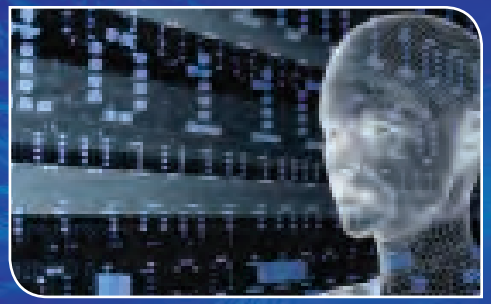
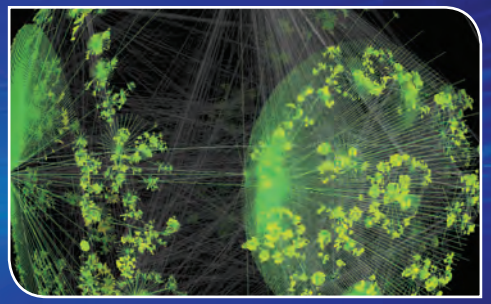
Australian Government
Department of Defence
Defence Science and
Technology Organisation

Cyber 2020 Vision

DSTO cyber science and technology plan

DSTO Science and Technology for Safeguarding Australia

Foreword

Chief Defence Scientist
Dr Alex Zelinsky

Deputy Secretary Intelligence and Security
Mr Steve Meekin

The ability of technology to profoundly shape our future is exemplified by the impact information and communications technology (ICT) has had on government, business and broader society. The creation of cyberspace has been a game changing transformation. Cyberspace is a global domain within the ICT environment that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers. The rapid development, adoption and adaptation of ICT has evolved cyberspace to being a domain within which, and through which, influence is exerted. This includes economic, social and strategic influence.

Today, there is a growing national and global dependence on cyberspace for economic wealth and societal well-being; the control and monitoring of critical infrastructure; the storage, processing and management of sensitive information; and it underpins both commercial and government business. Moreover, cyber technology has become an embedded feature of modern military systems. There is also a developing relationship between cyber and the military capability of electronic warfare driven by the convergence of technologies, techniques and concepts.

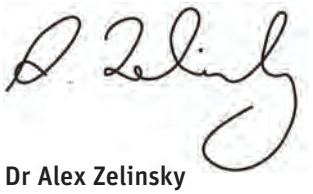
In addition to great opportunities, cyberspace also presents significant challenges. Investment by the commercial sector in ICT is resulting in an almost continuous innovation of new cyber devices and novel applications; deepening human-technology partnerships; and an evolving cyber threat that is continually growing and changing. All of these factors place high demands on cyber security. Australia has ranked cyber security as one of the key risk areas for the nation and in 2013 established the Australian Cyber Security Centre to lead the Government's response to cyber incidents and to protect Australian network and systems. Science and Technology (S&T) is a fundamental enabler of the work of the Australian Signals Directorate and the Australian Cyber Security Centre in protecting our use of cyberspace.

S&T is central to developing and seizing cyber opportunities, overcoming cyber challenges and achieving success for Australia as a digital nation. However, the magnitude and diversity of the cyber problem space is extremely large and the national innovation resources in cyber and cyber-related S&T are not abundant. To help strengthen Australia's cyber future careful choices on S&T investment and careful nurturing of the national cyber S&T capabilities (people, collaborative partnerships and infrastructure) is needed.

This plan outlines 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.
- Identifying measures for maintaining DSTO cyber capabilities that are relevant and responsive to Defence and national security needs, and which also help foster and grow an integrated, cohesive national cyber S&T community.

The Plan has benefitted greatly from consultation with Australia's defence, industry and academic communities. We have also received welcomed advice from our international partners. We would like to take this opportunity to thank everyone who has contributed.



Dr Alex Zelinsky
Chief Defence Scientist
6 May 2014

Mr Steve Meekin
Deputy Secretary Intelligence and Security
6 May 2014

Contents

Executive summary

The DSTO Cyber Science and Technology Plan was developed to guide the Organisation's activities in cyber and to provide key stakeholders, and the national and international science communities, a detailed view of the DSTO approach to address the current and future cyber challenges.

The Plan sets out the DSTO future directions in cyber research; how DSTO will address the emerging relationship between cyber and the allied defence capabilities of electronic warfare (EW), signals intelligence (SIGINT) and communications; the steps DSTO will take to ensure that DSTO science and technology is relevant, resilient and responsive; and how DSTO will engage with the national community to foster a cohesive, integrated national cyber science and technology capability.

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
- Cyber Influence and Data Analytics
- Sensing to Effects
- Autonomous Systems
- System Design for Resilience

The underpinning methodology used in the analysis of options and the selection of the research themes is described. The methodology provides an audit trail between the research themes and the outcomes they will help achieve. A summary is given of each theme including indicative research activities and its relevance and application in overcoming cyber challenges.

In addressing the relationship of cyber to other defence capabilities the concept of a Cyber-EW Continuum is introduced. A brief outline is given of typical Cyber-EW concepts and the broad directions in Cyber-EW research that DSTO will pursue over the next five years.

An important aspect of the Plan is identification of additional measures to ensure that the DSTO science and technology capability is relevant, resilient and responsive. This includes increasing the internal DSTO collaboration; broadening and deepening national and international partnerships (with universities, publicly funded research agencies and industry); maintaining a balanced short, medium and long term research program; and establishing and maintaining close partnerships with the end user community, including nurturing the DSTO presence in the Australian Signals Directorate (ASD).

The impact of the science and technology is described in terms of outcomes for Defence in the categories of support to operations, sustainment, acquisition and future proofing. 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.

Cyberspace trends, dependencies and vulnerabilities

Part I

Global trends

The exponential growth and global uptake of information and communications technology (ICT) has resulted in a digital world that rivals the physical world in providing opportunities and an alternative environment in which to socialise, conduct business and achieve a strategic advantage. Dependence on cyberspace for economic wealth, government operations and societal well-being is firmly established and growing in most nations. There is also a growing reliance on cyberspace to store and manage sensitive information, and to monitor and control critical infrastructure such as communications, power, and water 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 a strong relationship developing between cyber and EW and in the future we can expect to see integration of these capabilities into one continuum.

Concurrent with the increase in cyber dependence is an increase in cyber vulnerability. Technology progress promotes continual change in the cyber environment and emergence of new cyber threats. 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.

Cyber security is one of the most serious risks facing digital nations and has two unique challenges - technology and people. The rapid evolution of cyberspace and the threat demands deep S&T investment to keep pace with these changes. Moreover, achieving cyber security needs commitment, not only from government agencies, but also from the business sector and the individual user. S&T interface must also play a pivotal role in the education and training of cyber professionals and in the development of educational aids to raise public awareness.

National trends

Like most other nations, Australia has embraced ICT and the Australian population has proven to be an “early adopter” of new technology. The Australian Government recognises that to unlock the benefits of the digital economy, access to broadband must be universal and has committed to the completion of the National Broadband Network (NBN). The Government’s aim is that all households and businesses should have access to broadband with download data rates of between 25 and 100 megabits per second (Mbps) by the end of 2016. By the end of 2019 the Government expects the NBN to be completed and download rates of 50 to 100 Mbps to be available to at least eight out of ten Australians[2].

Defence also has embraced the digital and networked age. The 2009 Defence White Paper (WP09) heralded a strong move toward networked military capability, particularly in the maritime and air domains; and the 2013 Defence White Paper (WP13) highlights the critical dependency that modern military capabilities have on information systems[3,4].

Australia has ranked cyber security as one of the key risk areas for both Defence and national security. Defence of our digital networks is identified as one of the three national security priorities for the next five years and as a consequence the Australian Cyber Security Centre (ACSC) has been established[5]. Despite this, the general population has poor awareness of cyber risks, there is a critical shortage of suitably trained and qualified cyber professionals, and current S&T investment does not match the magnitude of the problem space. Cyber security has been cited as one of the top areas for investment in Australia’s 2012 Strategic Research Priorities[6,7]. However, the number of ICT graduates is in decline and the number of graduates in science, technology, engineering and mathematics (STEM) remains low. These trends potentially will impact our national cyber research capability and ultimately increase our cyber vulnerability.

Recent facts and statistics

Global

- Global IP traffic has increased eightfold over the past five years, will increase threefold over the next five years and will increase 18 fold from 2011 to 2016[i].
- By the end of 2013, more than 2 Billion iOS and Android Apps will be downloaded per week[ii].
- In Q1, 2012 a botnet consisting of 10,000-30,000 Android devices was detected. The total number of smartphones infected is in the hundreds of thousands[iii].
- 25% of Facebook users don't bother with any kind of privacy control[iv].
- During 2012, the average time to discover a data breach for the 450 attacks looked at by security firm Trustware was 210 days[v].

