Australian Government

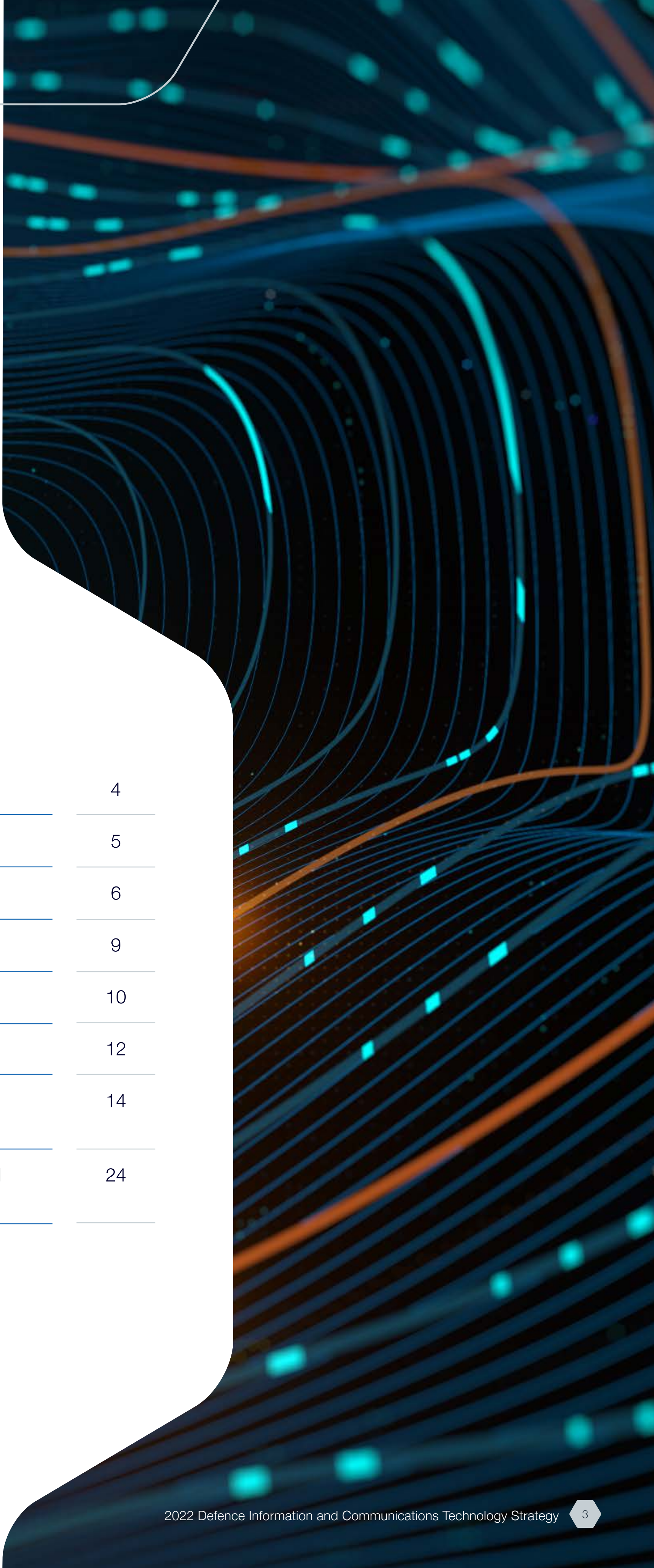
Defence

Ready to Fight and Win in the Digital Age

2022 Defence Information and Communications Technology Strategy

To defend Australia and its national interests in order
to advance Australia's security and prosperity

www.defence.gov.au



Contents

Foreword

Defending Australia, our interests and our way of life is the enduring responsibility of the Australian Government.

However the rapid pace of technological change has both accelerated military modernisation in the region and reduced our strategic warning time.

There is perhaps no greater example of that than recent advances in information and communications technology. Defence must now be **ready to fight and win in the digital age**: cyberspace has moved from an enabler to a warfighting domain in its own right. Defence must manoeuvre in and through this domain with greater speed and agility to counter the increasing sophistication and pervasiveness of the cyber threat.

Adaptive, assured, secure and accessible mission capable information and communications technology is a 'backbone' for our military power.

Modern warfare is characterised by high-tempo concurrent action in all domains. Only as a Joint Force can we fight and win, achieved through Command and Control, Communications and Computing, Intelligence, Surveillance and Reconnaissance (C4ISR) design. Defence has demonstrated its strengths to meet the challenges presented through heightened strategic tension, climate change, global pandemics and natural disasters, and technology has helped us seize these opportunities.

Consequently the *2022 Defence Information and Communications Technology Strategy* sets the direction for the whole-of-Defence to deliver mission capable information and communications technology. This Strategy includes an Action Plan to inform ongoing implementation planning and accountabilities to achieve this. It complements *Lead the Way: Defence Transformation Strategy* that provides clear guidance to support the transformation of information and communications technology across the whole-of-Defence.

Implementation of this strategy requires a commitment to action to respond to the challenges we jointly face, to value information and communications technology as a critical capability and achieve our goals.

I commend the *2022 Defence Information and Communications Technology Strategy* to everyone involved in Defence, including our people, key domestic and international partners, industry and academia.

Further, as our national security landscape changes, it is vital that our defence force remains positioned to meet global and regional security challenges. That is why the Government has committed to a Defence Strategic Review that will examine force structure, force posture and preparedness, and investment prioritisation, to ensure Defence has the right capabilities to meet our growing strategic requirements.

