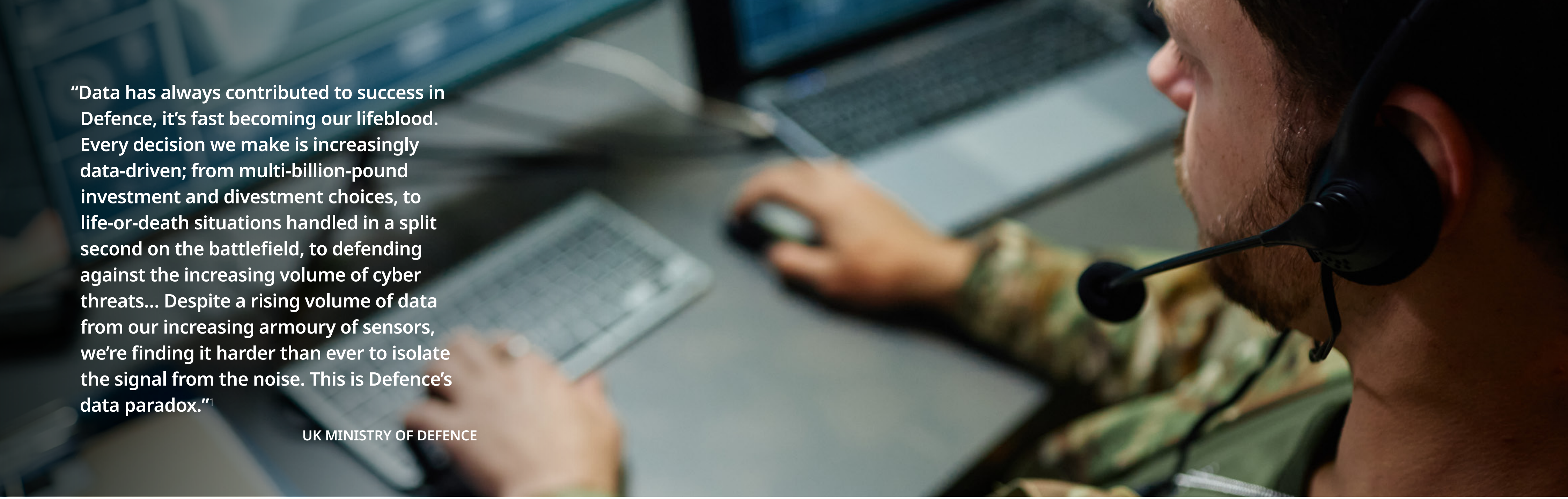
The role of advanced technology in a smart base

White Paper

Alcatel·Lucent Enterprise

Table of contents



> "Data has always contributed to success in Defence, it's fast becoming our lifeblood. Every decision we make is increasingly data-driven; from multi-billion-pound investment and divestment choices, to life-or-death situations handled in a split second on the battlefield, to defending against the increasing volume of cyber threats… Despite a rising volume of data from our increasing armoury of sensors, we're finding it harder than ever to isolate the signal from the noise. This is Defence's data paradox."[1]
>
> UK MINISTRY OF DEFENCE

Introduction

When it comes to advanced technology, the defence sector is well-known for its sophistication. Whether developed in-house or commercially, defence organisations around the world are aggressively adopting and adapting technologies for application in combat and warfare scenarios. And, more and more, what's driving their strategy is the acquisition, distribution, or management of data.

This is due not just to the sheer volume of data – which is seeing double-digit annual growth – but also to the nature of the threat landscape, which is now far more complicated by the need to constantly monitor and address the burgeoning problem of cybercrime and disinformation.

This is where a digital transformation strategy is crucial. By leveraging information and communications technologies (ICTs) to connect everything, everywhere, the sector can more fully exploit the available data and move it more efficiently and securely within their organisations.

