrastructure. It is made up of a number of Infrastructure Assurance Advisory Groups (IAAGs) for different business sectors, and overseen by the Critical Infrastructure Advisory Council (CIAC).

URI - <http://www.tisn.gov.au/agd/www/TISNhome.nsf> at 31 Aug 2007

## TISN – AUSTRALIA - BACKGROUND



The Hon. Daryl Williams, AM QC  
Attorney-General for Australia 1996 - 2003

## NII in Australia

- 1997 – DSD Report
- 1999 – Australian Federal government policy statement
- 2001 – Business Government Task Force on CIP
- 2002 – Task force recommendations (6)
  - Establish TISN

7 Sept 2007

(c) W. Caelli

5

The Hon. Daryl Williams, AM QC - Attorney-General for Australia 1996 - 2003

26 August 1999

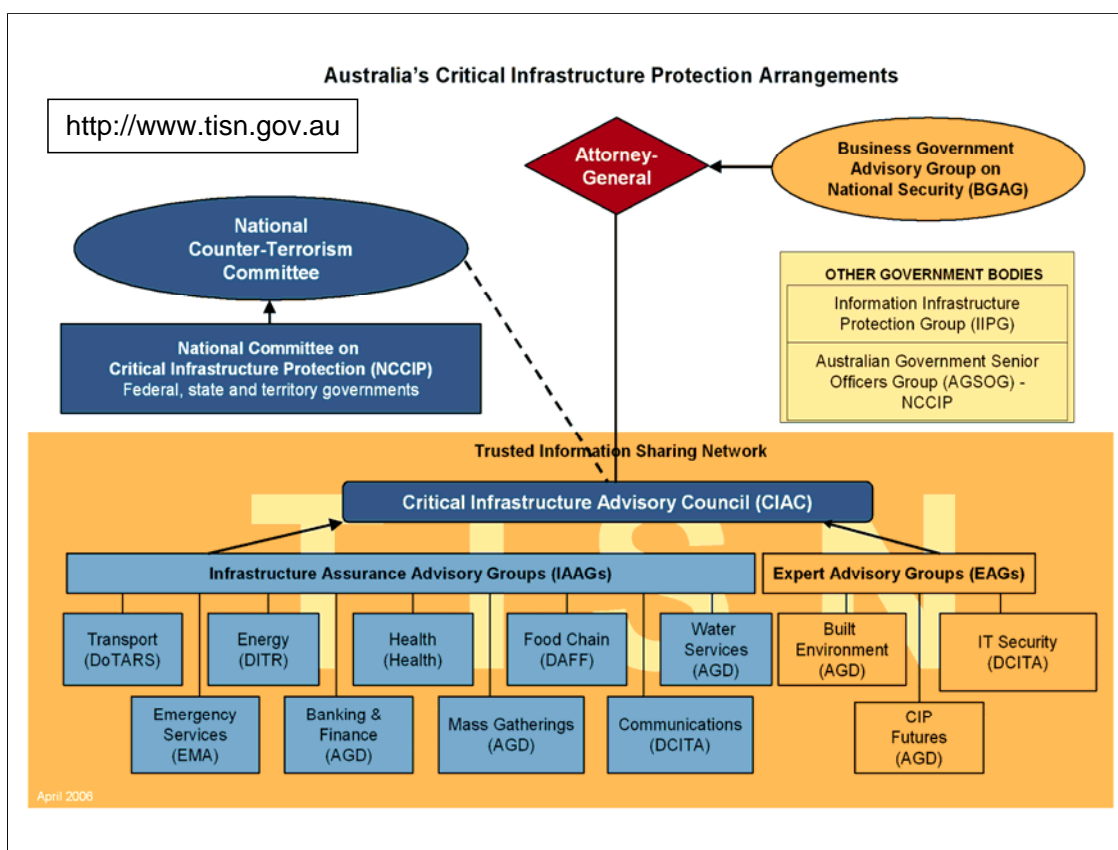
### **PROTECTING AUSTRALIA'S INFORMATION INFRASTRUCTURE**

I am pleased to announce that the Government will implement measures to protect the National Information Infrastructure (NII). This decision follows Government consideration of an interdepartmental committee report intended to carry forward a preliminary examination of the issues undertaken by a Defence Signals Directorate (DSD) consultant. The NII is the grouping of information networks essential to our society's well being. It comprises telecommunications, banking and finance, transport and distribution, energy and utilities (electricity, oil, gas and water), information services, and other critical government services including defence and emergency services. While Australia's developing information economy brings many benefits, we must also make sure that it does not leave us open to new kinds of threats. It has been widely recognised that the kind of damage that could previously be inflicted by organised, well-resourced groups could now be inflicted by an individual using a personal computer and a modem.

As society becomes increasingly interconnected, the vulnerability to attacks from hackers, criminals, terrorists or hostile foreign powers increases. The Government recognises that the NII extends beyond Commonwealth systems and it places great importance on working with the private sector and the States and Territories to develop appropriate protective measures. We have adopted a five point strategy intended to:

- develop cooperative arrangements between public and private sectors;
- integrate electronic and physical protective security and response arrangements;
- encourage further development of a response capability in both the private and public sector;
- build a threats and vulnerability data base; and
- develop review arrangements.

The strategy being pursued recognises that both the public and private sectors have an important role to play in ensuring the effective protection of important infrastructure and that coordination is needed to achieve this. To implement the strategy we will establish a framework to coordinate Commonwealth action through a standing interdepartmental committee and private sector arrangements through a consultative industry forum. The private sector will be involved in developing protective security measures. We will also work with the States and Territories to ensure their involvement in development of protective security. In developing our response to the emerging threats, we have consulted a number of governments including the US, UK and Canada and will continue to work with these and others government so we can respond to a truly global threat.



### History of Critical Infrastructure Protection : Protecting the National Information Infrastructure (NII)

In August 1999 the Australian Government released its policy on NII protection. This was based on the report of an interdepartmental committee set up following a report by the Defence Signals Directorate in 1997. As much of the NII is privately owned, this policy recognised the need to build cooperative arrangements between the public and private sectors. Because of the borderless nature of cyberspace, it also recognised the need to build strong international linkages for NII protection.

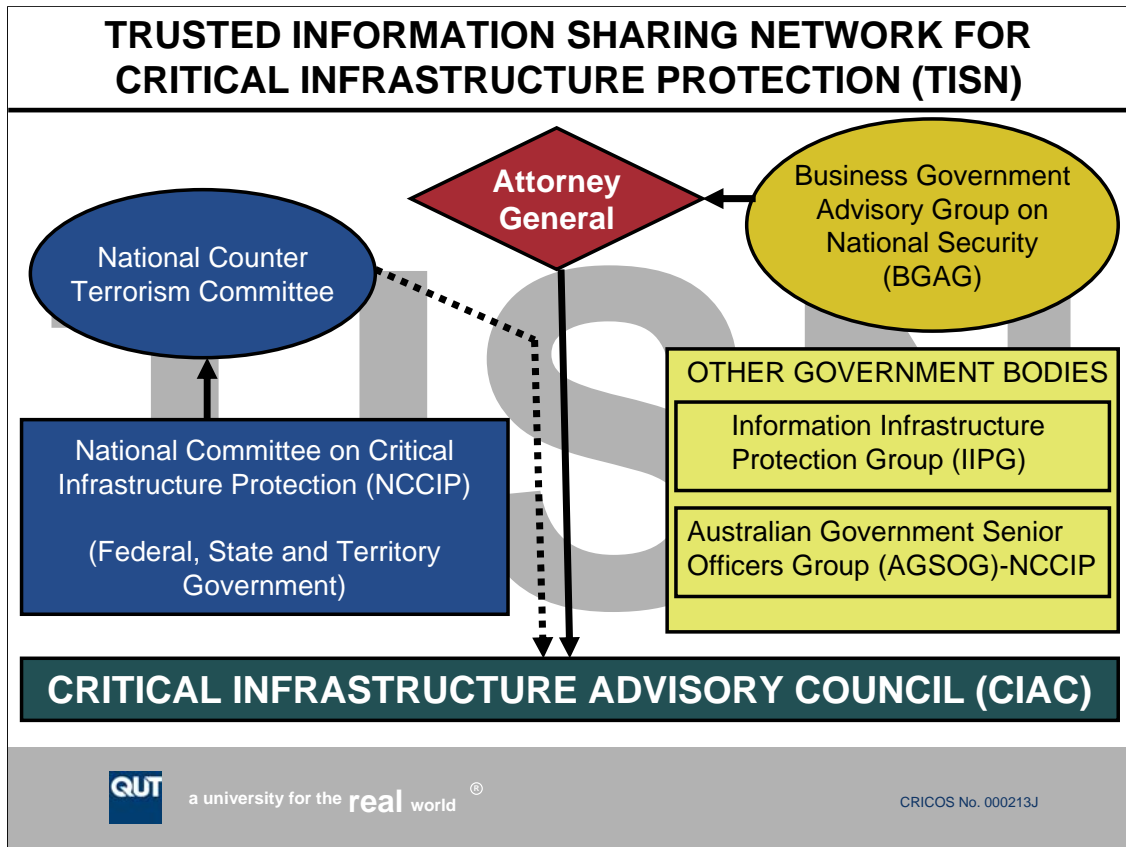
The legislative program relating to cyber-security included the Cybercrime Act, which came into force in 2001 and the Security Legislation Amendment (Terrorism) Act in 2002.

