
Information
advantage:
turning data into a physical effect
QINETIQ

Foreword

Over the past decade, the annual volume of data created and replicated worldwide has increased by over 3000 per cent. The figure has risen from two zettabytes in 2010 to 64 in 2020, according to research by the International Data Corporation (IDC)[1].

We tend to think of data and information as being positive forces, both in pursuit of our own objectives and the general advancement of society. Having more data available to us gives us the opportunity to become better informed, which in turn enables better decision-making and more effective problem-solving. And yet, the data explosion of the last ten years does not appear to have been accompanied by a proportional improvement in global stability or societal wellbeing. Far from fostering greater consensus, the ubiquity of information is perceived to have contributed to rises in ideological extremism, political partisanship, and pervasive conspiracy theories. More information is not a guarantee of better outcomes.

[1] IDC data creation and replication growth statistics

Meanwhile, governments and militaries are eyeing the data revolution as an opportunity to gain advantage over adversaries – but it would be dangerously naïve to assume that greater data availability equals greater advantage. As we have seen at a societal level, advantage is not an intrinsic feature of the information itself. Like any tool, its value comes from the way in which it is used.

Turning information into advantage is something defence and security forces have always done very well – but now that experience must be scaled up exponentially, at a pace dictated by the rate of global data growth. The challenges this presents can be categorised broadly into the following:

1. **Accelerating innovation and technological progress to keep pace with data growth**

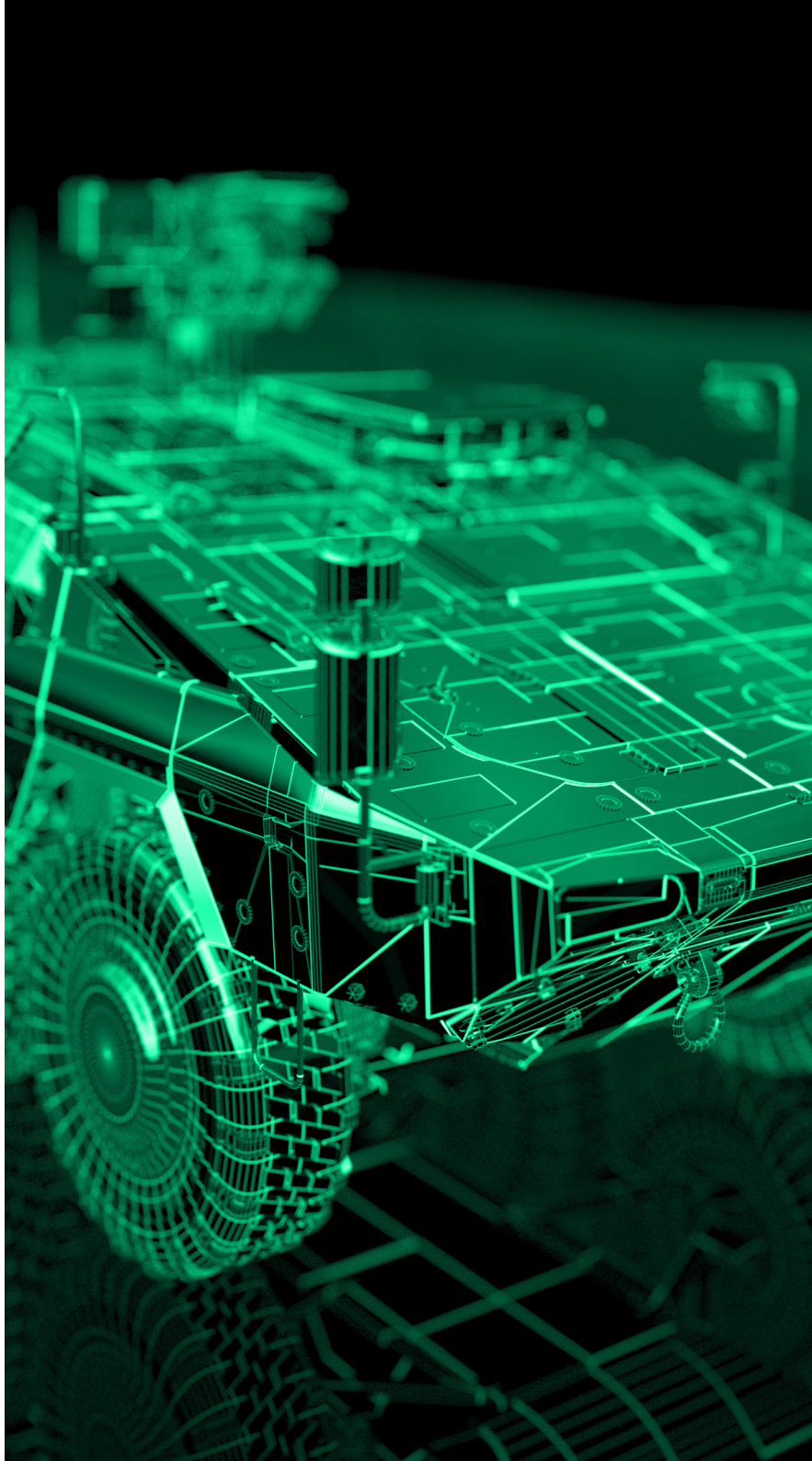
2. **Bridging the gap between information and real-world effect**

In this report, we will explore these challenges in detail and make practical recommendations on overcoming them.

