

National Security Australia 2010 Conference

**Speech by Mr Mike Burgess
Deputy Director Cyber and Information Security
Defence Signals Directorate
26 February 2010**

Thank you and good afternoon. My name is Mike Burgess and I am the Deputy Director Cyber and Information Security at the Defence Signals Directorate. It is my pleasure to be here today.

I will talk today about the newly established Cyber Security Operations Centre and the challenges we currently face in cyber security.

I will outline the cyber threat that formed part of the motivation for the establishment of the Cyber Security Operations Centre and I will also talk about denial of service attacks as one example of the challenges we face.

As a useful case study I was planning to discuss the denial of service attack that occurred last September, but given the recent events I will not cover this today. The current attacks are subject to ongoing enquires by the Australian Federal Police and therefore it would not be appropriate for me to comment.

This means my speech will not be as long as I intended, however I will talk generically about denial of service attacks and I will be happy to discuss these matters at the end.

But first some background. Everyone here will understand that Australians are becoming increasingly dependent on information and communications technology in many aspects

of their life, whether it is for government services, commerce and business, news and information, social networking or simply for entertainment.

Our dependence on information and communications technology makes us vulnerable to cyber attack.

The Defence Minister said at the opening of the Cyber Security Operations Centre in January

“Like all technologies, there is a dark side. Any technology can be turned to serve malicious purposes - and the more pervasive and accessible a technology is, the more easily it can be abused.”

We all face a number of risks when we go online, and cyber threats can have very real consequences.

I am not suggesting we should be overly alarmed by this threat but rather we need to be aware of the threat and we need to be aware of what we can do to protect ourselves.

The Internet is both an exciting and challenging environment in which to work. In addition to sustained and rapid technological change, it is also growing at an incredible pace.

32 million domains are being added each year.

The Internet is a group of complex, highly inter-connected networks, serving billions of users around the globe in a multitude of languages.

Security considerations as we operate in this environment, as in all environments, is a balancing act, where trade-offs are made between factors such as cost, convenience, and the level of protection required.

In order to make informed decisions about security, it is necessary to think carefully about the types of threats that are present, their probability of occurring and the consequences for individuals or organisations if these threats are realised.

The difficulty of this risk assessment is compounded by the fact that our networks and systems increasingly inter-connected and inter-dependant.

Spectrum of Threats

I will now discuss the spectrum of cyber threats. The stereotype when thinking about cyber threats is perhaps the lone hacker, hunched over a computer in a dim room working to build their reputation or discover secrets.

Hackers today are not only driven by fame, but also fortune.

Now the money is online organised criminal groups are behind a significant proportion of cybercrime.

Cyber crime techniques have been industrialised and are now used on a large scale.

One such technique is a mass email mail out pretending to sell to legitimate products. In reality the email contain malicious software that can be used to steal personal information such as bank account details.

Cyberspace can also be used by those who are interested in violence or causing harm to others in society. Cyber attack could pose significant threat to our national infrastructure and economic security.

In addition Issue Motivated Groups can also use cyberspace to send a political message.

There is also the threat of cyber espionage, which can also impact on our economic and national security. In October last year, the US-China Economic and Security Review Commission released a report detailing significant cyber espionage activity conducted against US government networks.

The report found that the coordinated, professional nature of the operations combined with the type and quantity of information stolen strongly suggested that the attacks were conducted by, or at least on behalf of, a state actor.

In short;

The cyber threat is real,

It is evolving and

It continues to test defences.

In the case of government networks, the risk is not just to the security-classified information.

Sensitive data, financial data and personal data is of high interest.

And the threats do not apply only to government networks.

Prime Minister Kevin Rudd included cyber security as one of his top national security priorities in his inaugural National Security Statement in December 2008. He emphasised that we are “highly dependent on computer and information technology to drive critical industries such as aviation; electricity and water supply; banking and finance; and telecommunications networks.”

Australia's national security could potentially be compromised by cyber exploitation of our defence, government, commercial or infrastructure-related networks.

We need to ensure we are developing capabilities to gain and preserve an edge in cyberspace. The government has taken several measures to ensure that we are able to adequately protect our information.

The Attorney General in November 2009 released the Government's inaugural Cyber Security Strategy. This strategy describes the policies, programs and capabilities it has in place to protect all Australians from cyber threat.

Integral to the implementation of this strategy are two organisations:

Australia's national Computer Emergency Response Team, CERT Australia and the Cyber Security Operations Centre.

Today I will be discussing the Cyber Security Operations Centre located in the Defence Signals Directorate.

The establishment of Centre was outlined in the 2009 Defence White Paper, and it was officially opened by Defence Minister on the 15th January this year.

