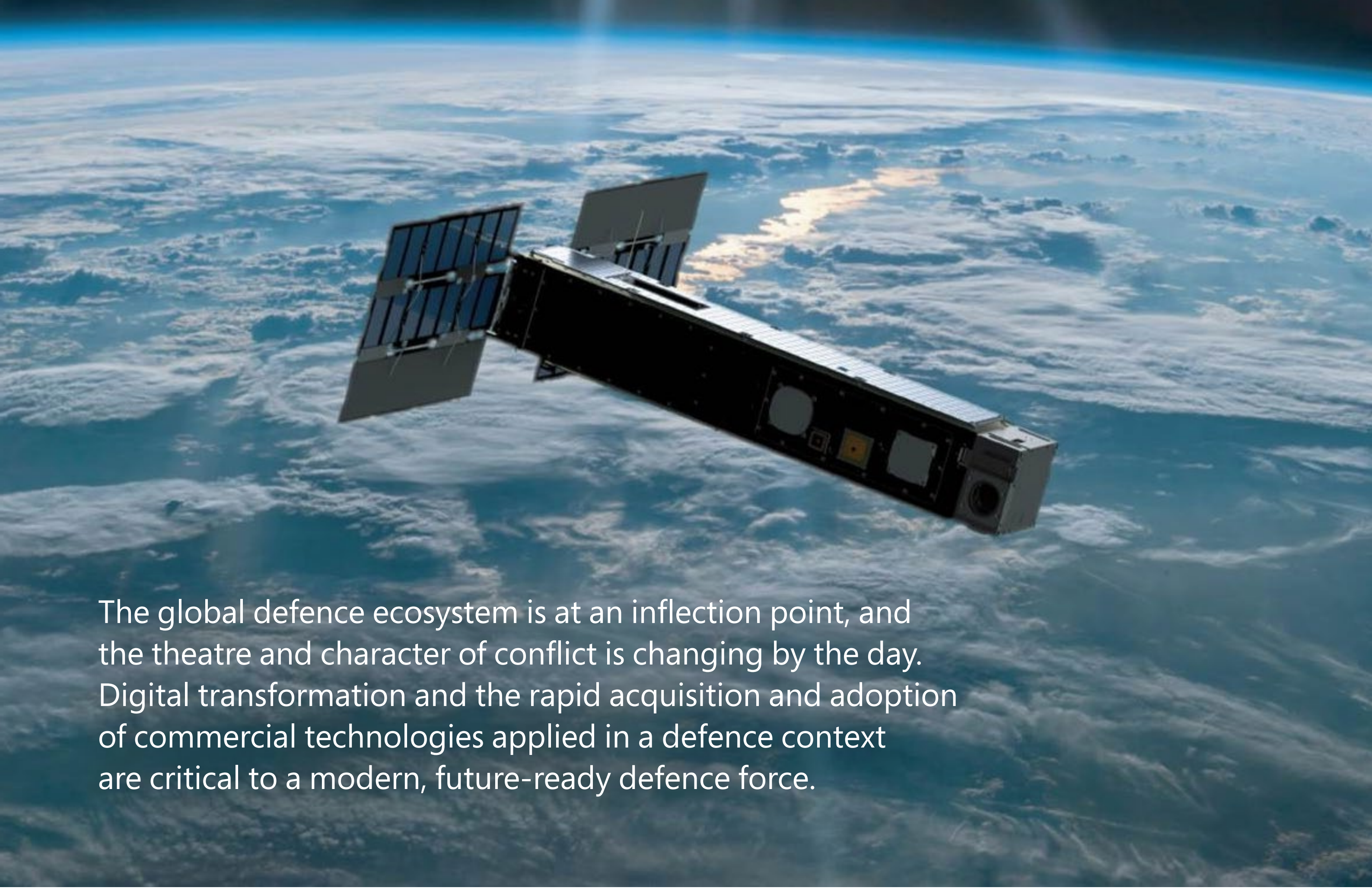
Deploying digital operations to protect national security

How to develop, procure and adopt commercial technology at speed to maintain competitive military advantage.

Microsoft



The global defence ecosystem is at an inflection point, and the theatre and character of conflict is changing by the day. Digital transformation and the rapid acquisition and adoption of commercial technologies applied in a defence context are critical to a modern, future-ready defence force.

In an expanded digital landscape for defence, the ability to develop, procure and adopt commercial technology at speed is critical to maintaining competitive military advantage.