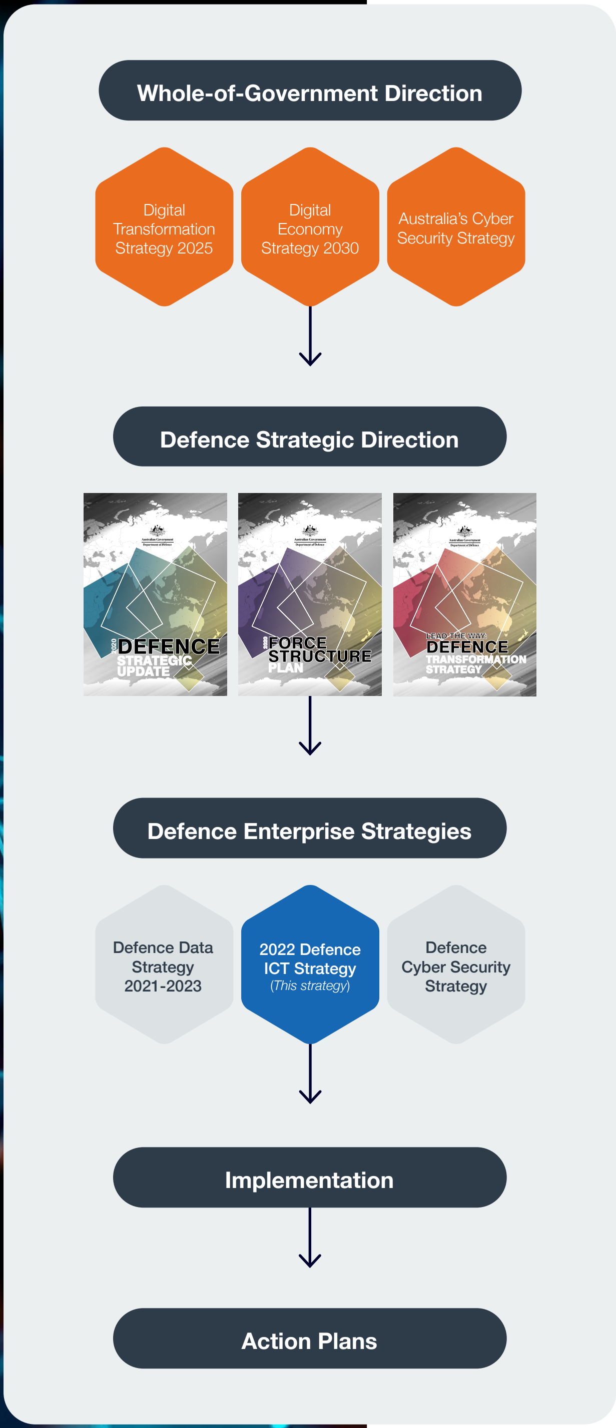
The *2022 Defence Information and Communications Technology Strategy* will be informed by the outcomes of the Defence Strategic Review to ensure that it remains responsive to our strategic needs.

Matt Thistlethwaite

The Hon Matt Thistlethwaite MP
Assistant Minister for Defence
Assistant Minister for Veterans' Affairs

Purpose

Diagram 1 - Hierarchy of Strategies



Whole-of-Government Direction
Digital Transformation Strategy 2025
Digital Economy Strategy 2030
Australia's Cyber Security Strategy
Defence Strategic Direction
2020 DEFENCE STRATEGIC UPDATE
2020 FORCE STRUCTURE PLAN
LEAD THE WAY: DEFENCE TRANSFORMATION STRATEGY
Defence Enterprise Strategies
Defence Data Strategy 2021-2023
2022 Defence ICT Strategy
(This strategy)
Defence Cyber Security Strategy
Implementation
Action Plans

The *2022 Defence Information and Communications Technology Strategy* sets out Defence's vision for information and communications technology from 2022.

As a future focussed document, this Strategy considers opportunities and threats that lie on the horizon, instead of on today's immediate activities or short-term plans.

Through four goals, this Strategy will shape our future Single Information Environment (SIE)[1] to be a critical capability in Defence. It will allow Commanders to deliver Joint Force effects across warfighting domains. Exchanges of trusted warfighting and battlespace information and intelligence with allies and partners over secure and survivable information and communications technology will allow us to meet Defence's strategic objectives to shape, deter and respond.

Informed by the *2020 Defence Strategic Update*, *2020 Force Structure Plan*, and *Lead the Way: Defence Transformation Strategy*, this Strategy translates Defence's strategic needs for the SIE. This Strategy is a critical input to meeting the ambitions of the *Defence Data Strategy 2021-2023* and provides high-level guidance to the *Defence Cyber Security Strategy*.

This Strategy is not a 'set and forget' document - it provides the direction for effective planning and transformation of the SIE as a Defence capability. The inclusion of an Action Plan guides Defence leaders, our allies and partners and decision makers to take action, so that Defence can **fight and win in the digital age**.

[1] The SIE encompasses the computing and communication infrastructure of Defence along with the management systems and people that deliver and sustain it.

Strategic Context

The world is becoming increasingly complex and connected, facing highly sophisticated and rapidly evolving threats. Information and communications technology is everywhere, from smartphones to military platforms; it is fundamental to Defence. Global connectivity is accelerating, with increasing reliance on information and digital communication to remain competitive and excel in everything we do. In parallel, there is an increase in the prevalence and sophistication of cyber threats.

Information and communications technology is no longer just an enabler. The Single Information Environment (SIE) is a critical capability serving as the landscape we fight in and through, as it forms part of the Cyber domain. The SIE is an ecosystem comprising a 'system of systems' that is a backbone of our military power. Mission capable information and communications technology integrates the operational domains of Cyber, Maritime, Air, Space, and Land, deriving military advantage from the ability to protect, value and exploit information to its full potential across an integrated Joint Force.

The rate of technological change is accelerating and keeping pace is becoming increasingly difficult. Increased regional military modernisation, coercive tactics in the grey-zone and the sophistication and prevalence of cyber threats demonstrate the ability of state and non-state actors to quickly exploit new technologies. Technology driven change could determine the winner in a future conflict.

The volume, size and type of data is increasing exponentially. Storage and distribution, including the integration, aggregation and availability of information coupled with shorter decision cycles, presents significant challenges. Data is a critical asset for warfighting – we must exploit it and protect it to remain ahead of our adversaries. It is critical for our ability to draw timely insights by connecting data sources to achieve military advantage. Our information and communications technology investments and capabilities are formidable for the defence of our nation across the conflict continuum.

The way we live and our work continue to evolve in response to crises. The everyday need for reliable and resilient information and communications technology to remain productive and digitally connected to communicate and collaborate, wherever we are, is greater than ever. The often degraded and disconnected deployed environment, where survivability and superiority of decision-making is paramount, requires resilient and adaptive information and communications technology.

A greater emphasis on self-reliance and development of sovereign capabilities is crucial to secure Australia's future. The workforce, skills and experience required to support our information and communications technology ambitions are in high demand across the public and private sectors, putting at risk the capacity to deliver the required military advantage to fight and win in the digital age.