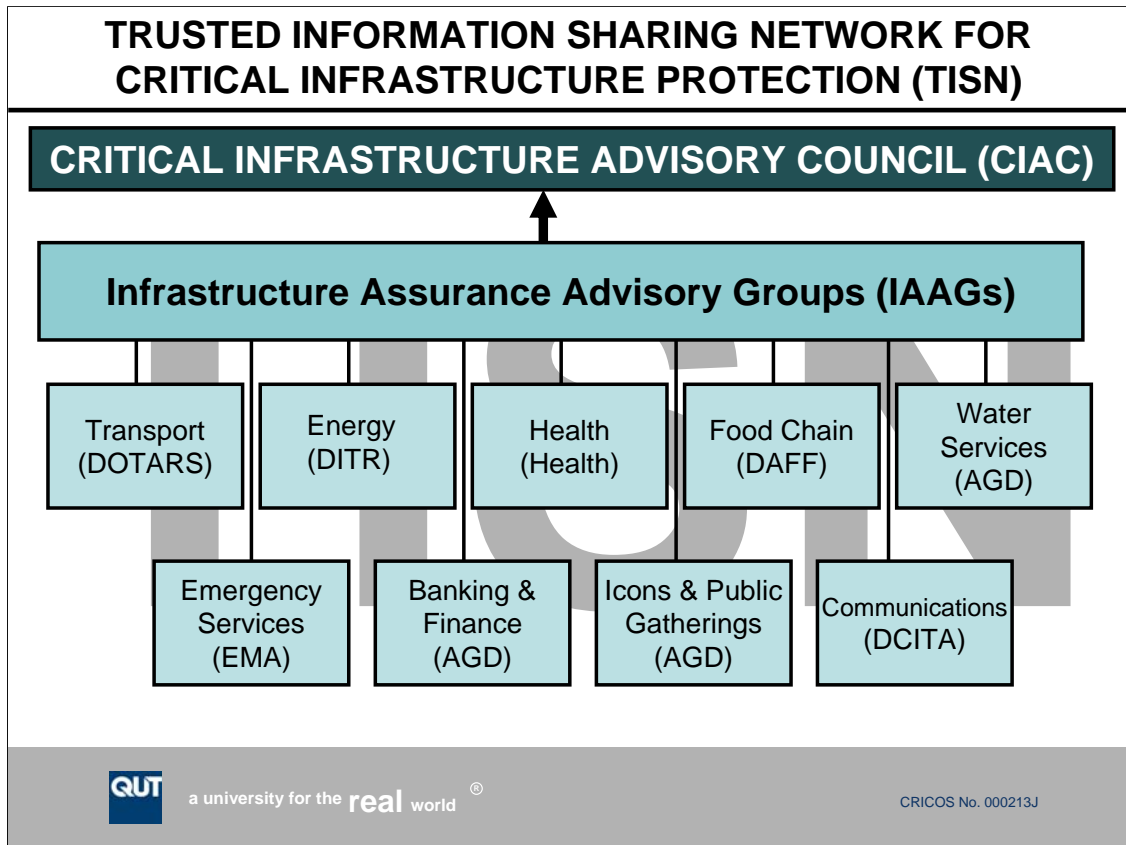
### Business-Government Task Force on Critical Infrastructure

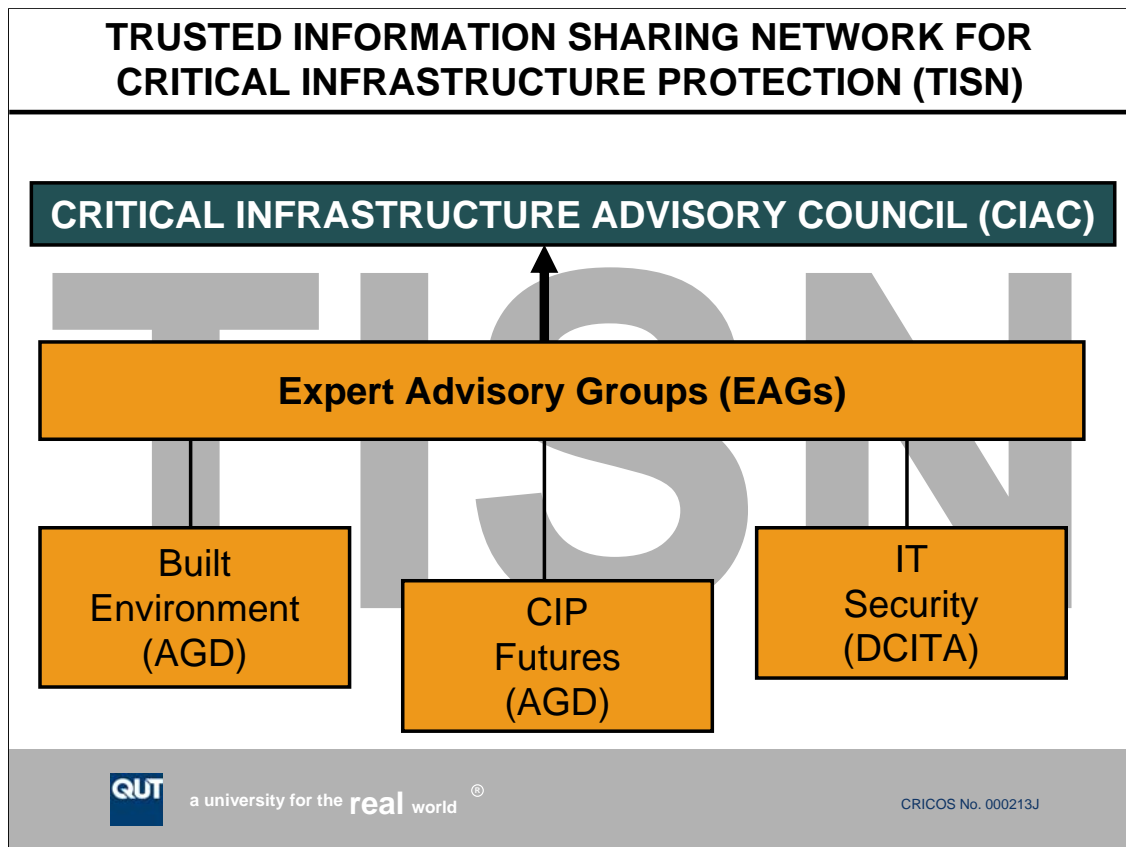
In November 2001, the Prime Minister announced the formation of the Business-Government Task Force on Critical Infrastructure. This announcement saw the Government broaden the scope of its interest in critical infrastructure protection to include all forms of critical infrastructure.


The Task Force met in March 2002, and brought together high-level representatives from the business community, State and Territory governments and Australian Government agencies. In May 2002, the Task Force reported to the Prime Minister and put forward six recommendations that were subsequently endorsed by the Australian Government. One of these recommendations was the setting up of a network to allow owners and operators of critical infrastructure to share information on security issues.

The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) is the direct outcome of this recommendation.









E-Security  
National Agenda



E-Security Policy and  
Coordination (**ESPaC**)  
Committee  
Chair:  
Attorney-General's Dept

**ESNA to:**

- reduce the e-security risk to Australian Government Information and communications systems
- reduce the e-security risk to Australia's national critical infrastructure, and
- enhance the protection of home users and SMEs from electronic attacks and fraud.

2  
0  
0  
7

(c) W. Caelli

10



E-Security  
National Agenda



**Identified risks:**

- continuity of government
- reliable delivery of critical services by both the public and private sector, and
- identity and financial information of home users and small-to medium-sized enterprises (SMEs).

