INTELLIGENT ENTERPRISE UNLEASHED

A defense sector perspective on the Accenture Technology Vision 2018.

2018 Defense Technology Vision

MOBILIZING THE INTELLIGENT MILITARY

This year's Accenture Technology Vision takes the Intelligent Enterprise as its overarching theme. In the defense context, becoming a more intelligent military organization is clearly a critical goal.

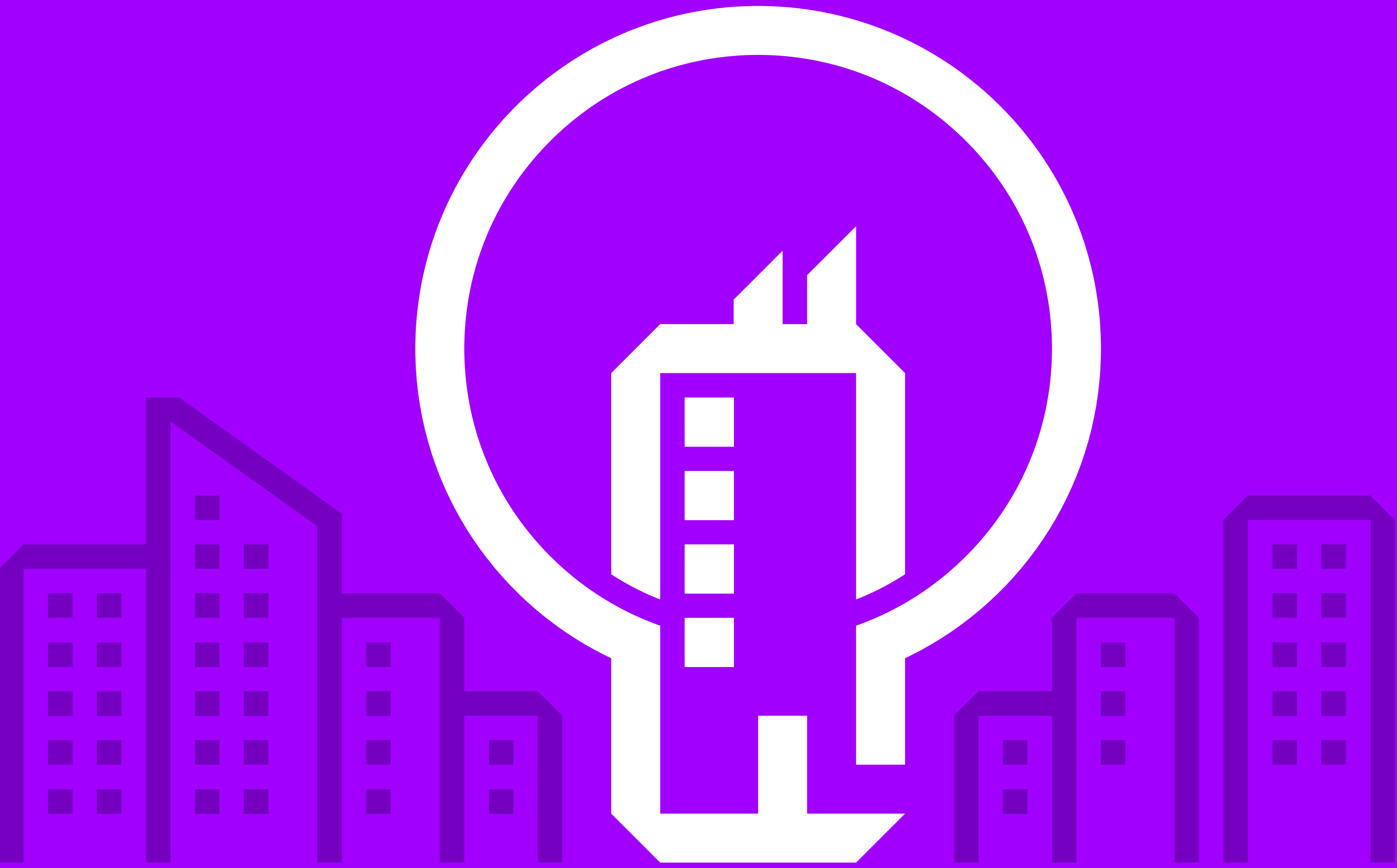
Achieving that goal requires unlocking the data that is currently held within silos and enabling it to flow to the right place at the right time and in the right way. That's critical to achieving enhanced mission readiness and outcomes.

