Australian Government
Department of Defence
Defence Science and
Technology Organisation

Future Cyber Security Landscape

A Perspective on the Future

DSTO | Science and Technology for Safeguarding Australia

DSTO would like to acknowledge and thank CSIRO for their contribution in analysing sectoral trends in health, energy and government services.

Executive Summary

Australia has an increasing dependence on an increasingly vulnerable cyber domain, resulting in potential national risk. This dependency pervades all elements of government, industry and society such that we have a national cyber-enabled enterprise with digitally-enabled networks, systems, services and business endeavours critical to Australia's national interest. Interconnectivity and interdependence within this enterprise mean that the impact of an unmitigated threat can cascade and be far reaching. Looking to the future there are potential new classes of threat: pervasive and non-discriminatory in nature and to which there are currently no known catch-all countermeasures. Elements within a future national enterprise which are not good cyber security citizens will therefore present vulnerabilities with potential national ramifications. This calls for alternative and innovative approaches to national cyber security, underpinned by strategic investment in associated Science and Technology.

This Future Cyber Security Landscape paper illustrates this increasing national dependency, threat and vulnerability by providing a view of a possible cyber security future. As a companion paper to the DSTO Cyber S&T Plan: Cyber 2020 Vision, it provides Australian context to strategic investment in cyber security capabilities and cyber security science and technology.

Dependence

Information and communications technology (ICT) is enabling transformation and evolution of the way government, industry and the general public organise, communicate, exchange knowledge and skills; use, process and store information; and conduct their business and everyday lives. The opportunities and pace of technology uptake, the drivers for business improvement and changing consumer expectations have given rise to new models of service delivery within government and industry. Against this backdrop, three exemplar sectors were analysed: Healthcare (focusing on health services), Government (focusing on government services) and Energy (focusing on electricity). Future trends analysis of the three sectors was conducted and government agencies and organisations across the sectors were consulted to confirm the trends. Telecommunications services and equipment providers were also consulted for a cyber backbone perspective. The analysis showed increasing use of ICT but also increasing dependency on ICT for greater productivity, reduced costs, and better livelihood. It is not difficult to imagine a future national enterprise that is critically dependent on ICT in an analogous manner to that of electricity, without which we cannot function.

Threat

Cyber threats are potential cyber events emanating from unintentional actions or as a result of attacks developed by malicious parties that exploit vulnerabilities and cause harm to a system or organisation. Understanding both existing and emerging threats is vital for the future development and correct operation of information systems. An analysis was undertaken of a future potential threat, Hardware Trojans: undesired, malicious, intentional modifications to electronic circuits. They are designed to compromise the behaviour of systems containing the circuits, presenting a persistent threat to their correct operation. Hardware Trojans can be inserted into an electronic circuit at any stage of design and development, manufacturing, distribution or maintenance. Modifications can include system level changes such as adding chips and circuitry, or changing existing chips by introducing new logic functions or subtle physical process variations during manufacture. Potential cyber threats can be seen to the trustworthy design, manufacture, supply, operation, maintenance and disposal of information and communications technology and systems, and the information and services that those systems manage and provide. This emerging threat challenges the foundations of current security models due to its potential to disrupt the core root of trust that system security relies upon. As a consequence, the current understanding of threats and how they are managed needs to be revised; future systems will need to operate in the presence of such threats yet maintain their desired operational and security goals.

Vulnerability

Within the context of increasing dependence and future cyber threats, five keys areas of vulnerability emerged through the analysis of interviews with ICT-dependent end-users and service and infrastructure providers. The five key areas of increasing digitisation, increasing complexity, increasing outsourcing, lagging security posture, and increasing interconnectedness are presented together with vignettes that describe how emerging threats could exploit these vulnerabilities. The analysis paints a picture of a future cyber security landscape, in which:

- there is more at stake due to Australia's dependence on ICT
- there is increasing exposure to potential cyber attacks
- security continues to lag technology
- future attacks may be more potent yet harder to detect, and
- response to attacks will be complicated by the complexity, interconnectedness and interdependence of systems.

Science and Technology is central to addressing these cyber security challenges and seizing opportunities. The cyber domain is defined by Science and Technology: it is progressed and shaped by technology and by how people adopt and adapt it. It is incumbent then that investment is made in the necessary science and technology to understand, shape and exploit the cyber domain such that the Australian national enterprise continues to effectively operate within and through it.

Introduction

Information and communications technology (ICT) is enabling transformation and evolution of the way government, industry and the general public organise, communicate, exchange knowledge and skills; use, process and store information; and conduct their business and everyday lives. The opportunities and pace of technology uptake, the drivers for business improvement and changing consumer expectations has given rise to new models of service delivery within government and industry.

Cyber threats exist to the trustworthy design, manufacture, supply, operation, maintenance and disposal of information and communications technology and systems, and the information and services that those systems manage and provide. Threats can be intentional or inadvertent and perpetuated by a range of actors with differing motivations and intentions. The confidentiality, integrity and availability of information and information systems are potentially vulnerable. **Interconnectivity and interdependence within Australia's critical infrastructure mean that the impact of an unmitigated threat can cascade and be far reaching.**

It is postulated then that Australia has an increasing dependence on an increasingly vulnerable cyber domain, resulting in potential national risk. Alternative and innovative approaches to national cyber security are needed with strategic investment in science and technology to manage and mitigate this risk.

Purpose

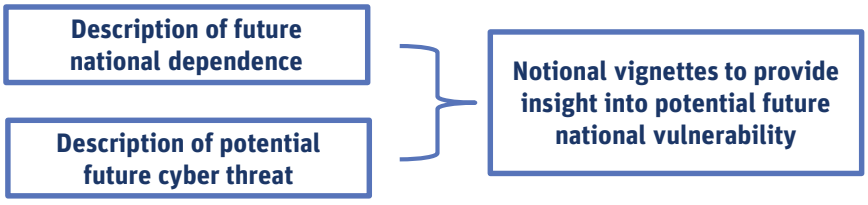
The purpose of this paper is to provide a view of a possible cyber security future. The document illustrates increasing national dependence, the nature and scale of emerging threats, and the increasing vulnerability of the cyber domain and associated challenges to national enterprise. As a companion paper to the DSTO Cyber S&T Plan: Cyber 2020 Vision, it provides Australian context to strategic investment in cyber security capabilities and cyber security science and technology.