Most people think of the Defence Signals Directorate as an intelligence agency that intercepts foreign communications.

But it also has an important information security role.

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

Given those two functions, you can see that the Directorate is both the **poacher** and **gamekeeper** when it comes to information.

On information security matters, the Directorate advises both Commonwealth and State Authorities on the security of their information.

While the Defence Signals Directorate will continue to provide information security advice and assistance to Commonwealth and State agencies, the Centre will also provide the government with significant new capabilities.

It is developing a comprehensive understanding of the cyber threat, focusing on the sophisticated threat to the security of Australia's information. This understanding will be used to provide the government with situational awareness in cyberspace.

The Centre will also facilitate and coordinate operational responses to cyber incidents of national importance, and give government response options.

The problems in cyberspace are shared and cannot be addressed by any single organisation acting alone.

For this reason, we work closely with our partners including the Australian Federal Police, the Australian Security Intelligence Organisation and CERT Australia.

We believe that a truly collaborative approach will be one of the keys to success. Staff from the Defence Signals Directorate, the Defence Intelligence Organisation, the Australian Security Intelligence Organisation, the Australian Federal Police, the Attorney-General's Department and the Defence Science and Technology Organisation will work together in the Centre.

Representatives of these organisations will have access to their own tools, data sources and networks to contribute effectively to the work at hand. In this way, Centre will draw on data from the intelligence and law enforcement community, industry and open sources to gain a greater understanding of the cyber threat.

We will also work closely with our allies.

The cyber environment poses a number of unique challenges, one of which relates to identifying the sources of threats.

In the event of an attack via cyberspace, it may not be immediately apparent whether the attack is coming from a computer down the block or across the globe.

And even once this can be determined, the identity of the individual or group controlling those computers may remain unclear.

In these circumstances, close and effective cooperation both domestically and internationally will be essential.

However the nature of the Internet makes it extremely difficult to attribute cyber attacks to a particular source.

The Centre will also provide essential information to CERT Australia to allow it to provide cyber threat information to Australian businesses that own or manage critical infrastructure.

CERT Australia is the national coordination point within government for providing cyber security information and advice for the Australian community and private sector. CERT Australia will be fully operational by July 2010.

Now I'll discuss Denial of Service Attacks

As I mentioned in my introduction I will not be discussing the recent denial of service attacks as they are subject to ongoing enquires by the Australian Federal Police.

But what am willing to say is that any denial of service attack is a public nuisance and is akin to vandalism. And any one involved is committing an illegal act.

Such attacks were described in a recent Australian Strategic Policy Institute report as the equivalent of an “electronic poke in the eye”.

Denial of service attacks can be achieved by several methods. One common approach is to flood a web server with network traffic.

Such traffic can take the form of requests for,

Web pages,

Network connection requests, or

Even requests which require database processing by the server being targeted.

In all of these cases, the server will attempt to respond to the requests in some way, which consumes resources.

If the activity is large enough, the web server is unable to cope and may crash or become unavailable.

A Distributed Denial of Service, otherwise referred to as, “DDoS”, is an attack where multiple computers are used to generate the malicious traffic.

This complicates defensive efforts - if there are only a small number of attackers, network administrators, will be able to easily identify them and block traffic from those points.

If the attacks are distributed, differentiating attackers from legitimate users may be more difficult and blocking all possible points of attack may be impossible.

This brings me to **botnets** - a large network of computers compromised by malicious software that can be used as a tool to generate huge volumes of traffic, which can affect high capacity computer systems.

Botnets were used in attacks against popular sites Facebook and Twitter.

Denial of service attacks are at the lower end of the threat scale though their impact can

be high.

The nature of distributed denial of service attacks means that there is **no guaranteed method** that can be employed to stop the attacks.

One approach to help manage the impact of such attacks is to increase the capacity of targeted computer systems.

But this comes at a cost and in some cases this additional investment may not be worth it.

Your choice of Internet Service Provider is also very important.

A good service provider can assist you in managing the impact of such attacks however your contract needs to allow for this.

So while stopping or defending against denial of service attacks is difficult, the Cyber Security Operations Centre will enable an effective and coordinated approach to any such attack.

In closing

Cyber attacks are a threat to Australia's national security and national interests.

The cyber threat is real; it is evolving and continues to test defences.

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

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

And with our partners from the Australian Security Intelligence Organisation, the Australian Federal Police and the Attorney-General's Department we will provide Government response options and ensure an effective and coordinate response to significant cyber events.

Finally the internet is about linkages and sharing.

And because the problems in cyber space are shared, the response to them must also be shared across:

Government,

Industry and

The community.

Thank you.

I am now happy to take your questions.