The world presents an increasingly volatile operational and security environment. The rise of non-traditional actors and challenges to democratic governance arising from cyberattacks and state-sponsored subversion also create new challenges. The ability to operate intelligently across multinational partners to address these threats is therefore a vital objective. NATO's Federated Mission Networking[1], for example, expressly calls for interoperability between people, processes and technology to create joint mission outcomes.

> **Focusing on outcomes and placing people at the center of a new approach will be key to an intelligent military.**

The defense sector has historically been at the forefront of technology development and innovation. Countless innovations now widely used in the commercial arena have their origins in the defense sector. But it's not the case today. In many of the advanced technologies highlighted in this year's Technology Vision—from AI to Extended Reality—the commercial sector is moving ahead rapidly, and the defense sector needs to catch up in order to achieve its mission objectives as intelligent organizations.

However, technology alone will not provide all the answers to the challenges defense organizations face as they adapt to a very different environment. New thinking and a new organizational approach will be equally important. Focusing on outcomes and placing people at the center of a new approach will be key to an intelligent military.



2018 Technology Vision

INTELLIGENT ENTERPRISE UNLEASHED

This year's Technology Vision covers five trends, each of which are essential components and capabilities for the intelligent organization.

Each of these resonates with the defense sector's objectives to become smarter, more connected and data-driven. The five trends are:

Trend 1

PRIVATE AI

Training AI as an effective Troop Member

As artificial intelligence grows in its capabilities—and its impact on people's lives—organizations must move to "raise" their AIs to act as responsible, productive members of society.

Trend 2

EXTENDED REALITY

The End of Distance

Virtual and augmented reality technologies are removing the distance to people, information, and experiences, transforming the ways people live and work.

Trend 3

DATA VERACITY

The Importance of Trust

By transforming themselves to run on data, organizations have created a new kind of vulnerability: inaccurate, manipulated, and biased data that leads to corrupted business insights, and skewed decisions with a major impact on society.

Trend 4

FRICTIONLESS DEFENSE

Built to Partner at Scale

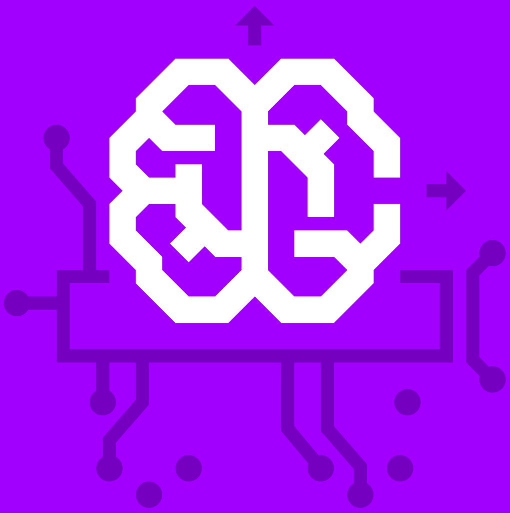
Organizations depend on technology-based partnerships for growth, but their own legacy systems aren't designed to support partnerships at scale. To fully power the connected enterprise, agencies must first re-architect themselves.

Trend 5

INTERNET OF THINKING

Creating Intelligent Distributed Systems

Organizations are making big bets on intelligent environments via robotics, AI and immersive experiences. But to bring these intelligent environments to life, they must extend their infrastructures into the dynamic, real-world environments they want to reach.



Trend 1

PRIVATE AI

Training AI as an effective Troop Member

With artificial intelligence (AI) growing in its reach throughout society, any organization seeking to capitalize on AI's potential must also acknowledge its impact.

