MULTI-LEVEL SECURITY: ENABLING THE FUTURE OF MULTINATIONAL MILITARY OPERATIONS

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

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. Today this paradigm no longer applies, with collaborative multinational operations becoming the norm.

This shift is a logical and well-justified response to the 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 to achieve common goals.

However, alongside the benefits, the move to multinational military operations also brings new challenges. Foremost among these is the need to sustain common situational awareness by sharing information and insight securely and instantaneously across forces, as well as with international agencies, non-governmental organizations and more.

Achieving this level of data-sharing among the armed forces of single nation is challenging enough, without having to contend with different languages, systems architecture, data standards and security classifications.

Shifting from vertical to horizontal...

The complexities of multinational operations are so great that they can only be overcome through a radical shift in how armed forces manage information, as well as a reorientation of the systems they use. 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 be shared **horizontally**, across the forces of different nations and partners.

The defense workforce, which has traditionally been highly protective of information, must move towards a more refined "need to share" attitude. The way to navigate this change successfully lies in taking a data-centric view of the entire environment by applying "Multi-Level Security".

accenture

Multi-Level Security entails 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 anything from a platform design document to positional information about forces on the ground. Whatever it is, it can be shared securely with and to the mutual benefit of coalition partners.

> **Accenture developed a Joint Cross Domain eXchange (JCDX) – an intelligence and target tracking system that draws on data from multiple sources**

Several years ago Accenture developed a Joint Cross Domain eXchange (JCDX) – 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. Now we've applied the same innovative drive and data-centric principles to create an overarching approach aligned with the security context. Multi-Level Security is a key part of this alignment.

Three pillars of Multi-Level Security

Implementing multi-level security is vital to help ensure military forces remain relevant, reliable and effective in the 2020s – and defense agencies must act if they want their initiatives to be operational within that timeframe. To make it happen, there are three key requirements:

1. The need for **horizontality**

The recalibration of data flows from vertical to horizontal is critical to achieving military objectives. In the past, the accuracy, reliability, security and timeliness of vertical data flow were critical to mission success; today, the same is true of horizontal. Only data flows of this type can create the level of situational awareness necessary for the coalition to deliver fast, high-quality decision-making and operational planning. To achieve this, defense organizations must break down old information silos and connect supporting functions to the front line in near real time.

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, it's the commercial sector that's at the cutting-edge – and defense agencies must now raise their game.

Terrorist organizations and non-standard paramilitary forces share information around the world using channels ranging from mainstream chat apps to the "dark net". This diverse array of communications options provides these groups with 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 must 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 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. And they must do this using universally accepted standards and rock-solid security – or they will become too slow or too insecure to be effective.

We're already seeing positive moves in this direction, such as NATO's Federated Mission Networking (FMN) initiative, part of

the Connected Forces Initiative, which aims to enhance interoperability and operational effectiveness. 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.

Four steps Defense agencies can take today

Moving to data focused Multi-Level Security may seem like a herculean undertaking. However, rather than a "big bang" transformation, this transition will take several years.

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.

Not if, but when: now is the time to act

In this digital age, defense forces must transform how they protect and share data – or they risk operational failure. And the urgency is growing by the day: put simply, a multi-level security approach is one that every military force **must** start implementing today. Indeed, the need 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.

If defense agencies fail to automate how they handle and share data, they risk exposing their operations, people and coalition partners to excessive and unnecessary risks. In the years to come, effective coalition operations will require across all partners. By the early 2020s, seamless, multinational data sharing will be an everyday reality for armed forces. It's time to get ready.

* This article was previously published by DefenceIQ in April 2018

About the authors:

Dr. Valtteri Vuorisalo
Senior Innovation Principal,
in Accenture's Global Defense business
www.linkedin.com/in/vvuorisalo
Twitter: @vvuorisalo

Yacine Zaitri
Managing Director and Security lead for Accenture's Health & Public Services business in Europe.
www.linkedin.com/in/yacine-zaitri-2373a3/
Twitter: @YazSec