The recent surge in global data is almost certainly just beginning. According to Dave Reinsel, senior vice president of the IDC's Global DataSphere project:

> *The amount of digital data created over the next five years will be greater than twice the amount of data created since the advent of digital storage.*

As governments and militaries seek to leverage this information revolution in pursuit of national defence and security objectives, critical decisions must be made today about how data will be harnessed and applied tomorrow. These choices will dictate whether a nation achieves meaningful advantage by riding the information wave – or simply drowns in data.



Defining information advantage

Senior military leaders have acknowledged that 'Information Advantage' is a young and loosely-defined concept. Attempts to produce pithy definitions have included the following:

> *The credible advantage gained through the continuous, adaptive, decisive and resilient employment of information and information systems.*
>
> **UK Ministry of Defence** [2]

> *…a favourable information situation relative to a group, organisation or adversary.*
>
> **Australian Department of Defence** [3]

While succinct – and technically accurate in a purely semantic sense – neither of these is especially informative when it comes to the nature of information, or that of advantage.

In the US, key military figures have similarly been wrestling with the concept as they move toward incorporating it into official doctrine. Commanding General of the United States Army Cyber Command, Lt. Gen. Stephen Fogarty, has described information advantage as the route to 'decision dominance':

> *Decision dominance is a desired state in which a commander can sense, understand, decide and act faster and more effectively than an adversary.*
>
> **Lt. Gen. Stephen Fogarty** [4]

Defining information advantage as the route to a destination, rather than the destination itself, is the key to understanding the concept.

Dominance is an idealised end state, which may or may not be attainable in practice. During the continual pursuit of dominance, advantage can be gained, held, lost, and regained. As noted in the UK Ministry of Defence definition above, efforts to maintain advantage must be continuous, and forces must be adaptive and resilient in their application of tactics.

In the constantly shifting information battlespace, we cannot talk decisively about victory or defeat – only the attainment or loss of advantage over time. Maintaining advantage is about mastering data and information to set favourable conditions under which to achieve objectives – as expressed in the Australian Department of Defence definition. This mastery is dependent on knowledge of what is required at a specific time – coupled with the understanding that the requirement could change at a moment's notice.

[2] Joint Concept Note 2/18 [3] Operation Series Information Activities Edition 3 [4] C4ISRNET: Out: 'information warfare.' In: 'information advantage'

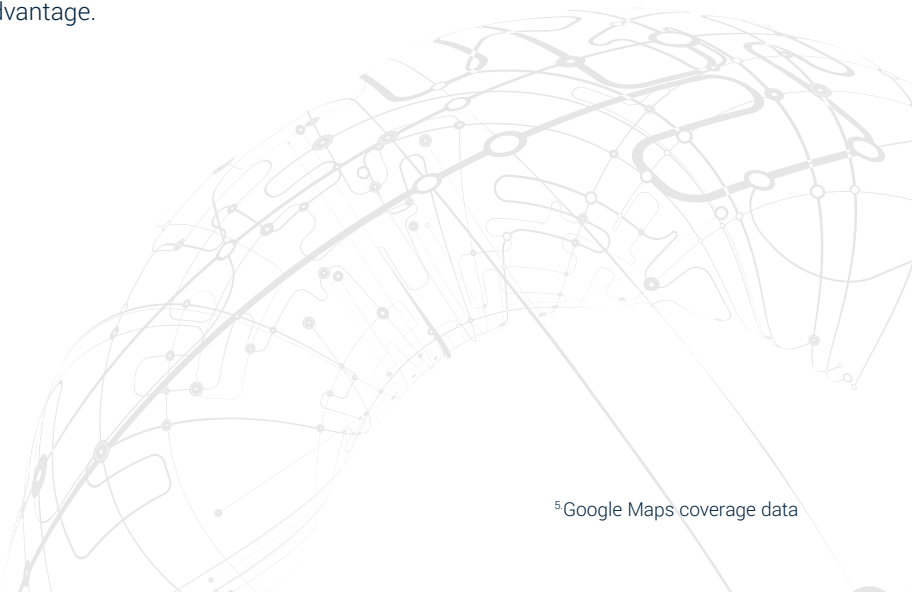
Mastering information

Of course, information has always been a key component of warfare – from Sun Tzu's ancient China, to the 20th century's World Wars, to the Cold War, and beyond. What makes today's conflict different is the sheer volume of data, along with the sustained pace of its growth. Virtually every citizen now has access to open-source information that would once have been available only to governments and their intelligence agencies.

For example, Google Maps provides high-definition satellite images covering 36 million square miles of Earth's surface – and over 98% of the population[5] – to anyone with an internet connection. Companies like BlackSky, Maxar, Planet, and Preligens are taking this capability to the next level, offering real-time, high-fidelity satellite imagery as a service to subscribers. Some of these services are augmented with artificial intelligence (AI) and machine learning to enable targeted monitoring of specific regions and alert the user to activity and change. Consequently, adversaries of all shapes and sizes can be better informed and better prepared than ever. Meanwhile, nations' own intelligence-gathering efforts may be hampered by 'digital noise' – overwhelming volumes of useless or misleading information that must be filtered and separated from genuine actionable intelligence.