AI's potential is no longer just about performing a specific task: it will increasingly take its place alongside people as a fully-formed member of the team. That means how it is trained as a trustworthy and efficient colleague in the military context is an increasingly vital task. Think about it as a boot camp for AI—this needs to be every bit as immersive and exhaustive for smart technologies as traditional boot camp is for human recruits. In effect, in order for AI to be trusted it has to be imbued with the same esprit de corps as its human peers.

There's no question that AI will transform (and in some senses already is) military capabilities. In 2016, for example, an AI 'pilot' powered by a $35 Raspberry Pi microprocessor defeated a seasoned combat pilot in successive simulated dogfights, every single time[2] .

Despite the clear potential, military investment in AI has been dwarfed by that of the leading tech players. Does that matter? Increasingly, the answer is a resounding yes. A failure to invest in and develop AI will leave military organizations significantly disadvantaged over the next few years.

Some of the areas where AI will have a major impact can be thought of as improvements to existing capabilities. Cyber defense is just one new threat. A cyber adversary equipped with advanced AI capabilities will not wait for its enemies' technology to catch up before launching an offensive. Defense logistics and the ability to collaborate internationally are other areas where AI offers significant benefits. But there are other, new forms of collaboration between people and smart machines that create possibilities to do entirely new things.

AI's ability to process and analyze vast amounts of information creates implications across the Observe, Orient, Decide, Act (OODA) loop. From augmenting human ability to detect new threats to analyzing countless variables beyond the scope of human capacity, AI could transform surveillance and situational awareness. Similarly, AI's evolution could make it a superior decision-maker to many of its human counterparts—and it never gets tired or overwhelmed by information. But for AI to collaborate with its human counterparts effectively, and achieve all that it's capable of, it has to be trusted.

Collaboration will be most successful if organizations ensure there are ways of understanding and trusting an AI system's outputs, whether that's by people or other artificially intelligent systems.

In 2016, for example, an AI 'pilot' powered by a $35 Raspberry Pi microprocessor defeated a seasoned combat pilot in successive simulated dogfights, every single time.

Trend 2

EXTENDED REALITY

The End of Distance

Virtual reality (VR) and augmented reality (AR) deliver immersive experiences that extend reality. Extended reality (XR) is the first technology to let people experience omnipresent abilities, relocating them in both time and place—effectively bringing about the end of distance.

For the defense sector, the ability to simulate and share a common view of an operational theatre is immensely powerful. For example, Accenture has created a proof of concept using Microsoft HoloLens along with a gaming engine, Unity, for mixed reality application that provides an interactive map showing real-time location and status data for troops and resources on the ground. By clicking on any unit, a user can see the status of personnel and supplies. And with another simple command, they can instantly order reinforcements and additional supplies. Users can also create and test different scenarios through the mixed reality interface that lets them interact with virtual objects in real physical space.

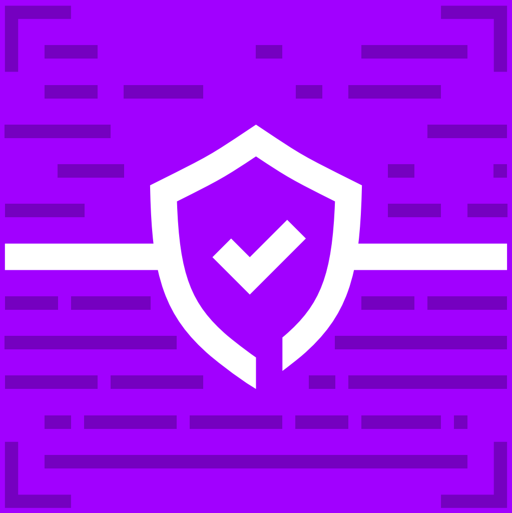
What's more the technology has implications for rapidly establishing operational command capabilities in the field. Think about the ability of AR goggles to provide dashboards and data visualization where and when they are needed—for example at a forward operating base. Rather than waiting for a command center to be built, relatively cheap and accessible commercial technology, along with a secure data connection, is all that's needed.