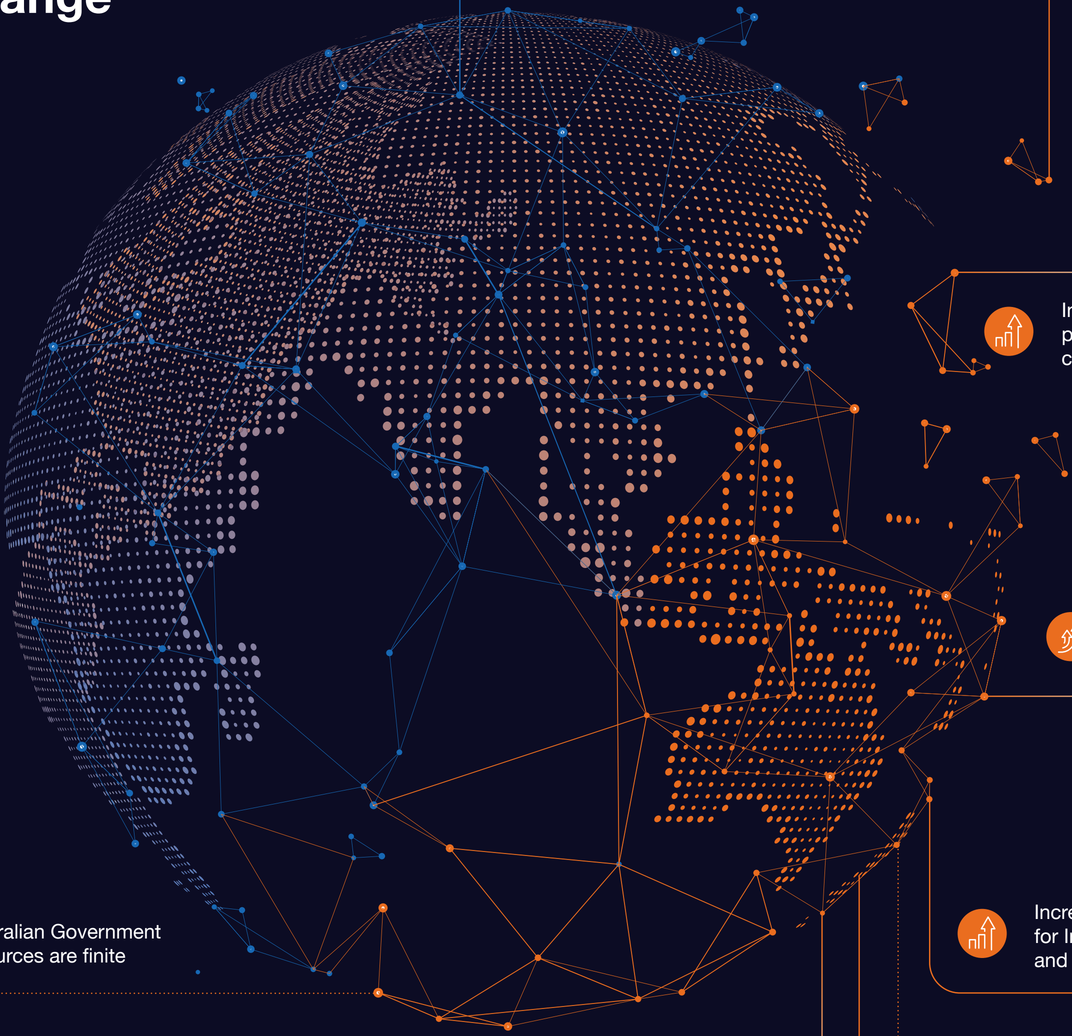
Defence is under increasing pressure to deliver capability faster. Over the coming decade, the Government plans capability investment in Defence, including the Australian Signals Directorate, totalling over $270 billion. More than $20 billion of that will be invested in Defence's information and communications technology, including enterprise information and communications technology and Information Environment and Cyber domain capabilities. This national capability investment recognises the **increasing criticality of cyber security, to defend Australia's future security.**

Australian Government investment in information and communications technology is expected to deliver broader impacts across government agencies. An ambitious digital transformation agenda has been set: that **Australia will be one of the top three digital governments in the world by 2025**. Through this digital reform, the Government aims to grow and streamline the delivery of information and communications technology services for use and reuse, improved efficiency and effectiveness. Australian Government data and information and communications technology, including critical infrastructure, must be a key priority when planning, designing, delivering, using and sustaining Defence's information and communications technology capabilities. Defence has a unique opportunity to contribute to the Australian Government digital and cyber agenda.

Defence **will continue to build strong partnerships with industry and academia** to address the national information and communications technology skills shortage and to support the development of sovereign capability to grow the required future workforce. We must work together, as **One Defence**, to maximise the value of information and communications technology.

Diagram 2

Drivers for Change



Volume, size and type of data is increasing exponentially

Increasing pressure to deliver capability faster

Rapidly changing environment

Increasing competition for Industry expertise and capacity

Vulnerabilities in Australia's supply chains

Australian Government resources are finite

Reduced strategic warning time

Increasing sophistication of cyber threats

Rate of technological change is accelerating

New threats from state and non-state actors quickly exploiting new technologies

Converging enterprise and operational technology

What will success look like?

Next generation, secure, sustainable and scalable information and communications technology underpins and integrates the future force to deliver Defence advantage in the digital age.

- Defence can harness the potential of our data and leverage it across the organisation to achieve advantage over our competitors, delivering enhanced awareness and faster, better decisions.
- Defence information and communications technology is modern and secure, protected and defended against evolving threats in cyberspace.
- The Single Information Environment is an integrated ecosystem, a ‘system of systems’ where consistent and reliable information can be accessed and exchanged seamlessly, from any device, at any location at any time.
- Defence has deliberate, integrated information and communications technology architecture, patterns and standards that support keeping pace with technology evolution and the operational demands of the future Joint Force.
- Information and communications technology is recognised as the backbone of our military power, as part of the Information Environment and Cyber domain, and as a key warfighting capability that is valued in Defence.
- Defence delivers lethal and non-lethal effects through a connected Joint Force based on trusted information and cyberworthy capabilities.
- Defence has a portfolio view of information and communications technology across Defence, including transparency of spend, and effective prioritisation of effort against available resources.
- Technology and application solutions are informed by clear and enforced business requirements, set by the strategic centre of Defence.
- Information and communications technology capability investment processes are customised to ensure they are maintaining pace with technological advancement.
- A risk-based approach is adopted to effectively balance the tension between the speed of information and communications technology delivery, expected levels of stability and cyber security requirements.
- Information and communications technology services deliver value, meet demand and capitalise on opportunities presented by innovative and disruptive technologies.
- Our close partnerships with industry, academia, coalition and allied partners deliver force multiplier effects and a regional capability edge.
- Defence has a professional, talented, skilled and experienced information and communications technology workforce to deliver and sustain mission capable information and communications technology.

Fight and Win in the Digital Age

Defence will invest in mission capable information and communications technology to deliver a Single Information Environment capability so that Defence is **ready to fight and win in the digital age**.