National

- In 2011, 68% of Internet users had used the Internet to purchase goods or services in the past year[vi].
- Australian mobile data traffic will increase 14 fold from 2011 to 2016[iv].
- In 2012, 5.4 million Australians fell victim to cyber crime with an estimated cost to the economy of $1.65 billion[vii].
- Less than 50% of survey respondents have installed anti-virus software and even fewer had firewalls or other protective measures on home computers[viii].
- In 2010, there were 4293 ICT completions in tertiary qualifications amongst Australian citizens, down by 53% since 2003[ix].

i. "CISCO Visual Networking Index: Forecast and Methodology, 2011-2016", Cisco, 2012
ii. http://istrategylabs.com/2013/03/all-about-apps-infographic-highlights-usage-downloads-and-economic-impact-from-mobile-marketplace/
iii. http://www.securelist.com/en/analysis/204792231/IT_Threat_Evolution_Q1_2012 (Data from Kaspersky)
iv. http://www.prdaily.com/Main/Articles/52_cool_facts_and_stats_about_social_media_2012_ed_11846.aspx
v. 2013 Trustware Global Security Report
vi. "Year Book Australia 2012", Australian Bureau of Statistics, 2013:
vii. "Australian Cyber Security Centre", Media release from the Press Office of the Prime Minister of Australia, 24th January 2013. http://www.pm.gov.au/press-office/australian-cyber-security-centre Accessed on 13th March 2013
viii. ASPI 2009 Cyber Security Report references "Australia in the Digital Economy Report 1: Trust and Confidence", Australian Communications and Media Authority, March 2009.
ix. "2012 Australian ICT Statistical Compendium", Australian Computer Society, 2012:

DSTO - cyber science and technology capabilities and role in the cyber community

Part II

DSTO cyber science and technology capabilities

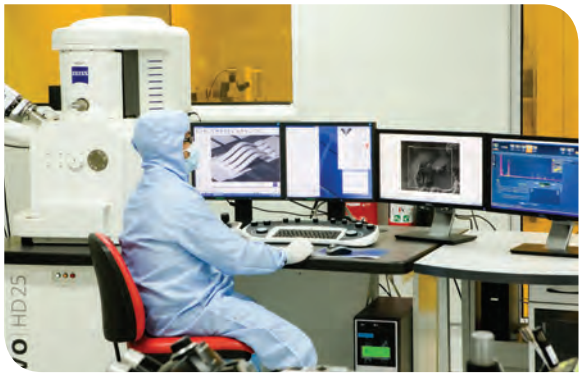
DSTO has over 20 years of achievement in cyber research, much of which is classified. It has a strong track record in providing science and technology support, trusted technical advice and specialised solutions across a broad spectrum of cyber technologies and applications to: Defence, the Australian Intelligence Community and national security agencies. Typical examples where DSTO research has had impact are:

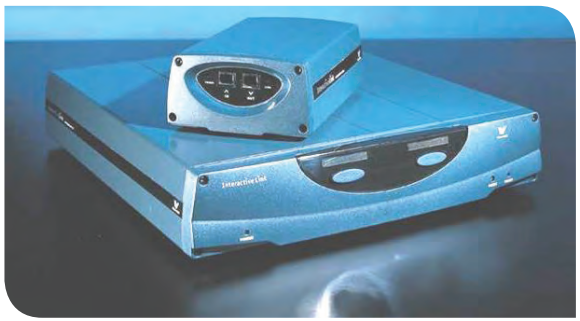
- **Crypto-mathematics.** Application of advanced crypto-mathematical S&T to provide a life-saving, bespoke intelligence capability in support of military operations.
- **Digital forensics.** Cross-correlation of multiple forensic data in support of client operations.
- **Computer network defence.** Development of novel computer network defence technologies and transitioning of this technology into operation at client sites.
- **Network analysis and management.** Widespread operational use of DSTO developed graph and statistical-based network analysis and change detection tools.
- **Multi-level security.** The Starlight data diode is an example of successful commercialisation of DSTO technology, in this instance by Tenix Datagate. Starlight allows users to access classified and unclassified networks, without compromising security, and has been accredited to Evaluation Assurance Level (EAL) 7 by the National Information Assurance Partnership (NIAP).

DSTO has a large multi-disciplinary team working in cyber-related S&T encompassing mathematicians; computer scientists; software; hardware and communications engineers; physicists; signal processors; psychologists and social scientists, most of who are located at DSTO Edinburgh.

Additionally, DSTO is able to leverage all of its multi-disciplinary expertise across the Organisation to develop integrated technology solutions to difficult cyber problems. This includes areas outside of “core” cyber S&T, such as command and control research, modeling and simulation, scientific and technical intelligence (STI) and operations research and systems analysis (ORSA) which assesses technology solutions within the context of the capability improvement they will provide.

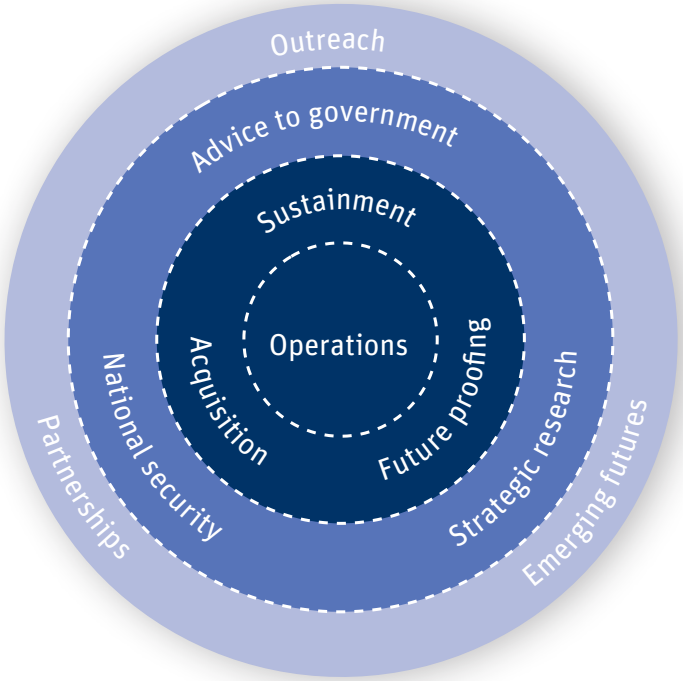
DSTO has made significant long-term investment to support its cyber S&T and has a range of specialised facilities at DSTO Edinburgh including: sophisticated computing capabilities; microelectronics, signal processing, network analysis, radio frequency, and optoelectronic laboratories; experimental communications infrastructure; modeling and simulation capabilities; prototype cyber environments; and secure facilities.





DSTO role in cyber

DSTO operates within the strategic context set by the Australian Government and the Department of Defence, and is the lead agency in providing science and technology support to Defence. Its core role centres on providing expert and impartial advice and support for the conduct of operations, sustaining the current force and acquisition of future Defence capabilities.



In supporting cyber operations DSTO has on-going engagement with the operational community to understand user requirements and build domain knowledge, provide science and technology support and develop and help transition technology solutions to priority problems. DSTO works closely with and has a number of permanent and rotational positions located within ASD.

Support to development and sustainment of Defence capability is provided through cyber security advice to Defence projects and advice to cyber acquisition projects, including technical risk assessments.

DSTO also has a mandate to coordinate science and technology support to other government agencies as part of Defence's contribution to whole-of-government national security. A policy framework for this role is being developed under the T2 initiative of the DSTO Strategic Plan, *Invigorating Australia's Research Efforts in National Security*[8]. Cyber security science and technology activities in support of national security agencies will be coordinated within this framework.

National Engagement

DSTO partners with industry, universities and publicly funded research agencies, to strengthen and shape national cyber science and technology and to develop and transition technology to operational capability. A number of mechanisms are invoked to achieve this, including bilateral research agreements, strategic alliances, and membership of Cooperative Research Centres (CRCs) and Centres of Excellence. DSTO also licences intellectual property to industry to develop products for use by Defence and the broader community.

International Engagement

Participation in international agreements and forums relevant to cyber is an important aspect of DSTO's role. Specifically, active collaboration is essential as it establishes a meaningful Australian presence in the community that leads the development of future capability. It is also a powerful capability multiplier through the sharing of ideas and knowledge, and avoidance of duplication of effort. Important forums include government-to-government classified arrangements such as The Technical Cooperation Program (TTCP) where DSTO is the lead agency on behalf of the Australian Department of Defence.

Cyber 2020 Vision – The DSTO cyber science and technology plan

Part III

Development of the cyber plan

Framework

This Plan was developed within a framework defined by three science and technology goals considered to be essential to strengthening Australia's cyber future. These are:

- Establish research themes that are enduringly relevant; sufficiently comprehensive to address the cyber problem space and support the development of future cyber capabilities; and that can be readily applied to priority problems.
- Understand and help shape the relationship between cyber and other Defence capabilities of electronic warfare (EW), signals intelligence (SIGINT) and communications.
- Ensure a relevant, resilient and responsive DSTO cyber capability and foster a cohesive, integrated national science and technology base.