To win back the advantage, defence must not only match the capability available to adversaries, but exceed it. This will require disruptive change in the way defence operates. Leaders must lay the foundations for managing ever-increasing volumes of information. This will only be achieved by accelerating the pace at which new technologies and practices can be adopted, so that the capacity to manage data increases in tandem with the rate of data growth.

Once these vital systems are in place, the information must be not only manageable, but effortlessly exploitable in order to reliably produce real-world effects. At the same time, defence will also need to protect the information systems upon which it will increasingly rely, knowing that adversaries will see them as an enticing threat vector. In the following sections of this report, we will examine each of these challenges in turn, identifying ways in which defence can master information to maintain the advantage.



[5] Google Maps coverage data

Accelerating innovation and technological progress

In his keynote address at 2021's Defence and Security Equipment International (DSEI) exhibition, UK Chief of Defence Intelligence Lt Gen Sir Jim Hockenhull identified the exponentially increasing volume of data as a significant defence challenge.

He referred to a number of technologies that – for better or worse – will be transformative in the coming years, including cloud computing, machine learning, artificial intelligence, quantum computing, and virtual reality. However, his assessment of defence's progress so far in adapting to these technologies was somewhat frank:

> *If we compare it with disruption in the private sector, we should recognise perhaps that we talk a good game on artificial intelligence and cloud, but, with some limited exceptions, we've got nowhere near exploiting the potential that they offer. We need to think more imaginatively about how these technologies can help us out-compete our adversaries.*
>
> **Lt Gen Sir Jim Hockenhull** [6]

At the root of this issue is that conventional defence and security approaches have not evolved rapidly enough to put information at their heart. Defence thinking throughout history has typically been product-focused: a vehicle is a product designed for mobility advantage; a weapon is a product designed for firepower advantage; armour is a product designed for protection advantage; and so on. Information advantage is different. While a product like a sensor or computer can provide information, advantage is the result of interactions between these products. Information is less a product and more a service, to which products including vehicles and weapons can 'subscribe' in order to increase their advantage. Information must therefore move from a secondary consideration to the primary one, with all other capabilities integrated into the information ecosystem.

This requires pace and agility that will seem alien within some corners of defence and security. Defence will need to seek inspiration from other sources, including the commercial world, in order to get fully up to speed. Many of today's largest and fastest-growing e-commerce companies owe their success to smart data strategies. The biggest of all – Amazon – employs data on a phenomenal scale: from tailored algorithmic product recommendations based on individual consumers' browsing histories; to complex supply chain management systems that deliver each purchase directly to the buyer's doorstep.

[6] CDI keynote address, DSEI 2021

Follow the leader?

It is easy to see why government defence departments might turn to such e-commerce companies as examples of best practice, seeking to emulate their successes by adopting similar concepts in pursuit of national security objectives. But is this really feasible? There are clearly some parallels. Like Amazon, a military must maintain a complex, mission-critical logistics chain. However, unlike Amazon, a military requires life-or-death decisions to be made in hostile environments while under threat of physical attack. There are areas in which commercial practices fall far short of stringent defence requirements, as well as numerous innovation pockets in which defence is leagues ahead of other sectors. It cannot be said that the commercial world has all the answers, nor that defence has been completely left behind.

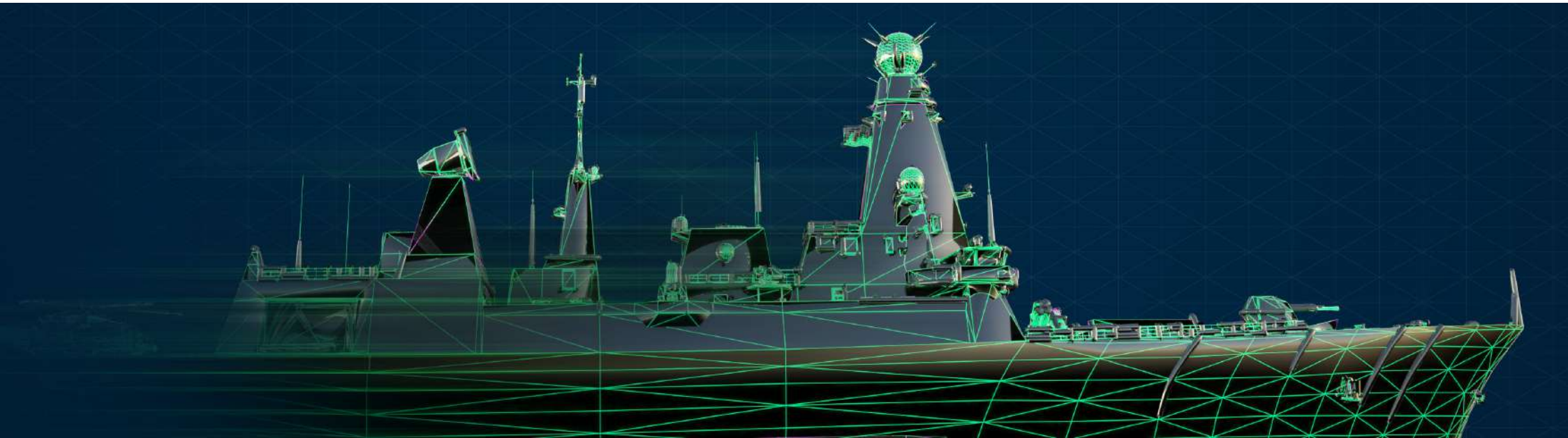
Which commercial practices can be adapted for defence and security purposes? And in which areas must defence pioneer its own bespoke solutions to meet its unique practical and ethical challenges?

