strategy&

Formerly Booz & Company

Reconsidering military ICT security

A risk-based approach to modernisation and information superiority for GCC armed forces

Strategy& is part of the PwC network

Contacts

Dubai

Haroon Sheikh
Partner
+971-4-436-3000
haroon.sheikh
@strategyand.ae.pwc.com

Chris Ford
Military ICT Expert
+971-4-436-3000
chris.ford
@strategyand.ae.pwc.com

Bassem Fayek
Manager
+971-4-436-3000
bassem.fayek
@strategyand.ae.pwc.com

About the authors

Haroon Sheikh is a partner with Strategy& Middle East, part of the PwC network, based in Dubai. He is the leader of the defence and operations practices in the Middle East. He has specialised experience in building defence support capabilities, focusing on logistics and supply chain strategies for militaries, linking these to national defence industrial strategies and innovative ways of militaries partnering with industry. He has led large military transformations covering logistics, IT, HR, and training components, managing change and communications at senior levels.

Chris Ford has been engaged with Strategy& Middle East as a military ICT expert for the last six years. He was previously a senior officer in the British army. He is an expert on military command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) through life management, logistics and supply chain strategies, policies, and programme implementation.

Bassem Fayek is a manager with Strategy& Middle East, based in Cairo. He has been part of the defence practice in the Middle East for over three years, and has experience working with multiple militaries in the region. He has led defence assignments across IT and logistics, and recently has managed assignments on career transition and morale, welfare, and recreation for military personnel.

Executive summary

Gulf Cooperation Council (GCC)[1] armed forces face an information security conundrum. On the one hand, they need to develop "information superiority" — the ability to meet the information requirements of supported forces with greater timeliness, relevance, accuracy, and comprehensiveness than an adversary. This involves investing in technology (such as networked assets) and processes that provide commanders greater situational awareness, enabling them to make better and faster decisions and disseminate orders with alacrity. On the other hand, the danger that such information could be breached by an adversary encourages the overprotection of information, rather than its sharing and exploitation.

Thus far, most GCC commanders have erred on the side of caution, relying on isolated systems that are not interoperable. Consequently, they are inefficient in peacetime. Worse, during military operations commanders have to function with partial information — possibly ceding information superiority to adversaries.

The best way to resolve the conundrum is through a risk-based approach that allows commanders to acquire and exploit the right information at the right time, while managing the information security based on the likelihood or impact of its loss. This approach involves four steps:

1. Develop the right strategies and translate them into specific policies and processes.
2. Generate buy-in among senior leaders to drive the change in culture and practices throughout the organisation.
3. Put the right organisational elements in place, including a chief information officer (CIO), a design and procurement function, and a systems operating authority, among others.
4. Keep pace with ongoing technological developments.

Initially, militaries can perform pilot tests on support functions such as procurement or maintenance. They can thereby build up their information security capabilities over time, while minimizing the potential damage from compromised data.

The information security conundrum

Modern military operations have been transformed by the use of technology to gather information and give commanders greater situational awareness. As a result, they can make better and faster decisions and disseminate orders more effectively, both in peacetime and during active operations. Even as most governments around the world have reduced overall military spending, they have invested more in technology to give themselves an edge through information superiority. According to ICD Research, global military spending on command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) is estimated at US$18.5 billion in 2017, with the total likely to grow to approximately $22 billion by 2021.[2] Although the GCC countries today represent a small percentage of this (between 2 to 3 percent), their spending is likely to increase exponentially as they seek to catch up with other countries.

We define information superiority 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.[3] The need to access and share accurate and timely information is particularly critical for GCC forces, which often operate as part of coalitions in which militaries operate side by side.

However, networking assets to share information brings a significant risk that information could be vulnerable to security breaches. For many commanders in the GCC, the potential for this kind of breach stops them from investing in, or effectively using, integrated systems. Instead, they have developed workarounds, typically running multiple isolated systems. Although this approach can protect information, it makes militaries far less capable. It is both manpower- and time-

intensive, as the data gathering, analysis, and presentation tends to be manual. Armed forces that function this way struggle to produce the accurate intelligence needed to give commanders greater situational awareness. Collaboration is nearly impossible, and additional systems are required in order to provide common direction to all. These issues are compounded during military operations, where available support personnel are limited and there is a far greater emphasis on timely decision making.