Consultation

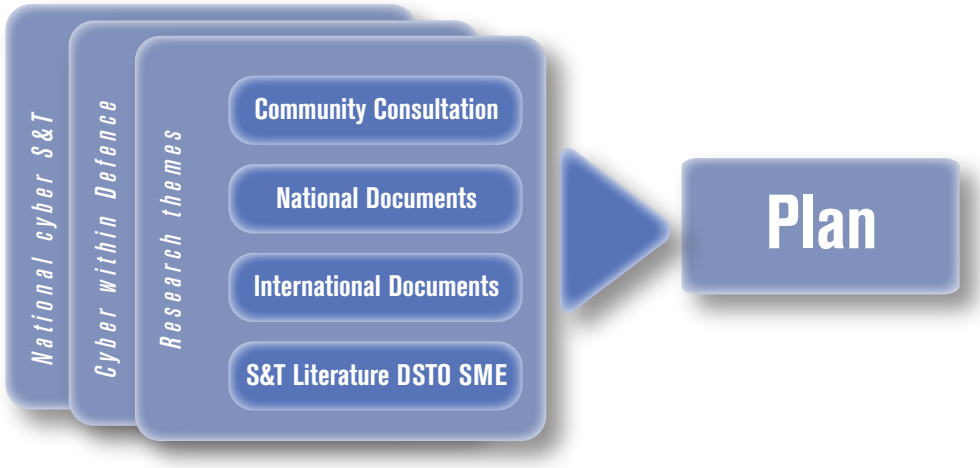
Extensive consultation was undertaken to shape the Plan. The primary inputs were:

External expert and stakeholder perspectives: More than 60 interviews were held with national and international organisations and communities involved in cyber, EW and communications. This includes Defence, government agencies, academia and industry. The interviews were guided by a series of questions relevant to the three goals identified above for the science and technology, however the format was sufficiently relaxed to allow for free-flowing comment. Interviews were recorded in writing and subsequently provided to the interviewees for validation.

Key national documents: Documents relevant to Defence and national security were reviewed. This includes the 2009 and 2013 Defence White Papers, the 2013 National Security Strategy and the DSTO Strategic Plan.[8]

International cyber strategy documents: A number of strategy documents produced by allied nations were used to provide a broader perspective of the strategic issues associated with cyber.

Science and technology trends: Review of the open literature, classified literature and discussion with DSTO subject matter experts, provided a good overview of the important science and technology trends in the cyber and EW area. (A bibliography can be found at the end of this Plan).



Foundational research themes

Overview of methodology

A major purpose of this Plan is to define the scope and content of the DSTO cyber program. The magnitude and diversity of the cyber problem space is very large and potential areas for science and technology investment are many. Careful choices must be made to ensure the research is enduringly relevant; sufficiently comprehensive to cover the problem space and support the development of future capability; and can be readily applied to priority problems. This section describes the underpinning methodology used to guide the analysis of the options and selection of the foundational research themes.

The methodology consisted of three steps and began by defining the strategic objective for the research:

Strategic Objective

"Help position Australian Defence and national security agencies to operate effectively within, and through, cyberspace."

This objective was derived using input from the consultation process that identified cyberspace as being a domain within which, and through which, influence is exerted, much like the land, air and maritime domains. This is an enduring objective that is relevant to Defence, national security, whole of government and the business sector, and is consistent with one of the goals in Australia's 2013 National Security Strategy:

"...developing sophisticated capabilities to maximise Australia's strategic capacity and reach in cyberspace..."

Fundamental to this strategic objective are the capabilities of: Threat Assessment, Intelligence, Situational Awareness, Information Assurance, and Planning and Shaping.

The second step of the methodology mapped out the enduring challenges in realising these five capabilities (and hence the strategic objective). The identified challenges are:

Prevent Environmental Surprise (technology progress and its adoption and adaptation can result in unexpected morphing of cyberspace)

Counter an Unknown and Persistent Threat (the cyber threat is highly variable, diverse and rapidly evolving)

Mitigate Untrustworthiness (includes hardware, software and people)

Data-to-Decision Reflex (the ability to respond appropriately, proportionately and in relevant timescales)

Evolve Cyber-EW concepts (an emerging area hence concepts are immature)

It is these enduring challenges that discriminate cyberspace from other domains and that drive the scope and content of the research. (Refer to the Annex for descriptions of the capabilities and enduring challenges.)

In the third and final step, analysis of the research necessary to overcome the cyber challenges was undertaken. This was categorised into broad areas that resulted in the identification of five foundational research themes:

Technology Forecasting (science and technology analysis of technology trends and their potential impact)

Cyber Influence and Data Analytics (processing and analysis of big data; social influence; behavioural analysis)

Sensing to Effects (sensor to effector concepts, techniques and technologies)

Autonomous Systems (automated/autonomous data processing, analysis and decision making)

System Design for Resilience (design of systems assuming untrustworthiness)

Defining the foundational research themes

Strategic objective

Help position Australian Defence and national security agencies to operate effectively within, and through, cyberspace.

- Intelligence
- Information Assurance
- Planning and Shaping
- Threat Assessment
- Situational Awareness

Enduring challenges

- Prevent environmental surprise
- Counter an unknown and persistent threat
- Mitigate untrustworthiness
- Data-to-decision reflex
- Evolve Cyber-EW concepts

Foundational research themes

- Technology Forecasting
- Cyber Influence and Data Analytics
- Sensing to Effects
- Automonous Systems
- System Design for Resilience

Characteristics of foundational research themes	
✓	Enduringly relevant
✓	Sufficiently comprehensive
✓	Readily applied to priority problems

Summary of foundational research themes

Technology Forecasting

Science and technology analysis of technology trends and their potential impact. Includes modelling 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; 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.

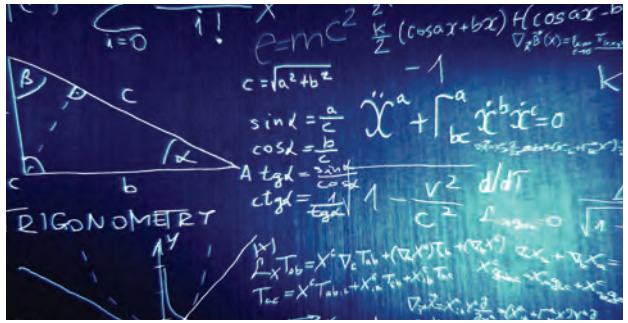
Autonomous Systems

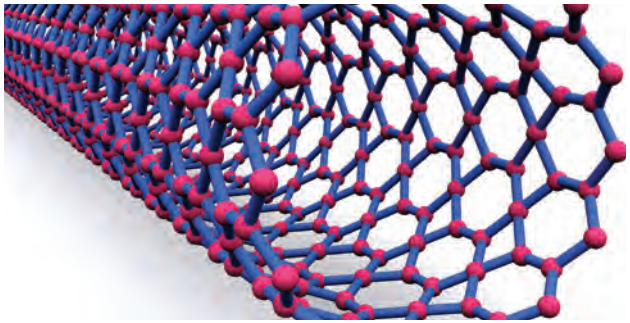
Research and development of concepts, techniques and technologies for automated through to autonomous data processing and analysis and decision making.

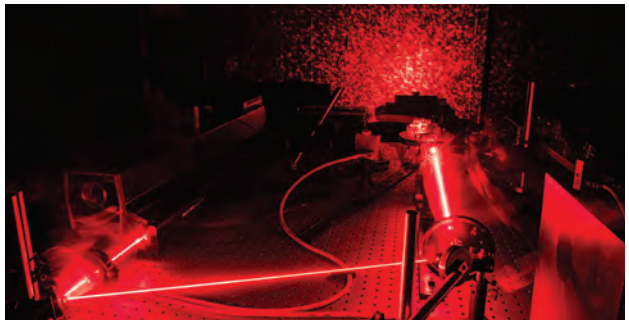
System Design for Resilience

The science and technology underpinning cyber systems designed to operate with the explicit assumption of untrustworthiness.

Foundational research theme 1: Technology Forecasting







Research Theme	Indicative Research Activities
Technology forecasting is the identification, strategic watch, predictive analysis and assessment of emerging and disruptive technologies in order to better anticipate and plan for their impact, including the emergence of new threats. Although breakthroughs in a single technology can be of profound importance, it is the parallel advancement of a number of technologies that results in the emergence of new capabilities. Technology forecasting is a multi-disciplinary, capability focussed activity, and typically includes scientific and technical intelligence, prototype building and testing, modelling and simulation, and operations research and analysis.	• Technology horizon scanning. • ICT adoption and adaptation trends analysis and forecasting (e.g. social media phenomenology). • Capability focussed multi-disciplinary ICT forecasting. • Prototype building and testing. • Threat emulator building and testing. • Threat modelling and analysis. • Red teaming.

Relevance and Application

This theme is relevant to *preventing environmental surprise* and *countering the unknown and persistent threat*.