Changing the approach: a service integration model

When procuring a complex physical platform, such as a battleship or tank, a government defence department typically appoints a systems integrator to bring together components from different suppliers and ensure they work as a whole. The end user is not provided with multiple, disparate parts that must be pieced together, but a complete and cohesive capability. To gain information advantage, data must be treated in exactly the same way.

It is not enough for the end user to be supplied with fragments of data from multiple sources, which must be manually pieced together. To sustain the pace of decision-making necessary to achieve advantage, the combined data must be presented as a whole, useable information capability. But what does this look like in practice?

We can draw a parallel from the world of commercial information technology (IT), in the form of Service Integration and Management (SIAM). Commonly used to great effect in industries such as financial services and corporate IT, the approach minimises the information burden on the host organisation by outsourcing data and supplier management to a trusted third party. This independent third-party organisation takes on the challenge of coordinating multiple suppliers, sorting the data they provide, and integrating it into a coherent information package. The end user, instead of wrestling with the data, receives only the output – accelerating decision making and allowing them to allocate more time to their own areas of expertise.



Applying SIAM in defence

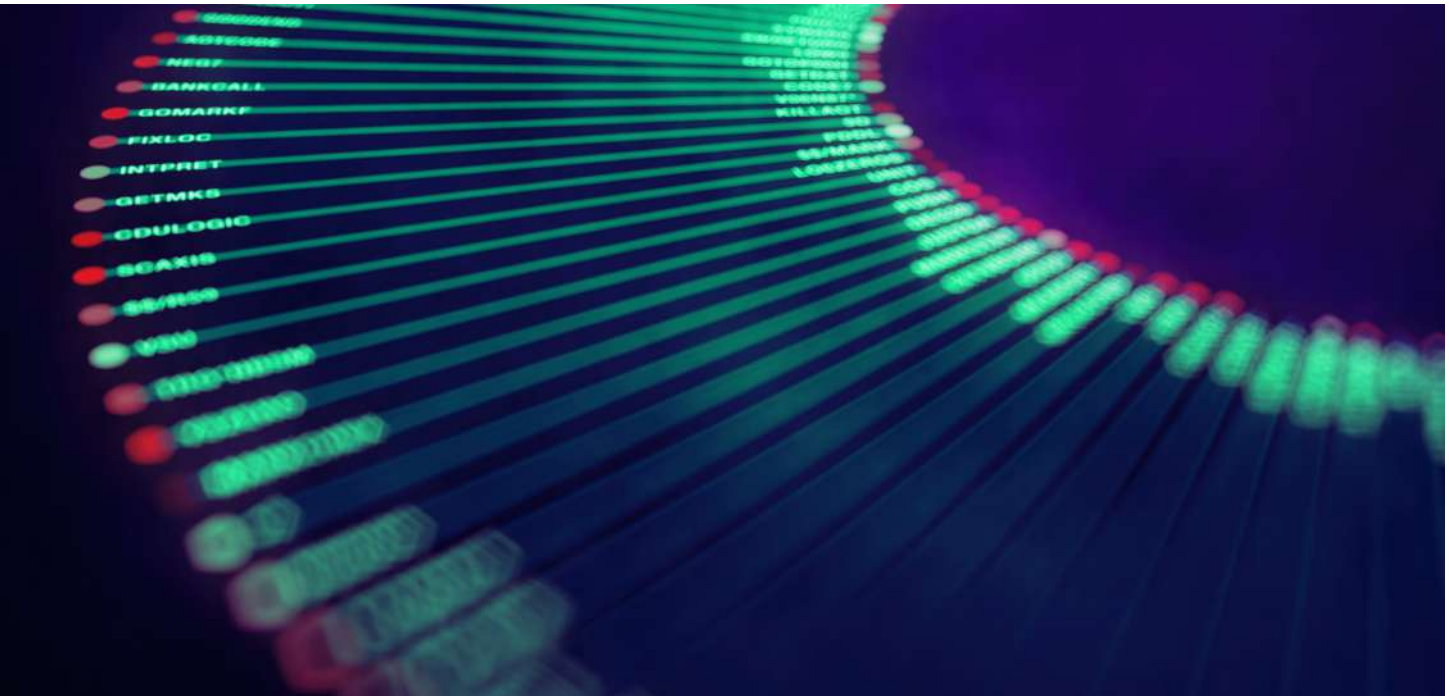
In defence, we want critical decision makers and war fighters to be focused on applying their operational strengths, not on sorting and interpreting data. But data and sources continue to multiply exponentially – whether battlefield sensors, open source intelligence, human information, or satellite relay. At the same time, adversaries will develop new ways to spoof data to deceive decision makers, or block sources to cause information blackouts. We see these techniques today in 'fake news', radio frequency jamming, and GPS spoofing. The cognitive burden on decision makers will continue to grow, making them less decisive and less effective. Advantage will quickly dissolve away.

