strategy&

Formerly Booz & Company

Achieving information superiority

Five imperatives for military transformation

Contacts

Abu Dhabi
Abdulkader Lamaa
Principal
+971-4-390-0260
abdulkader.lamaa
@strategyand.pwc.com

Canberra
Mark Jansen
Partner
+61-2-6279-1900
mark.jansen
@strategyand.pwc.com

London
Hugo Trépant
Partner
+44-20-7393-3230
hugo.trepant
@strategyand.pwc.com

Andrew Suddards
Senior Associate
+44-20-7393-3505
andrew.suddards
@strategyand.pwc.com

About the authors

Hugo Trépant is a partner with Strategy& based in London. He focuses on business and technology transformation, transformational change, enterprise architecture, and benefits realization. He leads the defence and security practice in the U.K. and Middle East.

Mark Jansen is a partner with Strategy& based in Canberra. He co-leads the Australia, New Zealand, and Southeast Asia region's defence and national security practice. He is an expert in public-sector strategy and capability planning and program management.

Abdulkader Lamaa is a principal with Strategy& based in Abu Dhabi. He is a member of the digital business and technology practice leadership team. He focuses on innovation and technology-enabled transformations, especially in the public and defence sectors.

Andrew Suddards is a senior associate with Strategy& based in London. He is a specialist in defence and engineered products and services. He focuses on armed forces capability development and acquisition and logistics transformation, including leveraging industry's technical and commercial capabilities.

Chris Ford also contributed to this report.

Executive summary

Military operations have been profoundly affected by the use of technology, particularly information technology. The achievement of "information superiority" is now a critical determinant of mission success. Information superiority is defined as the ability to meet the information requirements of supported forces with superior timeliness, relevance, accuracy, and comprehensiveness than can be achieved by an adversary. Although the benefits of information superiority are clear, the means of achieving information superiority are not. Many militaries resort to buying technology — both software and hardware — without an enterprise strategy and consequently find themselves with multiple systems that do not operate with each other and are redundant in some areas.

A better approach is to adopt a holistic view of information and technology, by considering all aspects of information superiority, doctrine, processes, people, training, and equipment. This approach looks at the entire life cycle of information, and it puts strategy at the forefront.

Specifically, developing an information superiority capability requires following five imperatives:

1. treating information as a strategic asset
2. having centralised governance
3. building an information culture
4. taking the right cyber security posture
5. designing and delivering an integrated ICT infrastructure

The rise of information superiority

The business world has been completely transformed by technology over the past two decades, and military organisations are undergoing a similar revolution. Increasingly, the success of a mission hinges on the ability to make better decisions faster than an adversary, based on more timely and higher-quality information. This is not new to conflict; Sun Tzu noted the vital importance of information more than 2,000 years ago. However, with the advent of digital technology, information superiority has become increasingly critical to successful defence and security.

A key enabler of information superiority is the capability to collect, process, and disseminate an uninterrupted flow of information while denying an adversary the ability to do the same. Despite the relatively recent introduction of digital technology to military operations, IT-enabled information superiority has already made a significant difference on the battlefield.

For example, during the First Gulf War in 1991, over 100 casualties, including multiple fatalities, were reported due to direct friendly ground fire. By the time of the Second Gulf War in 2003, the U.S. had developed a Blue Force Tracking system, which displayed the location of friendly forces, enabling fast, safer ground operations. As a result, fewer casualties, of which only one was a fatality, were reported due to direct friendly ground fire during the first phase of intensive operations.

IT-enabled information superiority has already made a significant difference on the battlefield.

Similarly, U.K. armed forces adopted an information-based approach to deal with the threat of improvised explosive devices during their recent operations in Afghanistan. Commanders compiled information from multiple sources — including unmanned aerial vehicles, which can detect displaced soil; intelligence databases; previous patrol records; and other sources — and fused it with newly identified threats to inform tactical patrols. The associated intelligence allowed tactical commanders to channel troop movements to avoid evolving threats. Hence, patrols were able to manoeuvre with less risk, resulting in a significant reduction in casualties and more effective operational patrols.

On a different scale, the anti-piracy campaign in the Indian Ocean presents a challenging problem because of the large expanse of sea that the multinational coalition forces have to cover. There are insufficient friendly ships to cover the entire area, and a threat can come from just a few pirates in a skiff. To address this large surveillance problem with the limited resources available, commanders are using information superiority resources — such as space-borne and airborne assets, human intelligence and signals intelligence, plus careful data analysis. This allows them to better predict threat behaviours and focus resources on higher-risk areas.