01100100 01100001 01110100 01100001 00100000
01100001 01101110 01100100 00100000 01101001
01101110 01100110 01101111 01110010 01101101
01100001 01110100 01101001 01101111 01101110

DEFENCE ENTERPRISE

Data informed, integrated processes and technology across the enterprise

Defence can quickly adapt and respond to the rapidly changing environment based on trusted and connected information

Greater awareness and ability to use trusted data to achieve faster, better decisions and insights

Greater ability to access information where and when needed

SINGLE INFORMATION ENVIRONMENT 2.0

Increased ability to collect, process and store data in the field

Increased ability to securely move large volumes of data to where it is needed when it is needed

Provide resilient and scalable platforms to support survivable decision making

New technology platforms provide a foundation to easily innovate to stay ahead

Defence has the people, skills and processes to deliver ICT faster

Defence can rapidly scale its ICT to meet immediate demands to respond to the environment

Defence ICT is simplified and remains new

ALLIES AND PARTNERS

Gain advantage through collaboration with partners

ACADEMIA AND INDUSTRY

Work with academia to gain advantage through our research and development and grow talent

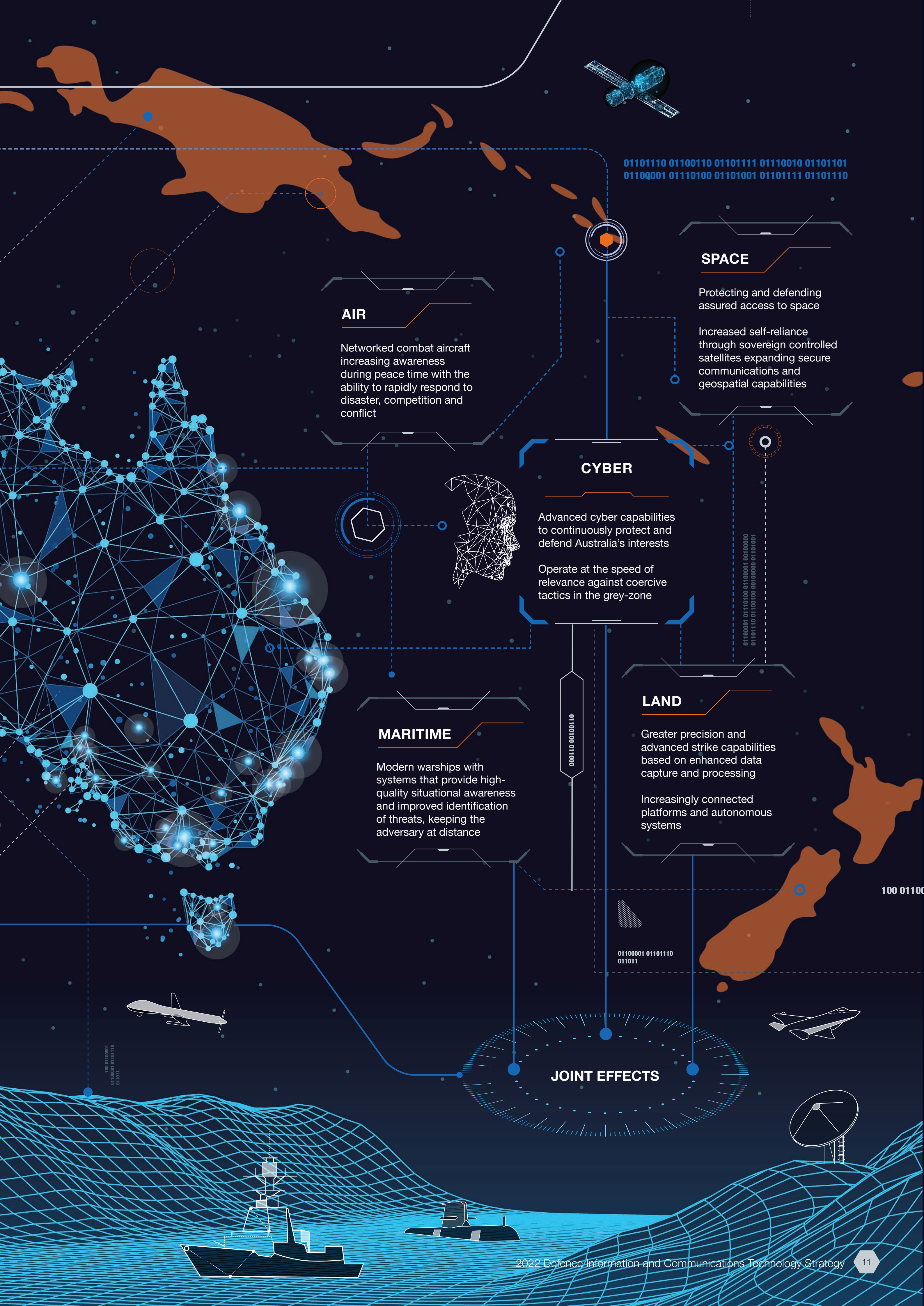
Gain advantage through better collaboration with industry to uplift security resiliency and sovereign capabilities

Reduced supply chain vulnerability and threat from disruption with increased self-reliance and sovereign capabilities

WHOLE-OF-GOVERNMENT

Optimised information and communications technology across Defence and whole-of-government to maximise Australia's investments

Contribute to keeping Australia safe whilst growing Australia's digital economy



AIR

Networked combat aircraft increasing awareness during peace time with the ability to rapidly respond to disaster, competition and conflict

SPACE

Protecting and defending assured access to space

Increased self-reliance through sovereign controlled satellites expanding secure communications and geospatial capabilities

CYBER

Advanced cyber capabilities to continuously protect and defend Australia's interests

Operate at the speed of relevance against coercive tactics in the grey-zone

MARITIME

Modern warships with systems that provide high-quality situational awareness and improved identification of threats, keeping the adversary at distance

LAND

Greater precision and advanced strike capabilities based on enhanced data capture and processing