Methodology

The study methodology consisted of projecting 5 to 10 years into the future and:

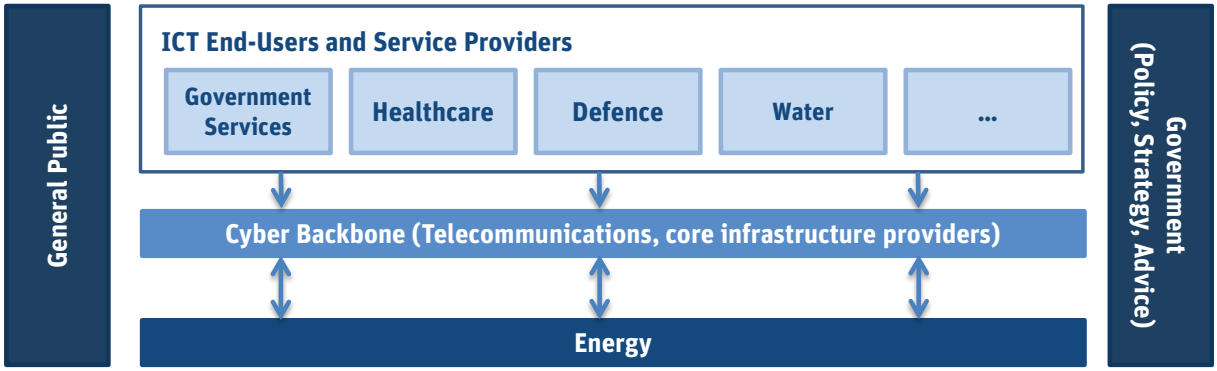
- representing the cyber-enabled enterprise as a tiered model to provide a broad overview of the dependencies and interdependencies;
- describing current and future national dependence on ICT, leveraging the experience of the CSIRO Digital Productivity and Services Flagship in trends analysis;
- leveraging DSTO's deep knowledge of classified threats to describe potentially significant future threats to the cyber domain; and
- using an overlay of the dependencies and threat, conducting interviews with ICT end-users and service and infrastructure providers to explore our potential future national vulnerability.

Methodology: Dependence, Threat and Vulnerability

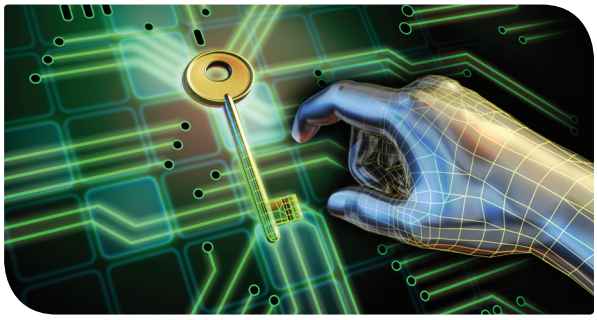


The cyber-enabled enterprise as a tiered model

A tiered model was used to represent the cyber-enabled enterprise. This model captures the reliance of end-users on the cyber environment, the role of ICT providers in developing and maintaining the core cyber domain infrastructure and the role of government. Most importantly this model captures the strong interconnectivities and interdependencies that exist within the cyber domain. These interconnectivities and interdependencies significantly contribute to the high vulnerability. The figure shows a three-tiered model. The first tier represents the technology end-users in business and government who use ICT for their internal needs and in the provision of ICT-enabled services to consumers. They are represented as individual organisations with individual technology needs. The end-users are dependent on the tier below, the cyber backbone, which includes telecommunications and core infrastructure providers. The backbone enables the interconnectivity and communications within and between organisations, and with the wider world. The next layer is energy, which, although not normally considered part of the cyber environment, is depicted here to draw attention to the critical interdependency between energy, the cyber backbone and end-users. There are many additional interdependencies within the tiers, reflecting interconnection through underpinning digital networks and common ICT supply chains, and interdependence within operational processes. Government supports all of these tiers through policy, strategy and advice on cyber operations and cyber security. The general public is a consumer of services from all.



A number of case studies from a vertical slice through the tiered enterprise were undertaken to gain an understanding of the dependencies and interdependencies. The case studies were informed by consultation with technology end-users concerning healthcare, government services, electricity supply, and telecommunication services and equipment providers, coupled with a strong awareness of Defence and the role of Government in cyber security.



National Dependency on ICT

Analysis of the future dependency on ICT began with mapping the trends in technology-use and then determining how these trends lead to dependency. Three exemplar sectors were analysed: Healthcare (focusing on health services), Government (focusing on government services) and Energy (focusing on electricity). Future trends analysis of the three sectors was conducted and government agencies and organisations across the sectors were consulted to confirm the trends (and help explore dependencies and vulnerabilities in light of the chosen future emerging threat). Telecommunications services and equipment providers were also consulted for a cyber backbone perspective.

ICT-use

Information and communications technology has increasingly transformed and become embedded in our personal lives, the way we do business, and the way we govern our nation. It underpins our critical services and infrastructure, and has changed both consumer and provider expectations.

ICT is a key enabler to helping business and government transform and evolve, through activities in:

- innovating the way we store, process and transfer data
- providing creative solutions to how we communicate and connect
- supporting operational improvements and increased efficiencies
- facilitating better ways to exchange knowledge and skills
- creating pathways for entirely new models of service delivery

In part these changes are aimed at raising productivity, increasing efficiency and effectiveness, and reducing operational costs. In each of the three sectors the drivers behind these changes vary:

- In Health services there is a need to reduce the demand and cost pressures caused by a growing and ageing population and the rise of lifestyle related and chronic disease.[1,2]
- Government services are faced with tightening budgets, reducing staff levels and increasing demand for services. Also the issues faced by the public sector are increasingly multi-dimensional and require more collaborative effort between governments, departments, agencies and public and private communities.[3]
- In the Energy sector, modernisation of the electricity grid is being driven by the need to manage peak demand, incorporate renewables, facilitate on-site generation, and reduce household electricity prices. Household electricity prices have increased by 70% between 2007 and 2012.[4]

Additionally, across the sectors better educated, highly informed, tech-savvy consumers and citizens with changing expectations are demanding consumer/citizen centric services, more engagement, easy interactions and greater personalisation.[5,6]

- Number of households with access to internet reached 83% in 2012-2013[24]
- Businesses placing orders over the internet increased 4% in a year to 55% in 2011-12[25]
- Mobile internet subscribers increased 22% during 2011-12 to reach 22.1 million[26]

Increasing uptake

- Value of income derived from the internet increased by 25%, from $189 billion in 2010-11 to $237 billion during 2011-12[25]
- Australia public cloud services estimated to grow from A$884.4 million in 2012 to A$2,671.9 million in 2017[13]

Increasing value

A framework was developed to analyse and capture the drivers and trends in technology use within the three sectors, characterised by a customer-provider model. The technology users are both the customers and providers, with importance placed on their interactions. The processes the technology users perform are supported by software and enabled by ICT support infrastructure.

Technology-use Framework

Customer/Citizen	**Provider** (Government or Business)	
Customer only	Provider only	**Technology Users**
Customer-to-customer	Provider-to-provider	
Customer-to-provider and Provider-to-customer		
ICT Support Infrastructure		**Enablers**
Networks, end-points, data storage, and processing infrastructure		

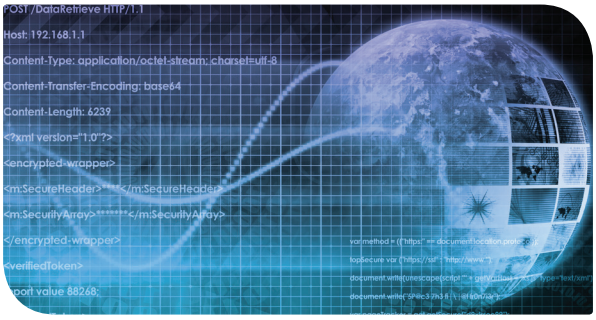
Findings specific to each sector were made plus a number of high-level drivers, general trends and early indicators were identified, as follows.

