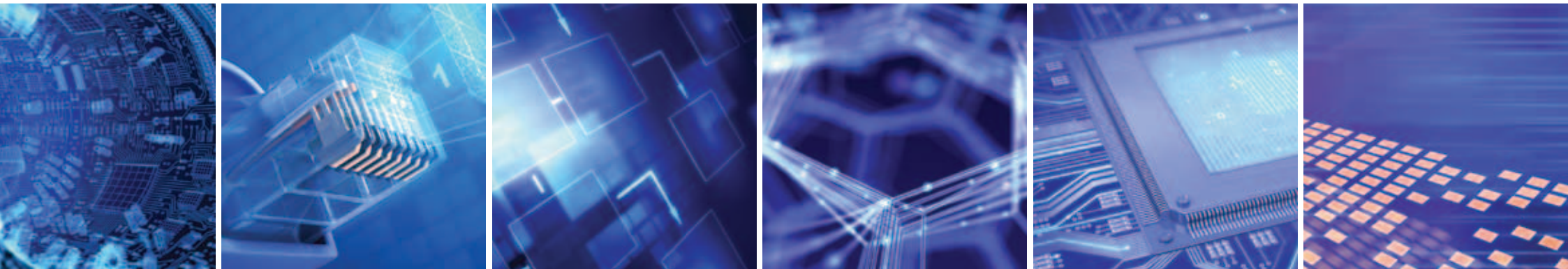
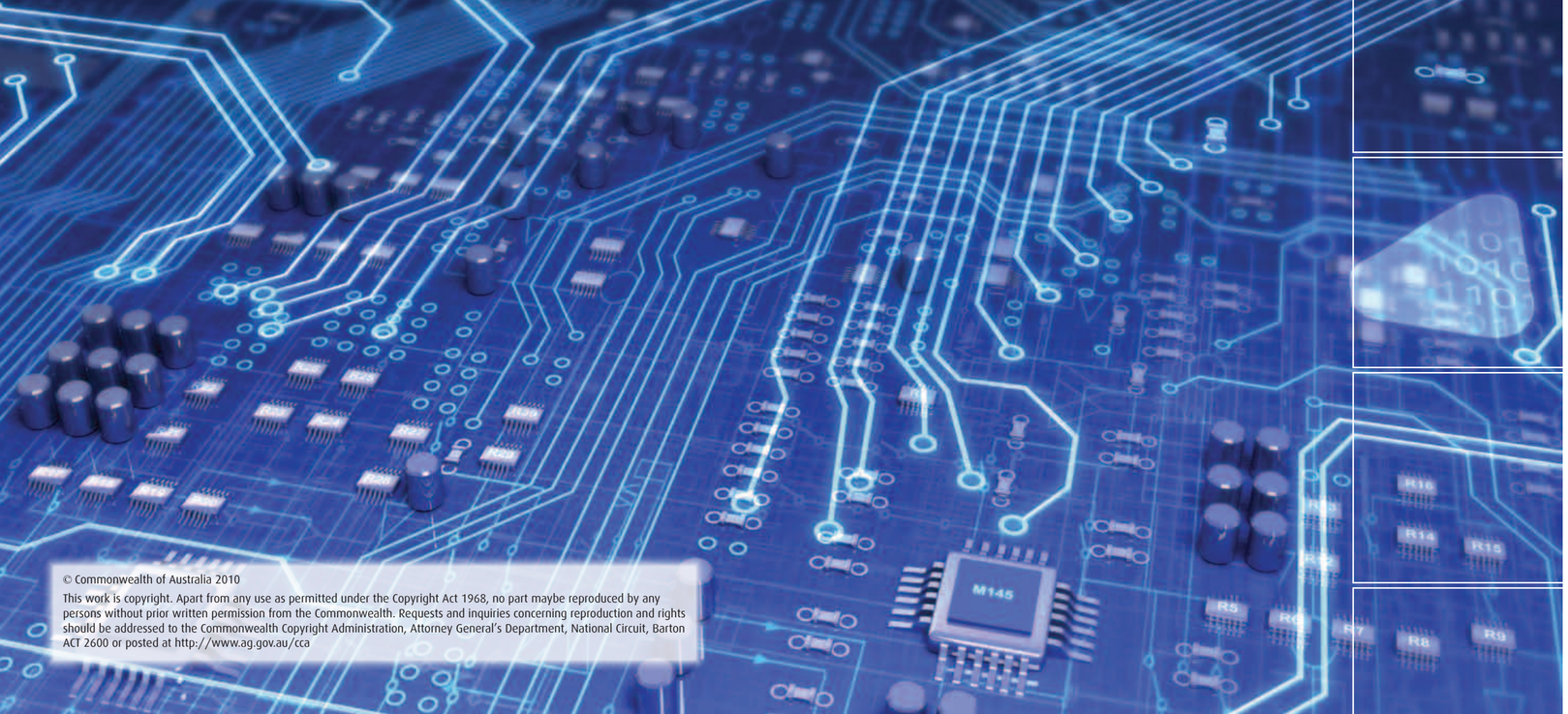
Australian Government