Buying new technology alone does not deliver information superiority

Many military organisations are now taking active steps to achieve information superiority because they understand the operational benefits and the need to maintain interoperability with allies. However, in many cases they are adopting the easy and wrong approach: They are acquiring technology, such as sensors and software, in large volumes and assuming it will all add up to something. Without an integrated strategy, the acquisition of large numbers of disparate technologies usually results in interoperability challenges, redundancy, and overload of stovepiped data. It may also lead to large numbers of employees working across the information life cycle doing activities that could be consolidated or automated.

Instead, organisations need to take a more holistic view of technology, by treating information superiority as a core military capability, similar to a deep strike or battlefield manoeuvre that can give them an edge over a range of threats and scenarios. In this approach, all capability components, such as information superiority doctrine, processes, people, training, and equipment, must be considered and developed as a coherent whole.

Additionally, commanders must consider the total life cycle of military information, meaning all phases of how information is handled. Specifically, this includes the following steps:

- *Collect:* This requires focused and coordinated data collection efforts across all forces and units. Some commanders make the mistake of collecting as much information as possible, thinking that they can sort through it all later, and separate actionable information from noise. Instead, the goal should be to prioritize objectives and identify the information that supports these objectives, as well as which are the appropriate sources, before collection begins.

- *Analyze:* This involves the real-time analysis of aggregated data that leads to relevant information that could affect the way in which deployed units act. As noted above, analysis is so critically linked to the collection phase that commanders must consider the two together.
- *Disseminate:* This involves enabling deployed commanders and units to better achieve their objectives by reliably and securely communicating relevant information to them. A key part of the dissemination phase is a set of unified policies and a culture that assess both the costs and benefits of sharing information.
- *Leverage:* This requires that there are trained decision makers who can successfully exploit trusted, timely, and relevant information that has been disseminated to them.

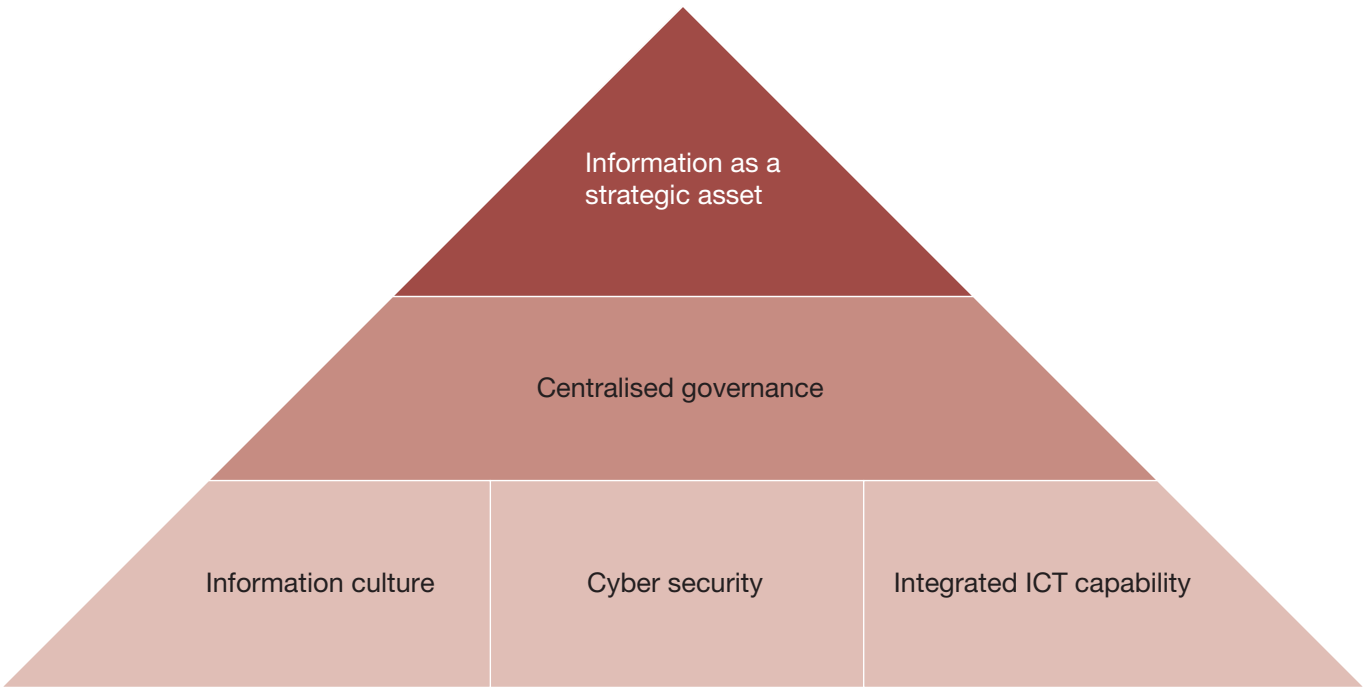
With a more coherent approach, in addition to the operational advantages, comes a very welcome extra benefit: military organisations can also achieve significant financial savings. Experience suggests that the current, uncoordinated approach to information technology wastes as much as 30 to 40 percent of the total procurement spending, and as much as 30 to 40 percent of manpower.[1] This alone is a powerful argument for adopting a more strategic approach.

