

ASIO chief warns on cyber attacks

■ Business at risk of global hackers

■ Resource, infrastructure targets

Geoff Kitney and John Kerin

STATE OF SECURITY

The nation's senior domestic intelligence official has warned business of a growing threat of cyber attacks on computer systems and says defending Australia from foreign cyber espionage was the big new challenge facing the intelligence community.

David Irvine, the director-general of the Australian Security Intelligence Organisation, told the *AFR Magazine*, in an exclusive interview published today, that corporate communications networks were as much a target as defence and security systems from increasing attempts by foreign cyber sleuths seeking to steal Australia's secrets.

Foreign cyber operatives had the capacity not only to get into business networks and steal corporate financial information and intellectual property but also to completely shut down strategically important systems, such as transport systems, telecommunications networks and air traffic control, Mr Irvine said.

'The third serious target and the one that is not talked about enough from my point of view is the whole concept of cyber attack as an act of war.'

ASIO's David Irvine

Concerns about the rising cyber threat have been reinforced by the release of details of the counter-cyber security operations of Australia's front-line electronic intelligence agency, the Defence Signals Directorate (DSD).

Defence Minister John Faulkner told the *AFR* that DSD had detected in 2009 more than 2400 "incidents" on networks considered to be of "medium to high risk". Only about 200 of these were directly defence related.

The Defence Department would not provide any information about the origins of the attempts or details of the targets but did say that DSD "responded to these incidents with no operations disrupted".

Continued page 4

ASIO warns on cyber attacks

rom page 1
 But intelligence sources have pointed the finger at foreign intelligence services including China, terrorist groups, organised crime and computer hackers. Chinese hackers are understood to have targeted the systems of iron ore producers Rio Tinto and BHP Billiton as well as firms in the infrastructure, communications and finance sectors.

Senator Faulkner also would not detail the targets but did say that DSD "responded to these incidents with no operations disrupted".

Mr Irvine's stark warning was enforced by Paul Twomey, one of Australia's leading authorities on internet security issues, who said Australia's corporate leaders might be exposed to legal action for negligence from a failure to adequately protect information in company computer systems.

Mr Twomey, former chief executive of ICANN, the global system for managing the internet and now head of Argo Pacific, an international consultancy on cyber issues, said Australian corporations needed to seriously consider the possibility that they could be liable to legal claims of negligence if "something went bad on [the company's] network".

Mr Twomey said the fact that nearly every business was now connected to the internet greatly increased "their risk framework" and every member of a board needed to be aware of this risk.

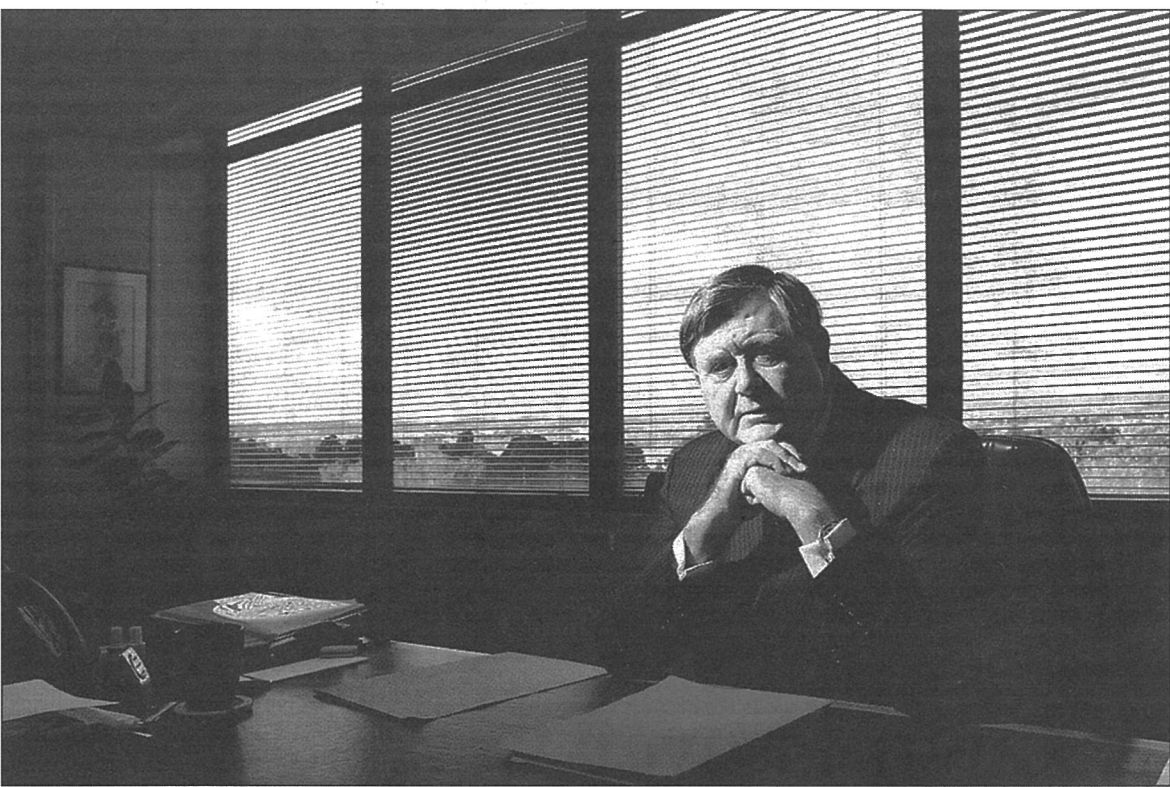
In the interview with the *AFR*, Mr Irvine said cyber attackers had three major targets.