The problem will only grow. Already, military equipment such as engines and aircraft frames are being designed with embedded sensors that can capture and relay information back to headquarters or to forces in the field (*see "The F-35: An aircraft and an information platform"*). That will give an even larger advantage to forces that have the capabilities in place to collect, analyse, and disseminate information of such greater detail and volume. Conversely, militaries that do not have such capabilities in place will fall further behind, ceding information superiority to the adversary. Putting security considerations ahead of information superiority is akin to never driving a car because one fears a traffic accident.

The F-35: An aircraft and an information platform

The F-35 is an aircraft and an information platform. As an aircraft it is the fifth generation of fighters able to conduct aerial combat missions. At the same time, it is a platform for information capabilities that are described as "information rich," according to the Australian government (one of the partners in the F-35 project). To achieve this capability, the F-35 has two features. First, it is tied into the armed forces' information, communications, and technology (ICT) infrastructure. Second, it can interact and interoperate with other platforms, systems, and sensors. Whenever the F-35 flies, it acquires significant amounts of mission-relevant data that needs to be stored, processed, and communicated — which demands considerable connectivity. Another burden on bandwidth is the F-35's Autonomic Logistics Information System (ALIS). To provide the necessary maintenance support to the F-35, ALIS is integrated with military and external contractor systems through multiple ICT networks and systems. ALIS is protected by multiple layers of cybersecurity, and it would be impossible to operate the F-35 without sophisticated and secure ICT networks.

Source: Australian Government, Department of Defence, "Defence ICT Strategic Direction 2016–2020" (http://www.defence.gov.au/CIOG/_Master/docs/Defence-ICT-Strategic-Direction-2016-2020.pdf).

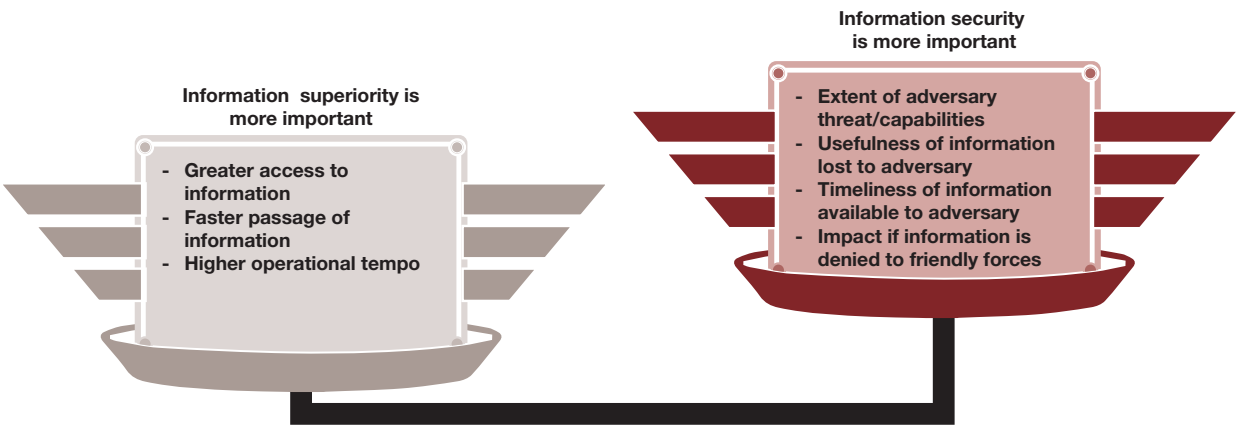
A risk-based approach to information security

To overcome this conundrum, GCC militaries can adopt a risk-based approach to information security. Such an approach involves weighing the importance of better, quicker access to information during high-tempo operations against the risk of that information being accessed or attacked by the adversary or denied to friendly forces (*see Exhibit 1*). Decision makers need to consider how useful the breach in information will be to the adversary and assess its impact on the success of the operation. By applying a risk-based approach, militaries can determine which information should be shared, at which times, and among which participants, along with creating a means to mitigate breaches should they happen.

To implement a risk-based approach, GCC militaries will need to develop four foundational elements.

