CANBERRA 22 April 2015. Can I acknowledge a few people, can I acknowledge Major General Stephen Day, Coordinator of the Australian Cyber Security Centre, Dr Margot McCarthy, the Associate Secretary of the Department of the Prime Minister and Cabinet, can I particularly acknowledge our distinguished international visitors including Elly van den Heuvel, Secretary to the Dutch Cyber Security Council, Mr Jonathan Couch of iSIGHT Partners, Ms Marcelle Lee of the Anne Arundel Community College CyberCenter in Maryland and I thank them in particular and others who have come from elsewhere in the world travelling to participate in this inaugural Australian Cyber Security Conference.

As the Minister responsible, with shared responsibility for the Australian Cyber Security Centre and more generally with responsibility for National Security, including the protection and resilience of Australia's critical infrastructure, cyber security is a key concern for me and my portfolio.

Cyberspace is no longer a separate 'online' environment but completely pervasive and relied on in virtually everything we do in our everyday lives. And that's why effective cyber security underpins confidence in our financial transactions, the accessibility of information and the reliability of critical infrastructure such as our electricity, telecommunications, even our road systems. In the digital age, the Australian economy has become reliant on cyberspace for continued growth and, therefore, strong cyber security is a necessary underpinning of economic security and national security.

You are no doubt aware of the sentiment articulated by the former FBI Director, Robert Mueller, who said, "there are only two types of companies: those that have been hacked and those that will be hacked. Even that is merging into one category: those that have been hacked and will hacked be again."

Cyber criminals routinely target Australian businesses and citizens to steal information that can be turned in to a profit. In 2013, it was estimated the global cost of malicious cyber activity, including cybercrime, is between AU$365 billion and AU$1.2 trillion. Last year, CERT Australia – within my Department – helped businesses to respond to more than 11,000 cyber incidents. Those are staggering figures.

The traditional distinctions between the various different types of cyber actors, their skills and tools, and even their motivations, are blurring. We no longer have neat divisions between State and non-State actors, with cyberspace being used for political and military advantage as well as profit. Some malicious cyber actors have little respect for boundaries or jurisdictions and cannot easily be placed in a particular category or profile.

Across the world, some state actors are involved in cybercrime, while hacktivists are conducting activities in support of Governments, not just for their own ideological causes.

Many of the cyber tools that threaten government agencies are also used to target Australian businesses. The international market for cyber exploitation tools is growing and becoming more accessible. So it is up to us to make sure our response is just as agile and networked so that we can meet – and ultimately defeat – the threats that these malicious actors pose.

In 2002, Richard Clarke, the former special adviser to the President of the United States on cyber security, famously said “if you spend more on coffee than on IT security, then you will be hacked. What’s more, you deserve to be hacked.” Since then the government and the private sector have been investing heavily in cyber security. But now we are looking to the next frontier – how do we maximise that investment? For us, that is about moving the conversation to investment in partnerships, rather than merely talking about funding.

That is why I am particularly pleased to be giving the opening speech of this conference today because this conference represents so much about the government’s commitment to cyber security. I see it as a launch-pad for the Australian Cyber Security Centre (ACSC) – which has only been operating for five months but which has already established its vital role. This conference provides a forum for industry and government to come together and discuss technical and non-technical innovations and solutions for responding to cyber threats.

The ACSC provides the opportunity to ensure todays discussions are ongoing and have long term practical effect. Our adversaries are resourceful and resilient so we must combine our skills and experiences to ensure we can match and exceed the challenges we face. The sharing of those skills and intelligences is the work of this conference.

It is self-evident that government needs to partner with business on cyber issues. Last November, the Prime Minister directed his Department to conduct a complete review of the government's approach to cyber security. I note that Dr McCarthy is our next speaker, without in any way wishing to pre-empt her remarks I will merely observe that when the Prime Minister announced the review he made it clear that it will look for practical ways to improve our national security and work with business to make online commerce more secure.

The majority of Australia's critical infrastructure is owned and operated by the private sector, hence the criticality of government-business partnerships. I know that Dr McCarthy and her team have been consulting extensively with business. It is now up to us to demonstrate that the government is listening, and responding, to the concerns that business may have.

Last year, prior to the review being announced, the Cyber Security Operations Board, which is chaired by the Secretary of my Department, surveyed 29 prominent Australian businesses across a variety of sectors. The aim was to gauge what business thought of how government was performing with respect to cyber security. Amongst the issues discussed, a recurring theme was that many businesses did not expect government to protect them against cyber threats. However, they want better, more timely and actionable information about cyber threats so they can better protect themselves. That is an important distinction and one that has not been lost on the government. In fact, it continues to factor as a major consideration as ACSC develops and comes to better understand the expectations of it out of its role.

Let me talk in a little more detail about the Australian Cyber Security Centre. When the Prime Minister opened the centre five months ago, it marked the beginning of new opportunities for Australian business to cooperate with government.