To ensure our defence force remains positioned to meet our global and regional security challenges, dramatically increasing the speed of technology development, procurement and partnership may be necessary. Increasing collaboration across the myriad of allied innovation organisations will help to accelerate innovation and limit duplication of research and development efforts across services and nations.

Why this matters now

- The age of the hybrid and remote warfare with an increased tempo of grey zone warfare has expanded network perimeters. As boundaries become less defined, the defence ecosystem must act to shore up systems, data and workers against adversaries aiming to take advantage of this modern and changing digital landscape.
- Sovereignty doesn’t necessarily equal security. As demonstrated over the past year, modern conflicts often include combined cyber-attack and kinetic effect on physical sovereign assets.
- The implications of wartime operations for global cybersecurity see multi-domain warfare playing out in real time. It is the world’s first ‘broadband war’.
- The legacy procurement environment of 30 years ago no longer makes sense in a multi-domain, integrated battlefield with an increased tempo.
- The next great power competition will likely be won or lost based on the speed at which new technology can be developed and adopted.

This expanded digital landscape for defence is ripe with opportunity, but it also presents that same opportunity for adversaries employing sophisticated cyber attacks targeting defence systems, data and people.

The Australian Defence Strategic Review will examine force structure, force posture and preparedness, and investment prioritisation, to ensure defence has the right capabilities to meet our growing strategic needs. Our forces need to work toward change-readiness for the coming recommendations.

No nation can fight alone, and it requires a collective approach across nations and industry – including non-traditional vendors – to maintain competitive advantage.

So, what must we do now to enable this posture?

1. Prioritise a trusted and secure digital backbone.
2. Enhance interoperability – enabling secure data and information sharing with partners, allies and agencies.
3. Maintain effective collaboration with allies and the defence industrial base (DIB) through a modern capability lifecycle.
4. Accelerate battlespace success through digital transformation.

Deliver a trusted and secure digital backbone

Technology is pervasive across the defence and intelligence environments, but legacy increases risk, especially with technologically advanced adversaries.

A hyper-scale cloud environment extended to the edge and built on a foundation of trust and security provides defence forces and partners with a digital backbone on which they can collaborate and develop, deploy and leverage capabilities.

Nation state actors are launching increasingly sophisticated cyberattacks designed to evade detection and further their strategic priorities. So, what must defence organisations do to defend against these persistent and ubiquitous cyber threats?

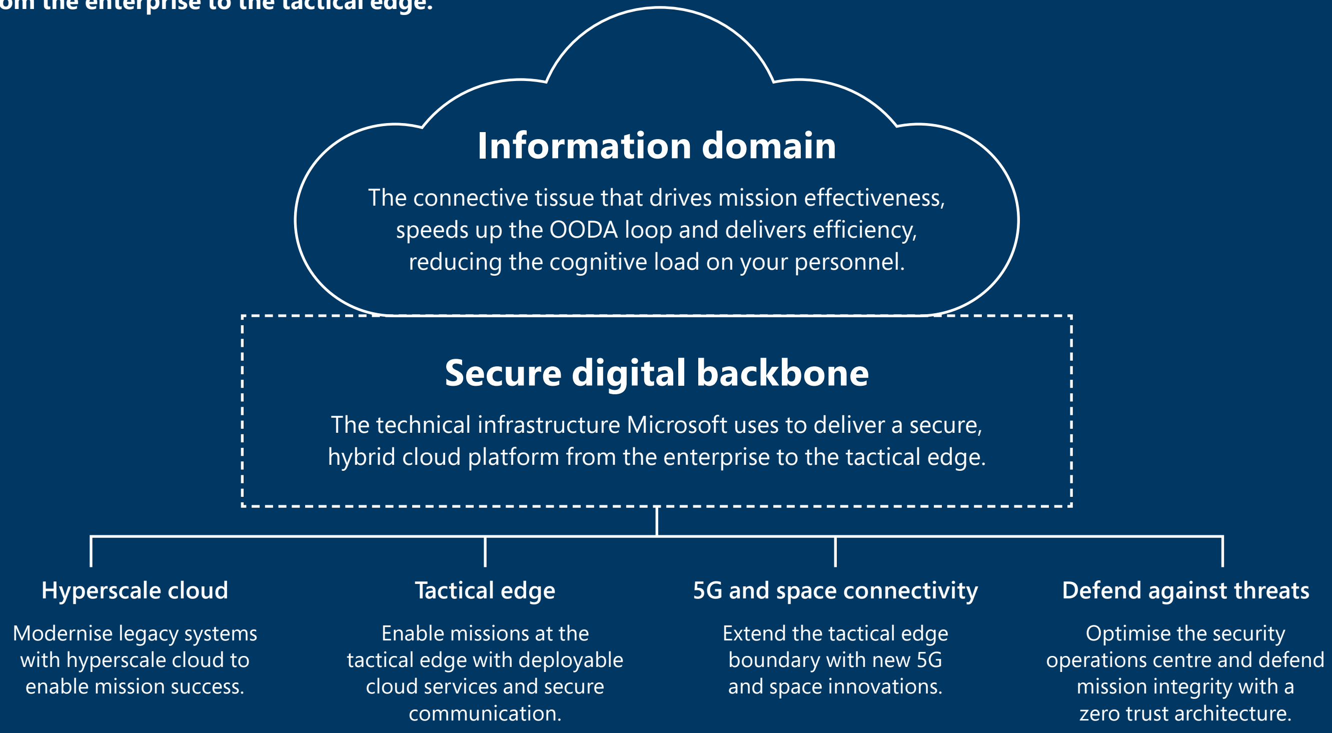
Digital technologies are the connective tissue that forces us to influence and harness the information domain. The key to Australia's digital resilience in wartime is the ability to keep data secure outside traditional sovereign borders while still readily connecting to it, wherever forces are based – for seamless digital operations.

