National Security Australia 2010 Conference

Speech by Mr Ian McKenzie

Director, Defence Signals Directorate

26 February 2010

Good morning. I am Ian McKenzie, Director of the Defence Signals Directorate.

I am pleased to have the opportunity to speak to you today about cyber security. Cyber security is a critical component of national security, as highlighted in Duncan Lewis's presentation yesterday.

I am going to talk about three things today:

- I am going to talk about what the Defence Signals Directorate does in the cyber security area
- I am going to outline the challenges we face in cyber security
- Finally, I am going to discuss some of the things we can do to improve our security.

First though, I feel the need to put a caveat up front. It is not very often that I speak publicly. I am here today to talk about cyber security, but I am not here to talk about DSD's other mission – intelligence. Also, I may be constrained in discussing current cyber security operations.

What is the Defence Signals Directorate and why are we here talking about cyber security?

Most people think of the Directorate as an intelligence agency that intercepts foreign communications, but it also has an equally important information security role.

The Directorate is both an intelligence and security agency and its functions are defined in the Intelligence Services Act 2001.

Given those two functions, you can see that DSD is both the poacher and gamekeeper when it comes to telecommunications. Hence our mission statement – reveal their secrets, protect out own, and it is the protect mission that I am here to discuss today.

On information security matters, the Directorate advises both Commonwealth and State Authorities on the security of their information. The Directorate does not normally provide assistance directly to industry but can do so at the request of another government agency.

The Directorate was established in 1947 to exploit foreign communications and be responsible for communications security in the Australian Defence Force and government departments.

For many years, in fact the first 50 years, the focus of the Directorate's information security activity was on protecting the

nation's secrets, primarily in the defence, diplomatic and intelligence domains.

This has changed dramatically over the last ten years, with advances in Internet technology and the rapid movement of Australia's governments doing business on-line.

We still have to do the more traditional work of protecting the secrets in the traditional national security realm, but in addition the Directorate also has to help government departments and agencies to protect sensitive information in cyber space. And this information reflects a broader understanding of national security.

It is now more broadly related to any sensitive information whether it is economic, commercial, or citizen's personal information. All of which federal, state and territory governments hold in increasingly large volumes and need to protect.

So how do we define the cyber environment?

Cyberspace is where the world conducts its business.

Almost every part of society depends on electronic systems and information stored electronically.

Put simply, the cyber environment is the Internet and any device that can be connected to the Internet in any way.

Today, governments, industry and the public alike all rely on communications technology in their everyday lives. According to the Australian Bureau of Statistics, Australia had 8.4 million Internet subscribers as of June 2009. And this has increased by 1.2 million in just one year.

Many of our everyday services are now being conducted over the Internet as a matter of course. Whether this is Internet banking, lodgement of tax returns, or changing personal details with our local government services, more of us are doing this online.

A report by the Department of Finance and Deregulation showed that more people dealt with the Australian Government online in 2008 than those via a phone or in person.

Technology makes it easy for us to access information on the run. Mobile devices that provide phone, text, Internet, email and other interactive services are increasingly popular. Technology also allows for national and local infrastructure providers to monitor critical systems over the Internet.

On-line has become the primary means of interaction.

However, Australia's reliance on communication technology makes us vulnerable to cyber attack that could disrupt the business of government, critical infrastructure or citizens. This reliance means that the security of electronic information, cyber security, is increasingly important.

Before I move on to talk about the cyber threat, I would like to set the scene for you by explaining one of the services the Directorate provides that helps us gain an understanding of the cyber threat.

This is through understanding vulnerabilities of different government systems.

The Directorate provides a service for government agencies that is known as an Active Vulnerability Assessment. Some of you might know this type of service as penetration testing or red teaming.

This involves hacking into the client agency's network to expose any vulnerability that might be exploited by someone with more sinister intent. The goal is to gain access to the agency's most sensitive information; what we call "trophy information".

I would like to stress that this work is conducted with a number of conditions and constraints:

- first, it is conducted legally. The program is approved by the Minister for Defence, and each operation is performed at the request of, and with the agreement of, the client agencys' Chief Executive Officer;

- It is conducted in an ethical manner – for example, we do not spoof government officials email addresses and pretend to be someone we are not;

- A memorandum of understanding is agreed to by the agency and the Directorate;

- Finally, when successful we don't name and shame. The purpose of the exercise is education and awareness, particularly for senior management to help them understand and manage the risk.

So, you can see that we have placed on ourselves limitations that a hacker does not typically have to worry about.

While I won't comment on the Directorate's success rate I can tell you the active vulnerability assessment is a very effective tool, helping agencies, and especially senior managers, to fully understand the risks they face.

It is also an effective tool for assisting the Directorate evolve its approach to information security to suit the current environment. Traditionally DSD's information security approach has been to advise agencies to protect their information using firewalls and high grade cryptography.