Customer Only

The focus in Health services is shifting from provider-centric to patient-centric, with customers taking a more active role in their own care through the use of personal health records, personal monitoring devices and mobile applications.

The Energy sector is shifting from a reactive and consumption-based model, to a model where customers (citizens and industry) are more actively monitoring consumption through real-time data from smart meters, applications connected to appliances, as well as generating their own energy (e.g. renewables).

Smart meters are enabling customers to monitor their electricity consumption. In Victoria they are mandated to become the standard meter. At November 2013 more than 90% of the rollout saw more than 2.5 million meters installed at homes and small businesses across the state[7].



Customer-to-Customer

Through the use of social media, the healthcare relationship is expanding beyond the traditional patient-doctor relationship to include a new customer-to-customer relationship, encompassing the patient, their family and the community.

Social media is playing an increasing role in the energy sector, particularly around sustainability and community interest about alternative generation methods (e.g. nuclear). However, as energy technology storage improves, in-home and distributed generation will likely increase, opening the door to new consumption models.

An international healthcare survey found that 39% of respondents used the internet to seek other patients' experiences[8].

Social media and online collaboration are enabling a new form of 'e-democracy', leading to unprecedented levels of citizen-to-citizen policy debate and discussion. As a result, public opinion and discourse is occurring at a faster rate and on a larger scale outside of government channels – e.g. forums, WikiLeaks, e-petitions.

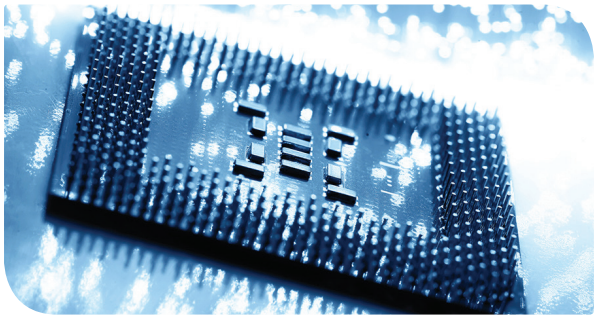
Provider Only

Health service providers are rapidly evolving service delivery through a transition to a digital environment enhanced by electronic records, cloud computing and mobility, and a new generation of diagnostic technologies.

Energy providers have for decades used technology to improve operations, for example control systems to drive greater efficiencies in energy management. However, access to real-time demand data via smart meters allows an increased use of automation and algorithms to improve decision making, and load prediction and management.

Australian hospitals are digitising business processes to increase healthcare worker efficiency and productivity. Investment has increased in wireless technologies to enable care from ambulances to rooms[9], biomedical and environmental machine-to-machine sensor integration[10], and the sharing, display and storage of data between central nursing stations and a physician's tablet or handheld device.

In addition to improving processes and allowing greater mobility of employees, individual government departments and agencies are digitising operations – eliminating paper processes, leveraging cloud services and developing analytic capabilities – to reduce costs and increase flexibility.



Provider-to-Provider

Integration of data, knowledge and expertise across providers will transform healthcare from siloed operations to a truly connected ecosystem of health services.

In energy, integration of information through the use of smart meters is set to transform electricity provider-to-provider relationships. Greater shared visibility of supply and demand is allowing more accurate forecasting, planning and management of peak demands.

Whole-of-government technology roadmaps and infrastructure consolidation are significantly reducing operating costs. Combining this with greater shared data and services, enables more effective inter-organisational linkages, reduced duplication, better decision making, and a comprehensive view of operations and national needs.

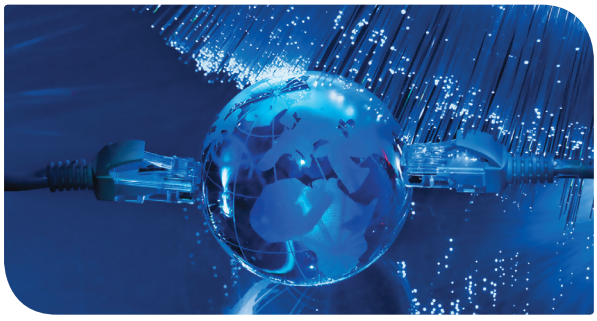
Customer-to-Provider and Provider-to-Customer

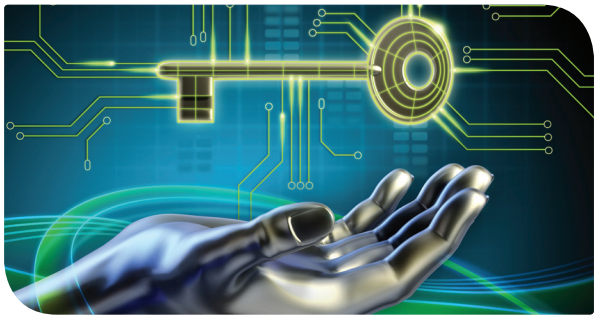
In healthcare the relationship between customers and providers will continue to deepen with greater personalisation, increased frequency of interactions and opportunities for preventative care through the use of new remote care and consultation models.

The relationship between electricity customers and providers is evolving rapidly as smart meters improve communication and real-time monitoring. This will lead to personalised energy pricing schemes and models to incorporate personal electricity generation back to the grid.

Citizen and business interactions with government are increasingly moving online, allowing for improved communication, greater control (via self-management), increased information accessibility, more efficient transactions, and lower costs. The net effect is an improved experience for citizens and businesses, particularly when dealing with multiple departments and/or agencies.

Across federal and state governments Australian citizens can now submit tax returns, pay bills, and apply for e-toll accounts or a birth certificate, etc. Online services are also available to the business community. The UK Cabinet office estimates that "For some government services, the average cost of a digital transaction is almost 20 times lower than the cost of a telephone transaction, about thirty times lower than the cost of a postal transaction and about 50 times lower than a face-to-face transaction"[11].