Why must nation states embrace secure, cloud-enabled distributed capabilities?
In 2022, cyberattacks targeting critical infrastructure jumped from 20% of all nation-state attacks to 40%. This spike was due, in large part, to Russia's goal of damaging Ukrainian infrastructure and aggressive espionage targeting Ukraine's allies.[1] However, these attacks had limited operational impact because Ukraine's digital operations and data were rapidly dispersed into the public cloud.

That's not to say that the cloud is appropriate for every single scenario. We know that's not the case in our industry. For instance, there are currently requirements for mission data to remain air-gapped. However, some governments around the world have pursued initiatives in recent years to centralise government digital operations in so-called sovereign data centres that are more specialised, locally controlled and located within a country's borders. While there are some factors that make this appealing from a national security perspective in times of peace, the situation in Ukraine illustrates the very different defence needs that prevail during a war.[2]

[1] Nation-state cyberattacks become more brazen as authoritarian leaders ramp up aggression, Microsoft, Nov 4, 2022
[2] Defending Ukraine: Early Lessons from the Cyber War, Microsoft, June 2 2022

Figure A. Provide a secure hybrid cloud platform from the enterprise to the tactical edge.



Information domain

The connective tissue that drives mission effectiveness, speeds up the OODA loop and delivers efficiency, reducing the cognitive load on your personnel.

Secure digital backbone

The technical infrastructure Microsoft uses to deliver a secure, hybrid cloud platform from the enterprise to the tactical edge.

Hyperscale cloud

Modernise legacy systems with hyperscale cloud to enable mission success.

Tactical edge

Enable missions at the tactical edge with deployable cloud services and secure communication.

5G and space connectivity

Extend the tactical edge boundary with new 5G and space innovations.

Defend against threats

Optimise the security operations centre and defend mission integrity with a zero trust architecture.

How this plays out in the field

Ukraine showcases the resilience of cloud and the concept of 'movable defensible targets' – in which a physical data centre is vulnerable while distributing data across NATO or FVEY countries builds excellent resilience.

The advent of cyberweapon deployment in the hybrid war in Ukraine is the dawn of a new age of conflict, seeing the use of destructive cyberweapons, including ransomware, as a staple of attacks. Nation-state actors have begun using advancements in automation, cloud infrastructure and remote access technologies to attack a wider set of targets.

Cybersecurity hygiene has become even more critical as actors rapidly exploit unpatched vulnerabilities, using both sophisticated and brute force techniques to steal credentials. These developments require urgent adoption of a consistent, global framework that prioritises human rights and protects people.

The conflict has brought into bold relief the use of sophisticated cyber operations by nation states. We are seeing foreign influence operations enacted in force in a coordinated fashion along with the full range of cyber destructive and espionage campaigns. These involve sophisticated and coordinated efforts to use digital technologies and the internet to create and spread false narratives to advance multiple goals.