The use of the Internet connected systems and the increase in threats to security of information due to this connectivity has led to a more sophisticated layered approach. It is important to focus effort on the protection of your important information, while still using the power of the internet to do your job.

Let me now turn to the threat.

To vary this presentation and give you a break from my voice, I would like to show you a short video, which we call "The threats we face."

[Play video – Threats we face]

At the 15th January opening of the Cyber Security Operations Centre the Minister for Defence, Senator Faulkner outlined the current cyber threat environment. I will do the same.

As I have stated previously cyber security is a top national security priority. The Australian Government's Cyber Security Strategy was released by the Attorney General in November last year.

The internet brings us flexibility and efficiency and blurs international borders, bringing the world into our homes. As individuals, we can

bank, shop, chat with friends, schedule events, in fact do most of our day-to-day activities on-line.

For the generation now entering the workforce, this convenience is so routine that losing it is inconceivable.

Like all technologies, there is a negative side. Any technology can be turned to serve malicious purposes - and the more widespread a technology is, the more the opportunities for abuse.

Our appreciation of the threat that modern technology can pose is often couched in terms of the ease with which it can be subverted by those who wish us or wish Australia, harm. Cyber intrusions on government, critical infrastructure and other information networks are a real threat to Australia's national security and national interests.

We judge that the cyber threat comes from a wide range of sources, representing a broad range of skills and varying levels of sophistication. They include:

- individuals working alone;
- issue-motivated groups;
- organised criminal syndicates, as well as

- state-based foreign intelligence services.

But I should caution, the very nature of the Internet makes it difficult to precisely attribute the source of individual cyber incidents. It is relatively easy for those who seek to compromise, destroy or steal electronic information to hide in cyber space.

Although we may be able to detect them, we cannot always trace their origins with absolute precision.

The threat is not theoretical. We have evidence of sophisticated cyber intrusions onto networks in Australia, both government and private. Not all are successful, but some have been - on a range of networks. We must meet the challenge of detecting and stopping threats in the ever-changing, ever-adapting world of cyberspace.

So the cyber threat is real, but there is more we need to know.

The establishment of the Cyber Security Operations Centre in the Defence Signals Directorate is part of a broader strategy and represents a significant step towards a comprehensive understanding of the cyber threat.

The Centre will provide understanding of the threat from sophisticated cyber intrusions and will play a fundamental role in

discovering and responding to threats to networks of national significance. The Centre is at the forefront of developing capabilities to gain the edge in cyber space.

The internet is, by definition, about linkages and sharing. And because the problems in cyber space are shared, the response to them must also be shared across government, business, and the community.

The new Cyber Security Operations Centre, while located in the Defence Signals Directorate, includes representatives from a number of government organisations.

These include the Attorney-General's Department, the Australian Security Intelligence Organisation and the Australian Federal Police, as well as other elements of the Defence organisation.

Each government agency represented in the Centre brings different expertise to respond to critical incidents. Each has responsibility for delivery of particular cyber security outcomes.

Of particular importance, the new Centre will work collaboratively with CERT Australia to respond to cyber security incidents. CERT Australia and the Cyber Security Operations Centre are two mutually supporting organisations.

CERT Australia is the national coordination point within government for providing cyber security information and advice for the Australian community and private sector.

It has responsibility for education across the broader Australian community and will provide information and tools in support of this education. CERT Australia will be fully operational by July 2010.

So what else helps defend against the cyber threat and protect information?

A good starting point is the policy manual that my organisation publishes on-line. The Australian Government Information Security Manual remains current and is an effective guide for people to protect their information against cyber exploitation. Application of the guidance contained in the Information Security Manual will help prevent cyber intrusions.

Most recently, we have developed a list of thirty five strategies to mitigate against cyber intrusions. At least 70% of the cyber intrusions the Directorate responded to in 2009 could have been prevented if organisations had implemented the top four of the mitigation strategies.

The strategies are ranked in order of overall effectiveness and are based on analysis of reported security incidents and vulnerabilities detected during the testing of Australian Government networks.

The thirty five strategies have been released and are available on DSD's website and through CERT Australia.

I strongly encourage your organisations to conduct a risk assessment and implement as many of the mitigation strategies as required to manage your particular organisations' level of risk.

Not all organisations are the same, and it is important that you understand your risks before implementing mitigation.

The top four strategies are:

- patching operating systems,
- patching software applications,
- minimising the number of people in the organisation with administrative privileges and
- controlling which programs are able to run on your organisation's computers.

I would especially like to stress the need to keep your software patching up to date. Most hackers will exploit vulnerabilities for which fixes have already been published. The Directorate's experience in testing government networks indicates diversity in patching: some do it well, others not so well.

We all know that there can be issues with patching, but why wouldn't you use the latest advice from your vendor to secure your system as the foundation of your security. It is one of the most effective ways to protect your information.