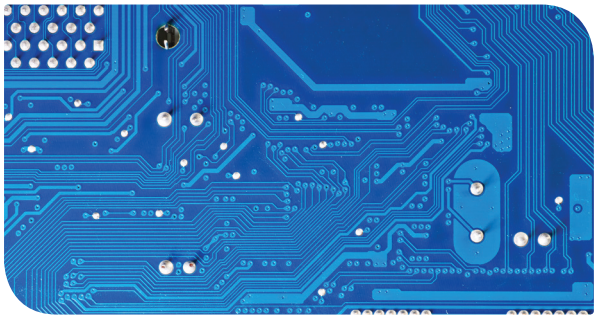




ICT Support Infrastructure

ICT support infrastructure will continue to provide opportunities for new ways of doing things and new capabilities across the three sectors. Cloud computing, mobile and location-aware technologies are currently enabling many of these new opportunities:

- Cloud services are being adopted to obtain flexible and cost efficient computing solutions[12]. As at May 2013, 44 percent of small and medium enterprises (approximately 900,000 businesses) had actively used cloud computing services. The most common uses were webmail services (57 percent) followed by file-sharing services (43 per cent)[13].
- Mobile technologies are enabling more convenient, easy-to-use services, increasing organisations' productivity and facilitating better engagement[14]. 7.5 million Australians used the internet via their mobile phone during June 2013, up 33 per cent compared to June 2012. Out of 189 countries, Australia was ranked sixth in terms of mobile broadband penetration per 100 inhabitants[15].
- Building on mobile technology, location-aware applications use a device's location data to provide information and services tailored to the user's needs and current location. Location based technology is offering the opportunity to crowdsource information on everything from road potholes to real time traffic flow information[5].



ICT-use and Dependency

Dependence can be defined as *the state of relying on or being controlled by someone or something else*.*

The increasing use of ICT across the three chosen sectors of healthcare, government and energy is clear. The national enterprise is enabled by the cyber domain; it is a cyber-enabled enterprise. The degree to which the national enterprise is reliant on ICT, however, cannot be judged by use alone. DSTO analysed ICT dependency within a framework of critical capabilities for society: create and use knowledge; communicate collaborate and form alliances; and perform actions.

Create and use knowledge: Knowledge was initially recorded in printed format in China during the T'ang Dynasty (618-909), but the globalisation of printing started with the creation of the printing press in the 15th century.[16] In the twentieth century digitisation of knowledge began, firstly through digitising extant printed knowledge and then through the creation of knowledge in digital format. In 1996 the Organisation for Economic Co-operation and Development (OECD) coined the phrase "Knowledge-based Economy" to recognise the role of information, technology and learning in economic performance, and to distinguish it from the earlier agricultural and industrial economies.[17] In particular, ICT has enabled the real time formation of knowledge to support critical operations such as disaster management, prediction and tracking of disease outbreaks, and predictive policing. In addition to providing the ability to create and store information, ICT enables intelligent retrieval of knowledge through advanced search capabilities. Given that ICT underpins the creation, access to and dissemination of knowledge, there is a clear dependence on ICT.

ICT is making the vast amount of medical knowledge available to support medical diagnosis. Healthcare workers can use Expert Systems to compare a patient's symptoms against the body of medical knowledge, to help them determine a diagnosis.

Communicate, collaborate and form alliances: ICT is enabling governments, organisations and individuals to communicate, share information, and collaborate without geographic constraints; to create knowledge from integrated resources. This ability is dependent on the cyber backbone of telecommunications and core infrastructure. Additionally, ICT users are dependent on each other to apply good cyber security practices that will keep cyberspace a safe domain to operate in.

Social media is providing individuals with greater opportunity for engagement and collaboration, and 'crowd sourcing' is harnessing knowledge and resources from the masses. Mobile devices are enabling people in developing countries, who might otherwise be excluded, to connect. In July 2012 the World Bank reported that around three quarters of the world's inhabitants have access to a mobile phone.[20] In developing countries, citizens are increasingly using mobile phones to create new livelihoods and enhance their lifestyles, while governments are using them to improve service delivery and citizen feedback mechanisms.[20] The advent of location-aware mobile devices is opening a new world of possibilities, including their use in collecting information during emergency situations. The use of social media and mobile devices is creating a dependency on ICT.

* https://www.oxforddictionaries.com/definition/english/dependence?q=dependence

Perform actions: A key element of taking full advantage of the digitised world is through the use of embedded processors. Embedded processors can now be found in most devices to control electrical and mechanical functions, for example they are found in power plants, medical devices, cars and aircraft, traffic lights, household appliances (microwaves, refrigerators, DVD players, printers, etc), portable devices (GPS, PDAs, watches, cameras, etc) and more. These devices are also increasingly interconnected giving rise to what is being called the Internet of Things*.

ICT is also being used by corporations, governments and industry to perform and, sometimes, automate their critical corporate and industrial processes. Organisations are employing ICT in an attempt to boost their productivity by undertaking existing tasks more quickly, cheaply and effectively by substituting ICT for other inputs, especially labour, and by using ICT as a means to innovate and develop new value-adding and efficiency-enhancing products, processes and organisational structures[19]. These two aspects have the following implications for dependency:

- ICT is reducing the ratio of workers to output. As this continues to decrease, there will be a point where, in exceeding some lower threshold, organisations will not have the required number of appropriately trained personnel to revert to some more manual process in the event of a technology failure. Maintaining a level of redundancy will be difficult and not cost effective in general circumstances.
- As digital maturity increases, new innovative processes will be dependent on ICT for their function. The diagram below shows the stages of digital maturity for a typical paper-based business process. Dependency on ICT to function is not applicable to the first three stages, in each of these cases the paper-based process can be reverted to, if there are enough people. It is the innovative processes that are technology led, that are dependent on ICT to function.

The Australian National Electricity Market is a complex system enabled by ICT. The transport of electricity from generators to consumers is facilitated through a spot market, where the ouput from all generators is aggregated and scheduled at five minute intervals to meet demand. The market uses sophisticated systems to send signals to generators instructing them how much energy to produce each five minutes so that production is matched to consumer requirements, spare capacity is kept ready for emergencies, and the current energy price can be calculated.[27]

Technological advances and ICT have combined to progress geospatial information systems; enabling layering of digitised and disparate data sets. Geelong's City Hall has developed a photorealistic 3D model of the city to help architects design better buildings faster and cheaper. Hills and valleys, trees, and man-made features such as building and traffic signs are included, along with sun angles and clouds, which can be adjusted to simulate conditions at specific times of the day on particular days of the year.[28]

*The connectivity built into all devices and appliances so that they can pick up information from various sources and automatically adapt to changing situations - Macquarie Dicitionary.com.au

Closing Remarks on Dependency

Parallels can be drawn between the introduction of electricity and ICT. Electricity supply started in Australia around 1880, with initial uses being lighting and electric tramways. Like ICT, electricity aided productivity, for example, in Sydney in 1879, at the Garden Palace, Botanic Gardens, arc lighting was installed at the urging of the Premier, Henry Parkes, to allow construction work to continue at night.[21] Similar to ICT, Australia was not dependent on electricity in the early days; candle or gas lighting could provide backup capabilities in case of power failure. As time progressed, electricity moved into industry, then small household appliances for heating, cooking and ironing. From there it gradually moved into large appliances such as washing machines, refrigerators and stoves, so that by the 1950s homes were 'all-electric'.[22] Progression has continued to the point where, today, the national dependence on electricity is a critical dependence in that the national enterprise, and society in general, cannot function without it.