1. Develop the right strategies and translate them into specific policies and processes. Militaries should start by developing new information security strategies, in line with their broader military strategies. These, in

Exhibit 1
Military factors for assessing balance of risk



Source: Strategy&

turn, need to be translated into specific doctrines, policies, processes, and standard operating procedures — with appropriate documentation — that guide the day-to-day actions of the lowest-level soldier. Forces need to reinforce this through training, inspections, and audits, until information management and administration within the risk-based security approach become the norm.

2. Generate buy-in among senior leaders and throughout the entire culture. In order for the strategic security vision to succeed, armed forces in the region will need to overcome resistance among some senior military leaders, who rose through the ranks in a period in which technology was not as critical. Many of these commanders have not been early adopters of technology, and they view some of the emerging new tools with scepticism. That will need to change if they are to catch up to other organisations — in both the public and private sector — in terms of their use of information technology. Quite simply, GCC armed forces need to embed the concept of risk-based security into the broader military culture, and that process starts at the top. This risk-based approach has become common in most Western militaries as well as in industry.

3. Put the right organisational elements in place. In order to cement the change, militaries will need to develop effective planning, procurement, training, and asset management across the ICT domain. These responsibilities are usually embedded in key organisations, such as a defence CIO who oversees all aspects of information superiority; with three key functions:

- a design and procurement function (which acts as the technical design authority and manages IT assets throughout their life cycle)
- a systems operating authority (often the ICT element of the military)
- a department that monitors and controls which critical information gets shared and how

These entities work under the CIO and closely with the operations teams and training authorities.

4. Keep pace with ongoing technological developments. In parallel with strategic and process considerations, armed forces need to remain at the forefront of security-related technology, to provide resilience and mitigation of potential damage if a cyber-attack is successful. This is particularly important given the rapid development cycles of such technology. The good news is that such technology does not need to be developed from scratch: leading financial institutions, utilities, and even other militaries already have similar tools in place; such as intrusion detection systems, advanced cyber software, and network monitoring systems. Once GCC armed forces have stronger capabilities in place, they can follow the lead of more advanced militaries and create their own internal research, development, and testing function, which can generate proprietary systems and coordinate the integration with allies' technology.