***In May 2007, the Government announced funding of \$73.6 million over four years for new measures to address these three priorities.***

7 Sept 2007

(c) W. Caelli

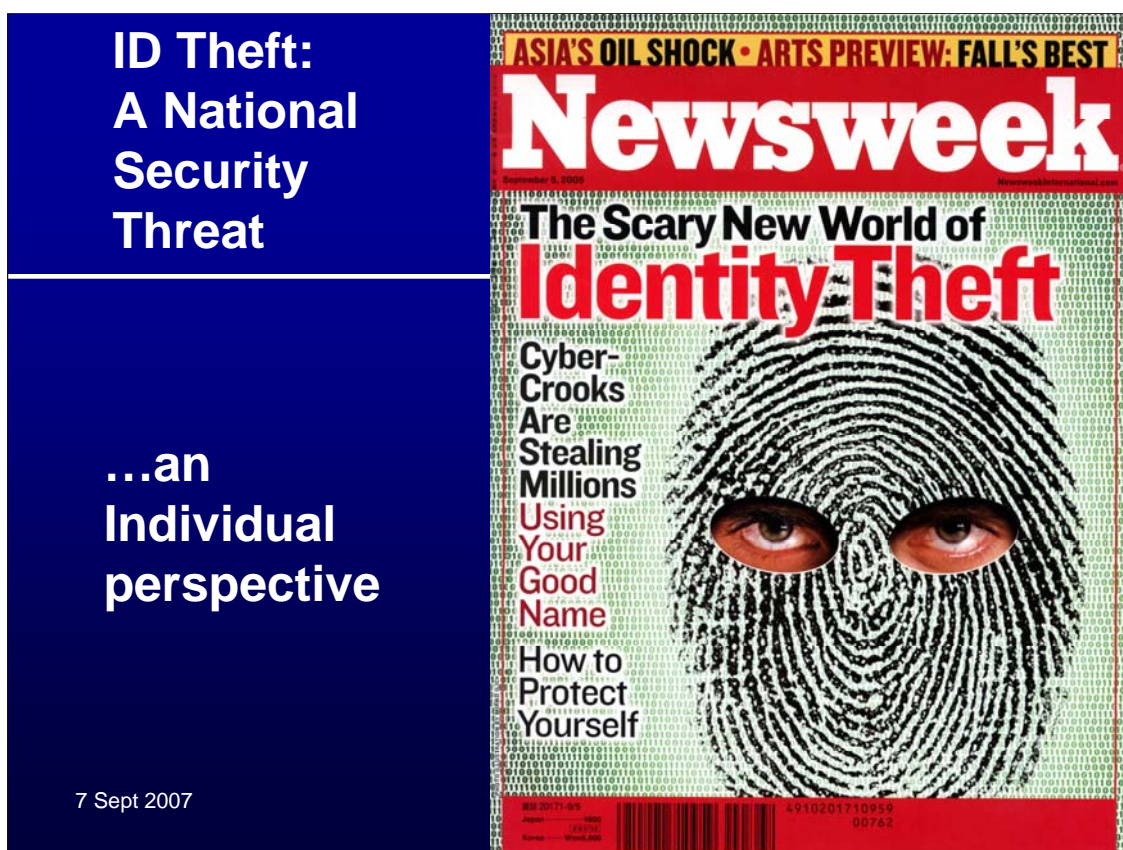
11

# THE THREATS

7 Sept 2007

(c) W. Caelli

12



### ***“ID Theft: A National Security Threat”***

Professor William J (Bill) Caelli, AO, Senior Research Fellow,  
Information security Institute (ISI),  
Queensland University of Technology (QUT)  
Brisbane. Qld. 4000  
AUSTRALIA.

(Email: [w.caelli@qut.edu.au](mailto:w.caelli@qut.edu.au) : Phone - +61-7-38642752)

#### Summary:

The pervasive use of mobile devices such as cell phones, personal digital assistants, laptop PCs, and others has meant that valuable personal information regularly stored in such devices is now backed up on the home and/or business PC system. Access to such detailed information, as well as allied personal data and documents from an unprotected or minimally protected home or small business system, means that fraudulent identity documents may be created based upon stolen data. The increased detail and volume of such data means that such storage becomes a threat to national security if electronic documents may be accessed, used and even appropriate detailed paper forms created. At a national level we have a new pervasive threat to security through simplified identity theft.

*The first time Scott Lunsford offered to hack into a nuclear power station, he was told it would be impossible. There was no way, the plant's owners claimed, that their critical components could be accessed from the Internet. Lunsford, a researcher for IBM's Internet Security Systems, found otherwise.*

*"It turned out to be one of the easiest penetration tests I'd ever done," he says. "By the first day, we had penetrated the network. **Within a week, we were controlling a nuclear power plant.** I thought, 'Gosh. This is a big problem.'"*

**America's Hackable Backbone**  
Andy Greenberg, 08.22.07, 6:00 PM ET

**Forbes**  
.com



## Security

### **America's Hackable Backbone**

Andy Greenberg, 08.22.07, 6:00 PM ET

The first time Scott Lunsford offered to hack into a nuclear power station, he was told it would be impossible. There was no way, the plant's owners claimed, that their critical components could be accessed from the Internet. Lunsford, a researcher for IBM's Internet Security Systems, found otherwise.

"It turned out to be one of the easiest penetration tests I'd ever done," he says. "By the first day, we had penetrated the network. Within a week, we were controlling a nuclear power plant. I thought, 'Gosh. This is a big problem.'"

In retrospect, Lunsford says--and the Nuclear Regulatory Commission agrees--that government-mandated safeguards would have prevented him from triggering a nuclear meltdown. But he's fairly certain that by accessing controls through the company's network, he could have sabotaged the power supply to a large portion of the state. "It would have been as simple as closing a valve," he says.

[http://www.forbes.com/2007/08/22/scada-hackers-infrastructure-tech-security-cx\\_ag\\_0822hack.html?partner=technology\\_newsletter](http://www.forbes.com/2007/08/22/scada-hackers-infrastructure-tech-security-cx_ag_0822hack.html?partner=technology_newsletter) at 30 Aug 2007

Richard A Clarke  
Former Whitehouse Advisor



**2003:**

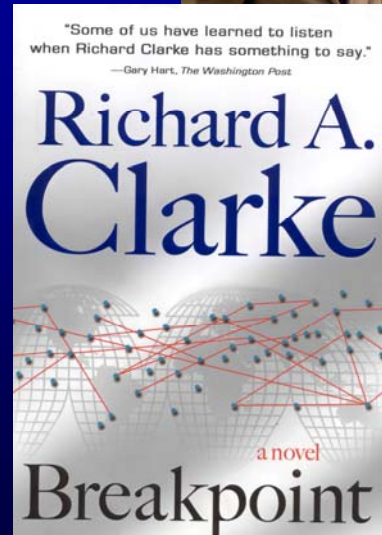
Clarke told attendees at Gartner's Symposium/ITxpo 2003 here this week, the cybersecurity situation isn't just going to get worse. It's going to get exponentially worse.

7 Sept 2007

(c) W. Caelli

15

***“.. some of the  
fixes the  
President  
approved after  
the Cyber Crash  
of 2009...”***



7 Sept 2007

(c) W. Caelli

16

## INTERNET INSECURITY

*The* ASSAULT  
ON REASON

AL GORE



*“..During this period of vulnerability for American democracy – while traditional television is still the dominant source of information and **before the Internet is sufficiently developed and secure as an independent medium** – there are other steps that can and should be taken to foster more connectivity in our self-government.”*

7 Sept 2007

(c) W. Caelli

17

# FEAR OF INFORMATION WARFARE RISING ?

7 Sept 2007

(c) W. Caelli

18

## SOUTH KOREA - Asymmetric action fear

- North Korea - 500/600 hackers – state trained – 5 year degree
  - Target South Korea – USA – Japan
    - Intelligence and/or cyberwar
  - Capable
- South Korea – broadband / low infosec
- “Spyware” allegation
  - 300 South Korean gov’t depts
    - National assembly
    - Nuclear research



**Financial Times (UK)**  
**4 Oct 2004.**

7 Sept 2007

(c) W. Caelli

19

***N Korea's computer hackers target South and US*** / Anna Fifield in Seoul – Financial Times (UK)

Published: October 4 2004 11:30 | Last updated: October 4 2004 11:30

North Korea has trained as many as 600 computer hackers to be capable of launching a cyber-war on South Korea, the US or Japan, South Korea's defence ministry said on Monday. Coming amid intelligence reports that Pyongyang might be preparing to test a ballistic missile, the report will exacerbate jitters over the extent of the communist state's destructive ability.