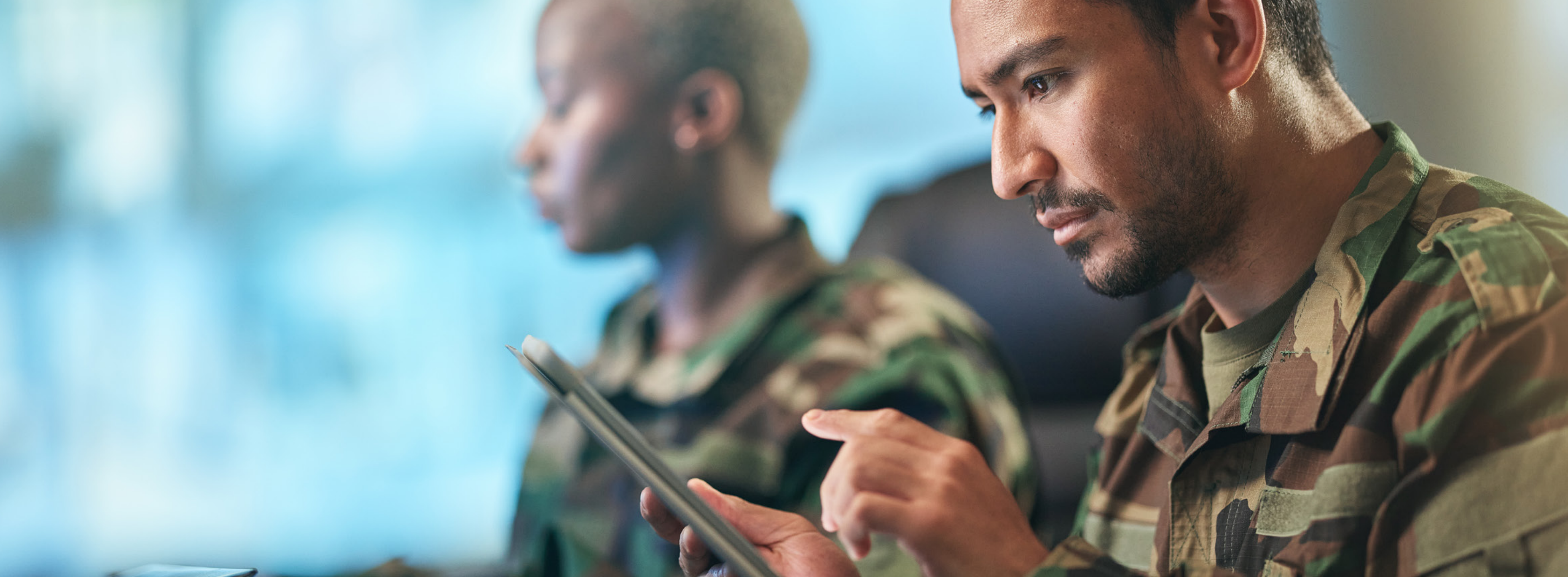
While legacy structures – such as administration, workplaces and offices – may have slowed a transformation in the past, ICT has advanced to the point where many of these concerns are no longer impediments to progress.

With the right digital transformation strategy and ICT technologies, defence organisations can now connect everything, everywhere. This will allow them to create smart bases, from which they can more efficiently meet operational objectives during peacetime and conflict, more effectively address cyberthreats, and more readily attract and retain top talent.

The right data at the right time can have dramatic benefits, optimising processes at HQ and on military bases, supporting more informed decision-making in the field, and augmenting connected personnel and equipment in all zones – across land, air, sea, space and cyberspace.

In this paper, we will discuss the roadblocks defence organisations face in undertaking a digital transformation as well as the drivers to do so. As well, we will cover key learnings from public and private sector organisations who have already transformed and how that can be ported to the defence sector.

[1] - "Data Strategy for Defence: Delivering the Defence Data Framework and Exploiting the Power of Data," UK Ministry of Defence, September 2021.



Roadblocks to change

Internal structure

One of the biggest obstacles to digital transformation in the defence sector is the very nature of defence organisations. Business and technology silos have created a unique operating environment with outdated communications systems – such as PBX-based telephony – that cannot support modern communications and collaboration features.

For the most part, existing systems operate in an independent environment, which is not connected to the internet or any cloud infrastructure.

So, while much of the world began its migration to IP technology 10 to 20 years ago, the defence sector resisted for a variety of reasons:

- **Security:** Regulatory compliance, privacy requirements, and the need to protect sensitive data made it difficult to adopt any technology that could be breached
- **Culture and governance:** A top-down management structure that mandates senior-level approval for major change initiatives meant the military missed out on the influx of millennials and digital natives in the private/public sectors who created bottom-up pressure to adopt digital technologies
- **Budget:** With limited resources, maintaining the readiness of equipment and personnel has been the priority
- **Competition:** Unlike commercial industries, the defence sector lacks direct competitors in the economy and has been primarily focused on ensuring the technological prowess of battlefield assets and connected warfare systems

Drivers for change

Geopolitics and technology

At the same time as these roadblocks have been hampering digital transformation, the world has undergone dramatic change.

The pandemic and geopolitical instability have shown how quickly global supply chains can be disrupted, with significant ripple effects in local economies.

And the pace at which technology evolves has impacted data management requirements.

Advances in machine learning (ML), artificial intelligence (AI), advanced sensors and autonomous systems are the foundation of a more sophisticated and connected generation of weapons. These technologies are all playing a major role in defence efforts on and off the battlefield and ushering in a shift to a more data-centric management process at home and during conflicts.