It will be applied to: prediction of game changing technology; providing advice on the impact of technology on capability development and capability obsolescence; prediction of the potential nature of future threats; development of multi-disciplinary frameworks for dynamic forecasting.

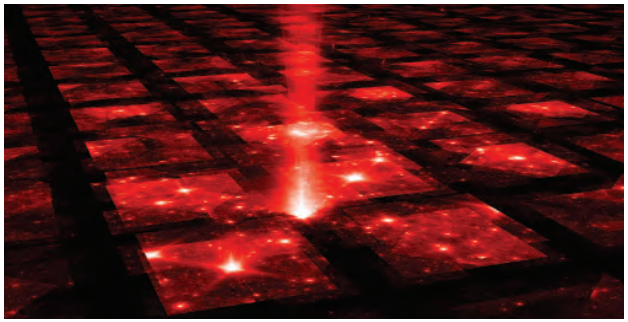
Foundational research theme 2: Cyber Influence and Data Analytics

Research Theme	Indicative Research Activities
Cyber data analytics is the process of ingesting, inspecting, cleaning, transforming and modelling data such that information, relationships and interdependencies are discovered and analysed to develop knowledge and understanding of cyberspace and connections with the physical world. Cyber influence builds knowledge of the role that cyberspace plays in enabling and encouraging social influence and behaviour, as well as the role that S&T can play in changing the intent of adversarial actors. The research is multi and inter-disciplinary, and seeks to integrate the technological, informational, psychological and social dimensions.	• Data Ingestion: data extraction; transformation; information extraction; knowledge representation; enterprise architectures. Data types include raw communication, disk and memory captures, audit events, and structured, semi-structured and unstructured content that may be in binary or text based formats and originate from a variety of sources. • Specialist Analytics: network characterisation; threat analytics; digital forensics. • Psychological and Social Analysis: social network analysis; social modelling and influence analysis, process modelling. • Reasoning and Decision Support: multi-level information fusion; reasoning under uncertainty; machine intelligence; automation; visual analytics.

Relevance and Application

This theme is relevant to *preventing environmental surprise, data-to-decision reflex* and *countering the unknown and persistent threat*.
It will support the development of tools and techniques to: manage big data; form products that are dynamic, presentable, communicable and actionable; provide analyst support functions across a range of tasks including normalcy pattern development, anomaly and intrusion detection, analysing cyber personalities and identities, and tracking the formation of social networks.

Foundational research theme 3: Sensing to Effects



Research Theme	Indicative Research Activities
Cyber (and Cyber-EW) sensing concerns the deployment of sensors to collect signals and data of interest regarding systems and environments. Effects concern the deployment of effectors to change the current or future state of an entity or system of interest. Sensing is the input to, and effects are the output of, planning and decision making. The Sensing to Effects theme focuses on support to the design and deployment of sensors and effectors; effective and timely processing of collected data; and efficient and effective planning and decision making.	• Development of sensing concepts, technologies and techniques, including sensing of wireless networks. • Development of effector concept, technologies and techniques, including combined Cyber-EW countermeasures. • Analysis and development of concepts, technologies and techniques to provide countermeasures to subversion or attack. • Modelling, analysis and experimentation of sensing and effects orchestration including: dynamic sensor network tasking; effects assessment; critical mission timelines analysis, dynamic planning and execution under uncertainty. • Crypto-mathematics for encryption and decryption of data.

Relevance and Application

This theme is relevant to *countering the unknown and persistent threat, data-to-decision reflex* and *evolving Cyber-EW concepts*.

It will find application in: development of specialised sensor capabilities, including location and tracking capabilities; specialised effector capabilities; development of tools for undertaking cyber surveillance; tools for planning and executing combined effects; and cyberspace battle management tools.

Foundational research theme 4: Autonomous Systems

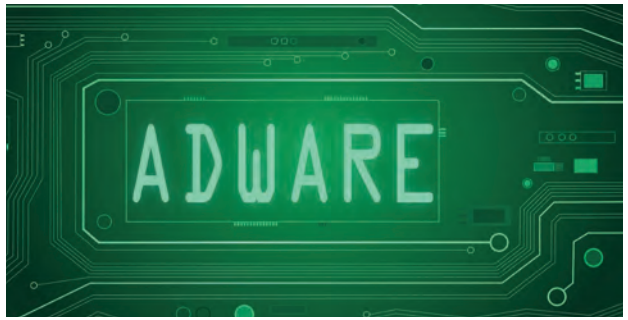
Research Theme	Indicative Research Activities
An autonomous cyber system operates in cyberspace with control delegated to computational elements that are capable of sensing their environment, making reasonable and timely decisions, and executing actions in support of objectives. Autonomous processes are needed for systems to operate in complex, uncertain, unexpected and hostile environments where humans are unable to act in a timely and effective manner. This theme will address computing systems that can execute delegated actions (automated) through to those that are self-managing, resilient and complex (autonomous) and able to perform operations at machine speeds.	• Control, graph and network theory. • Artificial intelligence, machine learning, automated reasoning and planning under uncertainty; human machine partnerships. • Autonomic computing. • Self-adaptive waveforms and algorithms. • Autonomous vehicles. • Distributed software agents. • Modelling, simulation and experimentation of complex adaptive systems.

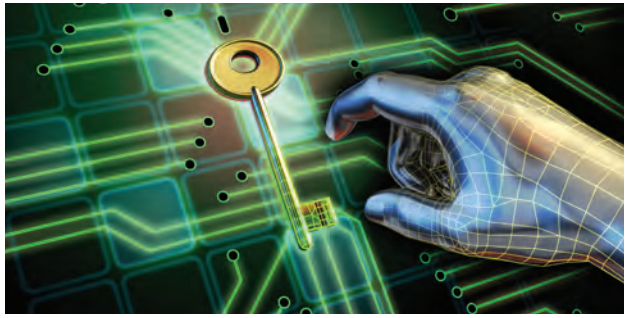
Relevance and Application

This theme is relevant to *countering the unknown and persistent threat* and *data-to-decision reflex*.

It will find application in activities such as: system monitoring and management; self healing communications networks; communication network management in contested environments; emitter geolocation; analyst workload reduction; course of action generation; round-the-clock vulnerability discovery and red teaming.

Foundational research theme 5: System Design for Resilience





Research Theme	Indicative Research Activities
The Design for Resilience theme embraces the fundamental assumption of the need to design a system to operate in the face of untrustworthiness in an evolving environment influenced by both technology and humans. Resilience to untrustworthy hardware, software and people, including persistent or transient elements of the system, is a key requirement. System designs will be emergent, guided by a continual process of sensing and responding to environmental influences; future threat and opportunity forecasting; and learning from interactions with the environment.	• Trusted, trustworthy and robust systems: security-context-aware systems and facilities; identity management; trust management; crypto-mathematics for encryption and decryption of data. • Hardware & software: mobile and transient technologies; assured communications - self-repairing and survivable networks; static and dynamic malware analysis; vulnerability analysis; hardware and software trojan analysis. • Secure architectures: resilient architectures; resilient operation in hostile environments; multi-level security (MLS) and cross domain architectures; dynamic security protocols (including identity management), systems architecture and policies; virtualisation security technologies; cloud computing; dynamic networks and communication systems.

Relevance and Application

This theme is relevant to *mitigating untrustworthiness* and *countering the unknown and persistent threat*.

It will find application in the design and development of systems and subsystems to ensure data confidentiality, integrity and availability and robustness to cyber and insider attacks.

Intensity of research activity

Foundational research themes	Emphasis on research themes 2015-20				
	Year 1	Year 2	Year 3	Year 4	Year 5
Technology Forecasting					
Cyber Influence and Data Analytics					
Sensing to Effects					
Autonomous Systems					
System Design for Resilience					

KEY

- Significant emphasis
- Moderate emphasis
- Minor emphasis

The Cyber-EW Continuum

There is a growing relationship between cyber, electronic warfare, signals intelligence and communications. This is being driven by common technologies and challenges, but most importantly by the evolution of military capabilities to networked, distributed cyber-physical systems whose functionality and performance is defined in software rather than hardware. The challenges in protecting and countering these complex systems-of-systems require the development of new concepts that will leverage all four areas of cyber, EW, SIGINT and communications.

This Plan introduces the concept of a Cyber-EW Continuum[9] where the individual areas and their growing relationship are represented. At opposite ends of the Continuum are cyber and electronic warfare where operations occur within a single environment, i.e. the cyberspace environment or the electromagnetic (EM) environment. SIGINT and communications lie between the two extremes, reflecting the fact that they can extend into both the EM and cyber environments and areas of overlap (e.g wireless networks).

