accentureconsulting

MULTI-LEVEL SECURITY

Enabling the future of multi-national military operations

To remain agile, secure and relevant in a fast-moving and increasingly coalition-based world, defense forces must transform how they protect and share data.

THE FUTURE IS DIFFERENT FOR DEFENSE FORCES...

With some honorable – and often famous – exceptions, military operations throughout history have usually involved the land, sea and air forces of one country working in close coordination, sharing information, insight and resources between them. But today this traditional paradigm no longer applies, with collaborative multinational operations involving armed forces from a coalition of multiple willing partners becoming the norm.

This shift is a logical and well-justified response to the ongoing rapid evolution and escalation of threats globally. And it's paying dividends in operations and theatres of action around the world, as like-minded countries work together successfully to achieve common goals and support local populations.

...AND THEY MUST TRANSFORM TO BE READY

However, alongside the benefits, the move to a world of multinational military operations also bring new challenges. Foremost among these is the need to achieve unity of effort and to sustain common situational awareness by sharing information and insight securely and instantaneously across forces from different countries – and with entities including international agencies, non-governmental organizations, local government entities, and more.

Achieving this level of data-sharing among the armed forces of a single nation is challenging enough. But expand the need for a shared situational awareness, underpinned by effective data sharing across the forces of several countries – each with their own language, systems architecture, data standards and security classifications – and the complexities multiply.

SHIFTING FROM VERTICAL TO HORIZONTAL...

We think that the complexities are so great that they can only be overcome through a radical shift in how we manage data and a reorientation of the systems used across today's armed forces. Why? Because today's approach to data sharing is essentially vertical – passing information up and down the command stack of a nation's military capability. In contrast, multinational military operations demand that data is also shared horizontally, across the forces of different nations and partners.

It's a seismic shift – one that demands fundamental change in all aspects of today's defense IT: every system, application layer, data storage layer, identity & access management (I&AM) layer, information exchange layer, and more. It also requires a change of mindset and culture, as a defense workforce that has traditionally been highly protective of information moves from sharing data on a "need to know" basis to a more refined "need to share" attitude. But crucially, one core asset is at the heart of all these changes: data. And the way to navigate the change successfully lies in taking a data-centric view of the entire environment.

...BY APPLYING MULTI-LEVEL SECURITY

Accenture has experienced this challenge first hand. Several years ago we developed Joint Cross Domain eXchange (JCDX)[1] – an intelligence and target tracking system that draws on data from multiple sources, to provide the United States and allied countries with near real-time information on a particular functional area. JCDX was a ground-breaking innovation at the time, and the skills and vision we applied in developing it remain relevant and valuable today. Now we've applied the same innovative drive and data-centric principles to create an overarching approach aligned with the security context.

A key part of this alignment lies in taking a horizontal view of data sharing – which is widely termed "Multi-Level Security". This is becoming increasingly important in military IT. At root, this concept is about securing every data object individually so it can be shared safely and responsively without compromising the security of the related data around it. The data object itself could be a platform design document, command structure chart, positional information about forces on the ground, or anything else held as data. Whatever it is, our solution helps to ensure it can be shared securely and to mutual benefit with coalition partners and others.

1. https://www.accenture.com/t20150527T210651__w__/es-es/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Local/es-es/PDF_3/Accenture-Defense-Joint-Cross-Domain-Exchange.pdf

NOT IF, BUT WHEN: NOW IS THE TIME TO ACT

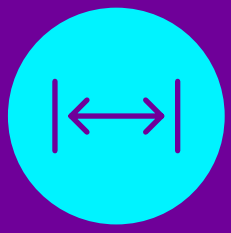
In Accenture's view, defense forces must transform how they protect and share data – or risk operational failure in theatre. And the urgency is growing by the day: put simply, Multi-Level Security is a solution that every military force must start implementing today. Indeed, the need for it extends beyond defense and across government as a whole – with forward-thinking nations around the world already starting to mandate its use in public sector systems.

The changing nature of military operations – combined with the increasing rate and complexity of security threats – makes the urgency of adopting Multi-Level Security in defense agencies all the greater. Given the scale of the required change, if defense agencies don't start implementing and investing in Multi-Level Security today in order for it to be operational in the 2020s, they will become too slow or too insecure in any coalition operations they undertake.

Why? Because if they fail to automate how they handle and share data securely, they will have to do it manually – which will not enable the required pace of operations. Or to avoid being slow, their only other option would be to transfer and share data openly with their coalition partners – which is inherently insecure. Either alternative would expose their operations, their people and their coalition partners to excessive and unnecessary risks, and see them suffer a rapid loss of relevance.