Training, simulation and planning, too, would benefit from the ability to share in the experience of exploring a common geographical location, regardless of where they happen to be. That could have major implications for training soldiers and pilots in highly realistic combat simulations, for example. And perhaps one of the most practical applications of extended reality is the ability to deploy expertise exactly when it's needed, without an expert having to be physically present. For example, that could be broken equipment or vehicles in the field Maintenance engineers could see 'over the shoulder,' diagnose and offer step-by-step guidance to fix the problem.

Today, extended reality is still evolving, and challenges around processing lag and content creation remain barriers to its full maturity. But thanks to its transformative potential, 74 percent of public sector executives agree that it is important or very important for their organizations to be a pioneer in XR solutions.

As XR becomes pervasive, immersive experiences will eliminate the most important distance of all: the distance between where defense organizations are today and where they want to be in the future.

74 percent of public sector executives agree that it is important or very important for their organizations to be a pioneer in XR solutions.



Trend 3

DATA VERACITY

The Importance of Trust

While defense organizations are becoming more data-driven than ever, inaccurate and manipulated information threatens to compromise the insights that the military relies on to plan and operate. Of course, in this context inaccurate data is about much more than losses of efficiency or operational challenges. It's potentially a matter of life or death.

Defense organizations can address this vulnerability by building confidence in three key data-focused tenets: provenance, or verifying the history of data from its origin throughout its life cycle; context, or considering the circumstances around its use; and integrity, or securing and maintaining data.

Having confidence in data is critical, for instance, to the effective operation and acceptance of AI. AI will only be as good (or bad) as the data that it acts upon. Of course, in the military context already skeptical about the possibilities of AI, being able to trust the technology and the data behind it is fundamental to its adoption.

Operating more collaboratively across multinational partnerships also depends on the ability to trust and verify not only that the data itself is secure, but how it flows between partners is equally well protected. This, clearly, is a major challenge as in the defense context the need to deliver only the right data to the right person, at the right time is crucial.

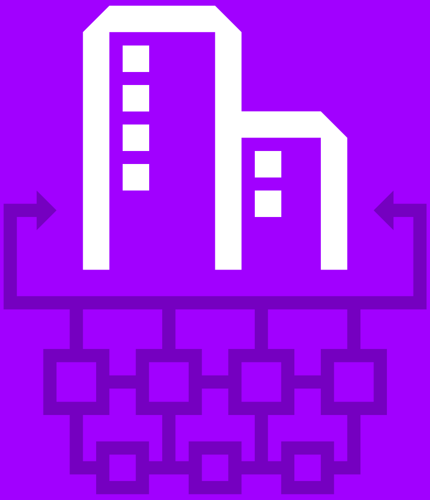
With many operational defense systems characterized as a complex mixture of new and legacy IT, sharing data effectively within one branch of one country's military is already challenging. Extending that to sharing across multiple forces from a number of international partners and the complexities and barriers, unsurprisingly, become formidable.

They can only be overcome by radical reorienting the systems in use across today's armed forces. Today's essentially vertical approach to data sharing involves 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.

This significant shift not only requires a technological shift, but also a profound change in mindset and culture. A defense workforce that has been highly protective of information moves from sharing data on a "need to know" basis to a more refined "need to share" approach. It's not simply a matter of architecting IT, it means rearchitecting the organization itself.

That requires what's called "multi-level security." This 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. This is essential to secure the trust required for successful multinational, collaborative operations.

> **AI will only be as good (or bad) as the data that it acts upon. Of course, in the military context already skeptical about the possibilities of AI—being able to trust the technology and the data behind it is fundamental to its adoption.**



Trend 4

FRICTIONLESS DEFENSE

Built to Partner at Scale

Collaboration between partners in response to common threats is the operational mantra across the defense sector. Achieving it requires interoperable technologies and secure trusted data flows.

The challenge facing the military is that in order for all this to happen, what have always been vertically integrated organizations now need to become horizontally integrated. People, technology, processes, roles and organizations must operate in a way that is in opposition to, in many cases, hundreds of years of tradition.

