AUSTRALIAN DEFENCE CYBER INDUSTRY CAPABILITY

Australian Government
Australian Trade and Investment Commission

OVERVIEW

For global defence forces and defence industries, cyber security is more critical than ever. A combination of more sophisticated attacks, heightened threat levels and the potential for wide-spread damage in distributed environments combine to increase perceived risk. Meanwhile, cyber threats are becoming harder to detect. The ability to take timely, mitigating action has never been more challenging.

New cyber threats are changing the competitive landscape of the cyber security industry. Global defence companies are transforming their operations and capabilities, investing in new and disruptive technologies, such as blockchain, quantum computing and artificial intelligence. These investments will drive further changes in military cyber security requirements.[1]

The Australian Government is deeply committed to cyber security. It is combining initiatives into a coordinated, whole-of-government strategy, which includes A$400 million worth of investment to support cyber security capabilities. Cyber defence will also be a prominent beneficiary of the A$730 million Next Generation Technologies Fund. With clear government prioritisation, there is now a strong commercial impetus in Australia to create new and innovative cyber solutions that have strong, global appeal.

The Australian Defence Cyber Industry Capability Matrix, page 5.

GLOBAL MARKET OPPORTUNITY

The global defence cyber security market was worth an estimated A$20.1 billion in 2018, and A$20.7 billion in 2019. It is expected to grow to A$24 billion by 2023 at a compound annual growth rate (CAGR) of 3.6 per cent. According to industry reports, the slight acceleration in growth early in the current decade is mainly due to an increase in defence budgets and the rising sophistication of cyberattacks.[2]

The defence cyber security market includes a wide spectrum of products and services. This is because defence forces require cyber security for a diverse mix of activities, from defensive and offensive operations to weapons and tactical networks. Defence forces also need to protect critical systems, data and data availability, information gathering and threat assessments.

There are many similarities between the defence and commercial cyber security markets. Common trends, drivers and disruptive technologies create similar products. There are major differences, however, such as the need for offensive cyber capabilities, military-grade encryption and segregated networks. Defence forces need cyber security to be hardened well beyond standard civilian levels.

AUSTRALIAN CAPABILITY

Australia has one of the strongest cyber security frameworks in the world. National capabilities are currently being strengthened by A$230 million worth of investment via the Australian Cyber Security Strategy. The Strategy's funding complements the Government's 2016 Defence White Paper investment in cyber capabilities.

With rising domestic demand, Australia's defence industry has a reputation for delivering defence-grade cyber security products and services. Many Australian cyber companies service existing international defence organisations and defence forces. Over the past decade, they have partnered with global defence primes to solve cyber security problems.

As a result, Australia's cyber-industry now creates world-class products that are swiftly incorporated into existing systems and platforms. Australian expertise includes:

- Secure mobility solutions
- Quantum encryption
- AI driven deception
- IoT security
- Cloud-security.

DEFENCE CYBER AND AUSTRADE

The Austrade Defence, Advanced Manufacturing and Space team provides Australian companies with advice on doing business overseas, including:

- international market selection and market entry/expansion strategies
- business culture and etiquette
- upcoming international promotions such as cyber security and defence trade shows and missions
- information on financial assistance and other government programs.

GLOBAL DRIVERS

The North Atlantic Treaty Organization (NATO) states that cyber threats are becoming more frequent, complex, destructive and coercive. They are continually evolving through changing attack patterns and development structures. This makes it harder to detect and enact proper mitigation procedures in time.

As cyber attacks evolve and become more widespread, civil and defence authorities are highlighting the importance of audits, risk assessments and penetration testing across critical assets. Defence budgets are rising, as non-state actors join hostile states in developing sophisticated attacks. Cyber security legislation is also driving demand for enhanced cyber capabilities.[3]

In response, global defence industries are transforming their operations and capabilities. They are investing billions into existing and disruptive technologies that will intensify cyber security innovation.

Future defence requirements for cyber security solutions will demand solutions with a range of possible applications. They will look for suppliers who can deliver a one-stop-shop delivery model that includes support systems and training services. This will permit faster implementation and enhanced support.

Additionally, defence-dedicated networks will look for enhanced protection, especially for legacy components.

As demand evolves, this provides opportunities for Australian cyber small and medium-sized enterprises (SMEs) to create tailored solutions that address skills enhancement and education in new and existing cyber technologies.

THE FUTURE OF CYBER WARFARE

From a defence standpoint, cyber warfare refers to an emerging domain, dubbed the fifth domain. It consists of new doctrines, concepts, organisations, strategies and tactics, and is applicable to offensive and defensive operations.

The cost, accessibility and anonymity of cyber warfare has made it a new weapon of choice in multiple scenarios. Cyberspace has already become a battlefield. It is where nations and non-state actors engage in operations to gather intelligence or gain diplomatic advantage.

Countries are enforcing mandatory implementation of cyber security standards. Measures include mandatory incident detection and reporting, safety audits and more secure defence acquisition.

Large cyber vulnerabilities remain, however. These include the need to secure weapon systems, protect legacy components, and bridge cyber skills gaps. Overcoming these vulnerabilities will be costly.

The Australian Defence Force (ADF) aims to enhance the cyber resilience of its deployed forces. Training programs will enhance the capabilities of the ADF's cyber workforce. New cyber-defence roles will be created, tasked with protecting cyber networks. Offensive cyber warfare capabilities, deception and disinformation will become key elements in the ADF's cyber defence capabilities.

The ADF's cyber goals create multiple opportunities. Currently, the cyber market is dominated by global companies that specialise in defence and enterprise IT systems. With a track record of supporting global primes, Australia's cyber companies have demonstrated their ability to match global needs with highly technical solutions.