THREE PILLARS OF MULTI-LEVEL SECURITY

The message is clear: implementing Multi-Level Security is vital to help ensure military forces remain relevant, secure and effective in the 2020s – and action to implement it must start now if it's to be operational within that timeframe. To make it happen, there are three key requirements.

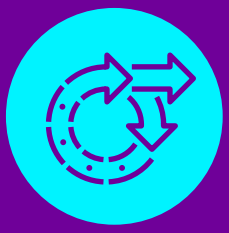


1. THE NEED FOR HORIZONTALITY

Historically, the data collected and used in a defense environment has flowed vertically in both directions, between the top and bottom of the organization. But the growing need to work in close collaboration with other nations' armed forces changes the core information requirement from "need to know" to secure/managed "need to share" – and, as we've highlighted, shifts the polarities of the data flows from vertical to horizontal, while also increasing the already pressing need for speed.

The recalibration of data flows from vertical to horizontal is critical to achieving objectives. In the past, the accuracy, reliability, security and timeliness of vertical data flows were critical to mission success; now, the same applies to horizontal. Only data flows of this type can create the level of situational awareness required across the coalition, if it's to deliver the required speed and quality of decision-making and operational planning. Achieving this demands comprehensive data flows that break down old data "silos" and connect supporting functions to the front line in near real time.

In today's complex global military environment, it's very rare that anyone can or should embark on any mission alone – so data, and data sharing, are key, and it's vital to be able to share the right data in the right way. But identifying the right nuggets of information from the masses of data now available is more difficult that ever amid the "four Vs" of data volume, veracity, velocity, variety. To sum up, it's all about the data – which is why the bedrock of Multi-Level Security is unwavering data-centricity.



2. THE NEED FOR AGILITY

A few years ago, the military led the way in technology globally, even playing an instrumental role in creating the internet. No longer. Today, as NATO acknowledges,[2] it's the commercial sector that's at the cutting-edge – and agencies must now raise their game in technology if they're to stay relevant and effective.

Harnessing the power of the latest technology is made all the more vital by the agile way in which terrorist organizations and non-standard paramilitary forces now share information around the world using channels ranging from mainstream chat apps to the "dark net". This diversity of communications options brings these groups speed and agility, which are increased further by their not having to comply with data protection laws or document what they do.

It follows that instantaneous and horizontal sharing of data across coalition partners is the only way for armed forces to keep pace with emerging threats. And agility isn't just an operational issue: it needs to be a comprehensive attribute that encompasses all aspects of military IT, including software development and implementation.

3. THE NEED FOR A SECURE METHOD

To realize the benefits we've described, armed forces will need the ability to share data both internally and externally with their coalition partners, making it available in near-real time across different physical network layers and data confidentially classification levels. Yet they need to do this on the basis of universally accepted standards and with rock-solid security – or they will become too slow or too insecure for effective operations.

We're already seeing positive moves in this direction, through initiatives including NATO's Federated Mission Networking (FMN) to help enhance interoperability and operational effectiveness, part of the Connected Forces Initiative. As such efforts gain pace and momentum, they will bring major implications for technology applications, data stores and I&AM across the Western military, and expand the "scope of the possible" as improving the efficiency of data transmission becomes an increasing priority across all coalition members.

2. Source: NATO Strategic Foresight Analysis 2017 Report – http://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf

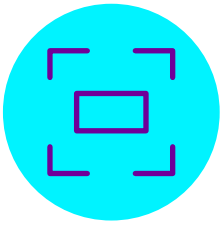
FOUR STEPS TO TAKE TODAY

Moving to data focused Multi-Level Security may appear a daunting undertaking. However, rather than a "big bang" transformation, it's a transition that will take several years. And it's one that armed forces must start now in order to be ready for the challenges of the 2020s.