That's why the shift is as much about mentality and culture as it is technology. Mission objectives, in this context, require outcomes-based thinking. Rather than deploying the army, navy or air force as relatively autonomous and independent entities, the desired outcomes—running simultaneous expeditionary missions or multiple maritime rescue mission for example—are defined which will then determine how a combination of forces delivers. That's the kind of thinking embodied in the UK Ministry of Defence's strategy document[3] that first and foremost defined the outcomes required rather than setting specific objectives to each discrete force.

When the strategic partnerships needed to deliver an outcome-driven approach are technology-based, they can expand partner networks—between industry, academia and other military organizations—faster and into more ecosystems than ever before. But legacy systems weren't built to support this kind of expansion, and soon, outdated systems will be major hindrances to multinational/multi actor collaboration. To build a strong foundation for technology-based partnerships, therefore, defense organizations must consider adopting microservices architectures and using blockchain and smart contracts. Those that invest in these changes today will redefine how they can collaborate in the future.

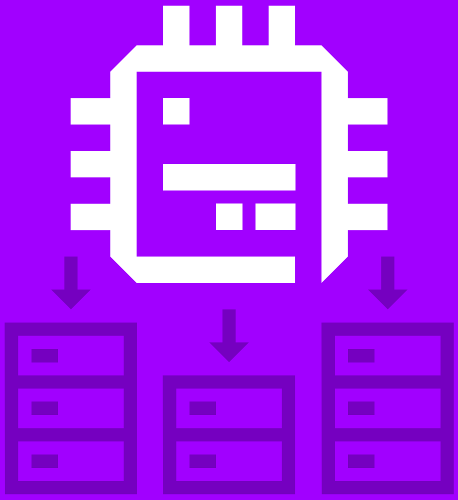
Already, our survey shows that 36 percent of public service leaders report working with double or more partners than they were two years ago. It's critical for them to recognize that their organization's own technology will serve as the foundation for these strategic relationships—but working with complex legacy IT systems could also be holding them back.

In order to accelerate and grow a new wave of technology-based partnerships, defense organizations must start inside their own walls and develop a new architecture, based on microservices. Microservices architectures won't get rid of complexity, but they do split it into more manageable segments. With well-defined context services organized around business capabilities, individual systems become more independent, easier to manage and closely aligned to tactical objectives.

Because they're independent, each system can move at its own speed (instead of being tied to monolithic legacy IT). Agility and flexibility get hard-wired into the organization. And because services are independent (and business and IT closely aligned), it's easier for an innovation culture to flourish, unimpeded by internal politics and/or resistance to change.

A microservices architecture will push organizations to clearly define the services they offer and turn each service into a potential enabler of technology-based partnerships.

36 percent of public service leaders report working with double or more partners than they were two years ago.



Trend 5

INTERNET OF THINKING

Intelligent Distributed Defense Capabilities

Robotics, immersive reality, artificial intelligence and connected devices are bringing a new level of technological sophistication to the physical world.

The next generation of technology demands an overhaul of existing infrastructures, with a balance of cloud and edge computing, and a renewed focus on hardware to deliver intelligence everywhere.

But whereas for most commercial organizations and many in the public sector, distributed systems become increasingly connected to one another, it's not the case for defense. Here, distributed systems in a federated mission network are better thought of as pockets of connections that can function independently as discrete bubbles of connectivity.

Current infrastructures are designed around a few basic assumptions: enough bandwidth to support any remote application, an abundance of compute in a remote cloud, and nearly infinite storage. But the demand for immediate response times in physical-world applications defies this approach. Current predictions suggest that by 2020, smart sensors and other Internet of Things devices will generate at least 507.5 zettabytes of data. Trying to do all of the computational heavy lifting offsite ultimately will become a limiting factor.[4] The resulting need for real-time systems puts hardware in focus: special-purpose and customizable hardware is making devices at the edge of networks more powerful and energy efficient than ever before.

The next generation of intelligent solutions are moving into physical environments, and key military strategies ride on pushing intelligence into the physical world. That's essential for collaborative joint missions.

But the flipside of this is that adversaries—from terrorist groups to criminals—also now have access to technologies that allow them to operate in new ways. Defense organizations therefore have to understand and shape the new operating models they need to enable high-speed data flows in order to harness the potential of distributed intelligence and successfully neutralize the new threats they face.