The gargantuan task of sorting relevance from irrelevance, and intelligence from deception, must not be left to operational decision makers.

To maintain the pace of decision making required to gain information advantage, the end user must receive actionable data – that which is reliable and useful. This requires integration at two levels:

Level one: technology integration

At the procurement stage, buyers must decide which technologies will collect information and supply it to the end user. Technologies such as platforms, sensors, and communications nodes must be interoperable so they can work together as a whole capability, greater than the sum of its parts. Defence has made good progress here, perhaps best demonstrated in the C4ISTAR realm, where multiple systems have been successfully networked via a single command and control console to provide an integrated situational awareness capability. However, this might be described as a 'closed system', designed to generate situational awareness for specified scenarios, using prescribed technologies within limited parameters.



Information advantage beyond the battlefield requires exploitation of myriad sources. At this level it is not enough to procure a bespoke intelligence-gathering capability that operates within a closed system. Information advantage rests on the ability to access data from open source and third parties, continually assess its relevance, identify key information, and incorporate it into the overarching intelligence picture.

Level two: service integration

The model of intelligence gathering described above presents a daunting challenge. Unlike a closed system, in which an operator receives data from a capped number of sources, an open system consists of data from virtually every conceivable source. Navigating this boundless information landscape – by seeking, reviewing and prioritising the information, understanding how it is transmitted throughout the battlespace and protecting/assuring it – places an insurmountable burden on both the procurement team and the end user. This is where defence can emulate the service integration model practiced by commercial entities, by appointing a customer-focussed body capable of funnelling raw information from a wide range of sources into actionable intelligence, and presenting it to the right people at the right times. The body draws from multiple service and product providers, linking disparate closed information systems to form an open system. That system can encompass everything from application integration to collaboration with bearer networks, cyber and electromagnetic (CEMA) resilience and overall assurance.

However, adopting the service integration model within defence is not without its challenges. Due to the risks to human life, national security, and both intellectual and physical property, defence must uphold higher standards of safety, security and accuracy than a typical commercial business. The following challenges must be considered:

Information relevance

Any organisation given responsibility for information architectures on behalf of defence decision makers must have a deep knowledge of the domain and the specific needs of the customer, to ensure only advantageous information is provided to the end user. User-centric design – another practice used in commercial technology companies – is vital in establishing the necessary understanding and trust. It provides a means of gaining continual feedback from the end user so that practices can be incrementally adapted and improved.

Validating information

The service integrator must be able to demonstrate how and why decisions about technology selection and data management were made. This is a critical element of building the user's trust in the system. Whether information is human or AI-curated, an audit trail of the decision-making process must be available for the user to interrogate. Inadequate transparency damages user trust and limits opportunity for incremental improvement. This is especially relevant when integrating third-party sources, where the origins of the data may not be immediately clear.

Information assurance and data protection

Data integrity is paramount in defence. The service integrator must itself be security-cleared at the appropriate level – but must also thoroughly understand data classification, plus the security clearances of end users and all other relevant parties. This ensures data is not delivered to recipients who lack sufficient clearance. Likewise, the integrator must have the strongest cyber security available. This is to protect sensitive information from espionage and leaks – but also to guard against the introduction of deception and disinformation into the intelligence picture.

The SIAM model is tried and tested within commercial organisations, and with the right expertise can be adjusted to provide information advantage in a defence context. However, the challenge does not end there. Once equipped with information, the war fighter must apply it to generate physical effects and meet other objectives in the physical world. The transition from information advantage to physical advantage presents challenges of its own – which we will examine in the following section.

SIAM: The external perspective

Large companies used to outsource all their information technology service requirements to a small number of software suppliers – usually big firms such as IBM or EDS – who would then ensure the successful delivery of those services. But digital transformation has made that much harder to do. Large organisations now rely on an enormous number of software applications to gain a competitive advantage, far more than they did even five years ago – more than 100 in a typical large organisation. Those applications may be niche/standalone or wrapped into a larger platform such as SAP. Either way – they all need to be supported by specialists who have deep knowledge of the technology.

As a result, large organisations have seen an explosion in the number of relationships with external parties they need to establish and manage. And it is not a linear process – those relationships are not just between the application specialists and the customer. They also need to be between the application specialists themselves as changes to one application may impact others. So a much more complex web of relationships is now required to achieve a successful outcome from information and technology, within which the enterprise needs to constantly pass support requests to specialist service providers to maintain both service provision and quality for employees.

Getting this right means organising differently and that is where Service Integration and Management (SIAM) comes in to play. This approach involves a third party sitting centrally within that web of relationships. Their role is purely to manage the flow of support requests and to drive interactions between suppliers to reduce complexity for customers, and ensure they gain maximum advantage from information and technology services. For example, Perfetti Van Melle (the confectionary manufacturers famous for Chupa Chups lollies) introduced SIAM to connect their use of SAP with customers and suppliers. It has simplified the process of liaising between all three parties and reduced the time taken to resolve issues and respond to enquiries.