“North Korea's intelligence warfare capability is estimated to have reached the level of advanced countries,” the ministry said in a report to the National Assembly's national defence committee.

North Korea's military command has 500 to 600 hacking staff who have undertaken a five-year university programme, the report said. Their main task is to gather intelligence from - or launch a cyber attack on - the US, Japan and South Korea. In a wave of attacks earlier this year, nearly 300 South Korean government computers at departments including the National Assembly and an atomic energy research institute were infected with viruses capable of stealing passwords and other sensitive information.

South Korea is particularly vulnerable to cyber-crime because it has the world's highest usage of broadband services and relatively poor levels of internet security. The South Korean intelligence traced the hackers to China, although it was unclear whether they were based in China or just using a Chinese network. The defence ministry's report comes as Pyongyang's relations with Washington, Seoul and Tokyo deteriorate.

North Korea is refusing to return to the diplomatic table for the latest round of six-party talks between the countries, as well as China and Russia. The talks have reached an impasse owing to what Pyongyang calls the US's “hostile policies” towards North Korea. The process has been further complicated by recent revelations that South Korea has enriched a small amount of uranium and separated plutonium in secret experiments during the past 22 years.

Mohamed ElBaradei, the head of the International Atomic Energy Agency, on Monday held talks in Seoul with Lee Hun-jai, the South Korean prime minister, as part of the agency's investigation into the experiments. ( Propaganda cartoon from wikipedia.org at 16-10-2004).

**SPIEGEL ONLINE**

DER SPIEGEL  
Heft 35/2007

Die gelben Spione  
Wie China deutsche  
Technologie ausspäht



German Chancellor Angela Merkel  
& Chinese Premier Wen Jiabao



7 Sept 2007

(c) W. Caelli

20



From The Times  
August 27, 2007

## China accused of hacking into heart of Merkel administration

Roger Boyes in Berlin

- *extraordinary economic espionage operation*
- *denied strenuously by the Chinese authorities*

7 Sept 2007 (c) W. Caelli 21

### China accused of hacking into heart of Merkel administration

Roger Boyes in Berlin

*China has hacked into the computers of Angela Merkel's Chancellery and three other German ministries in an extraordinary economic espionage operation that threatens to blight the German leader's already delicate trip to Beijing this week.*

*The claims, made in a detailed investigation by Der Spiegel magazine, were denied strenuously by the Chinese authorities yesterday, but there was no mistaking German anger. "If true, it is unacceptable," Ralf Stegner, a senior Social Democrat, said. "China is a competitor as well as a trading partner. Mrs Merkel has to get to the bottom of the affair on her China trip."*

From The Times, August 27, 2007



*"Well I don't want to make any specific comment on that now, but I just want to say that particularly in our relations with China we're paying a great deal of attention to the **protection of intellectual property**," she said.*

**REUTERS**   
27 Aug 2007



Dr. Angela Dorothea Merkel  
Chancellor of Germany  
Christian Democratic Union (CDU)

*Federal Office for the Protection of the Constitution (BfV) .... prevented a further 160 giga-bytes of information being transferred to China.*

**TIMES ONLINE**  
27 Aug 2007

*...Spiegel-Informanten, dass IT-Spezialisten nach der Entdeckung die Übertragung von 160 GByte Daten verhindert hätten.*

URL: [www.zdnet.de](http://www.zdnet.de) - 27 Aug 2007

7 Sept 2007

(c) W. Caelli

22

From The Times

August 27, 2007

### **China accused of hacking into heart of Merkel administration**

Roger Boyes in Berlin

China has hacked into the computers of Angela Merkel's Chancellery and three other German ministries in an extraordinary economic espionage operation that threatens to blight the German leader's already delicate trip to Beijing this week. The claims, made in a detailed investigation by Der Spiegel magazine, were denied strenuously by the Chinese authorities yesterday, but there was no mistaking German anger. "If true, it is unacceptable," Ralf Stegner, a senior Social Democrat, said. "China is a competitor as well as a trading partner. Mrs Merkel has to get to the bottom of the affair on her China trip." Mrs Merkel arrived in China last night with senior business executives determined to put concern about product piracy high on the agenda. "We are pursuing the issue of protection of intellectual property very strongly with China," said Mrs Merkel, who refused to discuss the espionage claims.

Der Spiegel, quoting senior officials from the German equivalent of Special Branch, said that the hacking operation was discovered in May. Computers in the Chancellery, the Foreign, Economics and Research ministries had been targeted. The Federal Office for the Protection of the Constitution (BfV) conducted a comprehensive search of government IT installations and prevented a further 160 giga-bytes of information being transferred to China. Commentators described it as "the biggest digital defence ever mounted by the German state". The information was being siphoned off almost daily by hackers in Lanzhou, northern China, in Canton province and in Beijing. The scale and the nature of the data being stolen suggest, the investigators say, that the operation must have been steered by the State and, in particular, the People's Liberation Army. "Does this Chinese man now know all our government secrets?" an outraged Bild am Sonntag asked yesterday next to a large photograph of General Cao Gangchuan, the Chinese Defence Minister. The content of the stolen data has naturally not been disclosed. "It can only have been interesting for state institutions," said a confidential report by the BfV leaked to Der Spiegel. "So we must assume that the Chinese State is involved in the electronic attacks." Investigators caution that businessmen should not leave their laptop computers in hotel rooms while at official functions because of the risk of data theft. And all information transferred from China to German corporate headquarters should be encoded. "I have become really worried about Chinese espionage in the technology area," says Hartmut Schauerte, parliamentary minister in the Economics Ministry and a China specialist. The suspicions are now so deep that the motives of Chinese researchers at German universities are being questioned. Yesterday the Chinese Embassy in Berlin described the accusation of state-steered hacking as "irresponsible speculation without a shred of evidence". (Source: <http://www.timesonline.co.uk/tol/news/world/europe/article2332130.ece> accessed on 28 Aug 2007)



Foreign Ministry Spokesperson Jiang Yu

中华人民共和国外交部  
Ministry of Foreign Affairs of the People's Republic of China

REUTERS

BEIJING, Aug 26 (Reuters)  
China rejected on Sunday a German magazine report that computer hackers believed to be linked to the Chinese army had infected German government ministries with spying programmes.

7 Sept 2007 (c) W. Caelli 23

Foreign Ministry Spokesperson Jiang Yu's Remarks on the so-called Chinese Hackers' Attacks against German Government Computers  
2007/08/27

**Q: German media reported that German government computers were attacked by Chinese hackers. What's your comment?**

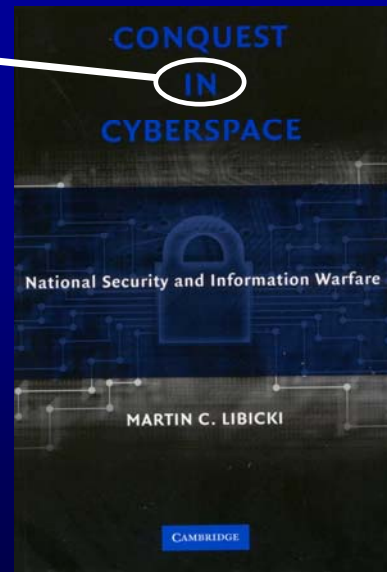
A: The Chinese Government has always opposed to and forbidden any criminal acts undermining computer systems including hacking. We have explicit laws and regulations in this regard.

Hacking is an international issue and China is also a frequent victim. China has established a sound mechanism of cooperation with many countries in jointly countering internet crimes. China is willing to cooperate with Germany in this regard.

(Source: <http://www.fmprc.gov.cn/eng/xwfw/s2510/2535/t355740.htm> accessed on 28 Aug 2007)

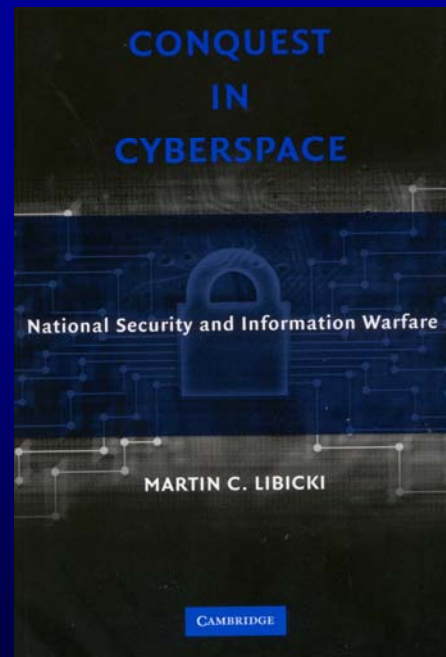
## CONQUEST IN CYBERSPACE

- “in” – **NOT** “of” ←
- **Theme:**
  - “ .. possibilities of hostile conquest may be less consequential than meets the eye while the possibilities of friendly conquest ought to be better appreciated...”