A recent power outage in Darwin, in April 2014, highlighted this dependency. Although only without power for fourteen hours it caused schools, businesses, public transport and the public service to close. Hotel guests were evacuated. Traffic lights, mobile phones, ATMs and fuel pumps did not work, and businesses that did open could only conduct cash-only sales. Seafood, ice-cream, and other perishables were lost due to the lack of refrigeration. Hospitals and the airport were only able to continue service because they had back-up generators.[23]

With the pervasive use of ICT to create and use knowledge, to communicate, collaborate and form alliances, and to perform actions, it is not difficult to imagine a future world where we are also critically dependent on ICT.

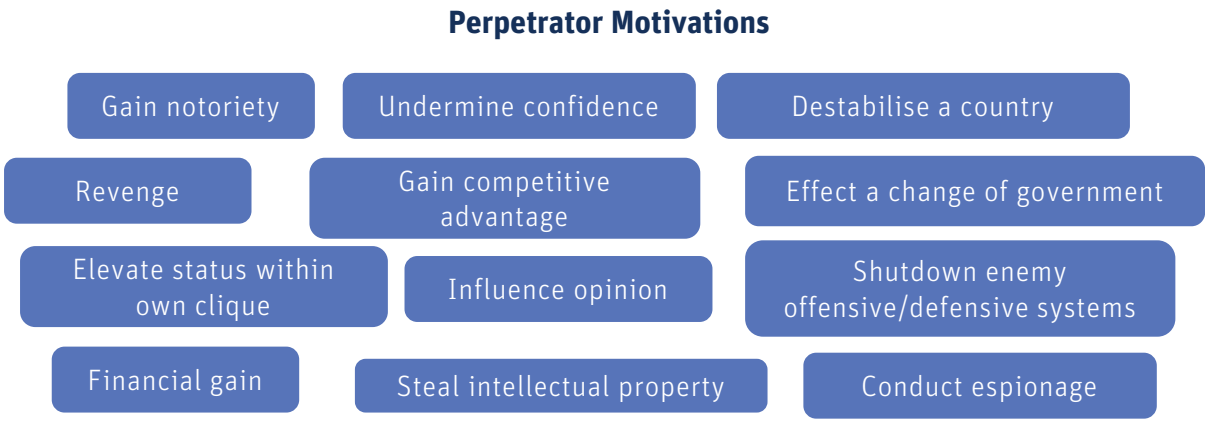
Threat Analysis

Cyber threats are potential cyber events emanating from unintentional actions or as a result of attacks developed by malicious parties that exploit vulnerabilities and that can cause harm to a system or organisation. Understanding both existing and emerging threats is vital for the future development and correct operation of information systems. Consideration must be given to threat origins, taxonomies of threats, influential environmental trends, and systematic prediction of emerging threats. Analysis of these aspects cannot be a static concept; the cyber domain is rapidly evolving thus requiring a continual process of monitoring and adapting to emerging threats.

This section presents a general overview of the threat landscape and then a future potential threat, Hardware Trojans, is analysed to determine its potential to impact the cyber domain. The analysis is based on a credible understanding of the threat and draws from **analytical and experimental work carried out within DSTO**. Hardware Trojans were chosen because they are a new class of threat to which there are currently no known catch-all countermeasures that can ensure that a device or system is free from such Trojans, or allow a system to operate in the presence of Hardware Trojans.

Perpetrators and their motivations

The perpetrators of cyber attacks, known as threat actors, include individuals (unintentional or malicious), issue motivated groups, organised crime, business competitors, terrorists and nation states. The sophistication of these actors can range from non-technical opportunists through to well-funded, long term strategic technical innovators. Perpetrators may also have one or more specific motivations driving their behaviours.



The Threat Landscape

The cyber domain is currently evolving at a rapid pace and scale with an increasing level of interconnectedness between physical and virtual systems, people and processes. Three broad types of threats that act on the cyber domain are:

- Software based - viruses, worms, spyware, root kits, exploit scripts, protocol exploits…
- Hardware based - Hardware Trojans, counterfeit components…
- People – Insider or outsider threats either from malicious or inadvertent actions or inaction.

These threats can affect data at any stage: during storage; when it is being processed; when it is in transmission across the network; or when it is accessed via a personal computer, mobile device, or other end point device. They attack the confidentiality, integrity and availability of information, information systems and hardware through:

- unauthorised disclosure of information (loss of confidentiality)
- unauthorised modification or destruction of information (loss of integrity)
- disruption of access to, or use of, information or an information system (loss of availability)

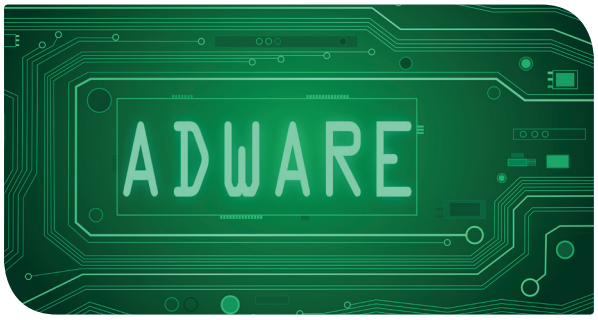
In the early days threats were enabled by immature cyber security, and coding and configuration errors were a primary source of vulnerability. This was partially mitigated by systems being less interconnected, and vendors owning the design and construction of their software and hardware. Today, cyber security has evolved but its current sophistication and maturity is being offset by:

- Increasingly sophisticated attackers and a threat-countermeasure cycle that favours the attacker.
- Software and systems designed and manufactured from a variety of sources giving rise to the possibility of compromised supply chains.
- Larger attack surfaces*, stemming from the increased complexity of systems and use models.
- Social and technology trends, such as the use of mobile devices, are leading to an increased number of insecure devices accessing networks and blurring the perimeters of systems.

In the future it is expected that:

- Attacks will become more opportunistic and difficult to detect or predict. Built-in threats will be become part of the landscape and be impossible to detect using current methodologies.
- Threats will become more potent because systems are more interconnected and people, business and government will have a greater reliance on ICT to function. Isolating systems as a protection mechanism will become impractical due to the need for interconnectedness.
- Effects or outcomes of attacks will not be as obvious and may go undetected for long periods of time and have longer term flow-on effects.
- There will be a move from code exploitation to manipulation of data, attacks on business processes and the introduction of systemic effects.

*The set of ways in which an adversary can enter a system and potentially cause damage - http://niccs.us-cert.gov/glossary



An Emerging Threat: Hardware Trojans

One example of a future threat is that of Hardware Trojans. This emerging threat challenges the foundations of current security models due to its potential to disrupt the core root of trust that system security relies upon. As a consequence, the current understanding of threats and how they are managed needs to be revised; future systems will need to operate in the presence of such threats yet maintain their desired operational and security goals.

Hardware Trojans are undesired, malicious, intentional modifications to electronic circuits. They are designed to compromise the behaviour of systems containing the circuits, presenting a persistent threat to their correct operation. Hardware Trojans can be inserted into an electronic circuit at any stage of design and development, manufacturing, distribution or maintenance. Modifications can include system level changes such as adding chips and circuitry, or changing existing chips by introducing new logic functions or subtle physical process variations during manufacture.