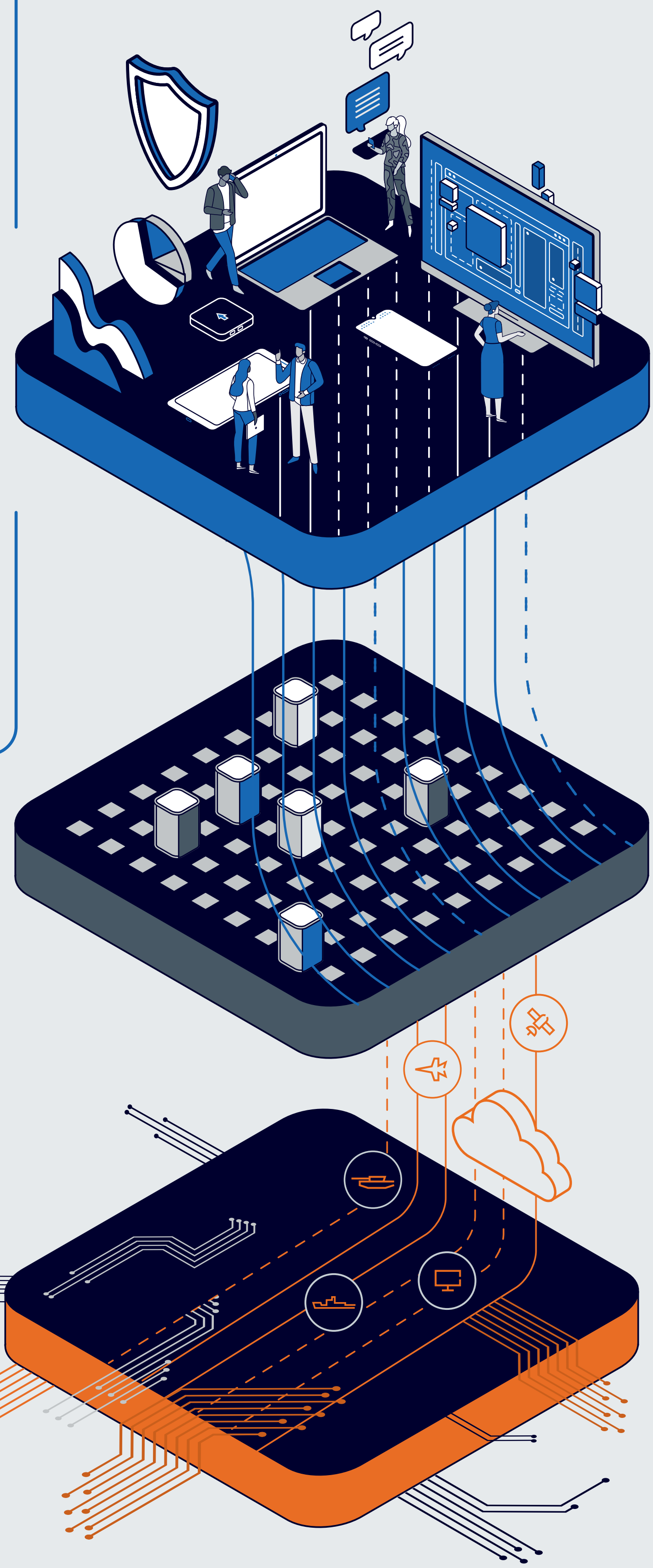
Increasingly connected platforms and autonomous systems

JOINT EFFECTS

Single Information Environment 2.0

The Single Information Environment (SIE) is Defence's ICT 'ecosystem'. It helps generate effects, whether on the desktop or in the battlefield. It encompasses the computing and communication infrastructure of Defence along with the management systems and people that deliver and sustain it. The SIE includes the data, infrastructure and service required for essential Defence functions including, communications, cyberspace warfare, logistics, Command and Control (C2), and Intelligence, Surveillance, Reconnaissance (ISR). To deliver mission capable information and communications technology, Defence will change the posture of the Single Information Environment to be more secure, resilient, survivable and scalable - increasing access to information where and when it is needed, whilst reducing vulnerabilities to threats that can impact decision making.

Diagram 3 - Single Information Environment 2.0



Fight and Win in the Digital Age

What is different?

Single Information Environment 2.0

Mission Capable Information and Communications Technology

Shape, deter and respond to protect and defend Australia’s interests

ICT investments are planned and governed	Defence ICT capability is managed as a single portfolio that can adapt quickly in line with changing Defence priorities to deliver lethal and non-lethal effects. Defence makes the most of its finite resources whilst leveraging industry provided capabilities and untapped capacity.
Defence information remains safe and secure	Defence information continues to be protected and defended against sophisticated threats.
Defence quickly adapts to stay ahead	Defence stays ahead of its adversaries, continuously improving the Single Information Environment and the way it is used, managed and sustained.
Simplified and standardised approaches in Defence	Defence ICT is built on improved business processes, data analytic capabilities, enterprise resource management and transformation that supports agility, interoperability and innovation.
Faster, better decisions	Defence ICT enhances human machine collaboration across the SIE, facilitating the integration of multiple sources of data to increase awareness, understanding and achieve faster, better decisions.
Easily collaborate to gain advantage	Defence can easily collaborate with its allies and partners including whole-of-government, academia and industry to share information and quickly convert innovation into industrialised capabilities to gain advantage.
Defence and its information are better connected	Defence information is increasingly connected and available where it is needed, when it is needed across Defence and its allies and trusted partners.
Defence operates at speed against threats	Defence is threat aware with the ability operate at speed against threats.
Future ready skilled ICT Workforce	Defence plans and grows a skilled digital and cyber workforce that can better leverage ICT to achieve the mission. A culture of excellence and continuous improvement ensures that Defence attracts and retains top talent and is able to better acquire and sustain the ICT needed to fight and win in the digital age.
Easy Access to ICT Services	Defence has access to contemporary and reliable ICT services that allows easy innovation, collaboration with partners and scalability at speed as the mission demands it. ICT functions that underpin operations will be automated for fast and efficient deployment of capability and interoperability with industry and allied partners.
Secure, resilient, survivable and scalable ICT Backbone	Defence has highly connected, interoperable and standardised platforms. Defence can transfer and extract value from large volumes of data across the SIE, safely with increased speed, reliability, scalability and survivability.

Increased ability to securely move large volumes of data where and when it is needed	Increased ability to collect, process and store data	Future focussed ICT services that can adapt to Defence needs	Resilient and scalable platforms to support survivable decision making	Defence can rapidly scale its ICT to meet immediate demands to respond to the environment	New technology platforms provide a foundation to easily innovate to stay ahead

Data Centric ICT	Transfer large volumes of trusted data securely across Defence, and with partners including warfighting domains, allies, whole-of-government, academia and industry.

New Network Types	Regional Edge Computing Platform Architectures	Hybrid Cloud			Scalable Applications
		Hybrid Cloud Business Models	Hybrid Cloud Environment	Single Virtual Distributed Data Centre	
New high speed and ubiquitous networking and gateway services that support movements of large volumes of data and allows rapid transport of data centre capabilities	New edge and remote computing architecture to better collect, process and store data, where and when it is needed	New business models to support service centric capabilities across software, platforms and infrastructure	Integrate selected software defined cloud service-based data centres onto the Defence network	Distributed systems architecture spans the network core between the central high-capacity data centres down to the peripheral edge based centres	New technology platforms provide a foundation so that Defence can easily create and implement new applications to meet Defence requirements

Cyber Security	Invest in defensive and offensive capabilities to protect and defend the evolving Single Information Environment against threats.
Interoperability	Allows Defence Groups and Services and its partners to coherently act together, share data and resources to achieve tactical, operational and strategic objectives.