## CONQUEST IN CYBERSPACE

- If hackers get in
- **Minimum:**
  - Steal information
- **Worse:**
  - Make systems go haywire
- **Worst:**
  - inject phoney information to distort what users think they absorb



7 Sept 2007

(c) W. Caelli

25

## CONQUEST IN CYBERSPACE

*Cyberspace on its own merits:*

- 1. ..replicable construct.*
- 2. ..to exist in cyberspace, your interactions must be recognised there.*
- 3... some aspects of cyberspace nevertheless tend to persist.*
- 4. ..cyberspace has separate layers, the conquest of each of which has vastly different meaning.*



# SOME DEVELOPING THEMES

7 Sept 2007

(c) W. Caelli

27

## NIIP

- CNI / NII
  - Critical National Infrastructure / National Information Infrastructure
- ICT systems:
  - From “*competitive advantage*” to “*complete dependence*”
- Changing demographics
  - “*Megacities*” - interconnected
- Global Internet – total convergence
  - 3 C’s
    - Computers, Communications, Content

7 Sept 2007

(c) W. Caelli

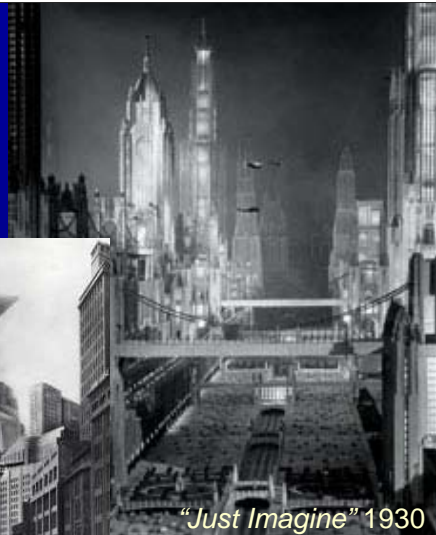
28

## NIIP & INTRUSION

### NEW DEMOGRAPHICS

- in CITIES
- where enterprises & people are
- which depend upon safe & secure ICT infrastructure