[1] For example, the UK Defence Information Infrastructure project is reducing more than 500 systems to a single enterprise-wide solution, and more than 20 data centers to just one. In terms of the manpower required to operate the new system, the Ministry of Defence (MoD) is scaling down from eight brigadier generals to one, and from 1,600 MoD employees to just 250. In total, the initiative will reduce spending by £1.6 billion (US$2.7 billion) over the lifetime of the project.

Five imperatives for achieving information superiority

A coherent approach to information superiority starts with an overarching strategy that provides the necessary guidance and framework. This is achieved by following five imperatives (*see Exhibit 1*).

Exhibit 1
Information superiority strategic imperatives



Source: Strategy&

1. *Information must be regarded as a strategic asset.* The starting point is a coherent and unifying information strategy. This information strategy must be directly linked to the highest-level military strategy and must be owned at the strategic level. The strategy should, for example, include the armed forces' vision of information superiority, the supporting roles and responsibilities, the key objectives to be achieved through information superiority, and the road map to achieve them. Thus information superiority should be treated as a primary capability alongside the traditional capabilities such as air defence, maritime control, and ground manoeuvre.

2. *Information must be centrally governed.* The information strategy must be driven by a strategic leader, commonly a chief information officer (CIO), who reports directly to the head of the armed forces. The CIO must have the authority to manage this vital asset, to make capability investment decisions, and to control the technical design authority. This is best achieved through a centralised approach with appropriate authority, organisational structures, policies, standards, procedures, and controls.

3. *Information culture is critical.* Militaries aspiring to achieve information superiority need to shift their cultural paradigm from "need to know" to "need to share." A culture of sharing cannot be achieved solely by specialist IT groups or organisational structures because it is more about mind-set than personnel or positions. Information affects everyone. Therefore, all personnel need to understand the importance of information and their role in developing the desired information capabilities. This can only be achieved by a top-down change program. Such a program should include change management by leaders on why information sharing is important, and the incorporation of information training as a critical element of appropriate course syllabi.

Information superiority should be treated as a primary capability alongside the traditional capabilities such as air defence, maritime control, and ground manoeuvre.

4. *Information and cyber security are vital.* It is not enough to acquire and utilize information; militaries must also protect against attempts by adversaries to attack, access, or exploit critical military information. Just as the advantages of information superiority are considerable, so the threats from cyber security failure can be just as significant. With the advance of technology and the changing nature of warfare, threats can develop at a rapid pace, and information capabilities must be nimble enough to respond. Given this imperative, forces must build on traditional information assurance methodologies to develop a wider cyber security approach that covers the entire military organisation. This must be done coherently with the physical and personnel security strategies.

5. *Integrated and agile ICT capability is an essential foundation.* The information and communications technology (ICT) system that undergirds the strategy should provide the ability to gather and disseminate information securely linking aircraft, ships, land platforms, and headquarters. In some cases, this poses a sizeable challenge, in that organisations cannot start with a blank slate; rather, they operate with legacy systems that must be integrated with newer technology. In addition, the ICT system must be interoperable across joint forces, coalition forces, and government agencies. Given the speed of technological change — and especially the importance of digital applications — the ICT capability also has to be agile and adaptable. Too many organisations spend years building the underlying ICT only to discover that the technology has grown obsolete and is now a limitation in conducting information operations.

Just as the advantages of information superiority are considerable, so the threats from cyber security failure can be just as significant.

Conclusion

The changing nature of warfare and the rapid advances in information technologies have placed an increased emphasis on information superiority to achieve mission success. By starting with an overarching information strategy and centralising governance, armed forces will formulate their requirements in an integrated manner. They will be far more efficient and effective in their procurement spending and manpower utilization. Their systems will be more interoperable — within their own military and with allied forces. Most important, the future delivery of information superiority will be enabled.

Strategy& is a global team of practical strategists committed to helping you seize essential advantage.

We do that by working alongside you to solve your toughest problems and helping you capture your greatest opportunities.

These are complex and high-stakes undertakings — often game-changing transformations. We bring 100 years of strategy consulting experience and the unrivaled industry and functional capabilities of the PwC network to the task. Whether you're charting your corporate strategy, transforming a function or business unit, or building critical capabilities, we'll help you create the value you're looking for with speed, confidence, and impact.

We are a member of the PwC network of firms in 157 countries with more than 184,000 people committed to delivering quality in assurance, tax, and advisory services. Tell us what matters to you and find out more by visiting us at strategyand.pwc.com.

www.strategyand.pwc.com