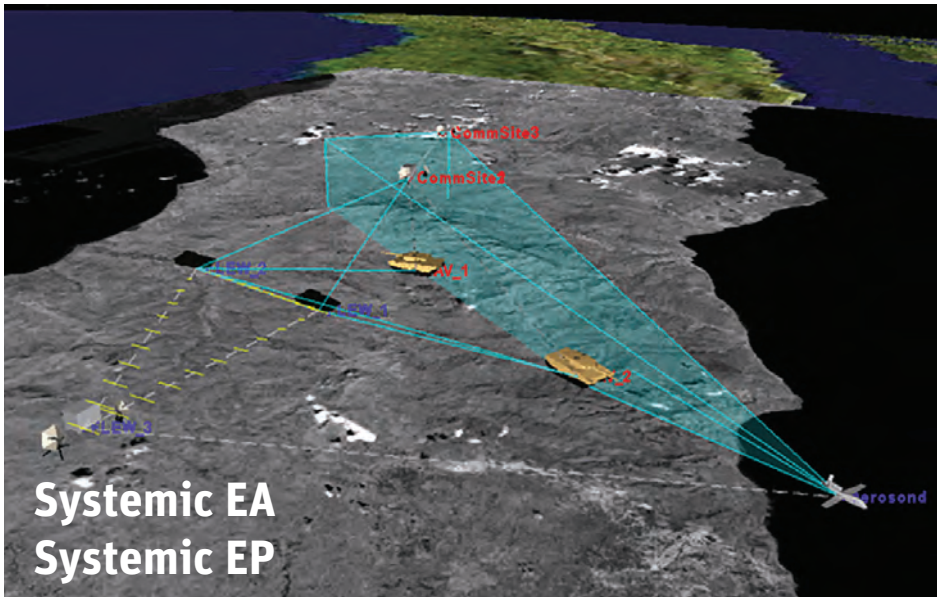
Two main unifying themes for cyber, EW, SIGINT and communications are: systemic effects and systemic electronic protection (EP). These themes emcompass the distributed, networked cyber-physical system-of-systems paradigm[10,11]. The area of systemic effects is focussed on countering the networked cyber-physical system as a whole, rather than a single element or node. Similarly, systemic EP is concerned with protection of the system as a whole.

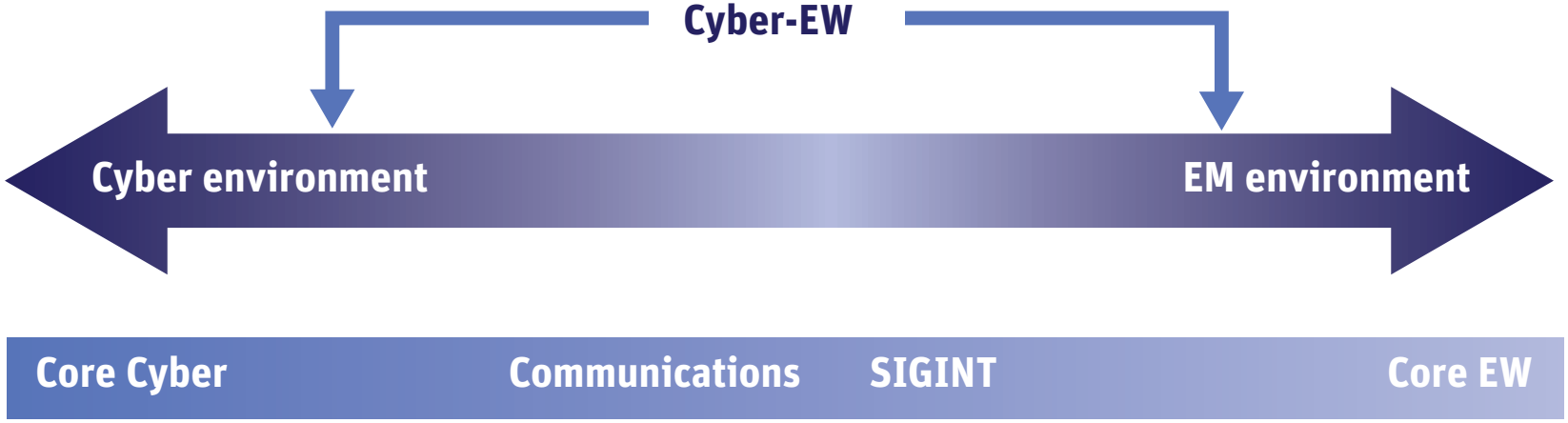
In systemic effects there are two main mechanisms that can be invoked: disruption of situational awareness and disruption of system homeostasis (i.e. system internal stability). In both cases the vectors to achieve this can be through the network nodes (e.g. sensors, combat systems), the network (e.g. data and communications links) and the digital data itself. Working within this extended framework results in traditional concepts evolving to include other areas. For example the traditional EW concept of false target injection evolves to non-core EW if the false targets are injected through communications links rather than sensors.

Systemic EP introduces new concepts such as system signature as opposed to platform signature, and considers other potential sources of signature such as communications, command and control, and data processes and processing.

The main challenge for Cyber-EW over the lifetime of this Plan is that of maturing the concepts and techniques. Science and technology activities to support this will need to be multi-disciplinary and involve researchers with domain expertise across all relevant areas. The Cyber and Electronic Warfare Division (CEWD) of DSTO brings together all four areas of cyber, EW, SIGINT and communications. The Division will align its S&T program with the concept of the Cyber-EW Continuum and will include analysis and development of concepts and techniques that cannot clearly be defined as falling into any single area (i.e. cyber, EW, SIGINT or communications); combined techniques from two or more of the areas to create an overall countermeasure effect; and the use of one capability (e.g. communications) to support the implementation of a technique from another area (e.g. EW).

The Cyber-EW Continuum (continued)





Broad directions in Cyber-EW S&T over the next five years

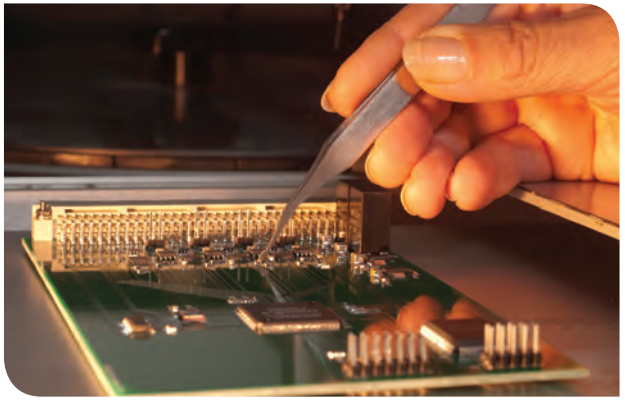
The structure and program of CEWD will be aligned with the concept of a Cyber-EW Continuum beginning FY 2014/15.

Continuum Position	Activities
Core Cyber	Niche science and technology capabilities in content analysis and host protection will be maintained and information assurance research will be supported through increased external collaboration. Cyber Defence research will be strengthened through: the application of machine learning and data science techniques for holistic discovery and characterisation of threats; network traffic and topology characterisation; modelling and knowledge representation. (Beginning FY 16/17) Research into cyber effects, including network shaping, will enable 'red teaming' for vulnerability analysis and development of complementary cyber security capabilities. (Beginning FY 14/15) Research into social and psychological aspects of cyber influence will be undertaken, noting that in the cyber domain it is possible for a minimally resourced few to influence a vast targeted audience almost instantly. Expertise in cryptomathematics will be leveraged to strengthen the mathematical foundations of cyber and will include foundational mathematics of machine intelligence. (Beginning FY 15/16) Autonomous techniques will increasingly be applied in support of cyber operations including resilient cyber systems, cyber situational awareness and course of action generation.
Cyber-EW	Wireless communications intelligence & EW will increasingly evolve a cyber alignment. Research will be conducted into systemic vulnerabilities and effects in complex distributed cyber-physical systems. (Beginning FY1 4/15) Research to improve survivability of communications in contested and denied environments will include self-adaptive waveforms and algorithms, together with autonomous vehicles and distributed software agents. (Beginning FY 14/15) Electromagnetic & cyber battle management concepts and tools will be developed. This work will lead to R&D into integrated Cyber-EW battle management concepts. (Beginning FY 18/19) Multidisciplinary research will be conducted into assured physical and logical positioning and timing. (Beginning FY 15/16)
Core EW	The core EW S&T program will be ongoing, as articulated through the 2010 EW Strategic S&T Plan.

DSTO cyber S&T: relevant, resilient and responsive

The five foundational themes identified in this Plan are a necessary, but not sufficient, condition for a vibrant research capability that is relevant, resilient and responsive. To achieve such a capability requires additional features beyond the research content. These are: depth of technical expertise and leadership across a comprehensive set of research areas relevant to the problem space; appropriate infrastructure (which, for cyber S&T, includes access to data); and an appropriately balanced short/medium/long term S&T program. The following table summarises on-going initiatives that DSTO will undertake to ensure that the cyber science and technology capability retains the necessary characteristics.