SIAM is well established in many sectors including retail, manufacturing, and IT. But it is very new in Defence and in many countries, still to be considered. This will change because SIAM is critical for taking advantage of the digital transformation that is taking place in defence and security to become faster and smarter than opponents.

This requires defence organisations to employ many more experts in information systems and services. But defence is a typically risk-averse environment, and the pay is significantly lower than equivalent roles in the technology industry (where innovation is best practice), making it unattractive to the right candidates. Outsourcing to specialists is therefore inevitable and needs to focus on accessing, fusing, processing and extracting value from raw data to deliver an advantage.

This also has the potential to add complexity. The sheer volume of data and the variety of services/technologies providing it could overwhelm operators. Multiple feeds from multiple sources need multiple specialist contractors. Working in a way that allows for efficient engagement with those contractors and between them is therefore critical and should be a trigger to organise differently, especially in a sector well known for having a stifling hierarchy.

Cor Winkler Prins - Cor is the CEO and co-founder of 4me, the first service management solution that enables collaboration between enterprises and their external providers.

Bridging the gap between information and effect

Possessing information is not enough. Advantage comes from exploiting that information to produce effects – and, ultimately, a physical advantage in the real world. Defence will always require a presence in the physical domain. Information can tell you there are enemy tanks crossing an international border, but it cannot defeat them. So, how can defence transform data into action, and what challenges exist at the interface between information and physical effect?

Lessons from the commercial world

Just as SIAM provides a commercial template for data integration and management, there are examples from other industries of seamless integration between information and effect that can be similarly adapted for defence. For example, online grocery solutions and logistics business Ocado Group claims to have "the world's most advanced end-to-end eCommerce, fulfilment and logistics platform." Data is a golden thread, which runs from forecasting product demand to route planning for its delivery drivers. Aided by AI, machine learning, and high degrees of automation, this data is collected, integrated and exploited to ensure 'last mile optimisation.' In layman's terms, that means gathering real-time data on changing road conditions, traffic volumes, and fuel levels, and using it to deliver groceries as efficiently as possible. The data optimises the real-world effect, creating an exploitable information advantage.

War fighters must be equally capable of capitalising on their information advantage. However, insufficient interoperability between systems and a lack of explainable AI processes may prove the greatest barriers to realising this goal. A business like Ocado has the luxury of proprietary technologies, integrated end-to-end throughout the logistics chain. The whole system is interoperable by design. A defence capability, on the other hand, is typically pieced together using technologies from myriad suppliers. If information cannot move freely between the platforms, technologies, and users that constitute a defence capability, it will lack the timeliness and availability needed to generate real-world advantage.

Data exploitation in defence

Defence organisations recognise this and are now starting to explore the shift from a platform-centric to an information-centric approach. In a platform-centric system, physical capabilities are developed separately, with information and communication added on as features. In an information-centric system, information is the capability, with platforms used to convert it into effect. Instead of augmenting platform-based capabilities with information, platforms augment the information-based capability – maximising the information's value by translating it into real-world effects.

This information-first approach requires the introduction of what has been termed a 'digital backbone' – an open information architecture that can receive and distribute data between all platforms and capabilities. The user can 'plug in' technologies to augment the information ecosystem, as and when they are needed. Given the vast array of information sources this approach makes available to the user, there must be systems in place to prevent cognitive overload by filtering and prioritising the inbound data. At the centre of this is an AI data fusion engine that can automate elements of data mining, prioritisation, and distribution. By training the AI to 'understand' what data is important, to whom, and when, the engine can significantly ease the administrative burden on the human decision makers. Edge processing is another useful filter – undertaking much of this processing and analysis before sending intelligence to the user. A rudimentary example is a CCTV camera that only records and transmits when a movement sensor is triggered.

Challenges for defence

When it comes to bridging the gap between information and effect, drawing analogies from e-commerce and logistics businesses like Amazon, Ocado and DHL has its limits in defence. They too must protect themselves against hacking, denial of service attacks, and other malicious online activity – but the cost of failure is measured in dollars, not lives lost.

Additionally, these businesses' real-world vehicle fleets and drivers do not typically come under physical attack. That is why there are additional considerations for defence when implementing an information-centric approach to war fighting:

Information assurance

Turning information into physical effect requires the transmission of data, and this creates risk. Every communication emits a signature that adversaries can detect or intercept, eroding the advantage by giving away clues about location or intent. The movement of data must be treated like the transit of any other goods around the battlespace. When a ground convoy is delivering fuel to a forward operating base, optimal routes are identified and secured, physical protection is assigned, and camouflaging measures are taken to mask the visual, thermal and acoustic signatures of the vehicles. Similarly, data transmission must be encrypted to prevent interception and disguised to avoid detection. Yet, perhaps the most effective way to limit opportunities for enemy attacks on vehicle convoys is to minimise fuel use and therefore reduce time spent in transit. Data is no different. It may seem counterintuitive to champion minimising data use in a report about the necessity of information, but there is a vital balance to be struck. Defence must be constantly alert to the tipping point at which the advantage of information becomes outweighed by disadvantage of signal emission. Understanding the minimum data requirement is a significant factor in exploiting information advantage in the real world. A federated organisational design that empowers local decision makers – as opposed to more bureaucratic, hierarchical structures – can reduce the need to move information between units.