To optimise processes and maintain a state of readiness, every defence organisation must find efficient and effective ways to collect, store and distribute all the additional data these new systems generate.

Cross-domain cooperation

Exacerbating the situation are more specific changes to the framework in which defence organisations must now operate.

Traditional delineations of air, land and sea operations have given way to a more complex global view. To be effective, those independent silos must now be part of a highly connected strategic framework focused on multi-domain operations and built on the seamless movement of data within and between all domains.

NATO, for example, has added space and cyber to its traditional maritime, land and air operations as a recognition of the data threat and the need to better orchestrate across these domains.

Further complicating this is defence cooperation agreements that Brandon J. Kinne in his article Defense Cooperation Agreements and the Emergence of a Global Security Network said: "...establish long-term institutional frameworks for routine bilateral defence relations, including coordination of defence policies, joint military exercises, working groups and committees, training and educational exchanges, defence-related research and development and procurement."[2]

These agreements are built on new operational models based on information sharing, interconnected dynamic operation, agile and rapid decision-making, real-time coordination and the need for information security and resiliency.

"Within NATO's structure there are five areas of operations: Maritime, Land, Air, Space and Cyberspace. Historically, operations in these domains have either not existed (i.e., Space and Cyber) or have functioned as largely independent entities within national militaries. Many Allied nations' militaries still function in this capacity today; however, given the speed of information, data flows and adversarial capabilities, the necessity of orchestrating military activities across all domains as a single force is crucial for long-term defence and deterrence initiatives within NATO."[3]

[2] - "Defense Cooperation Agreements and the Emergence of a Global Security Network,", Cambridge University Press, 2018.

[3] - "Multi-Domain Operations in NATO – Explained," NATO, October 2023.

Efficient and secure data processes

Ultimately, to enable multi-domain operations and support defence cooperation agreements, all defence organisations need systems that can more efficiently and securely move data. Thus, defence organisations are quickly adopting IP standards and Internet of Military Things (IoMT) technologies and systems to address the need to collect and process more and more contextual data from onboard vessels, vehicles, and unmanned assets and as wearables for augmented soldiers.

But while IoMT technologies can collect data, it is still challenging to efficiently deliver, distribute and process that data. As a result, many defence organisations are now considering how best to optimise processes by converging independent operational technology (OT) and information technology (IT) systems into one consolidated operational framework.

Additionally, the evolution and sophistication of technology has enabled states to wage more efficient cyberwarfare. Therefore, the scope of defence protection efforts must now include digital deterrence capabilities against cyberattacks on critical infrastructure, as well as misinformation, disinformation and malinformation campaigns.

Obviously, this can't be done with outdated and obsolete ICT systems. More importantly, outdated and obsolete systems cannot support multi-domain operations that include the cyber domain. Nor can they support defence cooperation agreements with partner countries who must share information and be assured that information will be protected and secure.

Employee attraction and retention

The defence sector faces the same challenges that commercial enterprises grapple with every day: how to attract and retain top talent. Defence organisations must have ICT tools to train personnel in all areas, create an efficient and rewarding work environment and enable the work-life balance that employees now expect.

> **"...a truly connected Enterprise will deliver integration, nationally and internationally, across all five domains: Maritime, Land, Air, Cyber and Space. This will enable Defence to fully unleash the power of its data, connecting sensors, decision-makers and effectors at scale and speed."**[4]
>
> **UK MINISTRY OF DEFENCE**

[4] - "Data Strategy for Defence: Delivering the Defence Data Framework and Exploiting the Power of Data," UK Ministry of Defence, September 2021.

Public/private sector learnings

While these external factors are all drivers for change, many defence organisations are still slow to adopt digital transformation strategies – even though digital transformation has shown to be an effective way for both public and private enterprises to create efficiencies and improve operations. And since many defence workforces are not combat personnel, the approaches to transformation and the lessons learned apply equally to defence administration buildings and military bases.

ICT technologies have also matured to the point where many of the technological concerns of the past are no longer an issue. Cost-effective, easy-to-deploy digital solutions built on standard protocols that can support digital defence workplaces with efficient communications and collaboration are available. And many provide the high level of cybersecurity defence organisations need.

Strategic digital transformation will equip defence organisations to better address the new reality in which they operate. An effective transformation will create a secure digital environment in which all available data can be moved faster and more securely to support and enable personnel in every domain. And to create that environment, defence organisations can apply proven approaches to digital transformation from the private and public sector.

In this next section, we will explore what has been learned by deploying digital transformation strategies in the public/private sectors and how that may port to defence organisations.