Cyber operations complement kinetic action

The war in Ukraine highlights governments' reliance on digital communications and data. Key to sustaining the Ukrainian government has been to disperse these digital operations into the public cloud and outside the country itself.

Prior to the war, Ukraine had a longstanding Data Protection Law prohibiting government authorities from processing and storing data in the public cloud. This meant the country's public-sector digital infrastructure was run on servers located within the country's borders. A week before the Russian invasion, the Ukrainian government's servers located within government buildings were vulnerable to missile attacks and artillery bombardment.[3]

Since the beginning of Russia's invasion of Ukraine, Microsoft has observed Russian cyber threat groups performing actions in support of their military's strategic and tactical objectives. At times, computer network attacks immediately preceded a military attack.

Cyber operations have been consistent with actions to degrade, disrupt or discredit Ukrainian government, military and economic functions, secure footholds in critical infrastructure and reduce the Ukrainian public's access to information.[4]

Ukraine's government successfully sustained its civil and military operations by acting quickly to disperse its digital infrastructure into the public cloud, where it has been hosted in data centres across Europe. This has involved urgent and extraordinary steps from across the tech sector.

Build your strategy to strengthen defences against cyber destructive, espionage and influence operations

The cyber aspects of the current war extend far beyond Ukraine and reflect the unique nature of cyberspace.

Destructive attacks observed in Ukraine have similar characteristics and mitigations to ransomware scenarios that Microsoft has identified worldwide in recent years.

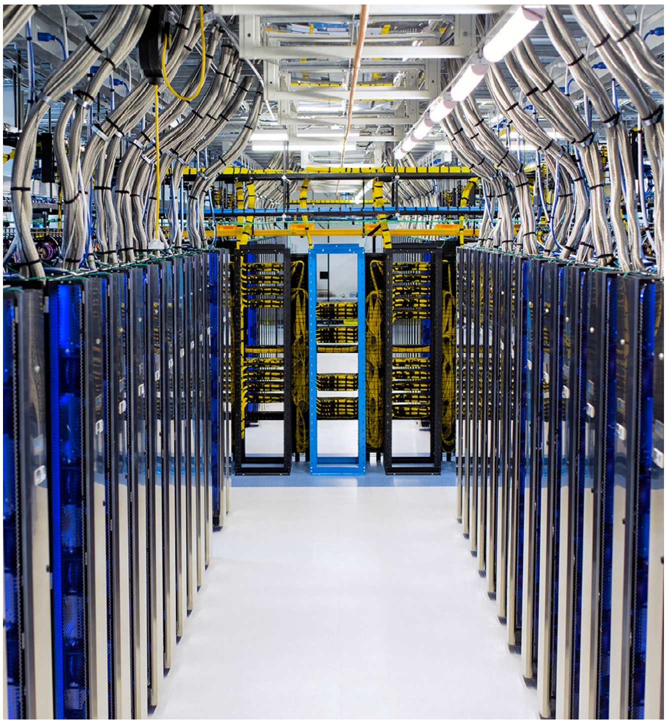
When countries send code into battle, their weapons move at the speed of light. The internet's global pathways mean that cyber activities erase much of the longstanding protection provided by borders, walls and oceans. And the internet itself, unlike land, sea and the air, is a human creation that relies on a combination of public- and private-sector ownership, operation and protection.

This requires a new form of collective defence.
The cyber defence of Ukraine relies critically on a coalition of countries, companies and NGOs.

An effective response must increase capabilities to better:

1. detect,
2. defend against,
3. disrupt, and
4. deter foreign cyber threats.

This approach is already reflected in many collective efforts to address destructive cyberattacks and cyber-based espionage.[5]



[3] Defending Ukraine: Early Lessons from the Cyber War, Microsoft, June 2 2022
[4] Special Report: Ukraine, Microsoft, April 27, 2022
[5] Defending Ukraine: Early Lessons from the Cyber War, Microsoft, June 2 2022

Enable cooperation in the future operating environment

Cooperation is critical to the success of modern defence organisations. Even today, operations require a high degree of coordination across allied nations and their defence forces.

As global threats evolve, the need for an integrated and coordinated response becomes increasingly vital. With an increasing focus on building alliances comes the need for greater interoperability.

The key context is that today's defence challenges exist at a scale, scope and complexity that no military can meet alone. In addition, the pace of change is such that defence organisations – particularly those of the middle powers, such as Australia – are having to decide how they balance their investment in mass against the need to modernise.