Additional Features	Initiatives
Technical Expertise and Leadership	Establish and maintain a multi and inter-disciplinary collaborative environment providing an enduring "talent pool" of expertise consisting of suitably cleared individuals working within the five research themes. This includes physicists; mathematicians; computer scientists; software, hardware, and communications engineers; psychologists; and social scientists.
	The DSTO R&D will be extended to include research in non-traditional cyber disciplines such as ORSA and command and control research.
	Active collaboration in cyber S&T is essential as it establishes a meaningful presence in the community that leads the development of future capability. As such DSTO will broaden and deepen its national and international collaborative partnerships in classified and unclassified forums. Nationally DSTO will contribute to the establishment and development of national S&T initiatives such as Cooperative Research Centres and Centres of Excellence. Internationally collaboration in classified government-to-government forums will increase. This includes engaging in bilateral staff exchanges and being an active partner in The Technical Cooperation Program Cyber Challenge initiative.
	Partner with the operational community to gain context, advice on priority problems and deepen domain expertise. Includes maintaining and nurturing the DSTO presence in ASD. To aid in this the DSTO staff in ASD will be placed within a single DSTO organisational group.
Infrastructure	Establish, maintain and extend critical infrastructure. Includes investment in classified facilities, test sites, networks and ICT.
Balanced Program	Develop the short and medium term DSTO S&T program in conjunction with client groups in a manner that is consistent with the initiatives of the DSTO Strategic Plan, science and technology excellence (D1); and strategic engagement with client focus (D2).
	Develop a long term research program around the five foundational research themes that is synchronised with national and international collaborative programs to best leverage the S&T investment in support of the operational community.
	Collaborate with industry to provide S&T and help transition technology to capability. This includes establishing and maintaining strategic alliances.



Delivering impact

Part IV

Delivering impact

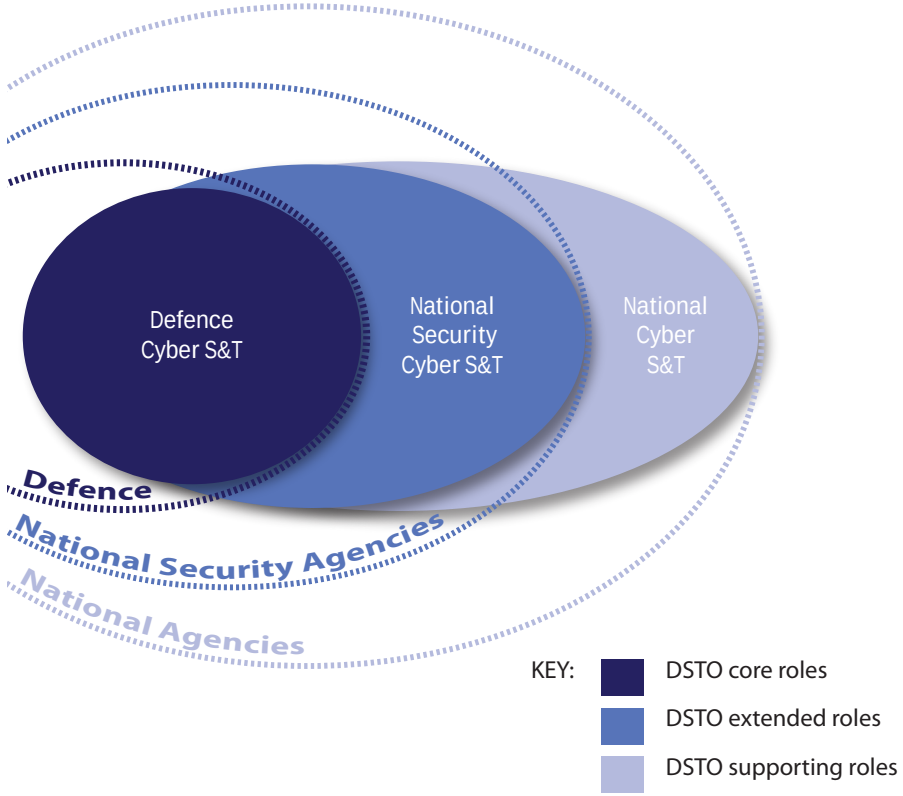
Cyberspace is a domain that extends across Defence, government, and the business and private sectors, with Defence and national security forming a strong core of cyber capability. DSTO delivers impact in cyber through its support to Defence and national security, and in shaping the national science and technology capability.

DSTO delivers impact to Defence through its core roles of:

- **Support to operations:** Supporting operational capability with science and technology expertise.
- **Sustainment:** Providing support to sustain and enhance current capability.
- **Acquisition:** Providing support through the genesis, development, acquisition and introduction into service of major capability projects.
- **Future proofing:** Investigating client focused future concepts, contexts and capability.

DSTO leverages its expertise to fulfill its extended role in leading the coordination and delivery of science and technology to enhance whole-of-government national security. In this capacity DSTO will collaborate with the national cyber science and technology community to define a research program that serves the needs of national security as defined by Government.

DSTO will have national impact through its supporting roles of outreach and partnership, and will seed and shape a national science and technology capability in cyber security that will enhance the scientific and professional skill base available to support Australia's cyber-enabled enterprise.



Based on a diagram by Michael Shoebridge.

Delivering impact to Defence

DSTO will strategically invest in the foundational research themes and strengthen its impact through an integrated cyber science and technology program that embraces the concept of a Cyber-EW Continuum. A balanced program will be established and executed that will focus on concepts, tools and techniques needed to protect Australia's military capabilities and Defence networks against sophisticated cyber and Cyber-EW threats, counter threat military systems and provide intelligence support within the cyber environment.

Role	Intelligence	Defence Networks	Protect Military Capabilities	Counter Military Threat Systems
Operations	S&T support to cyber operations and response teams. Development and provision of technology solutions for rapid transition to capability. Cyber operations support will be strengthened through a co-located presence of science and technology practitioners with operational staff.		Development and provision of Cyber-EW technology solutions for rapid transition to capability.	Support to Defence operational and intelligence threat assessment community.
Sustainment	Provide advice on techniques, technologies and systems for cyber capabilities. Development and provision of prototype tools. Support to cyber security.		Maintenance of state-of-the-art cyber capabilities through retrofitting advanced technologies to extant platforms and systems.	
Acquisition	Support to major projects on cyber and aligned capabilities. Includes system performance definition and technical risk assessment	Support to major cyber security projects. Includes system performance definition and technical risk assessment	Support to major projects linked to military cyber security. Will evolve to address systemic vulnerabilities and protection.	Support to major projects on counter-threat capabilities. Will evolve to address systemic effects.
Future Proofing	Advice on ICT trends and potential impact. Research, development and testing of new concepts, tools and techniques. Support to the Concept Technology Demonstrator program.		Concepts, tools and techniques for protecting networked, cyber-physical systems. Initial focus on maritime platforms.	Concepts, tools and techniques for countering networked cyber-physical threat systems.

Delivering impact to national security

ASD's vital role in Australia's cyber and information security is supported by DSTO's S&T program. DSTO will enhance this support by partnering with publically funded research agencies, universities and industry to lead the collaborative development of a proposal to establish a Cyber Security National Science and Technology Strategy. The key drivers for this are:

- Australia is increasing its reliance on cyberspace for economic growth, societal well-being, government operations and critical infrastructure monitoring and management. Concurrent with the increase in cyberspace reliance is an increase in cyberspace vulnerability, thus placing a high priority on cyber security.
- Cyberspace is progressed and shaped by technology and by how people adopt and adapt this technology. Investment in S&T is thus central to seizing cyber opportunities and overcoming cyber security challenges.
- The cyber problem space is extremely large and requires a strongly integrated multi-disciplinary approach. The Australian S&T community can contribute from a variety of disciplines to help develop future cyber capabilities. However, the national S&T resources are not abundant and must be nurtured, harnessed and appropriately orchestrated to address priority problems.

The strategy will seek to develop the national cyber science and technology capability in three areas, Program, Infrastructure and People:

- **Program:** Deliver a research program focused on developing concepts, tools and techniques to support the monitoring, management and protection of Australia's cyber domain by national security agencies.
- **Infrastructure:** Development of a national experimentation facility for validating cyber concepts, tools and techniques.
- **People:** Grow an Australian workforce that is relevant and responsive to the cyber security needs of end users.

The Program element of the strategy will solely focus on providing S&T solutions to the national security community. The primary aim of the experimentation facility will be to support the research program. The Infrastructure element will also have a secondary role of providing an environment for the broader cyber S&T community to gain experience in a realistic experimental environment. The People element of the strategy will provide benefit across all sectors of the cyber community including national security, Defence, government, businesses, organisations and individuals.

Drivers for a Cyber Security National S&T Strategy

Increasing national dependence on an increasingly vulnerable cyber domain.

Investment in S&T is central to seizing cyber opportunities and overcoming cyber challenges.

The national cyber-related S&T resources are not abundant and must be nurtured, harnessed and orchestrated to focus on priority cyber security problems.

Elements of a Cyber Security National S&T Strategy

Program: Primary aim of supporting national security agencies.