1. 2019 Frost & Sullivan, Global Military Cyber Security market, Forecast to 2023
2. 2019 Frost & Sullivan, Global Military Cyber Security market, Forecast to 2023
3. 2019 Frost & Sullivan, Global Military Cyber Security market, Forecast to 2023

ABOUT AUSTRADE

Austrade is Australia's leading trade and investment agency.

We have the power to open doors, unlock opportunities overseas and help Australian businesses go further, faster.

We also introduce foreign investors to Australian partners, strengthening global supply chains, creating local jobs and boosting the economy.

Promoting Australia's growth and prosperity is why we're here.

AUSTRADE CONTACTS

Adam Sandilands
Senior Adviser – Defence
Defence, Advanced Manufacturing and Space
T +61 2 6201 7372
E Adam.Sandilands@austrade.gov.au

Michael Riera
Adviser – Defence
Defence, Advanced Manufacturing and Space
T +61 2 9392 2403
E Michael.Riera@austrade.gov.au

AUSTRALIAN DEFENCE CYBER INDUSTRY CAPABILITY MATRIX

AUSTRALIAN COMPANY	GOVERN / IDENTIFY				PROTECT							DETECT & RESPOND						R&D	State – HQ
	Risk and Compliance	Professional Services	Education & Training	Managed Security Services Provider / SOC*	Information, mobile and messaging security	IoT Security & 3rd Party Mgmt	Identity and access management / Fraud	Encryption	Network (Firewall & VPN)	Endpoint, Application Security and Whitelisting	Cloud Security	Threat Intelligence / Detection	Penetration Testing	Security and Behavioural Analytics	Active Defence (Red teaming, Deception, Threat hunting)	Incident Response	SOAR / SIEM*		
Airlock Digital	●									●									SA
archTIS		●	●		●		●				●							●	ACT
Arkose Labs					●		●				●	●		●					QLD
Berkeley Solutions							●												NSW
Clearbox Systems	●	●			●			●	●			●		●				●	NSW
Cogito Group	●	●		●	●	●	●	●			●			●		●	●		ACT
Cipherpoint	●				●			●										●	NSW
Crypto Workshop								●		●									VIC
Cryptoloc Technology					●			●			●								QLD
Cybermerc	●		●	●							●	●	●	●	●	●	●	●	ACT
CyberMetrix	●		●			●													QLD
CyberOps	●	●			●	●	●	●	●	●	●	●	●		●			●	SA
Cydarm	●						●									●	●		VIC
Dekko Secure	●	●			●		●	●			●						●	●	NSW
DroneSec			●									●	●		●	●		●	NSW
ditno	●					●		●	●	●	●	●		●	●	●		●	NSW
Fifth Domain			●														●	●	ACT
Future Fibre Technologies												●						●	VIC
HackHunter						●				●		●	●	●	●	●			VIC
Huntsman Security	●				●	●	●			●	●	●		●		●	●		NSW
Hydrix	●	●			●	●	●	●	●										VIC
Hypersec	●	●	●	●	●	●					●	●		●		●	●	●	ACT
Ionize	●	●	●	●			●		●	●	●	●	●	●	●	●	●		ACT
Janusnet	●				●													●	NSW
KELSIEM	●	●					●				●	●		●		●	●		NSW

SOC: Security operations centre; SOAR: Security orchestration, automation and response; SIEM: Security information and event management

AUSTRALIAN DEFENCE CYBER INDUSTRY CAPABILITY MATRIX

AUSTRALIAN COMPANY	GOVERN / IDENTIFY				PROTECT							DETECT & RESPOND						R&D	State – HQ
	Risk and Compliance	Professional Services	Education & Training	Managed Security Services Provider / SOC	Information, mobile and messaging security	IoT Security & 3rd Party Mgmt	Identity and access management / Fraud	Encryption	Network (Firewall & VPN)	Endpoint, Application Security and Whitelisting	Cloud Security	Threat Intelligence / Detection	Penetration Testing	Security and Behavioural Analytics	Active Defence (Red teaming, Deception, Threat hunting)	Incident Response	SOAR / SIEM		
Kinetic IT	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	WA
Myriad Technologies		●	●		●		●	●			●					●		●	QLD
north	●	●	●	●		●	●			●	●	●	●	●	●	●	●	●	ACT
Nuix	●	●	●				●			●		●		●	●	●	●		NSW
OpSys	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	SA
Paraflare		●		●						●		●	●	●	●	●	●		NSW
Penten		●	●	●	●			●	●	●		●		●	●			●	ACT
Privasec	●		●	●		●					●	●	●	●	●	●			NSW
Prophecy International	●	●												●				●	SA
ProvenDB	●				●							●						●	VIC
Pure Security	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	VIC
QuintessenceLabs		●			●	●		●		●	●							●	ACT
Randtronics	●	●	●	●		●		●			●							●	NSW
RedFig Consulting									●			●		●				●	VIC
Red Piranha	●		●	●					●			●	●		●	●			WA
ResponSight	●											●		●					VIC
Sapien Cyber				●		●	●					●		●	●	●	●	●	WA
SecureStack	●				●		●	●		●	●	●		●			●		QLD
Secure Code Warrior	●		●							●									NSW
Seer Security	●	●			●	●												●	VIC
Senetas Corporation				●	●	●		●	●		●								VIC
Trellis Data	●				●	●						●		●	●			●	ACT
Vault Cloud	●		●	●	●	●	●	●	●	●	●	●	●				●		ACT
VeroGuard Systems					●	●	●	●			●	●							VIC
With You With Me		●	●									●	●		●	●			NSW

SOC: Security operations centre; SOAR: Security orchestration, automation and response; SIEM: Security information and event management

18-19-343. Published February 2020

austrade.gov.au

Australian Government

Australian Trade and Investment Commission