Department of Defence
Intelligence & Security

CYBER SECURITY OPERATIONS CENTRE

Reveal Their Secrets - Protect Our Own | Defence Signals Directorate





Contents

Message from the Director

Australians are becoming increasingly dependent on information and communications technology for a range of purposes and functions. With the increased benefits provided by this technology comes an increased dependence on it, and increased vulnerabilities. We all face a number of risks when we go online, and cyber threats can have very real consequences for organisations and individuals.

In the extreme, cyber warfare and acts of cyber terrorism may pose significant threats to our national infrastructure and economic security. The threats do not apply only to classified government networks. We have evidence of intrusions, both attempted and successful, directed against a range of Australian interests in both the government and private sectors. Notably, most of the hacking activity we see today is aimed at stealing sensitive information, not just security classified material.

Problems in cyberspace are shared and cannot be addressed by an organisation acting alone. There is a comprehensive national cyber security structure in place. It brings together the agencies responsible for cyber security and the protection of Australian Government information and National Information Infrastructure. This structure has been established through the 2008 E-Security Review, the 2009 Defence White Paper, and the recent release of the Australian Government Cyber Security Strategy.

The Cyber Security Operations Centre plays an important role in implementing the Government's Cyber Security Strategy to ensure the security of our information and networks. The Centre will provide comprehensive understanding of the cyber threat to government networks and networks of national importance and will assist the Attorney-General's Department and other government agencies to respond to cyber events across government and the private sector.

Ian McKenzie
Director, Defence Signals Directorate
January 2010

Cyber Security Operations Centre

The Defence Signals Directorate is the national authority on the security of information across government. DSD provides a range of information security services to ensure that sensitive government electronic information systems are not susceptible to unauthorised access, compromise or disruption.

The Cyber Security Operations Centre was established in DSD as an initiative of the Australian Government's Defence White Paper to mitigate the cyber threat to Australia's national security. The Centre meets two needs. It provides Defence with a cyber warfare capability and provides a resource designed to serve all government agencies.

In the past decade, the growing importance of operations in cyber space has become increasingly apparent. Our national security is under threat from a range of cyber actors. Our adversaries are often well resourced, highly skilled and able to defeat commercially available security solutions.

The Role of the Cyber Security Operations Centre

The Centre has two main roles:

- to provide government with a comprehensive understanding of cyber threats against Australian interests; and
- to coordinate and assist operational responses to cyber events of national importance across government and critical infrastructure.