Compromised EFTPOS Machines (UK Oct 2008) – Organised Crime[29]

Early examples of Hardware Trojans were the province of intelligence agencies. Today, the globalisation of the supply chain and the rise of open source hardware development targeted at electronic enthusiasts, brings the means of developing Hardware Trojans to individuals.

- An organised crime syndicate is suspected of having tampered with chip and pin machines, either during manufacture at a factory in China, or shortly after they came off production.
- The machines were opened, tampered with and perfectly resealed early in the supply chain.
- Victims' financial credentials were recorded at point of sale, stored, and later forwarded (via embedded cell phone circuitry) to overseas criminal gangs.
- The criminals waited some time before using the card's credentials.
- It took more than six months to discover the compromised chip and pin machines.

Hardware Trojan Characteristics

Hardware Trojans have diverse characteristics:

- how and where they are introduced (insertion),
- complexity of the hardware modifications performed (size),
- how they are enabled and controlled (trigger), and their intention (effect).

Insertion	Size
Design Phase Chip Fabrication Electronic Assembly Supply Chain	Zero Size Small Medium Large
Trigger	**Effect**
Always On Time Data Signature External Signal	Kill Switch Degradation of Service Logic Attack Leak Sensitive Information

Insertion: The globalisation of ICT has resulted in the design, and design inputs (components of the circuit design), of integrated circuits being outsourced, along with their manufacture. Chips, circuits, and circuit boards can all be modified and all parts of the supply chain are vulnerable to exploitation. Under this scenario all systems, and all parts of a system, are subject to suspicion and a Hardware Trojan in any part can introduce a vulnerability that is difficult to characterise let alone protect against.

Trigger: Sophisticated triggering mechanisms such as data signatures hidden within plain sight allow an adversary to activate and control Hardware Trojan enabled attacks from outside an enterprise and from across the world. Firewalls, logical isolation, and even physical isolation are all ineffective protective mechanisms.

Size: Size doesn't matter when it comes to potential effects. Larger sized Hardware Trojans can be more quickly developed and deployed and are now within the capability of individuals. Very small Hardware Trojans, including those that make no modifications to circuits, will deny the ability to develop practical methods of detecting generic Hardware Trojans in circuits and systems.

Effect: The cyber security community are only still coming to terms with the possible effects that Hardware Trojans can leverage. More sophisticated effects that facilitate secondary or tertiary effects, such as enabling software threats, or causing third party systems to malfunction, can be very subtle and mask the identification and detection of the root cause of attacks.

Countering the Hardware Trojan Threat

Early research into the Hardware Trojan threat focussed on detection and prevention. This is only a viable strategy when seeking to protect a small amount of specific and high value systems, typically those employed by the military and those critical for national security. This strategy requires close control of the manufacturing and supply chain, together with dedicated and secure chip fabrication facilities. It does not scale and is unattainable for countries such as Australia, who have no commercial chip manufacturing capability and little electronic manufacturing capability.

Prevention

Prevention aims to stop the introduction of Hardware Trojans into silicon chips and ultimately into our electronic systems built with these chips. Prevention requires:

- Secure design processes coupled with trusted skilled professionals.
- Secure supply chain control that encompasses full life cycle management.
- Compliance strategies that include timely acknowledgment and adaptation to emerging threats.

The difficulties in ensuring supply chain integrity, the scale and complexity of our ICT systems together with cost pressures and commercial realities means it will not be possible to prevent a determined attacker from positioning Hardware Trojans within our systems.

Detection

Preventative detection is challenging:

- Small size, dormant properties, broad placement opportunities and level of integration make detection by traditional inspection methods near impossible; detection at a component level cannot reliably detect the full spectrum of Hardware Trojans.
- Detection at a systems level is impractical due to the possibility of stealthy and subtle systemic effects.

In practice therefore, detection relies on intelligence (a tip-off) or observation of the effect of the Hardware Trojan (information leak, degradation of service, etc). Forensic analysis would then be carried out to work backwards from the effect to determine the cause. The elapsed time, however, between observation of effect and attribution to the cause can be lengthy, making reliable timely forensics difficult.

Remediation

Three primary methods are typically used for system vulnerability remediation: apply a system component patch, adjust a system configuration setting, and removal of affected system component. These methods, however, are more applicable for software based systems and do not readily map to a hardware context. For example, Hardware Trojans present in chips are fixed and cannot be practically patched; they may reside in system components responsible for configuration management therefore are able to negate changes; or may be present in critical system components whereby no suitable replacement component exists. A further complication is that even when remediation steps are taken, there are no guarantees that vulnerabilities have been mitigated. Hardware Trojans may still be present in replaced or other system components but lay dormant therefore avoiding test and verification procedures.

Formalised remediation procedures for managing a Hardware Trojan based cyber event are yet to materialise. They would likely include the immediate steps of nullifying the Hardware Trojan, cleaning and restoring system state including software and data, and identifying consequences and linkages requiring corrective action. Identifying affected equipment may be difficult, and replacing them with known clean systems may in itself be a large and disruptive task. Like all cyber-attacks the assessment of compromise and damage will be dependent on the length of the penetration and its level of sophistication and integration – areas where Hardware Trojans are likely to have greater impact.

Security measures aimed specifically at countering Hardware Trojans are unlikely to be addressed until a credible attack justifies action.

Vulnerability

Vulnerability can be defined as *the state of being exposed to the possibility of being attacked or harmed.*[*]

Five keys areas of vulnerability emerged from overlaying emerging cyber threats on the future national dependency, and through the analysis of interviews with ICT-dependent end-users and service and infrastructure providers. The analysis of increasing dependency and emerging threats was provided to the interviewees as context for the exploration of our potential national vulnerability.

The five key areas of increasing digitisation, increasing complexity, increasing outsourcing, lagging security posture, and increasing interconnectedness are presented below, together with vignettes that describe how emerging threats could exploit these vulnerabilities.

Increasing Digitisation

Across the sectors there is a move to paperless business processes, online services and the publication of information online. Additionally, industrial control systems (for example SCADA[#]) are now using digital technology.

This exposes potential vulnerabilities in the following areas:

- All information will be digital, increasing the speed and scale of effects such as theft or loss.
- SCADA, initially proprietary technologies, are now moving to standardised and open systems making them vulnerable to extant network attacks.
- Systems are being optimised for efficiency which leaves little room for error.
- Absolute authentication of identity is not yet achievable online.
- Data is being accessed by larger numbers of people (e.g. employees, other corporations/agencies, public, etc) which increases the threat from people.
- Efficiencies and increased productivity achieved through digitisation mean organisations will not have sufficient staff with required knowledge to manage workload manually when systems fail.
- Increased attack surface (data can be attacked during access, transmission, processing or storage).