Start with pilot tests on support functions

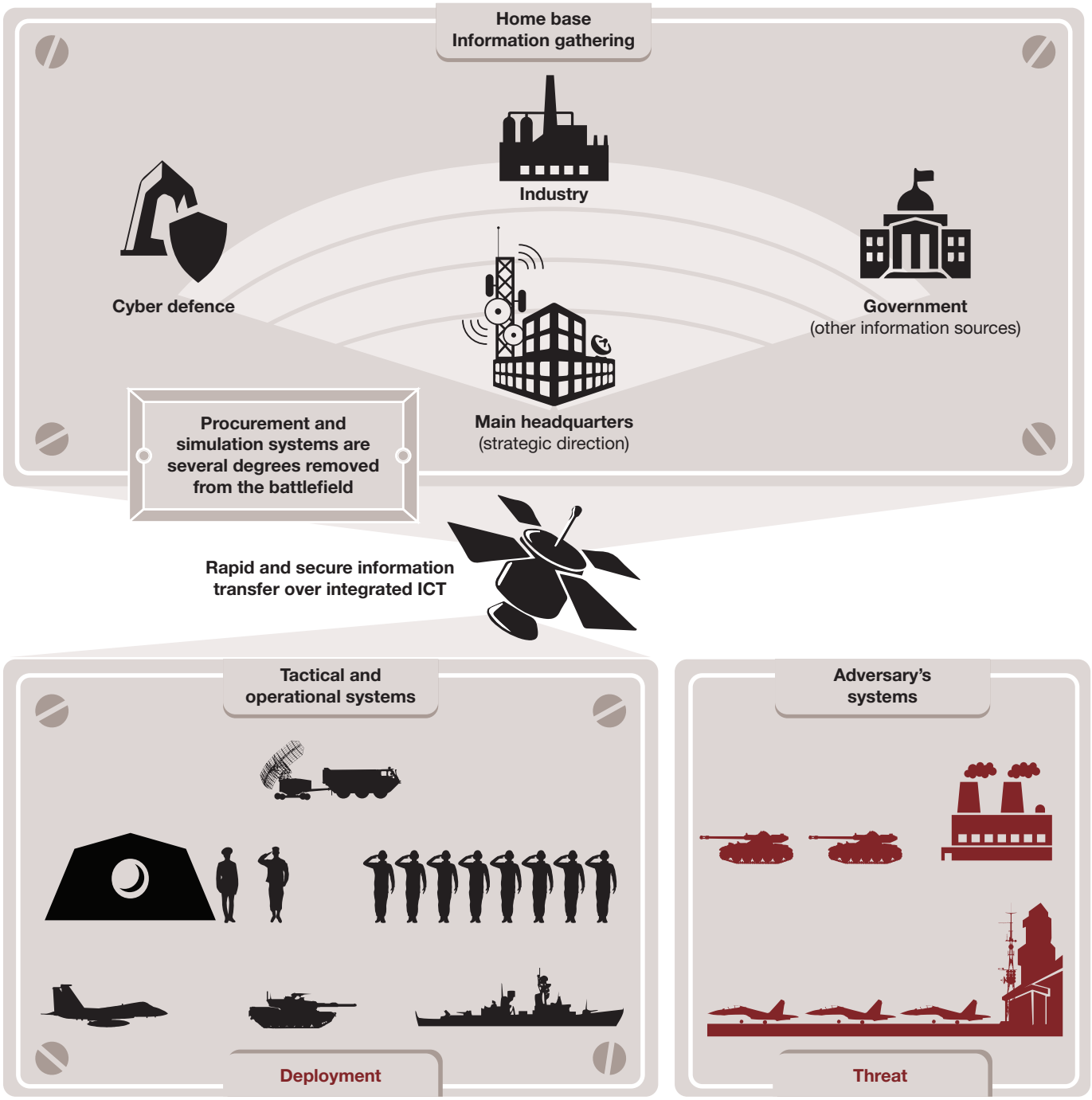
Given the understandable concerns about cybersecurity, militaries can take the first steps toward more integrated systems by applying the technology to support functions such as procurement and simulation systems. Although these are critical in ensuring the ultimate success or failure of a military, they are also several degrees removed from the battlefield, making them a lower-risk place to start (*see Exhibit 2*).

The advantages of doing so are clear. Regarding procurement, militaries can use technology to issue tenders, bundle acquisitions, secure better prices, better predict their needs, and eliminate situations in which they run out of materiel. Regarding maintenance, defence systems and platforms are increasingly being designed with sensors that can relay performance information to the manufacturer, the operator, or any other critical entity. Some platforms can even anticipate parts that are wearing down and automatically order supplies. By using technology in this way, militaries can begin to capture benefits while also building up their information superiority capabilities.

Notably, commanders who are concerned about information security can design systems that have clear processes to reduce the damage if a breach happens — such as a means to quickly shut down compromised networks.

Exhibit 2

Home base systems, several degrees removed from the battlefield, are a good place to pilot-test integrated systems



Source: Strategy&

Conclusion

Thus far, the approach among many GCC militaries regarding information — in which data is something to be protected at all costs, rather than exploited — has been a hindrance. This will worsen as technology advances. Military operations have changed significantly in the past several years, and the coming decade will see even greater changes, as the ability to share, analyse, and distribute information becomes the key determinant of military success. As GCC militaries acquire new, network-enabled platforms and systems, they will be forced to reconsider their approach to ICT security. Forces that begin adjusting to that new reality will build the capabilities to capitalize. Those that do not may pay the cost of that overly cautious approach on the battlefield.

Endnotes

[1] The GCC countries are Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and United Arab Emirates.

[2] ICD Research, “Command, control and intelligence to 2021: the global C2/C4ISR market” (http://www.army-technology.com/features/featuredssi-icd-research-c2c4isr-market/featuredssi-icd-research-c2c4isr-market-1.html).

[3] Hugo Trépant, Mark Jansen, Abdulkader Lamaa, and Andrew Suddards, “Achieving information superiority: Five imperatives for military transformation,” Strategy&, 2014 (https://www.strategyand.pwc.com/media/file/Strategyand_Achieving-information-superiority.pdf).

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 223,000 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/me.

www.strategyand.pwc.com/me