The ACSC represents a fundamental shift in the way that government wants to partner with business on cyber security. It is a centre to share information and develop solutions to defeat our adversaries and many of these adversaries are common to both the public and the private

sector. The ACSC provides a single location for government and business to collaborate on operational cyber security matters.

The ACSC co-locates the elements of the government's operational cyber security capabilities from within the Australian Signals Directorate, ASIO, the Australian Federal Police, the Australian Crime Commission, the DIO and CERT Australia. Combining the capabilities of ACSC agencies allows us to access a formidable stream of information and analysis of current cyber threats. The staff in the ACSC are some of the country's most dedicated and highly skilled security professionals. They are working together to protect government and industry systems, prevent cyber espionage and apprehend cyber criminals. The Centre is also developing products that provide a single government voice on cyber security issues which will directly benefit industries that are critical to national security.

Establishing the Centre has been a complicated task. It has not been a case of just flicking a switch, moving some desks and enabling different computers to talk to each other. Each of the agencies in the ACSC has unique capabilities and mandates. Some of those mandates are enshrined in legislation. The co-location model protects these individual mandates and retains the reporting lines and oversight authorities that are specific to each agency.

Within this environment, we are exploring how our enhanced situational awareness can support each of the distinct agency missions. By co-locating these agencies in the ACSC we maximise the opportunities to leverage the skills, information streams and resources of each agency to improve the way we approach cyber security overall. The ACSC is making the Australian Government and Australian businesses a harder target for malicious cyber actors. That, of course, is its core mission and it provides new opportunities for government to partner with business on cyber security matters. It is making it easier for industry and government to engage with each other.

For the first time in Australia's history, industry representatives will be invited into the heart of the Australian Government's cyber security operations. The aim will be to will provide access to near real-time information streams and the ability to work alongside one another.

We will have a team of cyber security professionals from industry and government engineering solutions to particularly complex technical issues impacting upon a range of sectors. There will be immediate pay-offs from this environment, including enhanced relationships and technical solutions that are readily applicable to a wider range of applications.

One of the key advantages of this deepening partnership will be developing more timely and relevant threat information that can be digested by the private sector. Because that is what business is asking for and we mean to deliver to business what it needs.

Of course, there are significant challenges for both government and business in sharing sensitive information that is sometimes derived from classified sources but we are determined not to place this in the 'too hard' basket. We will be asking industry to help us find the answers. Importantly, we want to understand how the ACSC's collective information stores can be distilled or filtered in a way that would allow industry better insight into the prevailing threats and opportunities to better protect their systems.

As much as possible, we want this information to be targeted and actionable. We know this is likely to mean building on the briefings that we already provide to particular sectors and working with industry to develop tailored information exchanges that are beneficial for both parties.

Importantly, the ACSC will not be offering a service that can, or is already being, provided by the market. We want to see further innovation and investment in cyber security, and the Government recognises that the ACSC has a niche role in fostering this environment and that development.

It is also important to recognise that government does not have all the answers and we will be looking to our private sector partners to share their expertise and information, which is often well in advance of that of the government sector. Australia is not alone in taking this approach. As you know, in February this year, President Obama signed an executive order aimed at encouraging companies to share more information about cyber threats with the American Government, and its agencies, and with each other, in part, in response to attacks against Sony, Target and other American corporations.

While what I have outlined might seem ambitious, our plans for the Australian Cyber Security Centre don't end there. We also recognise the importance of partnerships that reach beyond our borders and provide us with a rich regional and global picture of cyber threats and trends.

The agencies within the Centre already have, as you would expect, well-established operational relationships with many international counterparts – some of whom are attending the conference here today. The challenge on the horizon for the ACSC will be how to maximise these relationships to provide even better advice and support to government and industry on cyber security matters.

Again, this is not something the ACSC, or government, can achieve in isolation. We know that partnering with multi-national corporations and big business can provide access to the international stage in a way that partnerships with overseas agencies cannot always do. It is our challenge now to determine how that can be achieved in practice, and what government can offer in return for that cooperation. I believe this is another area that will be strongly influenced by the Cyber Security Review, and something that I believe Dr McCarthy will cover in her address shortly.

In closing, I'd like to remind everyone that, as I said at the start of these remarks, the Australian Government considers cyber security as a vital national security and economic security priority. But that doesn't mean that it is locked away in a classified locked box somewhere – inaccessible to industry and the public. Quite the opposite. We recognise the only way to develop resilient systems that continue to foster confidence in our economy is to partner effectively across the public and private sectors, as well as internationally. The Australian Cyber Security Centre is an evolutionary step forward in achieving that goal, and I am excited by the prospects it offers for a depth of industry relations beyond what we have previously enjoyed in the cyber security field.

But it is only a first step. I hope this conference and the early days of the ACSC provide opportunities to canvass not just evolutionary steps, but revolutionary ideas on enhanced government and industry collaboration in the ever changing cyber environment. With those words might I formally declare this important conference open and wish you well in your deliberations. Thank you.