■ ICT Effects ■ ICT Benefits ■ ICT Characteristics □ Description

Our path to success: to fight and win in the digital age

The *2022 Defence Information and Communications Technology Strategy* sets out four goals. The goals are structured to deliver Defence advantage – both military and business.

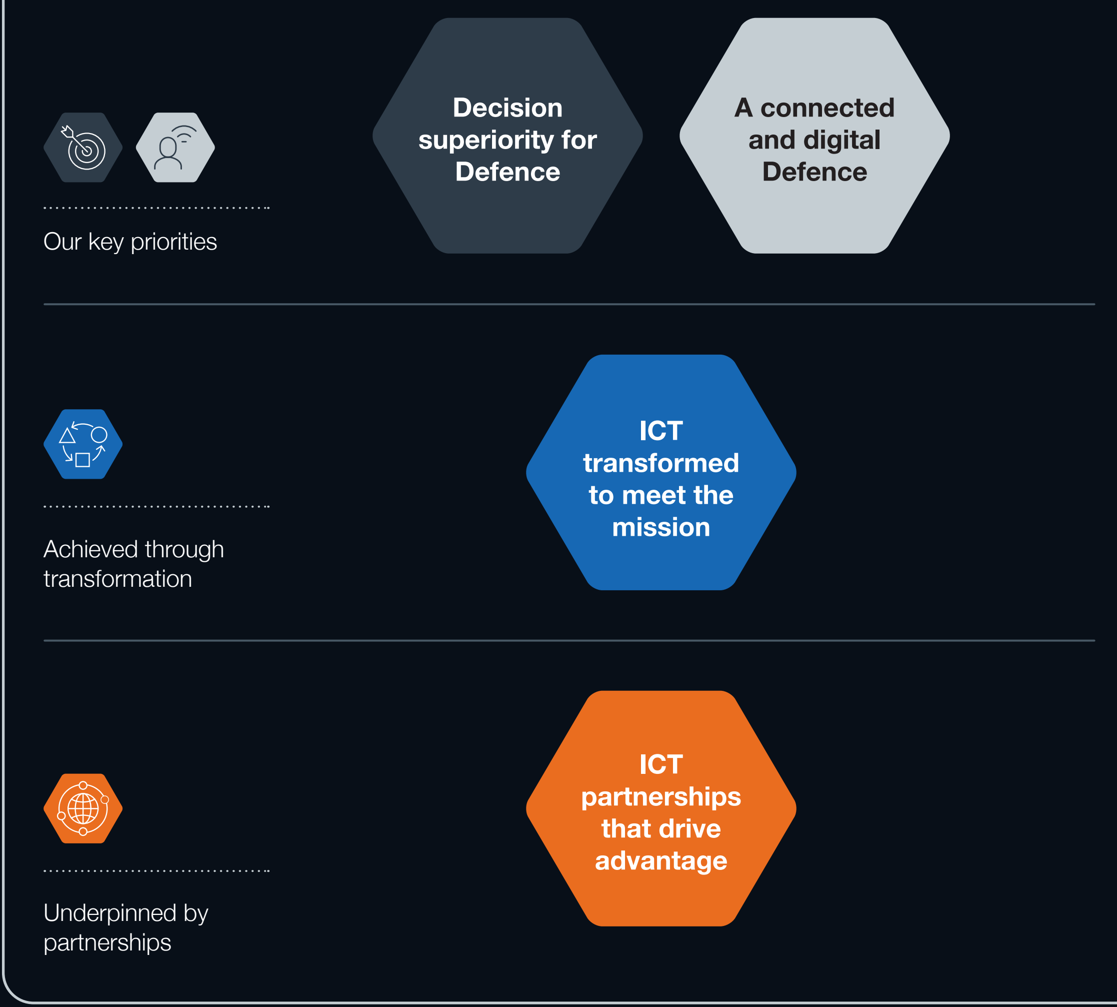
Extracting value and insights from our data that support faster, better decisions is key to Defence's decision superiority. Defence will be connected digitally to communicate and collaborate, including with our domestic and international partners. Information and communications technology is the backbone that integrates the Defence enterprise and the warfighting domains, contributing to the capability and effects of the Joint Force.

These priorities cannot be delivered without transforming Defence's information and communications technology capability. Defence recognises the importance of technology as an enabler, and values information and communications technology as a capability that is interoperable, secure, resilient and survivable, innovative and versatile – and can scale to meet Defence's evolving needs and operations.

Success is underpinned by our strong alliance, industry and Government partnerships forged to complement and supplement our resources and capabilities and deliver force multiplication effects.

[1] The Defence enterprise encompasses all of the Groups and Services within the Department of Defence, and their associated people, functions and outputs. *Page 16 Lead the Way: Defence Transformation Strategy*

Fight and win in the digital age



Our key priorities

Decision superiority for Defence

A connected and digital Defence

Achieved through transformation

ICT transformed to meet the mission

Underpinned by partnerships

ICT partnerships that drive advantage

Diagram 4 - 2022 Defence Information and Communications Technology Goals

Goal 1: Decision superiority for Defence

Information and communications technology empowers Defence decision-makers with access to information and insights for faster, better decisions in the modern battlespace.

Exploiting valuable insights from our large, diverse and disparate data is key to Defence's military advantage, delivering a unified operating picture and supporting warfighters to understand the environment in which they operate to generate the desired effects. Greater agility is needed to deliver Joint Force-level advantage across the competition and conflict continuum. The *Defence Data Strategy 2021-2023* seeks to empower Defence to become more data-informed in its decision making. Information and communications technology underpins this intent. Data, no matter its source, will be securely collected, protected, aggregated, stored and distributed across Defence, whole-of-government and with trusted partners. Investment in innovative and disruptive technologies, such as robotic process automation, artificial intelligence and machine learning will better store, move, process and visualise data, providing timely, new insights that contribute to Defence readiness, Command and Control (C2), and Intelligence, Surveillance and Reconnaissance (ISR).

Adaptive architectures, underpinned by peer-to-peer distributed networks and centralised patterns, are survivable within a congested and contested environment and drive warfighting capability and decision superiority. Investment in new network types and virtual distributed data centres will increase survivability of the Single Information Environment (SIE) and the ability to securely move large volumes of data to where it is needed, when it is needed.