Smart buildings and hyperaware infrastructure

Smart buildings have become part of urban centres around the world and can easily be created at defence administration centres and military bases. These buildings leverage IoT technologies to intelligently monitor and manage everything from lighting and heat to surveillance systems at key access and exit points.

The continuing evolution of IoT technologies has made it possible to create hyperaware infrastructures. These digitally connected structures combine operational automation with contextual space management to intelligently adapt how the building operates to meet traffic patterns in key areas and the comfort and security needs of its occupants and environment. The results are smart spaces that make workplaces safer, healthier, and happier, enhance the employee experience, and increase productivity.[5]

Smart city concepts

Since military bases are similar to self-contained cities, smart buildings and hyperaware infrastructures are key ingredients in creating smart bases built on proven smart city concepts.

Smart bases harness the data available on a base and create "a secured intelligent infrastructure, energy-efficient buildings, efficient transportation, cost-effective operations and higher quality of life for the inhabitants."[6]

The network infrastructure that enables a smart base can also be used to create a more effective security posture that not only protects data on the base but the physical security of personnel and facilities as well. This can be achieved with advanced security systems, such as perimeter surveillance and intrusion detection systems created with IoT and AI solutions connected to security centres.

Creating smart bases goes beyond installing the newest sensors and systems. It's about integrating all existing and new technologies and processes into a coherent ICT network framework built on the most advanced technologies and deployed through strategic digital transformation.

And that transformation can also be applied to other areas, such as:

- Field operations, where ICT technologies are used as the backbone of the information networks on military vessels and vehicles, and as the link for a connected warfighter that leverages sophisticated wearable sensors and equipment
- Command and control centres, where ICT technologies make it easier to support civil defence operations or conduct crisis management efforts with other government agencies during natural disasters

The power of advanced ICT

With the most advanced ICT technologies in place, defence organisations will be better equipped to share information, coordinate strategies and manage joint operations everywhere.

The key to an effective digital transformation is a purpose-built strategic communications and network framework that is optimised for the smart base.

That network must be secure, robust and engineered to support all connections at all times to more efficiently move huge volumes of data. And it must be built with ICT solutions that support the integration and interconnection of administrative operations, military bases, deployed personnel and assets on land, air, sea and space, and the containment of escalating and pernicious threats being generated in cyberspace.

5 - "Smart Buildings Get Hyperaware," John Hatcher, Smart Buildings Magazine, August 2020.
6 - "Building the Smart Base of the Future," Laura A. Nolan, National Strategic Research Institute, March 2020.

ALE: A partner for digital transformation

Alcatel-Lucent Enterprise understands the challenges defence organisations face as they plan and develop digital transformation strategies that leverage ICT technologies to meet the demands of today's military.

At ALE, we support digital transformation with resilient and secure solutions for connected defence, including:

- IoT-enabled LAN and WLAN solutions, including ruggedised switches, which address network requirements and provide secure and automated IoT onboarding for a variety of connected defence requirements
- Communications, collaboration and CPaaS solutions that can be delivered on premises (private cloud), cloud-based (public cloud) or in a hybrid mode
- Workflow and process automation solutions that monitor and proactively detect and address issues before they cause problems, thereby increasing operational efficiency and reducing costs
- Security with privacy by design built on a zero trust framework and with all relevant data privacy certifications in the countries in which we operate

ALE communications and networking solutions can be optimised to create redundant architectures that connect everyone and everything in a cohesive, fully integrated and highly available framework.

In addition, our solutions are designed with the highest security in mind. We strictly adhere to current security practices and standards, and build a range of related technologies into our products at no additional cost. Security is built on a layered approach that includes network integrity, device security and access policies based on user profiles and application visibility. Network software is verified by third-party validation of the underlying code. IoT systems and users are automatically and securely onboarded and placed in containers, which are structured to keep potential cyberattacks from a compromised device. And all data and communications are encrypted with strong encryption mechanisms to avoid eavesdropping and man-in-the-middle attacks.

For added peace of mind, our solutions also comply with the most stringent security certificates issued by independent organisations and government institutions.

And our Risk, Resilience and Security (RRS) framework addresses cyber and physical security for the government and defence sectors.

We also understand the importance of data sovereignty. Our cloud-based applications offer flexible hosting options – in advanced and highly secure data centres built to provide fast and reliable performance, or on premises with our Rainbow Edge private cloud solution. The data stored in the cloud is owned by our customers and we do not provide or sell data to any other company or country.

Learn more

To learn more about Alcatel-Lucent Enterprise solutions for the defence industry, visit our website or contact us to discuss how we can help you develop a digital transformation strategy customised for your defence organisation.

Alcatel·Lucent
Enterprise