The ASIO boss said he was particularly concerned by "the growing use of cyber attack to obtain information that's unclassified [not government secrets] but vulnerable information, theft of] intellectual property, that could include resource companies and for example infrastructure companies".

"The second serious target is government classified communications and we are constantly trying to keep head of other people's abilities to get into those communications.

"The third one and the one that is not talked about enough from my point of view is the whole concept of cyber attack as an act of war.

"If you think about our critical infrastructure in this country, you have the financial system, some elements of the resource industry, the electricity grid, the transport system," he said. "And don't think this is



Cyber onslaughts a growing threat . . . ASIO chief David Irvine.

Photo: ANDREW QUILTY

just futuristic stuff." Mr Irvine referred to the attacks on systems in Estonia that were believed to have originated in Russia as ushering in the modern era of web warfare.

In the April-May 2007 incidents, a cyber attack on the websites of the Estonian Parliament, banks, ministries and broadcasters caused serious economic disruption.

Russia was blamed for the attack because Estonia was involved in a row with Moscow at the time over the

ment agencies and private-sector websites also being regularly targeted.

The Australian Parliament and ministers' offices were also targeted by protest group Anonymous in February as part of its campaign against Communications Minister Stephen Conroy's proposal for an internet filter.

Attorney-General Robert McClelland said online threats from a range of sources including organised

be in a physical war. "This was one of the hot topics at the quintet of attorneys-general [meeting in April in Washington]," he said.

"The concern was whether there needs to be a Geneva Convention in the cyber area where nations agree that they are not going to attack electricity supplies given that would affect hospitals, attack local dams and cause flooding, whether that type of thing should be designated a war crime.

"It's very embryonic stuff but very important to consider."

He said the Attorney-General's Department was at the forefront of the national fight against cyber attack through its national Computer Emergency Team (CERT Australia), which is the peak body for co-ordinating information on cyber threats and takes a lead role in the event of a serious cyber security incident.

CERT worked closely with DSD, ASIO, the Australian Federal Police high-tech crime centre, state governments and the private sector on countering the cyber warfare threat.

The concern was whether there needs to be a Geneva Convention in the cyber area, whether that type of thing should be designated a war crime.

Attorney-General Robert McClelland

relocation of a World War II-era Soviet war memorial — the Bronze Soldier of Tallinn. Russia has denied any involvement.

The intrusions were "denial of service" attacks in which websites were deliberately overloaded with traffic, causing them to collapse.

Intelligence sources also warn that the number of denial of service attacks is also on the rise in Australia, with gaming websites, govern-

ment agencies and private-sector websites also being regularly targeted. crime, hackers and foreign intelligence services, had been elevated to one of the country's top security priorities with the release of a cyber security strategy in November last year.

He said a group of attorneys-general, from the UK, Australia, Canada, the US and New Zealand were considering whether cyber attacks affecting civilian facilities and services should be outlawed as they would

■ See the full interview, *State of security*, with ASIO chief David Irvine in today's *AFR Magazine*.