**2008:  
50% world's population  
lives in cities.**

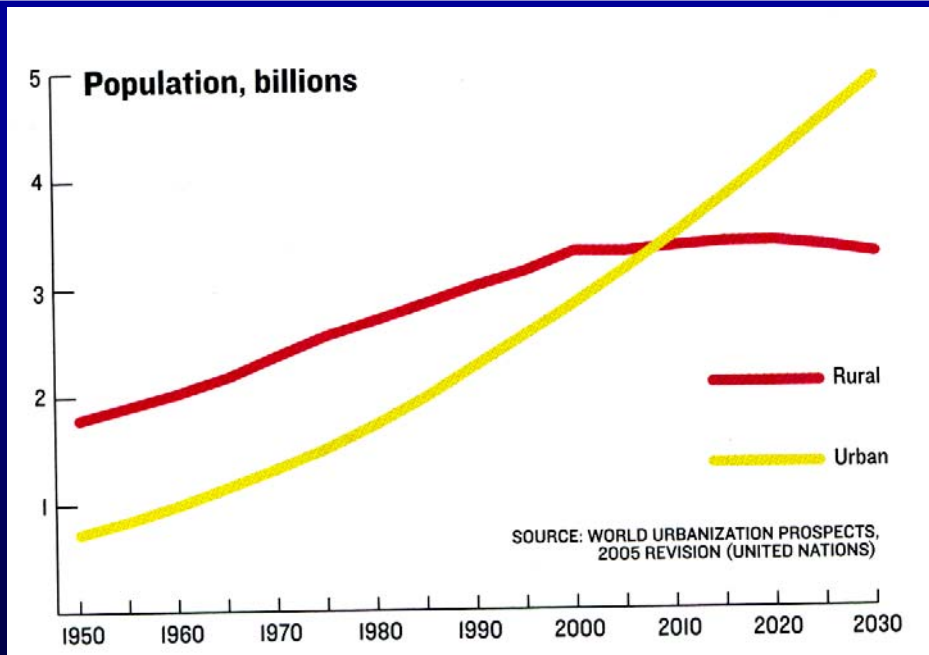


7 Sept 2007

(c) W. Caelli

30

## URBAN POPULATION GROWTH



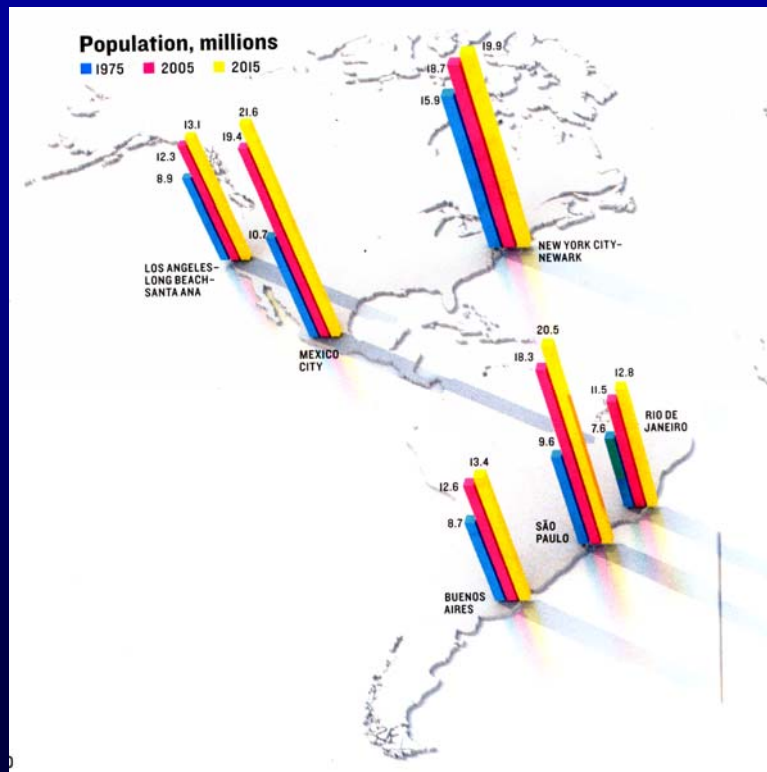
IEEE Spectrum, June 2007

7 Sept 2007

(c) W. Caelli

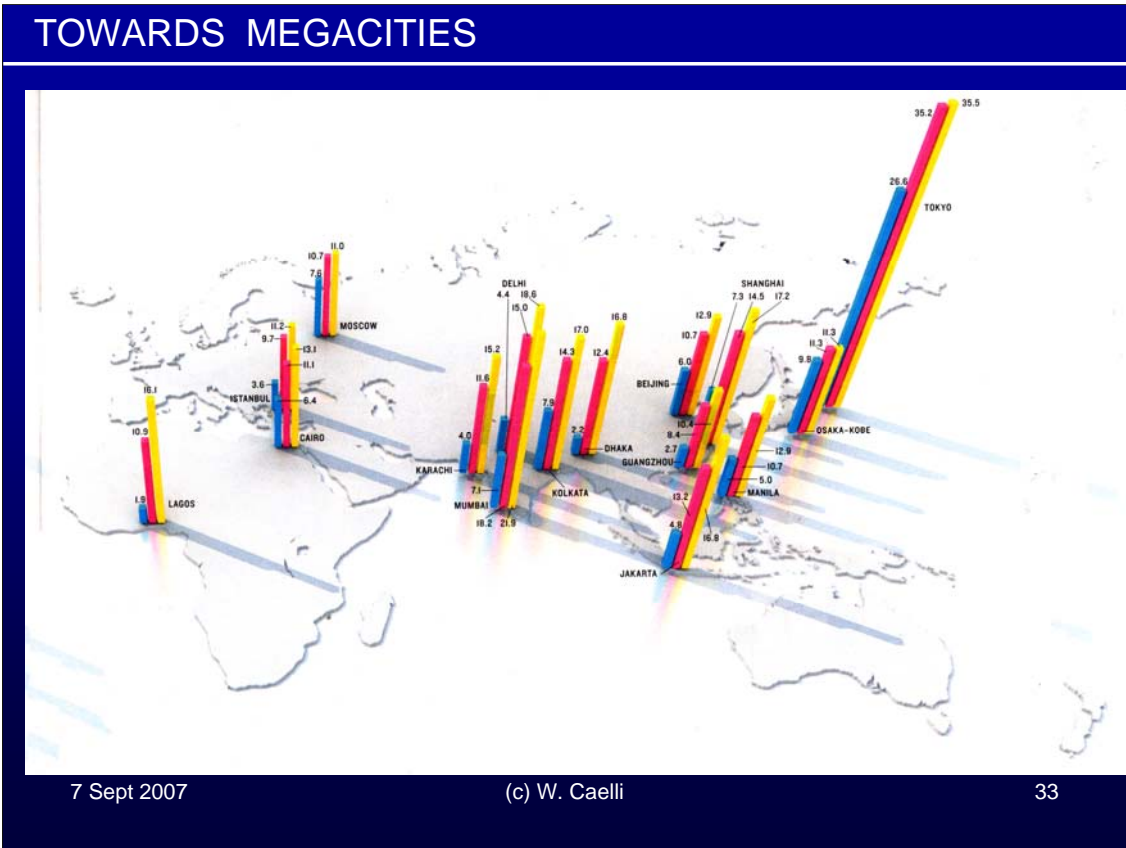
31

# TOWARDS MEGACITIES

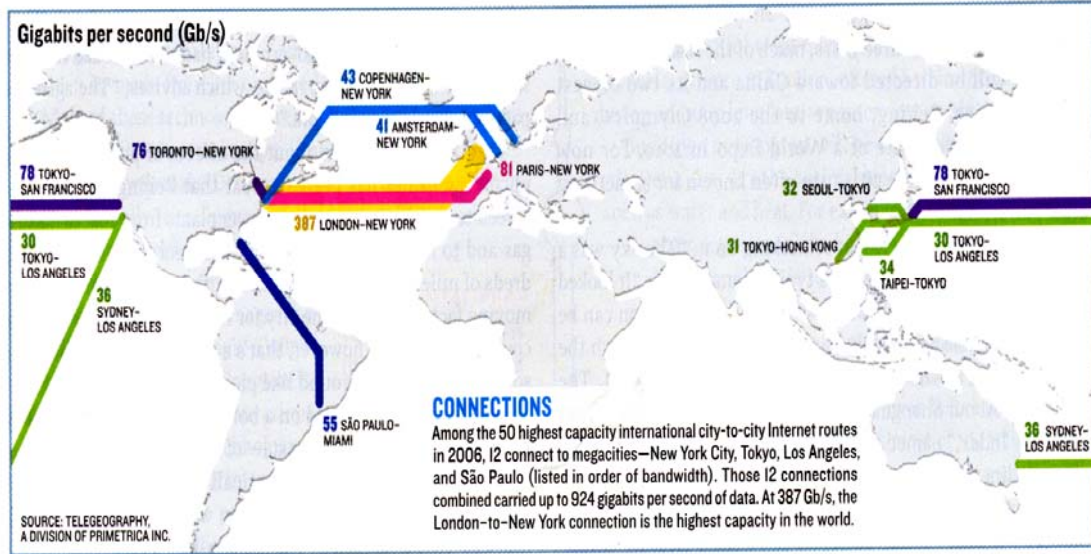


7 Sept 2007

32



## DEPENDENCE ON INTERNET BACKBONE



IEEE Spectrum, June 2007.

7 Sept 2007

(c) W. Caelli

34

# THE CHALLENGES TO NIIP

7 Sept 2007

(c) W. Caelli

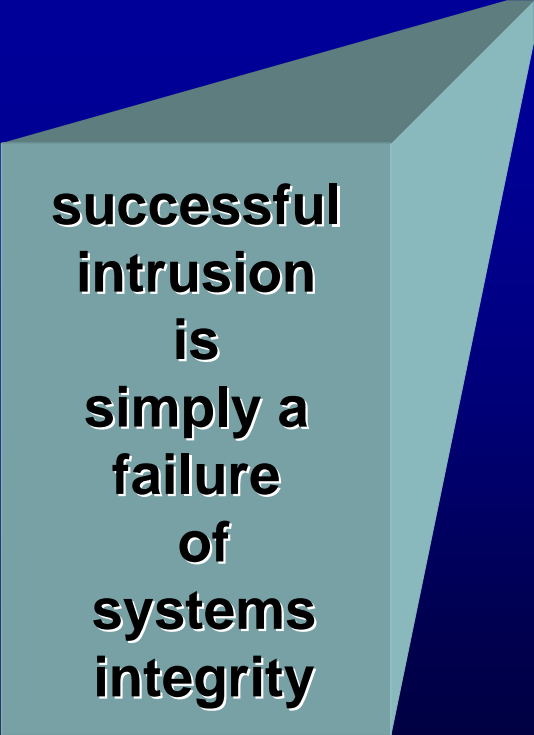
35

**NIIP**

**IDS  
IPS**

**BUT on a  
national  
scale  
for  
critical  
enterprises**

7 Sept 2007



**successful  
intrusion  
is  
simply a  
failure  
of  
systems  
integrity**

(c) W. Caelli

36

A20 VT THE NEW YORK TIMES TUESDAY, JUNE 14, 2005

**With Sprint, ING DIRECT is beautiful.**



**“ With 99% of their transactions taking place over the Internet or on the phone ING DIRECT’s customers don’t go to the bank. The bank goes to them.”**

**Sprint**

With 99% of their transactions taking place over the Internet or on the phone ING DIRECT’s customers don’t go to the bank. The bank goes to them. That’s why ING DIRECT turned to Sprint and the Sprint Peerless IP Network to address their unique security and reliability needs. This made it possible for ING DIRECT to integrate call center and Web traffic over a more secure, private network. And since then, they’ve experienced zero service interruptions. When every customer can be the first customer in line, banking is beautiful. **With Sprint, business is beautiful.**

> Visit [Sprint.com/beautiful](http://Sprint.com/beautiful) for case studies or call 877-777-5568 > Wireless. Data. Voice. IP.

©2005 Sprint. All rights reserved. Sprint and the Diamond logo are trademarks of Sprint Communications Company L.P.

7 37

## CHALLENGES TO IDS/IPS

### “*expert*” information worker

- “**BYO**” information terminal / workstation
- work anywhere, anytime
- devices
  - PDA, 3G cell phone, laptop
- connectivity
  - wireless
  - standards, multiplicity
- services
  - private, public, unknown

7 Sept 2007

(c) W. Caelli

38

## IDS – FROM THE INSIDE

- device drivers
- kernel / system functions
- BIOS / peripheral interfaces
- hardware sub-systems
- USB / FireWire etc



**SONY  
MICRO VAULT with  
Fingerprint Access.  
Slim, easy, convenient,  
and Secure!**  
Convenient docking station  
and USB cable. It's easy to  
connect Micro Vault.

**Experts raise alarm on Sony software**

Jim Finkle in Boston | August 29, 2007

*SOFTWARE included with high-end memory sticks sold by Sony can make personal computers vulnerable to attack by computer hackers, according to researchers with two internet security firms.*

The Australian 29 Aug 2007

7 Sept 2007

(c) W. Caelli

39

## IDS – FROM THE OUTSIDE

### SOA / Web Services

- IBM – 2007 – 70% projects SOA based
- Incomplete, multiple, conflicting security “standards”
- Security implications not well studied
- Nationally significant systems under development
- Australia:
  - Healthcare information systems (NEHTA)
  - Social security systems, etc (“Access card”)

7 Sept 2007

(c) W. Caelli

40

Fujitsu Consulting director Adam Neat believes clients will buy software services from "any number of vendors", with the bigger players offering a "generic service stack".

He says SOA represents the end of software "product" as we know it. The "utopia" in five to 10 years is for organisations to have a shopping list of all services they need and vendors "evolving over time to expose themselves through Service Level Agreements".