Information is both a weapon and a target. Grey-zone activities in cyberspace are pervasive. Defence information is protected and defended from capable adversaries meeting Defence and Australia's interests. The *Defence Cyber Security Strategy* sets the direction for Defence to transform cyber security practices, workforce and investments to meet evolving cyber threats.

The right people, with the right level of data literacy and digital skills to manage, support and extract value from our data are as valued as those with the cyber security skills to protect and defend the SIE.

> **“Artificial intelligence will play a vital role in Defence’s future operating environment. This emerging technology will be critical to delivering on our strategic objectives of shape, deter and respond. Maintaining a capable, agile and potent Australian Defence Force is becoming increasingly dependent on artificial intelligence technologies.”**

Defence Data Strategy 2021-2023, page 35

What success looks like

Faster, better decisions

Defence leverages technologies and the ICT backbone to facilitate easy access and analysis of information where and when it is needed to enable Commanders and other decision-makers to increase awareness and make faster, better decisions.

Defence operates at speed against threats

Defence monitors technology advances and rapidly adapts to be threat aware, staying ahead of adversaries to protect and defend Defence information and broader national interests.

Defence remains safe and secure

Enhanced capabilities, supported by technology, continue to protect and defend the SIE against sophisticated and evolving threats.

Data centric capabilities

The *Defence Data Strategy 2021-2023* supports transformation of Defence to become a more data informed organisation. Adopting data centric practices and enterprise approaches will promote seamless and secure business and military interoperability across Defence and with its allies and partners. Targeted investment in the Single Information Environment (SIE) to achieve an integrated ecosystem will deliver faster, better decisions.

Goal 2: A connected and digital Defence

Defence is connected to communicate and collaborate through mission capable information and communications technology, when and where it is needed.

Modern, reliable, secure and resilient information and communications technology will realise our ideal business practices, systems and service delivery. This will deliver a seamless experience for users, connecting Defence capabilities, trusted information and people, regardless of their role, function or location.

Military capabilities and platforms are interoperable across Defence's operational and security domains. An integrated Defence enterprise architecture increases the awareness of the Joint Force, driving military advantage in the increasingly complex, contested and congested battlespace.

Defence can adapt and respond as the mission demands.

Investment in next generation wireless networks and sovereign satellite capabilities will assure our use of the electromagnetic spectrum, ensuring that Defence remains connected to securely communicate, collaborate and co-ordinate where and when it is required, including in the deployed, degraded and disconnected environment.

Defence will consolidate and rationalise multiple disparate systems into standardised and connected military and enterprise capabilities, continuously reviewing and decommissioning obsolete information and communications technology. Reducing technical debt will improve our cyber terrain management practices to better secure and risk manage Defence's current capabilities.

Adopting contemporary methods of processing and storing of information across all security levels including the adoption of cloud computing, edge computing, data analytics processing and management tools, will deliver faster, better decisions on the move.

Security is all encompassing, it must be provided at every step of the capability journey to ensure information remains safe, secure and trusted by those who need it to achieve the mission. With a stable and secure information and communications technology backbone, it will be easier for Defence to explore and implement innovative, disruptive and emerging technologies based on priorities, value and contribution to lethal and non-lethal effects.

What success looks like

Defence and its information are better connected

Increased ability to exchange secure information across hybrid-cloud environments (including edge computing) allowing information sharing between Defence and its partners and allies at required security classifications.

Secure, resilient, survivable and scalable ICT backbone

New high speed network services and enhanced scalable distributed hybrid-cloud services facilitate movement and processing of large volumes of data securely, using modern enterprise and domain based applications.

Simplified and standardised approaches in Defence

Defence information and communications technology supports and drives overall efficiency and effectiveness across Defence, including process improvements and ability to access trusted information securely where and when it is needed to gain advantage.

Defence adapts quickly to stay ahead

New technology platforms and processes allow Defence to explore and adopt contemporary technology solutions to stay ahead.

Goal 3: ICT transformed to meet the mission

Defence embraces advanced, adaptable and responsive information and communications technology with a skilled and capable workforce ready for the digital age.

Information and communications technology is no longer just an enabler, it is a capability that underpins everything we do in Defence. The pace of technology advancement is accelerating – to achieve advantage, Defence must embrace the opportunity to harness both new and emerging technology and invest in future focussed solutions that meet Defence's needs.

The Defence Transformation Strategy sets out how Defence will learn, evolve, align and deliver to transform its culture. A culture of collaboration, education, lessons and mentoring will recognise the importance of a **One Defence** approach to information and communications technology that embeds discipline and accountability across Defence and strengthens our ability to meet the mission. Improved visibility of investment, sustainment and security of information and communications technology across Defence will empower decision-makers to agree and prioritise our effort, optimise resourcing and continuously improve performance.

Future capability must be resilient against current and emerging threats. Transformation of Defence's information and communications technology operating model will set clear accountabilities, optimise organisational structures and streamline processes. This recognises the unique requirements of customers while also delivering against the needs of the whole-of-Defence to balance flexibility, stability and security, fast-tracking the delivery of innovative and scalable solutions. Defence will uplift planning, implementation, operation and sustainment of information and communications technology through adoption of leading practices, methods and leveraging contemporary technologies.

Defence people can easily access the information and communications technology services they need, when they need them. Defence people have the right level of data literacy to be digitally savvy and able to navigate technology and data to gain new insights. A highly skilled digital, data and cyber capable Defence workforce that embraces technology and values information and communications technology as a capability will support Defence's capacity to continuously improve and adapt as strategic circumstances change.

A workforce that is designed to meet Defence's future needs with a culture of excellence and continuous improvement will ensure Defence attracts and retains top talent. Defence will be recognised as an employer of choice, and will foster an information and communications technology workforce that is ready to achieve the mission.

> **“Technology and systems will be essential in enabling our adaptation and our understanding of performance and capacity. However, it is people who will determine whether this transformation is successful and that it leads to a stronger, more capable and effective Defence enterprise.”**
>
> *Lead the Way: Defence Transformation Strategy, page 28*

What success looks like

Future-ready skilled ICT workforce

Defence plans and grows the digital and cyber skills required in the digital age for its workforce to better acquire and sustain ICT as well as increasing advantage through better use of ICT assets.

Easy access to ICT services

Defence’s information and communications technology services are supported by integrated service delivery and business models. Defence’s people can easily access service centric capabilities that can adapt to Defence’s needs, and are supported to extract value from information and communications technology.