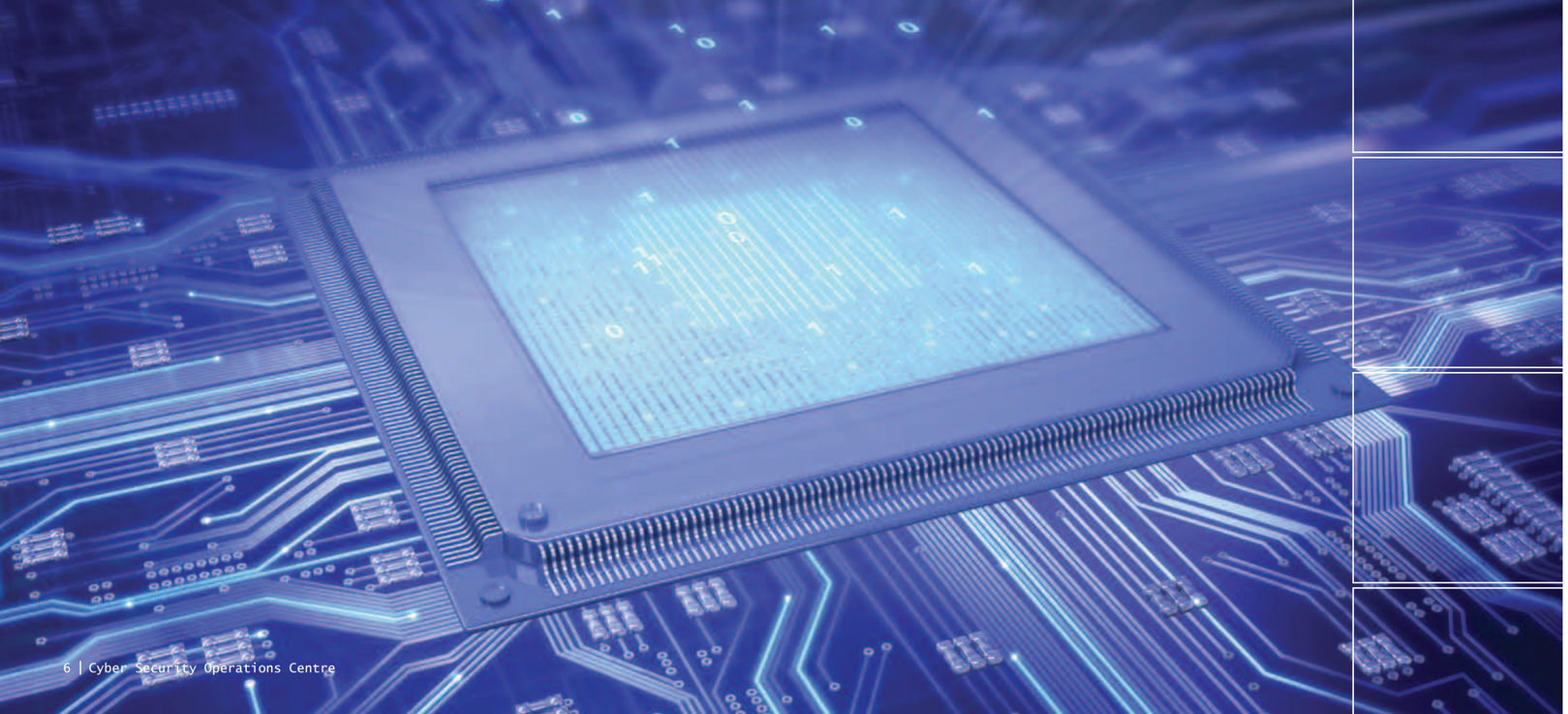
The Cyber Security Operations Centre's operations also complement DSD's other Information Security activities.

Detecting and Responding to Sophisticated Cyber Threats

The Centre identifies malicious activity conducted by sophisticated foreign hackers by using advanced analytic capabilities and techniques. The workforce includes staff highly trained in computer information technology and analysis. This, together with DSD's high powered computing resources, ensures the Centre is able to process large volumes of data to identify cyber threats.

Partners

The Centre has embedded representation from a number of Defence and other government agencies involved in assessing the threat to, and the protection of, Australian interests from sophisticated foreign threats. Representation includes personnel from the Attorney-General's Department, Australian Security Intelligence Organisation, Australian Defence Force, Defence Intelligence Organisation, Defence Science and Technology Organisation and the Australian Federal Police.



Cyber Security Strategy

Cyber Security Strategy

The aim of the Australian Government's cyber security policy is the maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy. The inaugural Australian Government Cyber Security Strategy was publicly launched by the Attorney-General on Monday 23 November 2009. The Strategy shows how the Australian Government is harnessing the full range of resources to help protect government, business and individual Australians.

The Strategy is available online at www.ag.gov.au/cybersecurity.

CERT Australia

As part of the Cyber Security Strategy, the Australian Government is bringing together Australia's existing computer emergency response arrangements under a new national computer emergency response team, CERT Australia. It will ensure that all Australians and Australian businesses will have access to information on cyber threats and vulnerabilities. CERT Australia will incorporate a range of current cyber security activities undertaken by Australian Government agencies, including the Australian Government Computer Emergency Readiness Team (GovCERT.au). It will begin initial operations in January 2010 and will be fully operational by July 2010. CERT Australia will work together with the Cyber Security Operations Centre (CSOC) to help protect Australia's computer systems.

More information on CERT Australia is available at www.cert.gov.au.

Conversation with Matt, a Cyber Event Coordinator

“The CSOC was stood up in July 2009, so that makes me the first ever cyber event coordinator. I came to DSD on the graduate development program in 2008, moving to Canberra from Western Australia. I was interested in a career in intelligence so that is why I applied for DSD. I studied a Bachelor of Arts majoring in media studies and languages and then I completed a Masters in Computer Science. It’s a pretty unusual combination, but it has been really useful for my position as cyber event coordinator.