Previously, exercises and military operations have led to certain interoperability capabilities. Now we're moving beyond a single collaboration. As capabilities build along with tactical employment of forces, it creates a need for common technologies on which data and the applications can reside.

Enable secure data and information sharing with partners, allies and agencies

The dynamics of future operating environments require operating forces and coalitions to share information, data, intelligence and technologies to outperform an aggressive and ever-evolving adversary.

Interoperability is an essential contributor to strategic advantage, because organisations that are interoperable can respond with agility, leveraging technology to manage massive amounts of data. But if defence and intelligence organisations are to evolve their ability to collect, analyse and share that data – from the edge to the joint command centre – they need to go beyond basic connectivity and incorporate capabilities that are interchangeable, where appropriate. This is how they will obtain decision superiority in a rapidly evolving defence context.

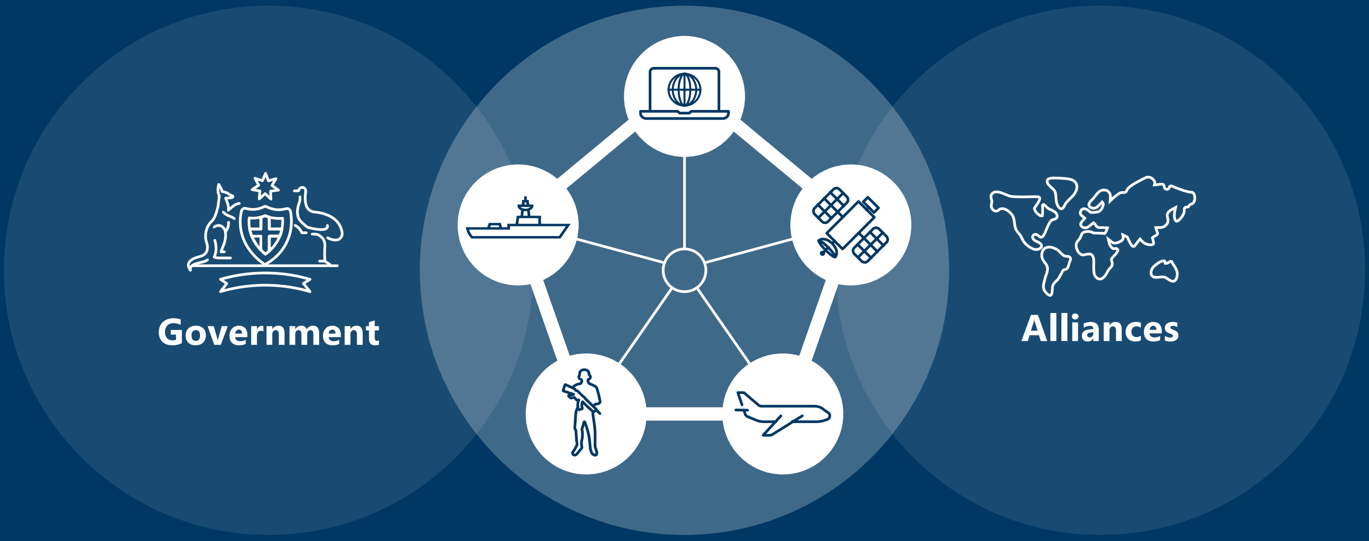
New and emerging capabilities to help you achieve interoperability with coalition partners

As military operations become increasingly data-driven, timely access to important information and applications is critical. For the military, edge computing puts computation and data resources closer to where relevant information is emerging.

Extending Azure services into denied, disrupted, intermittent, and limited bandwidth environments enhances near real-time decision making, giving elements in the field a chance to maintain their operational momentum and seize the initiative.

These sophisticated processes can exploit data and apply AI and simulations to make sense of many and varied futures, enabling a better understanding of any scenario.

Figure B. Communicate across multi-national, multi-agency and multi-domain boundaries to respond with agility.



How this plays out in the field

One of the biggest operational challenges for the field is the ability to access and share increasing volumes of data from remote locations quickly and securely, and then analyse the data to inform real-time decision making.

The creation of powerful space-based 5G networks allows defence agencies to distribute data securely across operational areas – linking force headquarters to the edge via satellite. Tools and services incorporated into Microsoft Azure Stack Edge portfolio can analyse that data, then use today's interoperability standards to knit together the space-based assets of allies.