I would also encourage organisations to continue reporting cyber incidents to the Defence Signals Directorate (in the case of government) and to CERT Australia (in the case of industry). This reporting is critical to the understanding of the threat and more importantly what can be done to defend against the threat.

A lot of what I have talked about is the role of organisations in cyber security. But everyone has a role to play. I would like to finish this talk with some practical advice for you as individuals.

As I have stated before, the internet and of course portable electronic devices brings us flexibility and efficiency and blurs international borders, bringing the world into our homes and allows us to conduct business while on the move and outside of the work environment.

We have found that user awareness and education is an effective tool in defending against cyber threats. Many of the successful cyber intrusions the Directorate has investigated are possible because of poor user awareness.

Your computer, whether it is at home or at work, holds a wealth of information that could well be of interest to someone. Everyone on the internet is vulnerable; all it takes is opening an infected email.

Now of course this doesn't mean that you should not use email, but simply keeping your software up-to-date, including your security software is a vital measure in protecting your information.

From the Directorate's experience a large proportion of attempted or successful hacks start with an ordinary looking email. And in most cases the danger lies in the attached document or web link contained in the email, which when opened or clicked on will activate malicious software, allowing an intruder to steal your information.

The Directorate assesses that when a hacker attempts to steal information from an individual or an organisation they will typically do their homework, most likely by searching the Internet for information about a person or organisation they may be interested in. They will then send a user an email with a subject line or information that grabs the attention of the user.

If the email is opened and the web link contained in the email is clicked on it can infect the user's computer. Once affected, the user's

computer beacons to the hacker.

With this information the hacker is then able to install more malicious software on the user's computer, enabling them to look around the network and steal information that is of interest to them.

The stolen information is often hidden in legitimate computer traffic leaving the network, thereby making it very difficult to detect.

So what can you do?

If you are not sure of the source of an email, or something looks suspicious, you should not click on a web link. Rather you should retype the web address yourself, and this may help spot a bad link.

Detecting an infected attachment is a bit trickier. Keeping your anti-virus software up to date will help in most cases.

Today mobile devices such as phones and laptops are very popular. They are used in everyday life and to conduct work on the move, both

locally and overseas. They can store a reasonable amount of personal or business information and this makes them an attractive and easy target.

These devices are easily lost or sometimes stolen so we all need to be careful given the information they may contain about us. And keep in mind that even if you have a pin code or password to protect your information there are tools freely available on the Internet that can be used to defeat this protection. You should ensure you always use a strong password and where appropriate use encryption options to protect sensitive information.

Connecting your phone or laptop to a public wireless hotspot can leave your information vulnerable to theft. It is not that hard for a hacker to eavesdrop on your conversation or redirect your communications to their computer so they can access your information.

Public terminals such as Internet cafes and those provided in airports or hotel terminals should not be presumed to be considered secured or trusted. A hacker could install a key logger that records every keystroke you make or copy every file you access and use the information to access your network later at his/her leisure.

Another thing that many don't realise when using these terminals is it is easy to retrieve any document you have opened on a computer, even if you didn't save it. Any document you open leaves a trace behind in memory that makes it possible for someone else to retrieve.

So fundamentally, we should always think carefully before using a public terminal or wireless hotspot to access anything that is sensitive to you.

Portable media provides a great opportunity to introduce malicious software onto your computer. And once infected, this can make it possible for someone to steal information. It is important not to plug any portable media into any computer if the computer doesn't have anti-virus software installed or the portable media itself hasn't been virus checked.

In closing, cyberspace is a 24 hours a day world, where old assumptions about geographic boundaries and time zones are obsolete. This is one of the great benefits of modern technology – cyberspace is always open for business. But this also brings great challenges to those of us who guard our electronic information.

Cyber intrusions on government, critical infrastructure and other important information networks are a real threat to Australia's national security and national interests.

We have evidence of successful sophisticated cyber intrusions into networks in Australia, both government and private.

The threat comes from a range of people or organisations including individuals acting alone, issue motivated groups, criminal elements through to foreign intelligence services.

Last week you would have seen the press reports about 'Anonymous' protesting against the Government's internet filtering. We will continue to see groups like this who are loud and a public nuisance, somewhat akin to vandalism on the Internet. However, in addition, there are people with better capabilities and who do not want to be seen and this is a growing problem.

The Defence Signals Directorate is working towards gaining a comprehensive understanding of the cyber threat with the establishment of the Cyber Security Operations Centre.

In addition to the information about the threat environment from the Cyber Security Operations Centre, conducting active vulnerability assessments for government departments and publishing information security policy the Directorate can provide tailored policy and technical advice and is always happy to do so. This is for both Commonwealth and State agencies.

I would like to finish by leaving you with three messages:

- Cyber threats are real and so are the consequences;
- The challenges in cyber security are significant; however
- There are practical steps that you and your organisations can take to defend against the cyber threat.

Thank you.

I am happy to take questions.