Infrastructure: Primary aim to support S&T program; secondary aim to nurture S&T community.

People: Primary aim to grow national science, technology and professional capability for the national good.

Delivering impact to national science and technology

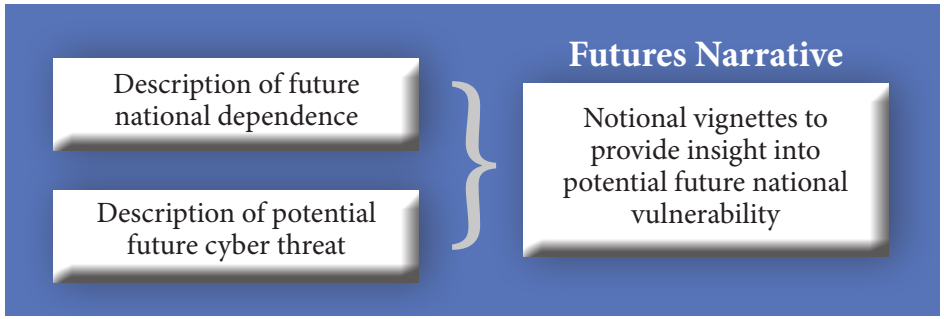
As part of its outreach role DSTO will seed and shape a national science and technology capability in cyber security that will enhance the scientific and professional skill base available to secure Australia's cyber future. It will increase its engagement with industry and research organisations to augment its impact including:

- Being a leading and supporting member of appropriate cyber-related Cooperative Research Centres.
- Promoting the establishment of, and being a key collaborator in, Centres of Excellence in science disciplines relevant to cyber.
- Leading, promoting and contributing to cyber science events (e.g. conferences and summer schools).
- Supporting and promoting the establishment of cyber professional bodies and accreditation authorities.
- Leading the Cyber Security National Science and Technology Strategy proposal.

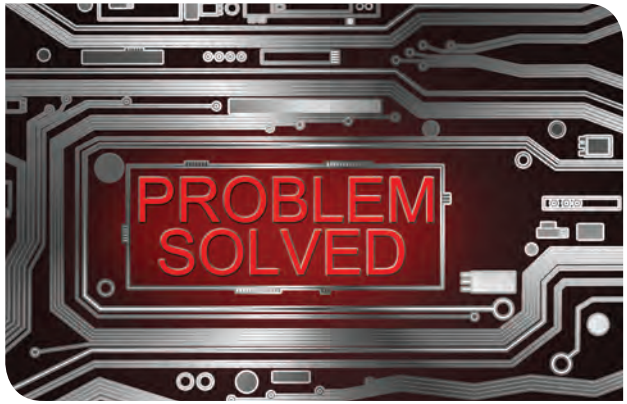
To help provide an understanding of the problem space in cyber security science and technology, DSTO will work with others in the cyber community to develop a Cyber Futures Narrative that provides a view of the nature and scale of some of the potential challenges associated with emerging cyber threats. This narrative will be based around the concept of:

"Increasing national dependence on an increasingly vulnerable cyber domain"

The narrative will be the outcome of an analysis that broadly projects national vulnerability based on the future dependence on cyberspace and its potential vulnerability to emerging threats.

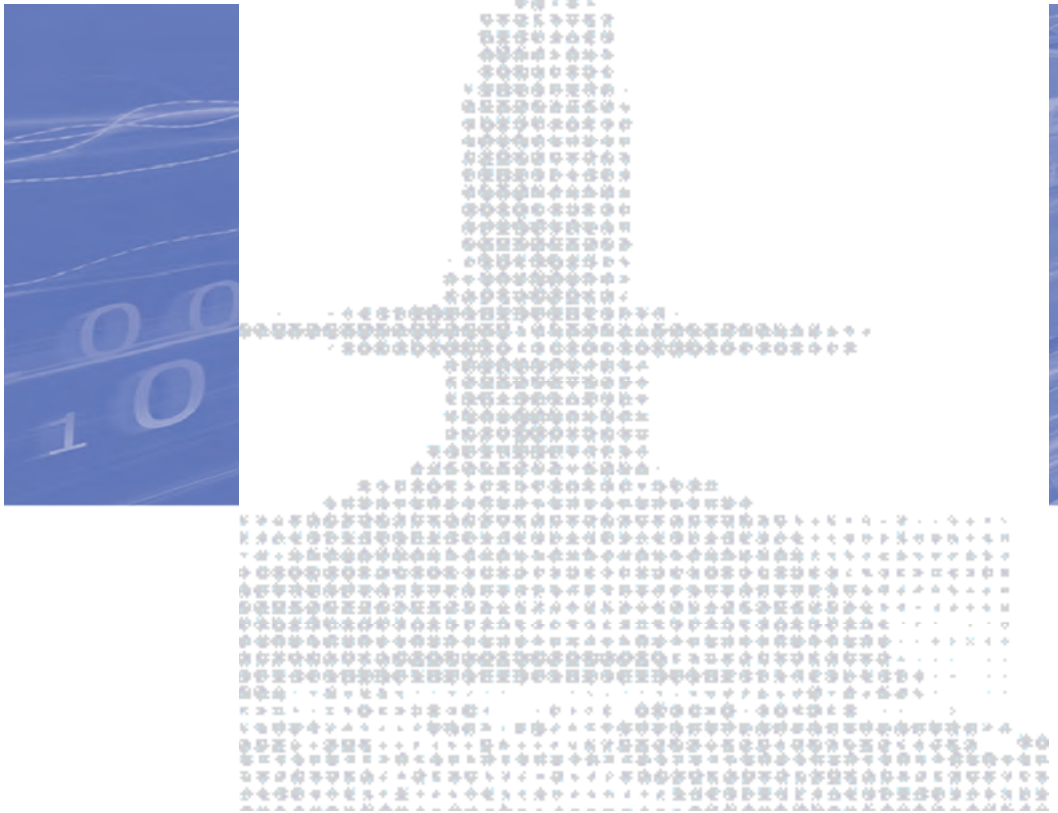


The future dependence description will be derived from a future trends analysis of exemplars occurring within the societal, critical infrastructure, and government categories. The future potential cyber threat and its potential to impact cyberspace will be derived from analytical and experimental work carried out within DSTO.


PROBLEM
SOLVED


SECURITY

Critical capabilities and enduring cyber challenges



Annex

Critical capabilities for cyberspace

Threat estimation (know what to worry about) Threat estimation is the ability to estimate potential threats to infrastructure, information or operations that are within, or rely on, cyberspace. It is a crucial underpinning element of cyber security and influences cyber system design and development and deployment of cyber incident responses. Threat estimation includes judgement 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. Threat estimation is both a real-time (operational) and longer-term, future-looking activity.

Information assurance (the ability to trust and access information) Information is a critical national resource and is increasingly being stored, used and moved around in cyberspace. Loss of access to, or loss of trust in, information or its management has the potential to cause serious disruption or harm. 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 (know the status of, and what may impact, the cyber environment): Intelligence is the collection, processing and analysis of information pertaining to cyberspace and its actors. Intelligence information is derived from a large range of sources, including open sources such as the Internet. Intelligence on cyberspace can include information on network topologies, cyber system technical capabilities and vulnerabilities, potential threats, cyber component supply chains, cyber identities and social network formation and activity.

Situational awareness (know what's going on around you): 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. Situational awareness is formed using all-source intelligence and is regularly updated by integrating new information. In cyberspace this update rate is extremely high and the situational awareness picture can be very complex due to the magnitude of cyberspace, lack of national boundaries, the very large number of potential actors, and difficulty of attribution.

Planning and shaping (the ability to plan and execute actions): Planning and shaping is the reasoning about, development and pursuit of goals and actions within and through cyberspace. This includes the selection and use of capabilities to influence and shape the cyber environment to support operations. In the case of Cyber-EW it also includes coordinated actions and combined effects.

Enduring cyber challenges

Prevent environmental surprise: Cyberspace is shaped by technology and man-made concepts. It has a significant ability to morph and present surprise – for example the rapid emergence of mobility and cloud computing. Environmental surprise also has a societal aspect as cyberspace supports and encourages the rapid formation and sustainment of virtual communities that cross national and cultural boundaries. This results in a reduced understanding of societal heartbeat as it is difficult to predict the underlying drivers and imperatives of cyberspace communities, and their influence on population thinking, culture and response.

Counter an unknown and persistent threat: The cyber threat is variable, diverse and rapidly evolving. Typically the cyber threat has a very high tempo; and attribution of malicious cyber activity is difficult. As cyberspace and its use evolves our knowledge and understanding of the threat degrades. Additionally, the cyber threat is being constantly exercised, with each day bringing new threats. "Tomorrow, When The War Began"[12] - every day is a battle in cyberspace and every day is a different battle.