By unlocking the power of SATCOM, 5G and cloud computing, defence organisations can remain connected in remote locations, share data quickly and securely to enhance strategic awareness and perform deep analysis of data to improve decision making.

Remain connected in remote locations

In a proof of concept in 2022, Microsoft, SES (an Azure Orbital ground station–as-a-service partner) and Nokia successfully delivered secure access to the Azure cloud platform over private 5G and satellite communication (SATCOM) networks.

Military vehicle data was streamed over private 5G network, viewed and analysed in the field, then delivered in real-time to an enterprise maintenance system in Azure.[6]

Azure Orbital is a fully managed cloud-based service that allows military forces and government to streamline operations by ingesting space data directly into Azure. It leverages Microsoft's global infrastructure and low-latency global network along with an expansive partner ecosystem of ground station networks, cloud modems and telemetry, tracking and control (TT&C) functions.

Azure Orbital off-loads the responsibility for deployment and maintenance of ground stations, enabling the use of cloud services anytime and anywhere, including remote and austere environments, to enable federation of networks and edge.

[6] Microsoft, SES and Nokia demonstrate satellite and 5G integration for Australian Defence remote access to Azure cloud services, Microsoft, 5 April 2022

Facilitate effective collaboration with the defence industrial base

Partnering with a strong defence industrial base (DIB) helps the allied defence community keep armed forces at peak readiness, as well as being critical to achieving supply chain security.

To ensure competitive advantage in a rapidly evolving security environment, allied militaries must adopt a system and portfolio-based framework. This framework should align strategic decision-making on future capabilities to the mission areas required for integrated deterrence. And, while kinetic effects remain important, technical superiority has emerged as a key lever in maintaining this advantage, especially when it comes to piloting new acquisition pathways, modernising concepts of operations and driving transformation goals..

Transforming military capabilities through concept, design, procure, build, maintain and dispose can all happen in partnership with the DIB. However, this kind of effective technology adoption requires a policy adjustment to procurement.

Most defence acquisition processes have been around for decades. They were well-suited to building large, complex, platforms and systems with well-defined requirements and waterfall development and deployment methods. But as defence organisations are now more frequently addressing mission capabilities that are increasingly software centric, and are looking to buy those in accelerated timescales, legacy procurement methods are no longer fit for purpose.

Digital engineering for mission success

Digital engineering is an integrated digital approach using authoritative sources of systems data and models as a continuum throughout the development and life of a system – from concept through disposal.

This approach modernises traditional systems-engineering practices to take advantage of commoditised technology, modelling and simulation, modern development approaches and AI to enable innovation at speed.

In parallel, the defence capability lifecycle as it is today sees information and capabilities being siloed. We need to break down these boundaries and provide a common platform on which all stakeholders can collaborate collectively. The mission capability lifecycle must be driven by culture and policy, rather than the technology itself.

Capitalising on a modern mission capability lifecycle

Modernising the capability lifecycle has the potential to unlock innovation at speed for defence forces. By being iterative, defence can capitalise on greater agility in requirements, development and deployment of new mission capability.

The feedback loop is central to the entire lifecycle – customer feedback and external validation are constantly being fed back into the design, as it advances through its development.

It's possible to leverage an accredited, cloud-enabled platform to provide secure, interconnected infrastructure, a collaborative environment, a deployment sandbox and development tools to enable this reality.

Figure C. Modernising the defence capability lifecycle

Current state	Desired state
Highly stove-piped; information and capability silos	Common dev environment and collaboration platform
Waterfall methods – slow, rigid, manual, disconnected	Digital DevSecOps – fast, agile, automated, connected
Limited collaboration	Open and modular architectures
Risk averse	Healthy risk postures and fail-forward cultures
Security bolted on at end	Security baked in from start
Evolutionary innovation	Balanced innovation – evolutionary and revolutionary
Proprietary systems and capabilities	Leverage open source and commoditised tech

Image courtesy of Rolls-Royce

How this plays out in the field

Partnerships between defence forces and the DIB can address capability lifecycle challenges and import commercial capability into the defence environment.

Modernising your development methods can be fast-tracked by working side-by-side with commercial experts who have done similar work many times over. They can help navigate the common challenges and pitfalls associated with digital transformation and digital engineering adoption.

Microsoft frequently engages in co-engineering initiatives with military and industrial partners. Our Commercial Software Engineering team joins as members of the customer team while building new mission capability using modern development paradigms and methods.