Example exploitation of vulnerability: *A Hardware Trojan residing in network communication chips performs a synchronized attack against network traffic on the corporate network of an energy company. The Hardware Trojan is distributed across many network attached devices and is intermittent and stealthy in its operation. Its effect is to significantly drop the bandwidth (throughput) of the network and increase its latency (introduce delay). Real-time consumer demand information supplied by smart meters is disrupted, denying power companies the ability to predict demand and ensure adequate generation capacity is on-line. Unaccounted for consumer generated electricity brings down portions of the power grid. Due to the scale, placement, and nature of the attack, the attack proceeds for weeks whilst remedial actions attempt to identify and isolate the cause.*

[*] http://www.oxforddictionaries.com/definition/english/vulnerable
[#] Supervisory Control And Data Acquisition

Increasing Complexity

Demands for more efficient processes and better data are leading to highly integrated systems and the aggregation of data. Together these are leading to complex systems composed of legacy programs and newer additions.

This exposes potential vulnerabilities in the following areas:

- Risk-managed security is being adopted because the perimeter of a system is too large to secure.
- Full visibility of a system may be hard to achieve.
- The number of lines of code in programs is increasing to where it is impossible to prove correctness.
- Complexity can hide subtle threat effects which may mean they go undetected for long periods of time and have longer term flow-on effects.
- Increased attack surface (many integrated systems).

Example exploitation of vulnerability: *The finance sector commonly employs a third party software application suite to manage stock exchange transactions. The code size and complexity of the software prevents skilled professionals with a current technology tool from evaluating the correctness of the software. A nation state actor, via an insider in the third party software company, inserts code segments that allow manipulation of transaction timing. When an attack is exercised, the nation state actor is able to influence stock exchange transactions, undermining investor confidence and causing stock market crashes. The subtlety of the transaction manipulations evades detection opening opportunity for future attacks.*

Increasing Outsourcing

Resource constraints and economies of scale are driving the increased use of local and offshore service providers, including cloud computing and overseas data centres.

This exposes potential vulnerabilities in the following areas:

- Dependence on systems/services not in your control e.g. a supplier's supply chain management.
- Outsourced services/supplies may be a vector for introduction of subtle exploits or vulnerabilities.
- Insider threat increased to encompass service provider staff.
- Increased attack surface (possibly spanning multiple organisations, countries).
- Immature understanding of 'trust' in the digital age and how it can be engendered in external relationships: policies can be written but there will be challenges in making them exhaustive and ensuring adherence.
- Dependence on services/systems which are subject to different threat environments and security regimes, causes misalignment with an organisation's assumptions for risk.
- Outsourcing arrangements not fully promulgated or too complex for consumers to understand, leading to consumers accepting risks they are not aware of.
- Understanding and adherence to each partner's legislative and regulatory obligations, and understanding of different jurisdictions may be too onerous for organisations without large resources leading to unwitting acceptance of risk.

Example exploitation of vulnerability: A sophisticated organised crime syndicate is able to insert computer memory modules containing a Hardware Trojan within a cloud computing installation dedicated for Australian government use. The Hardware Trojan allows an attacker running within one virtualised environment to access the data and services of another virtualised environment on the same cloud computing platform. The crime syndicate utilises a less protected public website of a government organisation to gain access to a virtualised environment. Utilising the Hardware Trojan, the organised crime syndicate is then able to access and compromise private information within a different virtualised environment run by the ATO to process tax data. The sophisticated nature of the attack coupled with the complexity of the underlying hardware, software, and cloud environment ensures that authorities are unable to pinpoint the cause of the data compromise when it finally comes to light.

Lagging Cyber Security Posture

The approach taken to security, from planning to implementation, affects the level of protection from both internal and external threats. The security posture of organisations includes the cyber security workforce, policies, procedures and controls. Investment needs to keep up-to-date with the dynamic and rapidly evolving cyber threat.

This exposes potential vulnerabilities in the following areas:

- Continued shortage of skilled cyber security personnel.
- Resource constrained security investment.
- Security solutions becoming very complex and difficult to implement fully.
- Security lags technology so security tools become less effective.
- Limited supply chain risk management including supplier/component diversity.
- Business processes do not adequately factor-in security issues.
- Inconsistent maturity of cyber security across and within the sectors.
- False belief that compliance equates to security.
- Inconsistent flows of cyber security information within and between sectors.
- Current threats absorbing all resources such that future threats are not addressed.

Example exploitation of vulnerability: *A sophisticated state based actor inserts a Hardware Trojan into real time clock modules present on commodity computing equipment. The Hardware Trojan allows an attacker to alter the computer system time reference used to manage security-critical functions such as passwords, certificates or building proximity access. An attacker intermittently adjusts the timing reference enforcing broad scale denial of service to time dependent systems, in part due to expiry requirements specified as part of standard business processes (for example passwords and certificates required to have an expiry date). The attack causes initial business disruption, however, the intermittent nature results in difficulties detecting the cause thereby exposing the business process to future attacks.*

Increasing Interconnectedness

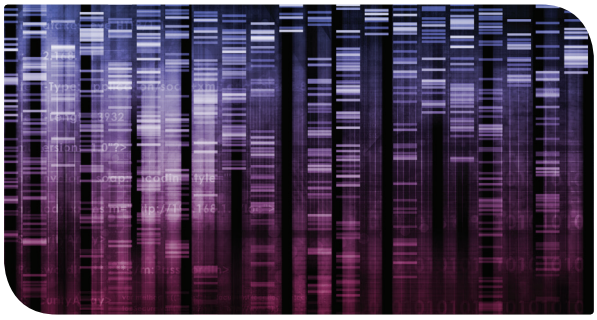
Digital information sharing is increasing between Federal, State, local governments and corporations, and the number of end point devices (e.g. PCs, laptops, smart phones, smart meters, wearable devices, medical devices, sensors, supervisory controls, etc) accessing or attached to networks is rising.

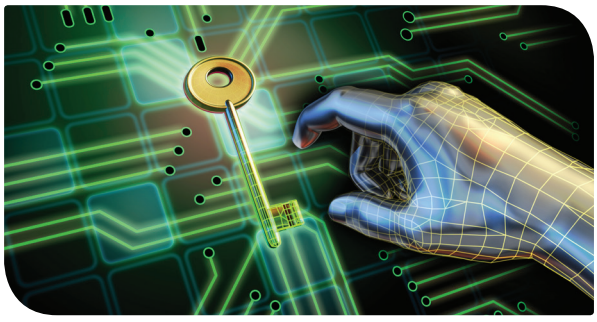
This exposes potential vulnerabilities in the following areas:

- Insecure end points due to limited security standards (and auditing) applied to devices because of lack of awareness or limited resources, or due to poor consideration of life cycle for cheap devices.
- Diminishing security focus from the centre of an organisation radiating out e.g. central government system out to private end point devices, giving rise to the potential to vector through weak links to achieve effects on the central system.
- Aggregated data more attractive to theft.
- Failure of one part causing cascading effects through an interconnected system.
- Increased attack surface (all links and connected systems).