The requirement for information assurance does not cease once data arrives. It is likely that artificial intelligence will have a role to play in the subsequent fusion, processing and onward communication of the raw data to warfighters or strategists.

Today, a great deal of that AI is based on algorithms that are hidden from users. It is far harder to assure information that has gone through a process you cannot access than one where you have total transparency.

Preventing data dependency

According to a 2019 study commissioned by mapmaker Ordnance Survey[7], 60% of millennial adults (aged 23 to 38) 'rely' on mobile phone navigation apps when going somewhere new. If their phone was lost, stolen, or broken, or if the battery ran out, many would struggle to find their way around an unfamiliar location. Unless there are mitigating measures in place, there is always a risk that information advantage will turn into information dependency. In defence, that could be hugely problematic. The electromagnetic (EM) spectrum, on which all digital communication relies, is a highly contested domain within the modern battlespace. Communication can be disrupted by physical attacks on infrastructure, or denial-of-service (DoS) attacks by hackers; whilst location data can be jammed or spoofed using readily available off-the-shelf devices. Consequently, the ability to continue operating in EM-denied environments is critical. Resilience and redundancy must be integral parts of training programmes, and information technologies must be adopted in parallel with working practices that support operational continuity in the event of information loss or denial. Returning to the aforementioned millennials – a drained phone may not be a disadvantage for a driver who can read a map.

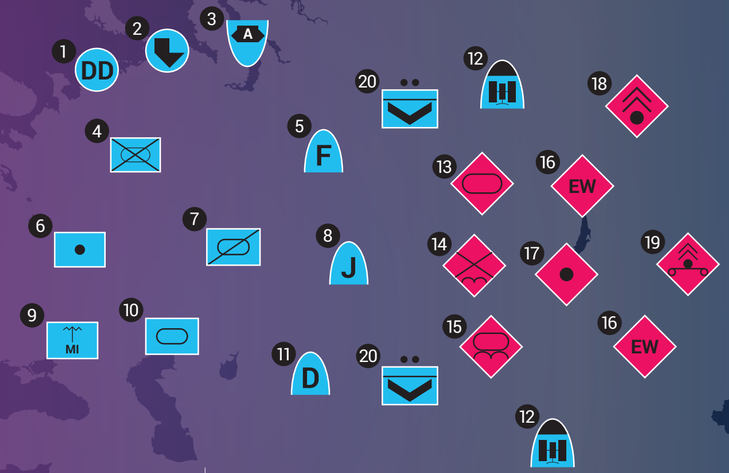
These challenges are certainly pressing, but they are not insurmountable. In the closing section of this report, we set out a series of recommendations to ease defence's transition into an integrated, information-centric way of operating – which is ultimately the key to seizing and maintaining the information advantage.

[7] Ordnance Survey press release

5 focus areas

for improving physical effect in live operations

We recognise that the five areas of Information Advantage we cover in this visual representation can all mean very different things to the domains of air, land, maritime, CEMA, and space. In this visualisation we take a multi-domain integration view of these areas to simplify the narrative and to recognise the aim of closer ties between military domains.



1. Destroyer	**9.** Signals intelligence	
2. Aircraft carrier	**10.** Armour	
3. Attack submarine	**11.** Airborne C2	
4. Armoured infantry	**12.** Space-based ISR	
5. Fighter	**13.** Hostile armour	**17.** Hostile artillery
6. Artillery	**14.** Hostile airborne infantry	**18.** Rocket artillery
7. Armoured reconnaissance	**15.** Hostile light airborne armour	**19.** Self-propelled rocket artillery
8. Electronic attack	**16.** Hostile electronic warfare	**20.** Unmanned Aerial Vehicle

C4ISTAR

C4ISTAR allows forces to sense and see – informing their decisions based on situational awareness and the manoeuvre of information around the battlespace. It covers the collection of raw data and how it moves through networks and data links to bring it all together. The West operates in a military environment based on precision effects. So this information and intelligence provides the basis for how militaries observe, orient, decide, and act.

Data intelligence

The C4ISTAR enterprise generates volumes of raw data that can overwhelm operators and saturate the decision making process with excess information. Data intelligence is about the fusing and processing of raw data so operators can convert it into intelligence that can inform decisions about how to translate that to effect and advantage on the ground. It helps determine what assets and effects are required and where they need to be deployed to achieve the best possible outcome.

Human machine teaming

Data intelligence enables the more effective deployment of assets and is critical for the successful use of Human Machine Teaming (HMT). Humans can't be everywhere. They are a finite commodity. So information-enabled, physical assets are now being placed into the battlespace where humans cannot or do not want to be present. Data intelligence is essential to ensure that the combination of humans and machines works, because achieving a significant force multiplier effect is fuelled by information.

CEMA

A considerable range of military assets in operation, all using data and all working over electronic architectures and infrastructure, present a cyber and electromagnetic (CEMA) threat vector for an adversary. But while CEMA is a potential vulnerability, it can also be one of a military's greatest assets. It allows forces to shape the battlespace so physical assets can survive and execute their functions. And while offensive CEMA cannot remove a conventional physical effect from the environment, it can be used to shape a force's own decisions about that effect – basing those choices on a rich information picture, while simultaneously degrading the enemy's ability to do the same.