Case study: Rolls-Royce

Microsoft has been working with Rolls-Royce to leverage digital engineering techniques as well as modelling and simulation in an advanced visualisation lab. This allows them to interact with digital models of products that have not even gone to production yet. This 'zero cost prototyping', accelerates what would typically be post-production testing into earlier phases of the design lifecycle.

To win the B-52 Commercial Engine Replacement Program with the US Air Force, Rolls-Royce digitally built the B-52 bomber's wing with the company's F130 engines 'installed'. The model demonstrated that the F130 would perform in a superior fashion, driving down the maintenance burden.[7] This example shows how the US military is exploiting commercial technologies to drive down the sustainability cost of products they rely on.

The digital approach becomes the collaboration tool that unlocks speed while helping Rolls-Royce to drive down their development, maintenance and sustainment costs.

Case study: NATO Software Factory

The NATO Software Factory (NSF) is a centralised platform on which developers can onboard to use services for keeping track of their work items, storing their code in a versioning system, building their software using pipelines and leveraging the flexibility of the Microsoft Azure Cloud for creating dev/test machines.[8]

NSF is a leading example of a modern, collaborative environment for software innovation built on a shared cloud infrastructure serving a security capability. These fundamentals enable teams to work according to industry best practices for development, security and automation (DevSecOps), become more agile and improve the quality of their work.

The NSF enables NATO members, industry, non-traditional vendors and academia to work together in a common environment, with easy transition between environments.

[7] Rolls-Royce Digitally Modeled Wing and Pylon With Engine to Win B-52 Contract, Air & Space Forces Magazine, 7 October 2021

[8] NATO Software Factory

Unlocking effective digital transformation for defence

With technology playing an ever-increasing role in modern conflict, effective digital transformation must be a key priority for defence decision-makers.

Despite the defence sector being synonymous with innovation in some regards (including specialty materials, weapons systems and digital communications), it is behind the curve in effective digital transformation.

This is because traditional acquisition and development techniques lack the agility required to deliver mission-critical technology solutions in the defence and intelligence domain.

Digital transformation of defence and intelligence is not just about technology, it is also about people, process, governance and culture.

How digital transformation is advancing defence and intelligence

Success in the modern battlespace hinges on information dominance – secure connectivity and joint interoperability from headquarters to the tactical edge along with the ability to turn data into insights so forces can make informed decisions at the time of need.

Speed of transformation to deliver innovative mission capability requires our forces, the DIB and the partner ecosystem to be agile.

The Microsoft Defence and Intelligence team can support military and government to achieve this by prioritising a trusted and secure digital backbone; enhancing interoperability with partners, allies and agencies; and maintaining effective collaboration with the DIB through a modern capability lifecycle.

How can militaries trial and adopt technology rapidly?

Microsoft is working to empower defence and the DIB through greater knowledge, predictability and insights. To achieve this, Microsoft Defence Industry Accelerators bring together code, documentation and education aligned to mission use cases.

Accelerators provide practical ways to help you accelerate time to value through such engagements as envisioning sessions and cloud adoption workshops – helping to inform major projects, innovation activities, defence exercises and skills development.

To find out more about Defence Industry Accelerators, contact Carly Macmeikan, Defence Industry Executive, at cmacmeikan@microsoft.com.

Carly Macmeikan

Industry Executive – Microsoft Defence & Intelligence

With a 28-year career in technology, Carly has worked in the defence and intelligence sector for more than a decade. Carly understands the problems agencies face and how technology can be applied to solve those problems, improve missions and transform operations. She is focused on solving national security issues with secure cloud solutions including artificial intelligence, analytics, collaboration and mixed reality. Carly works extensively with Microsoft's local and global Defence and Intelligence units as well as industry partners to empower the people who protect and defend Australia.

E: cmacmeikan@microsoft.com

Lloyd Hewitt

Business Lead – Microsoft Worldwide Public Sector Defence & Intelligence

With nearly 40 years' experience in the Royal Australian Navy, Lloyd Hewitt served as a logistics officer on submarines, surface ships and land operations. Lloyd sub-specialised in IS development, working on a series of technology transformations, culminating in the Defence ERP program. He brings military expertise and passion for technology to the Microsoft Defence & Intelligence team, to help enact positive change in defence.

E: lloydhewitt@microsoft.com