Here are four steps that military organizations can take today to get under way:

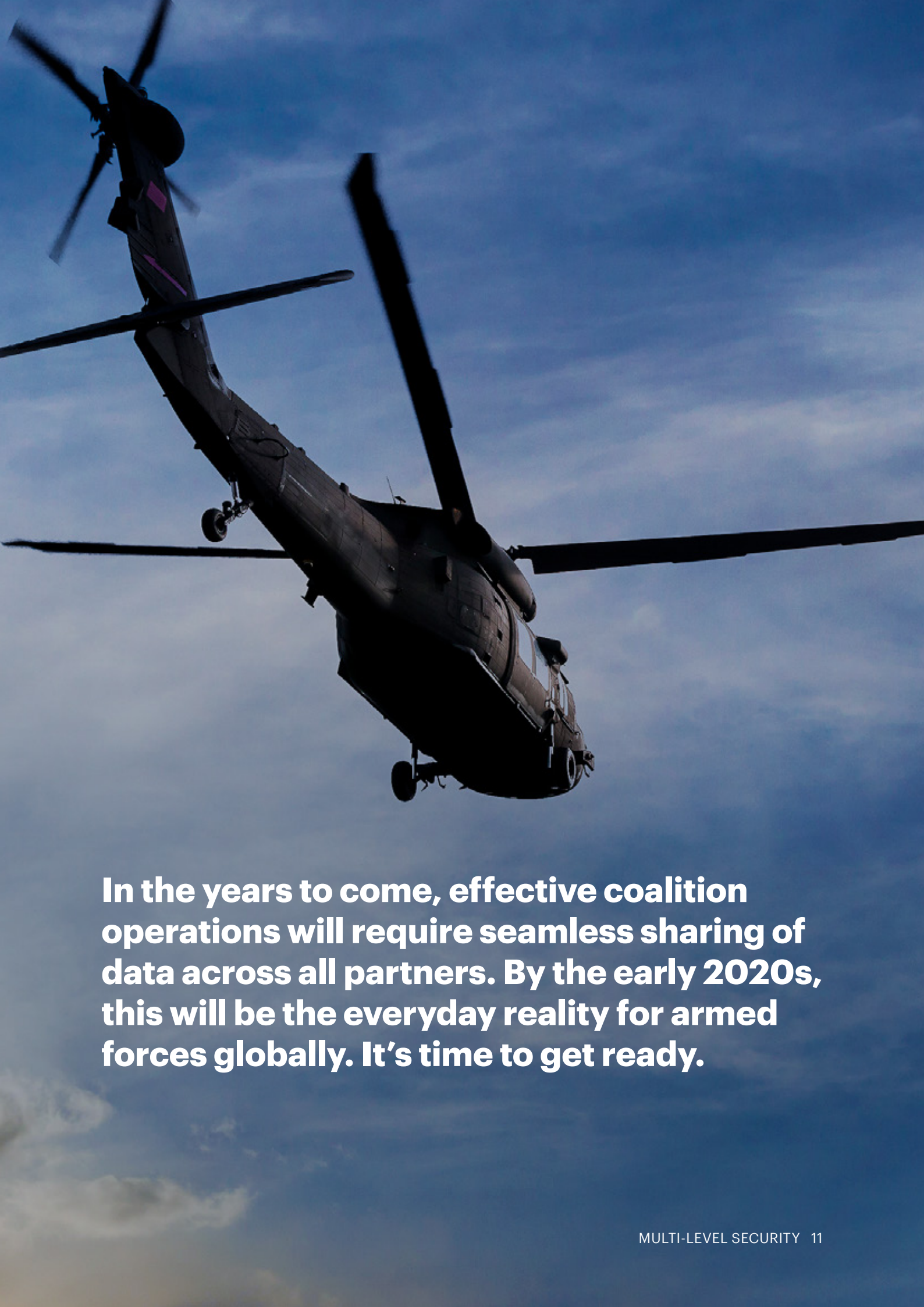
1. Assess the impacts on your current technology of moving from vertical to horizontal data-sharing.

2. Map out the must-have operational requirements that you will tackle first.



3. Establish the scale and scope of the benefits that will result from the change, to create a robust business case and build buy-in and momentum.

4. Collaborate actively with coalition partners and with industry, academia and the commercial sector – around your Multi-Level Security program, to coordinate approaches and agree standards. Any attempt to move to Multi-Level Security alone or in isolation will almost certainly end in failure.



In the years to come, effective coalition operations will require seamless sharing of data across all partners. By the early 2020s, this will be the everyday reality for armed forces globally. It's time to get ready.

EXPERTS

Dr. Valtteri Vuorisalo
Senior Innovation Principal,
Global Defense Industry

valtteri.vuorisalo@accenture.com
www.linkedin.com/in/vvuorisalo/
@vvuorisalo

Yacine Zaitri
Managing Director, Accenture Security

yacine.zaitri@accenture.com
www.linkedin.com/in/
yacine-zaitri-2373a3/
@YazSec

Robert Fox-River
Global Health & Public Service
Security Programme Lead

robert.fox.river@accenture.com
www.linkedin.com/in/rob-fox-river
@Rob_Fox_River

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 442,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

180489