(The Australian, 28 Aug 2007)

## INTRUSION DETECTION / PREVENTION - VOIP

- Threat = turn ON to listen
- Threat = interception at “line” level
- Untrusted “end-of-line” equipment



7 Sept 2007

(c) W. Caelli

41

## INTRUSION DETECTION &amp; INTELLECTUAL PROPERTY

**National eResearch Networks**

- New data, information & knowledge generated and stored electronically
- Available over national/international high speed networks
- Very high speed access – Gbit/sec
- Terra/Peta-byte stores

**IDS / IPS challenges**

7 Sept 2007

(c) W. Caelli

42

## EDUCATION AND TRAINING – THE GAP IN THE WEST

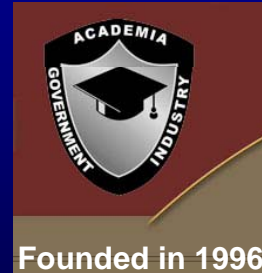
- Australia
  - retrenchments of teachers in ICT at universities
- USA
  - lack of demand for places
  - CRA reports
  - NSF / NatAcad

**Education/experience of IA teachers ?**

## EDUCATION AND TRAINING – THE GAP IN THE WEST

**CISSE****The Colloquium for  
Information Systems Security Education**

<http://www.cisse.info>



**Education/experience of IA teachers ?**

7 Sept 2007

(c) W. Caelli

44

# POLICY CHANGES

7 Sept 2007

(c) W. Caelli

45

## RESPONDING TO INTRUSION

**The “Talk-Back” View**

*Would not this be a great way to destroy the Chinese military servers? Insert a virus into data made attractive enough to be stolen; then wait for the complete destruction of all Chinese defence capabilities relying on computers. Back to the stone age again!!!*

Ben Genevieve, Perth, Western Australia

(Source: <http://www.timesonline.co.uk/tol/news/world/europe/article2332130.ece>  
at 28 Aug 2007)

7 Sept 2007

46

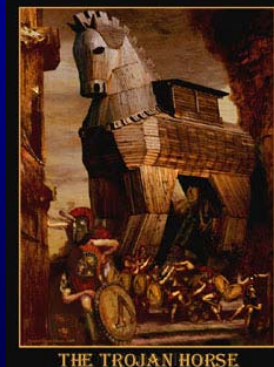
## INTRUSION DETECTION

**“Hardening” commodity operating systems**

- LSPP, RBAC, CCAP
  - Modernised “MAC”
  - Redefining the intrusion risk
- BUT**
- industry/user willingness?
  - CIO “friendliness”?
  - education & training?
  - legislation / regulation? (FISMA)
  - placement of IDS/IPS ?
    - “covert channels” (B2) ?




Germany - Blitzkrieg

THE TROJAN HORSE  
Greeks – Troy

7 Sept 2007



(c) W. Caelli

47



# Build Security In

*Setting a Higher Standard for Software Assurance*





National Information Assurance Partnership

## Common Criteria Certificate

*is awarded to*

### Hewlett-Packard



The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 2.3) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

<p><b>Product Name:</b> Red Hat Enterprise Linux Version 5  <b>Evaluation Platforms:</b> HP ProLiant DL, BL and ML Systems; HP Integrity Superdome, rx, cx and BL Systems; HP xw workstations; HP Compaq dc desktops  <b>Assurance Level:</b> EAL 4 Augmented ALC_FLR.3  <b>Date Issued:</b> 26 June 2007</p>	<p><b>CCTL:</b> atsec information security corporation  <b>Validation Report Number:</b> CCEVS-VR-07-0054  <b>Protection Profile Identifier:</b> Labeled Security Protection Profile, Issue 1.b, 8 October 1999 Controlled Access Protection Profile, V1.d, October 8, 1999; Role-based Access Control Protection Profile, Version 1.0, July 30, 1998</p>
---	---

**Original Signed By**

---

*Director, Common Criteria Evaluation and Validation Scheme*  
National Information Assurance Partnership

**Original Signed By**

---

*Information Assurance Director*  
National Security Agency

7 Sept 2007
(c) W. Caelli
48

## RESPONSE OF GOVERNMENTS - WEST

- 25 years of “*Thatcherism*” and “*economic rationalism*” ?
- domination of the ethic, principles and methods of business and commerce
  - security is a “cost centre” to be minimised
- “small government”
- coincides with “*information revolution*”
- not conducive to acceptance of NIIP responsibility by private enterprise

7 Sept 2007

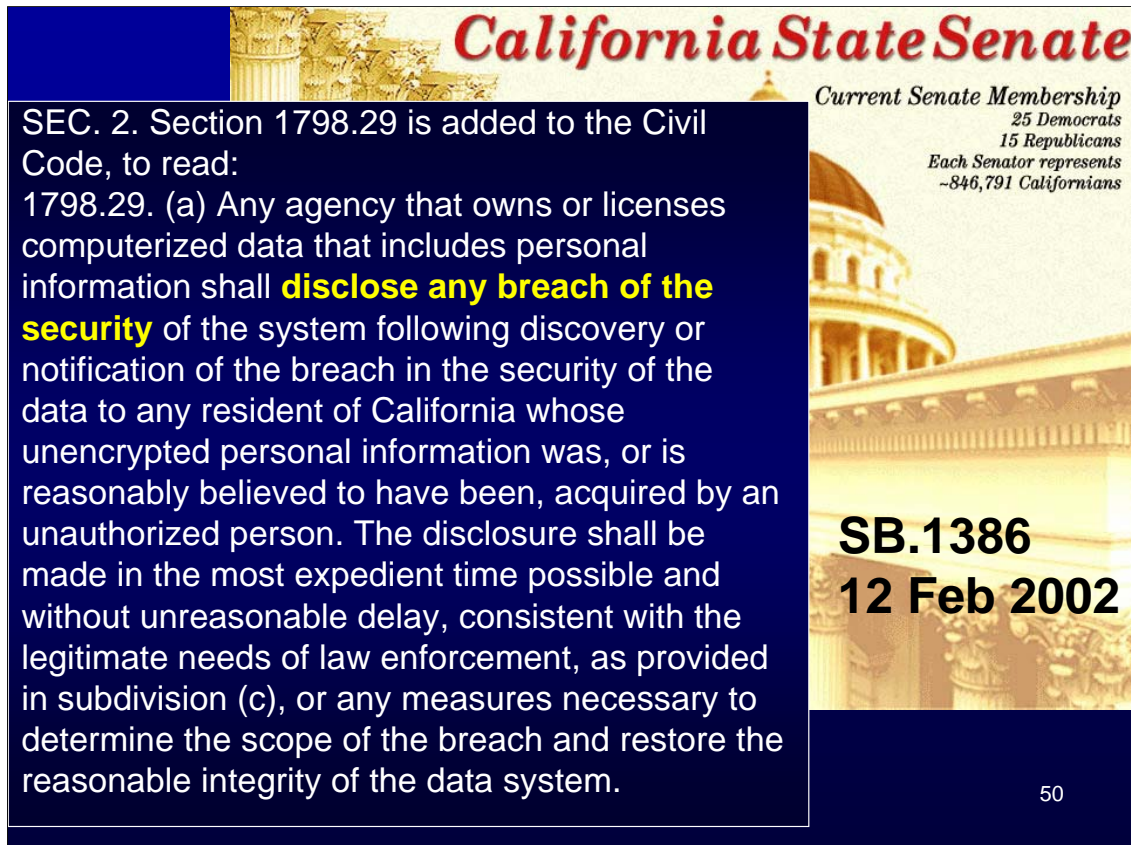
(c) W. Caelli

49

### “What is Economic Rationalism?” by [Gregory Whitwell](#)

‘Economic rationalism’ is debated with great intensity and frequency, but it is rarely defined. It is a convenient label for a great variety of things. Much of the debate about economic rationalism takes as its reference point Michael Pusey’s book, “Economic Rationalism in Canberra” (1991). Curiously the book does not provide a succinct definition of economic rationalism. Pusey has argued elsewhere, however, that Economic rationalism is the dogma which says that markets and money can always do everything better than governments, bureaucracies and the law. There’s no point in political debate because all this just generates more insoluble conflicts. Forget about history and forget about national identity, culture and ‘society’ ... Don’t even think about public policy, national goals or nation-building. It’s all futile. Just get out of the way and let prices and market forces deliver their own economically rational solution. Pusey takes an extremist view. The use of words such as ‘always’ and ‘everything’ make it a definition applicable to few economists. More satisfactory is Robert Manne’s argument that what characterises economic rationalism is ‘a profound suspicion of all forms of state intervention in economic life and an almost equally profound faith in the beneficence of unfettered, or almost unfettered, market forces’. Better still is John Stone’s definition: In their most basic form, economic rationalist views simply hold that, generally speaking, markets usually provide more satisfying answers to questions of choice, consumer preference and so on—and in doing so, provide a more rapidly advancing level of total well-being for all concerned—than decisions by diktat, whether those be by politicians, bureaucrats or controllers generally. Economic rationalists are, of course, aware that markets can ‘fail’. That is why ... they are not the re-emergent disciples of crude laissez-faire, and why they will support such bodies as Trade Practices Commissions and the like to ward off, so far as possible, the effects of such market failure (eg private monopolies). But they will generally believe that, whatever the problems of market failure may sometimes be, they are as nothing to the demonstrated and persistent proofs of government failure where governments are employed in place of markets.