Basically, I am the bridge between outside government agencies and the CSOC. When a government agency has been the victim of a sophisticated malicious incident that can’t be handled internally by the agency’s designated IT security staff, it is referred to the CSOC. I usually work closely with IT security staff. The easiest way to describe the difference between what I do and the agency IT security staff is they are like the paramedic who is the first to the scene of an accident. As the cyber event coordinator, I come in after the incident has occurred. The CSOC is like a hospital emergency room, it has all the resources and specialists that we need to call upon in a crisis. I assign resources and staff who can provide advice and response options and coordinate the investigation, the clean up and future mitigation. It is my job to make sure the victims of an incident have a seamless experience during a cyber event and the CSOC is carrying out its function as Australia’s cyber security authority.

I draw upon a wide range of resources across the spectrum of the CSOC, from intrusion analysis and detection to threat assessment and incident response. I also reach out to the Australian Intelligence Community and partner agencies. It is my job to stay across everything, all events and what everyone is doing. So I juggle the tasks and manage the relationships. I connect the technical and non technical players by describing in plain terms why a certain cyber event is important or not. I explain the real nature and context of a cyber incident to the victim government agency and my seniors. For example, I have to advise whether or not a malicious cyber attack on a government agency poses a serious threat and if the CSOC should look at things more closely.

What I love about my job is the people I work with and the fast paced environment. Under pressure, I figure out who to talk to, what to do and make judgement calls. The strong sense of team and the feeling of achieving something everyday is rewarding for me. I think it suits my personality.”

Information Security at DSD

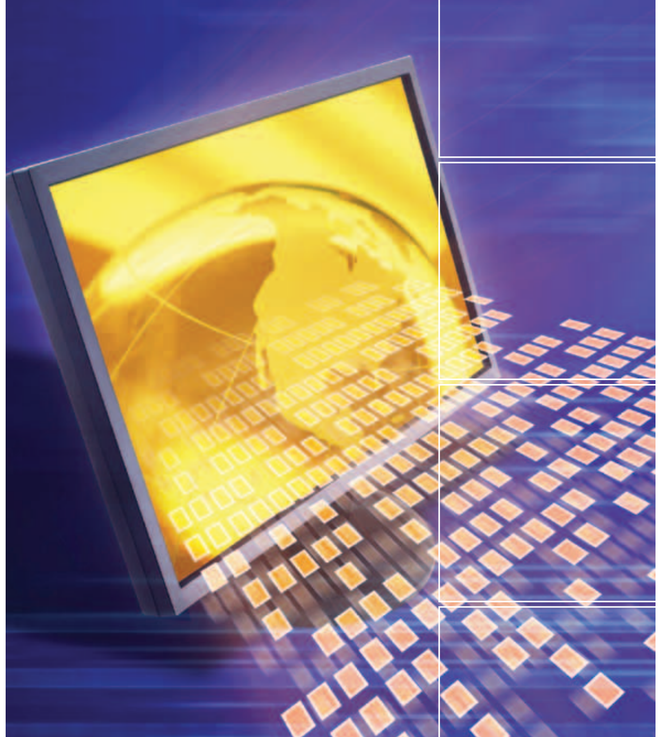
DSD's Information Security function is outlined in the *Intelligence Services Act 2001*. As the Government's national authority on the security of information, the Directorate provides advice and other assistance to Federal and State authorities on matters relating to the security and integrity of information.

Policy Advice and Assistance

As part of this function DSD is responsible for producing the ICT security policy and standards for government and promulgates these via the Information Security Manual. The Directorate liaises with government and academia stakeholders on a wide range of issues, including research, policy, education and projects. DSD is heavily involved in specialised information security training, policy guidance and professional forums in support of the Australian Government and related ICT practitioners and managers. It draws widely on the expertise within DSD, and aims to add unique value to the practice of ICT security in Government.

Cryptographic Services

DSD makes sure Australia is at the international forefront of cryptology by keeping abreast of emerging cryptographic equipment and technologies. The Directorate also advises the Australian Government on high-grade cryptographic equipment and cryptographic modernisation. Areas within Cryptographic Services include the Accreditation Team, the Australian Electronic Key Management System, Cryptographic Project Liaison and the Emanation Security Program.