Mission Data

For offensive CEMA to have an effect in the real world, it must be powered and coordinated through accurate, trusted mission data. That is why military assets can be loaded with threat data that enables rapid adjustment of defensive posture based upon accurate and timely intelligence. If data intelligence is a wide view of the overall environment to determine an enemy's strategy and course of action, mission data is specifically about orientating a defensive posture such that when in a highly technical fight, that stance is underpinned by accurate data.

Recommendations

Whether or not the term 'information advantage' is uniformly defined and understood, the importance of data and information in today's defence and security landscape is beyond dispute. The world's most influential decision makers already know this. In 2020, the US Department of Defense's Chief Information Officer, Dana Deasy, said:

> *Data is the ammunition in the Digital Modernisation Strategy and is increasingly central to war fighter advantage on and off the battlefield.* [8]

However, there is a significant difference between knowing the importance of information, and actually leveraging it to generate sustained strategic advantage. To achieve that, governments and their defence departments must take the following practical and cultural steps:

1. Build all capability on a foundation of information

Collecting platforms and gadgets will not provide an advantage in the information domain. Information advantage arises from the connections between technologies and their users, meaning information infrastructure must be the primary consideration in building capability. While defence procurement and capability generation have a tendency to be platform-centric, today's most successful e-commerce and logistics businesses show what can be achieved using a data-first approach. This comes with the caveat that there are clearly stark differences between commercial and defence capabilities. Among these differences is that most modern commercial operations have information at their heart from conception, while many defence processes and capabilities in use today predate the digital revolution and therefore require a conscious commitment to transform.

That commitment must be made now so that future capability can be information-led by design, rather than integrated upon commission at higher cost and in slower time. Infusing information into new capabilities must begin at the earliest stages of acquisition and development. This requires developers to adopt an approach commonly practiced in commercial industry, in which the end user's required outcomes remain the guiding principle throughout the entire development and lifecycle. In defence, it means understanding what advantage looks like to the end user and designing the capability accordingly, with subsequent improvements made iteratively based on user feedback.

2. Engender trust

If information is to become central to war fighter advantage, it is vital that the end user trusts the information they are expected to act upon. Building this trust rests on two elements. The first is the actual trustworthiness of the information. Nothing erodes user trust faster than unreliable information, so the information management system responsible for filtering, integrating and prioritising data must uphold the highest possible standards of accuracy, timeliness, and relevance. The second element is ensuring the user perceives the information to be trustworthy. Any potential advantage gained from even the most valuable information will be lost if the recipients doubt it and consequently hesitate to act on it. One of the greatest barriers to trust is insufficient user understanding of the sources of data, and the reasoning behind the filtering and prioritisation process. It must be possible to explain to the end user why a specific piece of information is being presented to them at any given time – but the increasing use of AI in the capture, fusion, processing, and management of data can make this difficult.

[8] DoD press release

AI decision making often takes place in a 'black box' – data goes into the system, a conclusion comes out of the other end, but the process in between is not known to anyone on the outside. In high-stakes environments, like defence and security, this context can be vital to turning information into advantage. As such, AI systems should be explainable by design, offering the end user the opportunity to interrogate the decision making process. Familiarisation with these tools and techniques must take place throughout training and mission rehearsal. If the user is given room to test and second-guess AI decisions in a safe environment, two things will happen: the first is that user feedback can be applied to improve the system; and the second is that trust will be established before it is demanded in an operational setting.

3. Collaborate

The information sphere is colossal and defies boundaries between sovereign nations, defence operating domains, and industrial sectors. To be leveraged for advantage, it must be considered as a whole – and that means defence having to work across those very same boundaries. As US psychologist Abraham Maslow observed:

> *I suppose it is tempting, if the only tool you have is a hammer, to treat everything as if it were a nail.* [9]

One could argue that defence's hammer is battlefield intelligence, surveillance, target acquisition, and reconnaissance (ISTAR). However, in today's information environment, the most valuable data may not be collected solely from military sensing technologies in a physical battlespace, but aggregated from combinations of military, commercial, and public sources.

This brings us back to the need for a service integration model for information in defence – one that can cross the boundaries to bring multiple suppliers and technologies together, integrating their data output into a coherent information picture from which the user can gain genuine advantage.

There is a thread that runs throughout all three of these recommendations – that information advantage is not a destination, but a never-ending race. The information sphere is not one that defence can, or should, seek to control. As it continues to grow exponentially it will give rise to new threats and opportunities. Advantage will be continually gained and lost as circumstances evolve and adversaries adapt. The key to sustaining an information advantage over time is the ability to evolve and adapt faster than the adversary – and that will require new urgency and creativity in defence's ways of working.

[9] The Psychology of Science: A Reconnaissance. By Abraham H. Maslow

Cody Technology Park
Ively Road, Farnborough
Hampshire, GU14 0LX
United Kingdom

+44 (0)1252 392000
ia@qinetiq.com
www.QinetiQ.com

QINETIQ

QINETIQ/21/04548