Mitigate untrustworthiness: Most cyberspace users have an expectation that access, reliability, privacy and security are guaranteed. However, this expectation does not match reality. There are no guarantees that hardware devices and components; software, firmware and applications; data and information; and people can be trusted. Untrustworthiness is closely linked to the cyber threat but encompasses a broader context as it relates to vulnerabilities of a system that could be exploited, including failure of benign users to follow security guidelines or poor auditing failing to reveal an insider threat.

Data-to-decision reflex: Malicious cyberspace activities can very rapidly propagate and/or result in considerable damage. Response to cyber events must be swift, often within the sub-second timescale, and be both appropriate and proportionate. The biological equivalent of this is a reflex – where the response to an external stimulus is: almost instantaneous; an appropriate response (i.e. the arm, not the leg responds to catch a falling object); and proportionate (i.e. the hand applies sufficient pressure to catch the object but not damage it). Cyberspace is very large and complex and the ability to confidently predict the final outcome of a response (e.g. the degree of success and potential collateral damage) is non-trivial. Developing, mounting and implementing such responses is one of the greatest discriminating challenges associated with cyberspace.

Evolve Cyber-EW concepts: The relationship between cyber and electronic warfare is in the early stages. Cyber-EW concepts are nascent and within the lifetime of this Plan the main challenge will be in nurturing these concepts through to maturity.

Bibliography

1. The definition of cyberspace, DepSecDef Memo to the Military Departments et al, " The Definition of Cyberspace", 12 May 2008.
2. Coalition's plan for Fast Broadband and Affordable NBN, April 2013 http://www.liberal.org.au/fast-affordable-sooner-coalitions-plan-better-nbn see also http://www.communications.gov.au/broadband/national_broadband_network
3. Defence White Paper 2009 Defending Australia in the Asia Pacific Century: Force 2030 http://www.defence.gov.au/whitepaper/
4. Defence White Paper 2013 http://www.defence.gov.au/whitepaper2013
5. Strong and Secure: A Strategy for Australia's National Security, 2013 http://www.dpmc.gov.au/national_security/docs/national_security_strategy.pdf
6. Australia's Strategic Research Priorities http://www.innovation.gov.au/StrategicResearchPriorities
7. 2012 National Research Investment Plan http://www.innovation.gov.au/research/Documents/NationalResearchInvestmentPlan.pdf
8. DSTO Strategic Plan 2012 http://www.dsto.defence.gov.au/
9. Craig, J., Technology trends leading us towards an EW-Cyber Continuum, Association of Old Crows US Convention, Phoenix, 2012, http://www.crows.org
10. Staromlynska, J. et al, S&T for Future Electronic Warfare, DSTO GD-0611
11. Technology Impact on the Emerging EW Threat Landscape, TTCP DOC-EWS-1-2011
12. Marsden, J., Tomorrow, When the War Began. First in a series of popular Australian novels for adolescents
13. Jennings, P. and Feakin, T., The emerging agenda for cybersecurity (Special Report) Australian Strategic Policy Institute, July 2013, no. 51 http://www.aspi.org.au/
14. The National Cloud Computing Strategy, 2013 http://www.dbcde.gov.au/cloud
15. The Current State of Cyber Crime 2013: An Inside Look at the Changing Threat Landscape, EMC2 White Paper, 2013 http://www.emc.com/collateral/fraud-report/current-state-cybercrime-2013.pdf
16. Clement, D., Compelled to Control: Conflicting visions of the future of cyberspace (Special Report), Australian Strategic Policy Institute, October 2013, http://www.aspi.org.au
17. Advancing Australia as a Digital Economy: An update to the National Digital Economy Strategy, 2013 http://www.archive.dbcde.gov.au/_data/assets/pdf_file/0006/173049/Advancing_Australia_as_a_Digital_Economy.pdf
18. Cyber Crime and Security Survey Report 2012, Computer Emergency Response Team (CERT) Australia, 2012 http://www.canberra.edu.au/cis/storage/Cyber%20Crime%20and%20Security%20Survey%20Report%202012.pdf
19. Cybersecurity and Australia-US Relations (Special Report) Australian Strategic Policy Institute, April 2012, http://www.aspi.org.au

Bibliography (continued)

20. Strategies to Mitigate Targeted Cyber Intrusions, Defence Signals Directorate, October 2012 http://www.asd.gov.au/
21. 2012 Year Book Australia, Australian Bureau of Statistics, 2012 http://www.abs.gov.au/ausstats/abs@.nsf/mf/1301.0
22. #au20: National Digital Economy Strategy, 2011 http://www.archive.dbcde.gov.au/_data/assets/pdf_file/0016/173050/National_Digital_Economy_Strategy.pdf
23. Critical Infrastructure Resilience Strategy 2011 http://www.tisn.gov.au/
24. Blackburn, J. & Waters, G., Optimising Australia's Respsonse to the Cyber Challenge, Kokoda Papers February 2011
25. National Security Information Environment Roadmap: 2020 Vision, 2010 http://www.dpmc.gov.au/national_security/docs/national_security_information_environment_roadmap.pdf
26 Cyber Security Australia, Attorney General Dept., 2009 http://www.ag.gov.au/Nationalsecurity/Pages/home.aspx
27. Gibbons, A., Cyber Security: threats and responses in the information age (Special Report), Australian Strategic Policy Institute, December 2009 http://www.aspi.org.au/
28. Department of Defense Strategy for Operating in Cyberspace, July 2011 http://www.defense.gov/news/d20110714cyber.pdf
29. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, The White House, May 2011 http://www.whitehouse.gov
30. Trustworthy Cyberspace: Strategic plan for the federal cybersecurity research and development program, Executive Office of the President, National Science and Technology Council, December 2011 http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf
31. National Initiative for CyberSecurity Education (NICE) Strategic Plan, US National Institute of Standards and Technology, 2012 http://www.nist.gov/
32. US Navy Information Dominance Roadmap 2013-2028, http://www.public.navy.mil/fccc10f/Strategies/Information_Dominance_Roadmap_March_2013.pdf
33. Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision 2012-2025 December 2012 http://www.globalsecurity.org/security/library/policy/usaf/cybervision2025_afd-130327-306.pdf
34. Cyberskills Task Force Report, Homeland Security Advisory Council, Us Dept. Homeland Security, Fall 2012 http://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf
35. Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight, US Government Accountability Office (GAO) Report to the Committee on Armed Services, House of Representatives , July 2012 http://www.gao.gov/assets/600/592211.pdf
36. Foundational Warfare (Plan X), Broad Agency Announcement, DARPA-BAA-13-02, US Defence Advanced Research Projects Agency, 20 November 2012 http://www.darpa.mil/Our_Work/I2O/Programs/Plan_X.aspx

Bibliography (continued)

37. The UK Cyber Security Strategy, November 2011 https://www.gov.uk/government/publications/cyber-security-strategy
38. The UK Cyber Security Strategy, Report on progress, Forward Plans December 2012 https://www.gov.uk/government/collections/cyber-security-strategy-progress-so-far--2
39. The UK Cyber Security Strategy: Landscape review, National Audit Office, 12 February 2013 http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf
40. Defence and Cyber-Security, UK House of Commons Defence Committee, 9 January 2013 http://www.parliament.uk/
41. Neville-Jones, P. & Phillips, M., Where next for UK cyber-security, Rusi Journal, December 2012, vol. 157, no. 6
42. Partnering for Cyber Resilience: Risk and Responsibilities in a Hyperconnected World – Principles and Guidelines, World Economic Forum, March 2012 http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf
43. Rid, T. & McBurney, P., Cyber-Weapons, Rusi Journal, February/March 2012, vol. 157, no. 1
44. Schmitt, M. N., International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed, Harvard International Law Journal, December 2012, vol. 54
45 Top 10 Cyber Vulnerabilities for Control Systems, 2012 http://www.ge-mcs.com/controlsolutions
46. Understanding Cybercrime: Phenomena, Challenges and Legal Response, ITU September 2012 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf
47. Vulnerability Analysis of Energy Delivery, Idaho National Laboratory, Sept. 2011 http://www.inl.gov
48. 2013 Global Security Report, Trustwave, 2013 http://www.trustwave.com/GSR
49. Greenleaf, G., Comparative Study on Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments – Country Studies, B2-Australia, Directorate-General Justice Freedom and Security, European Commission, May 2010
50. Holliday, P., Cyber Security, CISCO Networking Academy, 2010
51. Internet Security Threat Report 2013: Volume 18, Symantec Corp. http://www.symantec.com
52. Does EW + CNO Equal Cyber? The Journal of Electronic Defense, Vol 31, No. 9 September 2008 http://www.crows.org
53. Fisher, K., High Assurance Cyber Military Systems, May 2012 http://www.cyber.umd.edu/sites/default/files/documents/symposium/fisher-HACMS-MD.pdf

For further information please contact:

Director Coordination, Cyber and Electronic Warfare Division

Tel: (08) 7389 5714

Email: CEWDDirCoord@dsto.defence.gov.au

Web: http://www.dsto.defence.gov.au/