Source URI at 1 Sept 2007 - <http://www.abc.net.au/money/currency/features/feat11.htm>

The graphic features a background image of the California State Capitol building. At the top, the text "California State Senate" is written in a red, serif font. Below this, on the right side, is the text "Current Senate Membership" followed by "25 Democrats", "15 Republicans", and "Each Senator represents ~846,791 Californians". In the center-right, the text "SB.1386" and "12 Feb 2002" is displayed in a large, bold, black font. A dark blue rectangular box on the left side of the graphic contains white text detailing a legislative change to the Civil Code.

**California State Senate**

*Current Senate Membership*  
25 Democrats  
15 Republicans  
Each Senator represents  
~846,791 Californians

**SB.1386**  
**12 Feb 2002**

SEC. 2. Section 1798.29 is added to the Civil Code, to read:  
1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall **disclose any breach of the security** of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

50

## GOVERNMENT MUST ACT NOW TO MAINTAIN CONFIDENCE IN THE INTERNET

- *“The IT industry has not historically made security a priority..... more radical and rapid change is needed if the industry is to keep pace with the ingenuity of criminals and avoid a **disastrous loss of confidence** in the Internet.”*
- 31 conclusions & recommendation

Personal Internet Security - Vol. I: Report  
10 August 2007

7 Sept 2007

(c) W. Caelli

51



### Select Committee on Science and Technology [Fifth Report](#)

#### ABSTRACT

The Internet is a powerful force for good: within 20 years it has expanded from almost nothing to a key component of critical national infrastructure and a driver of innovation and economic growth. It facilitates the spread of information, news and culture. It underpins communications and social networks across the world. A return to a world without the Internet is now hardly conceivable. But the Internet is now increasingly the playground of criminals. Where a decade ago the public perception of the e-criminal was of a lonely hacker searching for attention, today's "bad guys" belong to organised crime groups, are highly skilful, specialised, and focused on profit. They want to stay invisible, and so far they have largely succeeded. While the incidence and cost of e-crime are known to be huge, no accurate data exist. Underpinning the success of the Internet is the confidence of hundreds of millions of individual users across the globe. But there is a growing perception, fuelled by media reports, that the Internet is insecure and unsafe. When this is set against the rate of change and innovation, and the difficulty of keeping pace with the latest technology, the risk to public confidence is clear. The Government have insisted in evidence to this inquiry that the responsibility for personal Internet security ultimately rests with the individual. This is no longer realistic, and compounds the perception that the Internet is a lawless "wild west". It is clear to us that many organisations with a stake in the Internet could do more to promote personal Internet security: the manufacturers of hardware and software; retailers; Internet Service Providers; businesses, such as banks, that operate online; the police and the criminal justice system. We believe as a general principle that well-targeted incentives are more likely to yield results in such a dynamic industry than formal regulation. However, if incentives are to be effective, they may in some cases need to be backed up by the possibility of direct regulation. Also, there are some areas, such as policing, where direct Government action is needed. So Government leadership across the board is required. Our recommendations urge the Government, through a flexible mix of incentives, regulation, and direct investment, to galvanise the key stakeholders. The threat to the Internet is clear, but it is still manageable. Now is the time to act, both domestically, and internationally, through the European Union and through international organisations and partnerships.

House of Lords, UK 24 July 2007.

- Increase the resources and skills available to the police and criminal justice system to catch and prosecute e-criminals
- Establish a centralised and automated system, administered by law enforcement, for the reporting of e-crime.
- Provide incentives to banks and other companies trading online to improve the data security by establishing a data security **breach notification law**.



2007

(c) W. Caelli

10 August 2007.

52



- Improve standards of new software and hardware by taking the first steps towards the establishment of legal liability for damage resulting from security flaws.
- Encourage Internet service providers to improve the security offered to customers by establishing a "kite mark" for Internet services.



7 Sept 2007

10 August 2007.

(c) W. Caelli

53

## NIIP - ERA OF EXPERIMENTATION

### Who, what, where & how

- military
- intelligence
- government
- private sector

## CERT

- USA – “Morris worm” – CERT
- To more “CERTs”
- International responses
  - National CERTs
  - Government CERTs
  - Private CERTs
- FIRST

MILITARY – USA – 8<sup>th</sup> AIR FORCE*National Military Strategy for Cyberspace Operations*

*defines cyberspace as "domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."*

*"Our own nation's neural network resides in cyberspace,"*

Secretary of the Air Force  
Michael W. Wynne



Operational  
Cyberspace  
Command

1. Control the domain
2. Integrate operations
3. Offensive operations



Arch Bevis - Member for Brisbane

Shadow Minister for Homeland Security; Territories  
Shadow Minister for Justice and Customs

*Since 9/11, Labor has approached this issue with a strong belief in the vital importance of a **single Homeland Security Department** that encompasses the key agencies involved in information and intelligence gathering, border protection, a national coast guard, transport security and incident response capability.*

URI: <http://www.archbevis.com/335.html> accessed at 31 Aug 2007

7 Sept 2007

(c) W. Caelli

57

Homeland Security Department [The Need for a Single Homeland Security Department](#) - Since 9/11, Labor has approached the issue of Anti-Terrorism response and preparation, with a strong belief in the vital importance of a single Homeland Security Department that encompasses the key agencies involved in information and intelligence gathering, border protection, a national coast guard, transport security and incident response capability. Arch stated in his address to Safeguarding Australia 2005 Fourth Homeland Security Summit & Exposition that, "The Howard Government's insistence on splitting these functions over a number of Departments invites overlap, wastage, confusion and missed opportunities. In national security, confusion and missed opportunities can be fatal".

<http://www.archbevis.com/252.html> accessed 31 Aug 2007.



Arch Bevis - Member for Brisbane

Shadow Minister for Homeland Security; Territories  
Shadow Minister for Justice and Customs

*In government, purpose designed agencies need to be focused on the task, within a **dedicated Homeland Security Department** where responsibility ultimately stops with one Minister. We need to remove the overlap and potential for gaps that the current structure creates and which undermines security.*

Australian National Security Summit 2006 - 15/11/2006

URI: <http://www.archbevis.com/338.html> accessed at 31 Aug 2007

7 Sept 2007

(c) W. Caelli

58

Homeland Security Department [The Need for a Single Homeland Security Department](#) - Since 9/11, Labor has approached the issue of Anti-Terrorism response and preparation, with a strong belief in the vital importance of a single Homeland Security Department that encompasses the key agencies involved in information and intelligence gathering, border protection, a national coast guard, transport security and incident response capability. Arch stated in his address to Safeguarding Australia 2005 Fourth Homeland Security Summit & Exposition that, "The Howard Government's insistence on splitting these functions over a number of Departments invites overlap, wastage, confusion and missed opportunities. In national security, confusion and missed opportunities can be fatal".

<http://www.archbevis.com/252.html> accessed 31 Aug 2007.



The Hon John Winston Howard MP - Member for Bennelong  
Prime Minister

## PM rejects calls for homeland security dept

*"Prime Minister John Howard has rejected calls for a US-style Department of Homeland Security, saying the American organisation has been condemned for its response to Hurricane Katrina..... it hasn't been the all embracing bureaucratic solution that people said it was going to be. "*



Posted Thu Sep 22, 2005 3:41pm AEST  
Updated Fri Sep 23, 2005 5:24am AEST

7 Sept 2007

(c) W. Caelli

59

Remarks by Vice President Al Gore at National Press Club December 21, 1993

*.....there are certain public needs that outweigh private interests.*

**The time has come  
for decisive political &  
governmental action in  
securing / defending  
cyberspace ?**



Al Gore  
Vice-President USA  
(1993-2001)

7 Sept 2007

(c) W. Caelli

60



# TIME FOR TEA

7 Sept 2007

(c) W. Caelli

61