Example exploitation of vulnerability: *Advancements in drug-delivery systems results in broad adoption of actuators that are biometrically bound to patients and require network triggered administration and monitoring of treatments. Actuator allocation is authorised by GPs with biometric binding technology allowing distribution of chemically charged actuators direct from pharmaceutical manufacturers and therefore replacing current day pharmacy services. System effectiveness is critically dependent on network connectivity between GP, pharmaceutical manufacturer and patient. An organised crime group concurrently exploits a zero day vulnerability* common to a broad set of pharmaceutical manufacturers. The group enacts a ransom motivated attack by encrypting biometric records preventing charging and distribution of actuators. Patient treatment is critically disrupted causing broad scale public loss of confidence in system.*

* "...a flaw in an application for which there is no patch available", Macquarie Dictionary





Conclusion

There is an evident trend towards increased use of ICT. It is transforming the sectors analysed - healthcare, government and energy - and helping to raise productivity, increase efficiency and effectiveness, and bring down operational costs. Additionally, these sectors are using ICT to respond to changing consumer demands by offering consumer-centric services, more engagement, easier transactions, and greater personalisation.

In addition to increased usage, society is increasingly dependent on ICT to create and use knowledge, to communicate, collaborate and form alliances, and to perform actions. Australia's dependency is expected to continue to increase over the next 5 to 10 years. Drawing a parallel to the history of electricity usage in Australia, it is not difficult to imagine a future world in which Australia is critically dependent on ICT, such that the national enterprise, and society in general, cannot function without it.

Concurrent with this increase in cyber dependence is an increase in cyber vulnerability, thus placing a high priority on cyber security. Technology progress promotes continual change in the cyber environment and emergence of new cyber threats.

Analysis of emerging threats points to a future in which attacks will be more opportunistic and difficult to detect or predict. Built-in threats (e.g. Hardware Trojans) will become part of the landscape and be impossible to detect using current methodologies. There will be a move from code exploitation to manipulation of data, attacks on business processes and the introduction of systemic effects.

Australia's cyber-enabled enterprise will be increasingly vulnerable to these threats due to increasing digitisation, complexity, outsourcing, and interconnectedness, and a lagging cyber security posture. Dependency combined with complexity and interconnectedness also have the potential to increase the potency of future attacks.

Together these paint a picture of a future cyber security landscape, in which:

- there is more at stake due to Australia's dependence on ICT,
- there is increasing exposure to potential cyber attacks,
- security continues to lag technology,
- future attacks may be more potent yet harder to detect, and
- response to attacks will be complicated by the complexity and interconnectedness of systems.

This document provides analysis which helps validate the hypothesis of increasing dependency on an increasingly vulnerable domain. The impetus for this document was stimulated by the DSTO Cyber S&T Plan: Cyber 2020 Vision, to underpin the case for developing a Cyber Security National S&T Strategy.

S&T is central to addressing these cyber security challenges and seizing cyber opportunities. The cyber domain is defined by S&T: it is progressed and shaped by technology and by how people adopt and adapt this technology.

References

1. Productivity Commission Research Report. An ageing Australia: Preparing for the Future. November 2013
2. National Health Priority Action Council (NHCPAC) (2006), National Chronic Disease Strategy, Australian Government Department of Health and Ageing, Canberra.
3. World Economic Forum. The Future of Government: Lessons learned from around the world. Switzerland: 2011
4. Productivity Commission. Caring for Older Australians. Canberra: 2011
5. Victorian Government ICT Strategy, Update: 2014 to 2015, Draft for Public Consultation
6. Queensland Government, Public Service Commission, Discussion Paper, Innovations in ICT for Improving Service Delivery: e-Government, http://www.psc.qld.gov.au/publications/subject-specific-publications/organisational-management.aspx, accessed 9/4/2014
7. http://www.smartmeters.vic.gov.au/home/latest-news/Smart-Meter-rollout-arrangements, accessed 9/4/2014
8. Bupa Health Pulse 2010, Online Health: Untangling the Web
9. Varyai R. Evolving Technology and its Effect on Healthcare. Frost & Sullivan, 2009
10. Romeo S. The Evolution of Mobile Health. Frost & Sullivan, 2012
11. https://www.gov.uk/government/publications/digital-efficiency-report/digital-efficiency-report, accessed 9/4/2014
12. Australian Public Service Information and Communication Technology Strategy 2012 - 2015, Department of Finance and Deregulation, 2012
13. Communications Report Series, Report 2 – Cloud Computing in Australia, Australian Communications and Media Authority, Australian Government, March 2014
14. Australian Public Service Mobile Roadmap: Adopting Mobile Technology Across Government, Australian Government Information Management Office, June 2013
15. Communications Report 2012 – 2013, Australian Communications and Media Authority
16. http://www.livescience.com/43639-who-invented-the-printing-press.html, accessed 22/4/2014
17. The Knowledge-Based Economy, OECD Paris 1996, OECD/GD(96)102
18. http://web.worldbank.org/WBSITE/EXTERNAL/WBI/WBIPROGRAMS/KFDLP/0,,contentMDK:20269026~menuPK:461205~pagePK:64156158~piPK:64152884~theSitePK:461198,00.html, accessed 22/4/2012
19. Productivity Commission Research Paper, ICT Use and Productivity: A Synthesis from Studies of Australian Firms, Commonwealth of Australia 2004
20. http://www.worldbank.org/en/news/press-release/2012/07/17/mobile-phone-access-reaches-three-quarters-planets-population, accessed 23/4/2014
21. A Dictionary on Electricity, Contribution on Australia, prepared for the Australian National Committee of CIGRE, 1996

References Continued

22. http://museumvictoria.com.au/discoverycentre/discovery-centre-news/2009-archive/first-electrical-appliance/, accessed 23/4/2014
23. http://www.abc.net.au/news/2014-03-12/blackout-closes-all-darwin-schools/5314480
24. http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/8146.0Chapter12012-13, accessed 22/4/2014
25. http://www.abs.gov.au/ausstats/abs@.nsf/Products/4C4A170C572B354DCA257BCE0012316F?opendocument, accessed 22/4/2014
26. Smartphones and tablets—take-up and use in Australia, Australian Communications and Media Authority, January 2013
27. http://www.aemo.com.au/About-the-Industry/Energy-Markets/National-Electricity-Market, accessed 2/5/2014
28. http://www.geelongadvertiser.com.au/news/d-modelling-for-geelongs-cbd/story-fnjuhxh0-1226790491371, accessed 2/5/2014
29. http://www.telegraph.co.uk/news/uknews/law-and-order/3173346/Chip-and-pin-scam-has-netted-millions-from-British-shoppers.html, accessed 2/5/2014

This page has been left blank intentionally.

For further information please contact:

Director Coordination, Cyber and Electronic Warfare Division
Tel: (08) 7839 5714
Email: CEWDDirCoord@dsto.defence.gov.au
Web: http://www.dsto.defence.gov.au

DSTO | Science and Technology for Safeguarding Australia