Australia's Cyber Vision 2020, cyber security strategy, cyber science and technology plan

The exponential growth of information and communications technology (ICT) technology that includes Internet, telecommunications networks, computer systems, and embedded processors and controllers, has led to creation of Cyberspace, a global domain within ICT. The economic, social and strategic influence is exerted within, and through cyberspace domain, much like the land, air and maritime domains.

Cyber technology has become an embedded feature of modern military systems. Defence and other critical national systems are rapidly evolving to become software defined (i.e. cyber-physical) systems and are also increasingly relying on networks for their operation. There is also a developing relationship between cyber and the military capability of electronic warfare driven by the convergence of technologies, techniques and concepts and in the future we can expect to see integration of these capabilities into one continuum.

In addition to great opportunities, cyberspace also presents significant challenges. According to leading cybersecurity market intelligence agency, Cybersecurity Ventures, cybercrime will continue to rise and cost businesses globally more than $6 trillion annually by 2021.

The australian government unveiled its cyber security strategy in April 2016, and allocated A$230m to various initiatives over four years. The pilot Joint Cyber Security Centre was opened in Brisbane on 24 February 2017. More than 20 organisations are represented from the energy, water,

finance, transport and mining sectors, as well as Queensland Government, CERT Australia, the Australian Federal Police and the Australian Criminal Intelligence Commission. Priorities for the Centre are automated information sharing and targeted analysis of specific cybercrime threats against Australian industry networks.

Following the declaration of Australia's offensive cyber capability in the Cyber Security Strategy¸ the Prime Minister announced in November 2016 that offensive cyber capabilities are being employed in support of Australian Defence Force operations against Islamic State. This contributes to our national deterrence posture, and promoted mature discussion about the application of such capabilities under international law, says the annual update.

The DSTO realeased Cyber Science and Technology Plan outlining the DSTO strategy to help strengthen Australia's cyber capabilities and deliver impact to Defence and national security.

Cyber Threats and challenges

In addition to great opportunities, cyberspace also presents significant challenges. Investment by the commercial sector in ICT is resulting in an almost continuous innovation of new cyber devices and novel applications; deepening human-technology partnerships; and an evolving cyber threat that is continually growing and changing.

The proliferation of ransomware – where the victim is prevented from accessing their systems or data until a ransom is paid
– remains an endemic problem across the globe. In Australia, reports of ransomware activity reported to the Australian Cybercrime Online Reporting Network roughly doubled in 2016 compared to 2015. Australia remains the main target of

malicious software – predominantly ransomware and software that steals personal information – in the Asia Pacific region in 2016, likely due to our economic prosperity and high adoption of technology.

Cyberspace has no national boundaries, has the potential for strong asymmetry and provides global reach for nation states, organised groups or individuals to mount an attack or use cyberspace for malicious purposes. Australia has ranked cyber security as one of the key risk areas for both Defence and national security

The enduring challenges identified are: Environmental Surprise : technology progress and its adoption and adaptation can result in unexpected morphing of cyberspace– for example the rapid emergence of mobility and cloud computing. Unknown and Persistent Threat: the cyber threat is highly variable, diverse and rapidly evolving.

Untrustworthiness: There are no guarantees that hardware devices and components; software, firmware and applications; data and information; and people can be trusted. Data-to-Decision Reflex: the ability to respond appropriately, proportionately and in relevant timescales. Cyber-EW concepts, are an emerging area hence concepts are immature.

Advancing the cyber strategy

Strong cyber security is a fundamental element of our growth and prosperity in a global economy. It is also vital for our national security. In April 2016, the government of Australia forwarded a cyber security strategy proposal to solidify its cyber space and fend off the increasing digital threats hurled by enemy states, cybercriminal organizations, and amateur opportunists.

The strategy establishes five themes of action for Australia’s

cyber security over the next four years to 2020: A national cyber partnership, Strong cyber defences, Global responsibility and influence, Growth and innovation and a cyber smart nation.

The policy proposes “five themes of action” to see the strategy through to its execution and implementation.

A National Cyber Partnership: To develop co-operation and co-leadership between government bodies and business leaders for the design and implementation of the strategies. Also, to understand and estimate the cost of the cyber threats to the Australian economy.

Strong Cyber Defenses: To evaluate the cyber security performance of government agencies and use advanced technologies to reinforce the security systems of Australia, thereby making the Australian cyber infrastructure resilient to online threats.

Global Responsibility and Influence: To join International partners and promote an “open, free and secure Internet”, and find and terminate the cyber spaces that cyber criminals consider a safe haven.

Growth and Innovation: To bring about innovation in the cyber security defense system by establishing a research and development department. Plus, to empower cyber security businesses to build, promote, or export cyber security products and services.

A Cyber Smart Nation: To spread cyber security awareness in the country as well as to bring on board more cyber security professionals.