ICT security product evaluation

DSD facilitates the evaluation of ICT security products for the Australian Government. Its evaluation programs include cryptographic, high assurance and cross domain solutions. DSD also manages the Australasian Information Security Evaluation Program (AISEP) which allows the security claims of ICT products to be independently assessed against internationally recognised criteria. This gives both government and non-government sectors assurance that a product will meet individual security needs. The Evaluated Products List (EPL) can be accessed via DSD's website.

Industry Coordination

Countering the threat to the security of Government's information requires DSD to work closely with the ICT industry to deliver threat and vulnerability information and to help DSD to build capability and expand its capacity to secure government ICT.

Network Vulnerability Operations

DSD provides critical support functions, technical advice and practical expertise in ICT systems and network security. Its expertise is also used to identify and help mitigate vulnerabilities within the Australian Government and National Information Infrastructure. The Directorate's services revolve around ICT security incident response, ICT system forensics and specialist assistance, vulnerability assessments, education and awareness.

A Day in the Life of an Infosec Techie

What do you like about DSD?

It is a great place to work, I am amazed by my colleagues every day. The commitment and contribution people make at work is pretty amazing. It really is a place where people are making a positive difference in supporting Australia's national security. Apart from the importance of DSD's work, it is a very supportive, innovative and fun place to be.

What is the most challenging aspect of your job at DSD?

There are many challenges including keeping up with changing technology, providing the right advice to government when there are many different systems and uses, and helping government users understand their key role in the security of computer systems. As users adopt new technologies, they need to understand and manage associated risks. There are no absolute answers for maintaining the right balance between good security and enabling government to be effective. In a fast paced environment, every day there are new problems to solve. In short, it's never dull!

How is the IT environment changing and what is the greatest danger facing people online today?

The online and computer world changes practically every day. People have different expectations from their computers and mobile device and are more reliant on them than ever before. There are many concerns working in the online environment, but it is impossible not to work online. So the challenge is how best to work protecting ourselves but at the same time practicing good security in our work environment.

How is DSD helping Government secure their systems against online threats?

DSD continues to assist Australian Government agencies with assessing and enhancing the security posture of their networks. DSD's IT security policy guidance is continually evolving to meet the threats of today and into the future. DSD is committed to ongoing IT security education and awareness. Partnerships with industry facilitate the provision of improved security products to government agencies.

OUR VALUES

We make a difference

We give our customers the critical edge
Our output affects operations and safety
Our products are unique

We belong to a great team

We succeed through teamwork
We recognise others' input
We support and care about each other

We strive for excellence

We seek and foster talent
We are world class
We are committed and enthusiastic
We are flexible and responsive

We are meticulous in execution

We always act legally and ethically
We are accountable to the public through government for everything we do
We manage risk effectively

We are audacious in concept

We operate in the slim area between the difficult and the impossible

OUR MISSION

Reveal Their Secrets – Protect Our Own

About DSD

DSD's mission, "Reveal their secrets – Protect our own", says a lot about what it does. The Directorate is the national agency responsible for foreign signals intelligence and is the national authority for information security.

As part of the Department of Defence, and sitting in the Australian Intelligence Community, DSD incorporates some of the most powerful leading edge technologies in a dynamic environment to support Government objectives, including:

Combating International Crime, Weapons Proliferation and Terrorism
Supporting Military Operations
Protecting Australian Government Computer Networks

DSD's functions are outlined in the *Intelligence Services Act 2001* and its activities are subject to independent oversight by the Inspector-General of Intelligence and Security. The *Intelligence Services Act 2001* also provides for the Parliamentary Joint Committee on Intelligence and Security to conduct regular reviews of the administration and expenditure of DSD along with Australian Security Intelligence Organisation, Australian Secret Intelligence Service, Office of National Assessments and the other Defence intelligence agencies.

For more information about DSD visit www.dsd.gov.au

Media contacts

Defence Media Liaison
Phone: 02 6217 1999
Email: mediaops@defence.gov.au

DSD Organisational Chart

Director DSD
Ian McKenzie

INTELLIGENCE DIVISION
Deputy Director Intelligence
Maria Fernandez

CAPABILITY DIVISION
Deputy Director Capability
Lynwen Connick

CYBER AND INFORMATION SECURITY DIVISION
Deputy Director Cyber and Information Security
Mike Burgess

ASCNO
Assistant Secretary Computer Network Operations
Michael Scotton

ASISO
Assistant Secretary Information Security Operations
Tim Scully

CYBER SECURITY OPERATIONS CENTRE
Lynn Moore