ICT investments are planned and governed

Defence ICT capability is managed within a consolidated portfolio that provides a single prioritised view to decision makers, and can adapt as priorities change. Defence can adapt quickly, guided by patterns and standards that direct investment to achieve Joint Force effects.

Goal 4: ICT partnerships that drive advantage

Strong information and communications technology partnerships across whole-of-government, industry, academia, allies and international partners contribute to Australia's security, resilience and sovereignty.

Collaboration with partners delivers Defence force multiplier effects. Interoperability for military operations, both with our coalition and allied partners and our domestic partners is critical to Defence's advantage.

The *Australian Government's Digital Government Strategy* sets a vision for Australia to be one of the top 3 digital governments in the world by 2025. As one of the largest information and communications technology footprints in the southern hemisphere, Defence makes an important contribution to supporting the Government's digital transformation agenda.

Defence has the support and expertise of industry for information and communications technology capability, including a sovereign industrial base that meets Australia's security, self-reliance and resilience requirements. Industry partnerships contribute to reduced supply chain vulnerability and risk of disruption and, particularly for cyberspace warfare, Command and Control (C2), Intelligence, Surveillance and Reconnaissance (ISR) capabilities, delivering an industrial and technological leap forward.

Industry will play an important role in realising this Strategy. Greater connectivity will help reduce obstacles for industry to contribute as part of the Defence information communications technology ecosystem. Interconnection with industry partners will exploit the opportunities presented by Industry 4.0 such as innovation, dynamic and resilient supply chains, information sharing, automation and advanced manufacturing.

Modern sourcing solutions with industry partners will deliver modern, scalable and flexible information and communications technology that meet the demands of our military and business operations.

In collaboration with academia, an established skills pathway will build and maintain a talented and capable information and communications technology workforce, while growing innovation and sovereign capability.

Defence will collaborate to deliver against broader national objectives, working together to achieve economies of scale and set best-practice approaches for the design and delivery of shared services, where they align with the Defence mission. We will contribute to the Australian economy through investment to support jobs and the growth of sovereign capabilities and contribute to the protection of Australian data, systems, networks and critical infrastructure.

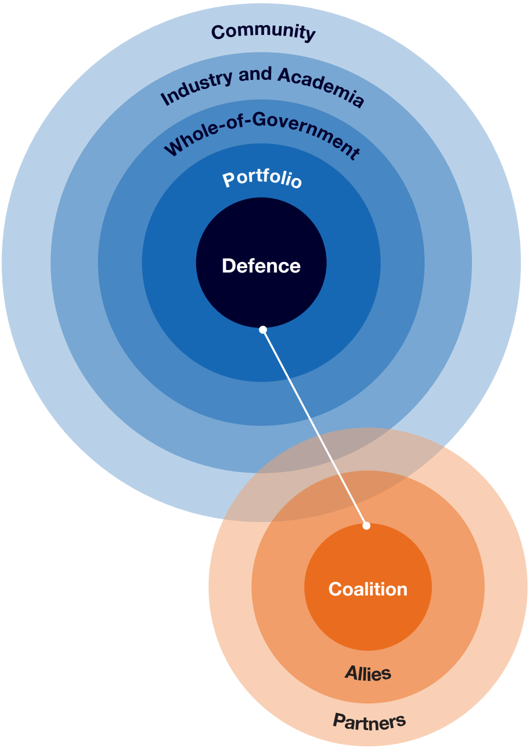
Defence will connect, synchronise and integrate capabilities and effects with coalition partners and allies. Enhanced interoperability and collaboration with a broad set of partners will realise asymmetric advantage, force multiplication effects and increased resilience of the Joint Force.

What success looks like

Defence can easily collaborate to gain advantage

Defence can efficiently and securely collaborate and share information, knowledge and innovation with allies and partners across whole-of-government, academia and industry to increase awareness and to innovate to gain advantage, including co-development of sovereign capabilities

Diagram 5 - Australian Defence ICT Ecosystem



"The Government will further invest in this sector ('Defence innovation ecosystem') to rapidly develop technology into capability and feed the innovation pipeline through the exploration and development of disruptive, leap-ahead technologies and technological adaptations and innovation emerging from Australian industry"

2020 Force Structure Plan, page 97 (Chapter Nine: Australia's Defence Industry)

Realising the 2022 Defence Information and Communications Technology Strategy

Action Plan

The *2022 Defence Information and Communications Technology Strategy* is supported by the accompanying Action Plan, which provides more detail on the initial actions for the next 24 months.

The Action Plan provides a framework for a more detailed implementation planning across the Defence enterprise and builds on the current foundations and in-flight ICT investments to modernise Defence's ICT backbone to be resilient, survivable and scalable to meet Defence's evolving needs and rapidly respond to threats in a dynamic environment.

The Action Plan will be assessed every six months to determine what has been achieved and establish the next six months against Defence priorities. This will provide a transparent and consistent approach to communicate progress of the Strategy across Defence and to Government, while providing flexibility to adapt and change.

Our People

The Strategy aligns to the Defence Values and Behaviours - **Service**, **Courage**, **Respect**, **Integrity** and **Excellence**.

Defence leaders, technical experts, customers and users across the enterprise play a critical role in achieving this Strategy. To meet the challenges in our environment, support secure and assured access to information, to collaborate and contribute to national endeavours, we must all play our part in the delivery, integration and sustainment of information and communications technology.

A culture of continuous improvement means striving to collaborate across **One Defence**, and to reflect, learn and improve.

Our people can act with purpose for Defence and the nation, and be adaptable, innovative and agile to the changing environment. Ultimately, our people will determine the success of this Strategy; modelling excellence through Our Values and Behaviours leads to a more capable, effective Defence Enterprise.

Defence will invest in skills and partnerships across Government and with academia, industry and our coalition and allied partners, build a culture of excellence and continuous improvement and become a sought after place for top talent to thrive in. As an employer of choice, Defence will position itself to be recognised for its digital contribution across Government.

Together as One Defence Information and Communications Technology Community

To achieve Defence's strategic objectives, Defence must operate with discipline as a single strategy-led and centrally-directed organisation – one that is flexible, proactive and effective in responding rapidly to changes in our environment. The successful implementation of this Strategy will be delivered through a high-performing, collaborative, **One Defence** approach to information and communications technology.

The **One Defence** approach relies on the commitment of all the Groups and Services within Defence and the broader Defence community, including the Australian Signals Directorate, Defence industry, and other partners. We will harness leading-edge Australian innovation and technological expertise that will provide capability and competitive advantage for Australian industry and the Australian Defence Force.

We must all work together to be **ready to fight and win in the digital age**.

INTENTIONALLY LEFT BLANK

INTENTIONALLY LEFT BLANK