It requires partnership involving governments, the private sector and the community. The Australian Government will take a lead role and in partnership with others, promote action to protect our online security.

Much of our digital infrastructure is owned by the private sector, so securing Australia's cyberspace must also be a shared responsibility. It will be important that businesses and the research community work with governments and other stakeholders to improve our cyber defences and create solutions to shared problems.

The new Critical Infrastructure Centre in the Attorney-General's Department – in cooperation with the Australian Cyber Security Centre – will work closely with our national critical infrastructure companies to identify cyber vulnerabilities, develop risk assessments and risk management strategies.

Cyber security incidents also offer an opportunity to learn. A new mandatory data breach notification law has come to Australia. Effective in early 2018, if not sooner, the new law will require businesses to notify serious data breach incidents to the Australian Information Commissioner and customers whose data has been compromised. This should place cybercrime high on Australian boards' agendas and drive the revamping of existing cyber security systems.

To grow our cyber security capabilities to anticipate and respond to cyber threats, we must address our shortage of cyber security professionals. Government has partnered with industry and academia to build research and workforce capability in cyber security by establishing Academic Centres of Cyber Security Excellence,

The Prime Minister and the Minister Assisting the Prime Minister have led international collaboration on cyber security. Australia has continued cyber policy dialogues with China, India, South Korea, Japan, New Zealand and will shortly hold its inaugural dialogue with Indonesia. In February 2017, cyber security was permanently added to the agenda of the Australia-Indonesia Ministerial Council on Law and Security. Bilateral cyber policy engagement has been expanded with other

Indo-Pacific nations, including Singapore, Fiji and Samoa.

Cyber Capabilities and S&T plan

The critical capabilities for cyberspace are threat assessment, intelligence, situational awareness, information assurance, and planning and shaping. Threat estimation includes judgment of the possible technical nature of threats (e.g. hardware or software based), likely manifestations (e.g. intermittent loss of communications) and the potential impact on cyber and interdependent systems.

Information assurance encompasses the confidentiality, availability and integrity of information whether it is stored (at rest), being processed (in use) or transmitted (in transit). Intelligence is the collection, processing and analysis of information pertaining to cyberspace and its actors. Situational awareness is the dynamic understanding of the current and projected state of own and other systems and actors and is necessary for decision making. Planning and shaping includes the selection and use of capabilities to influence and shape the cyber environment to support operations.

The DSTO Cyber Science and Technology Plan outline the **DSTO strategy** to help strengthen Australia's cyber capabilities and deliver impact to Defence and national security by:

• Identifying foundational research themes that are enduringly relevant, can be applied to priority problems and underpin the development of cyber capabilities.

• Developing the ideas, concepts and methods that will forge the relationship between cyber and other defence capabilities such as electronic warfare.

• Ensure a relevant, resilient and responsive DSTO cyber

capability and foster a cohesive, integrated national science and technology base.

Five foundational research themes

S&T is central to developing and seizing cyber opportunities, overcoming cyber challenges and achieving success for Australia as a digital nation, says Dr Alex Zelinsky Chief Defence Scientist. The Plan identifies **five foundational research themes** that are enduringly relevant; sufficiently comprehensive to cover the cyber problem space and support the development of future capability; and can be readily applied to priority problems.

These are:

• **Technology Forecasting:** Technology forecasting is a multi-disciplinary, capability focused activity, and typically includes Science and technology analysis of technology trends and their potential impact, prototype building and testing, operations research and analysis and modeling and analysis of potential future threats.

• **Cyber Influence and Data Analytics:** Research and development of data processing and big data analytics; social influence and behaviour analysis; multi-level information fusion; reasoning under uncertainty; machine intelligence; reasoning and decision support.

• **Sensing to Effects:** Research and development of sensor to effector concepts, techniques and technologies, and the associated planning and decision making, includes Cyber-EW effects.

• **Autonomous Cyber Systems:** Research and development of concepts, techniques and technologies for automated through to autonomous data processing and analysis and decision making; Artificial intelligence, machine learning, automated reasoning and planning under uncertainty, self-adaptive waveforms and algorithms.

• **System Design for Resilience:** The science and technology underpinning cyber systems designed to operate with the explicit assumption of untrustworthiness. Trusted, trustworthy and robust systems; self-repairing and survivable networks; static and dynamic malware analysis; vulnerability analysis; hardware and software trojan analysis; Secure architectures, dynamic security protocols (including identity management), systems architecture and policies and cloud computing.

The Plan ends with the outline of a proposal to establish a Cyber Security National Science and Technology Strategy designed to: integrate and orchestrate the national resources to focus on cyber security research in support of national security, and grow the national science, technology and professional capability to benefit all sectors of the cyber community.

References and resources also include:

https://www.contino.io/insights/new-data-breach-law-drives-australias-cyber-security-focus

https://cybersecuritystrategy.pmc.gov.au/cyber-security-strategy-first-annual-update-2017.pdf