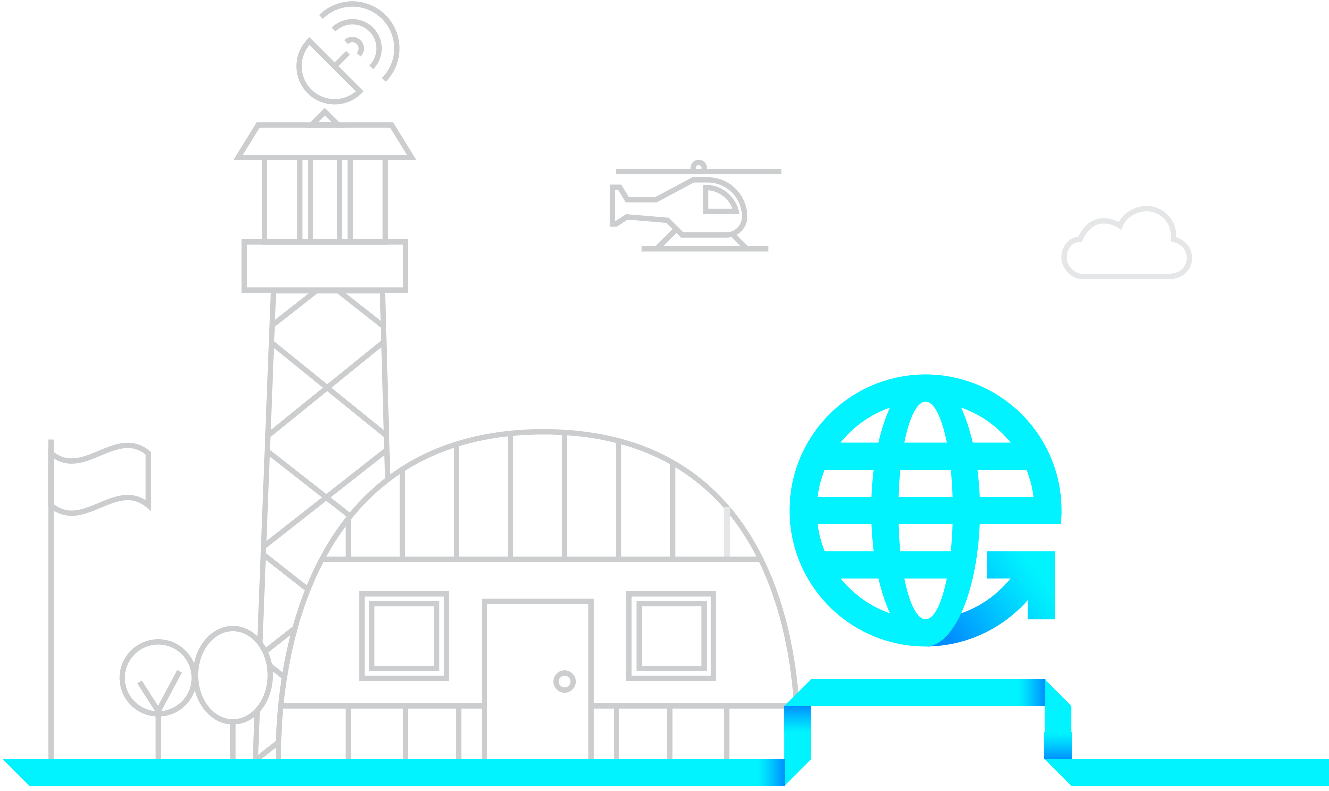
This extended infrastructure calls for a renewed focus on hardware, at a time when many companies have grown accustomed to software-driven solutions as their go-to strategies. Public service organizations are taking note: our Technology Vision 2018 survey indicates 79 percent of executives believe it will be very critical over the next two years to leverage customer hardware and hardware accelerators to meet the computing demands of intelligent environments.

Current predictions suggest that by 2020, smart sensors and other Internet of Things devices will generate at least 507.5 zettabytes of data.

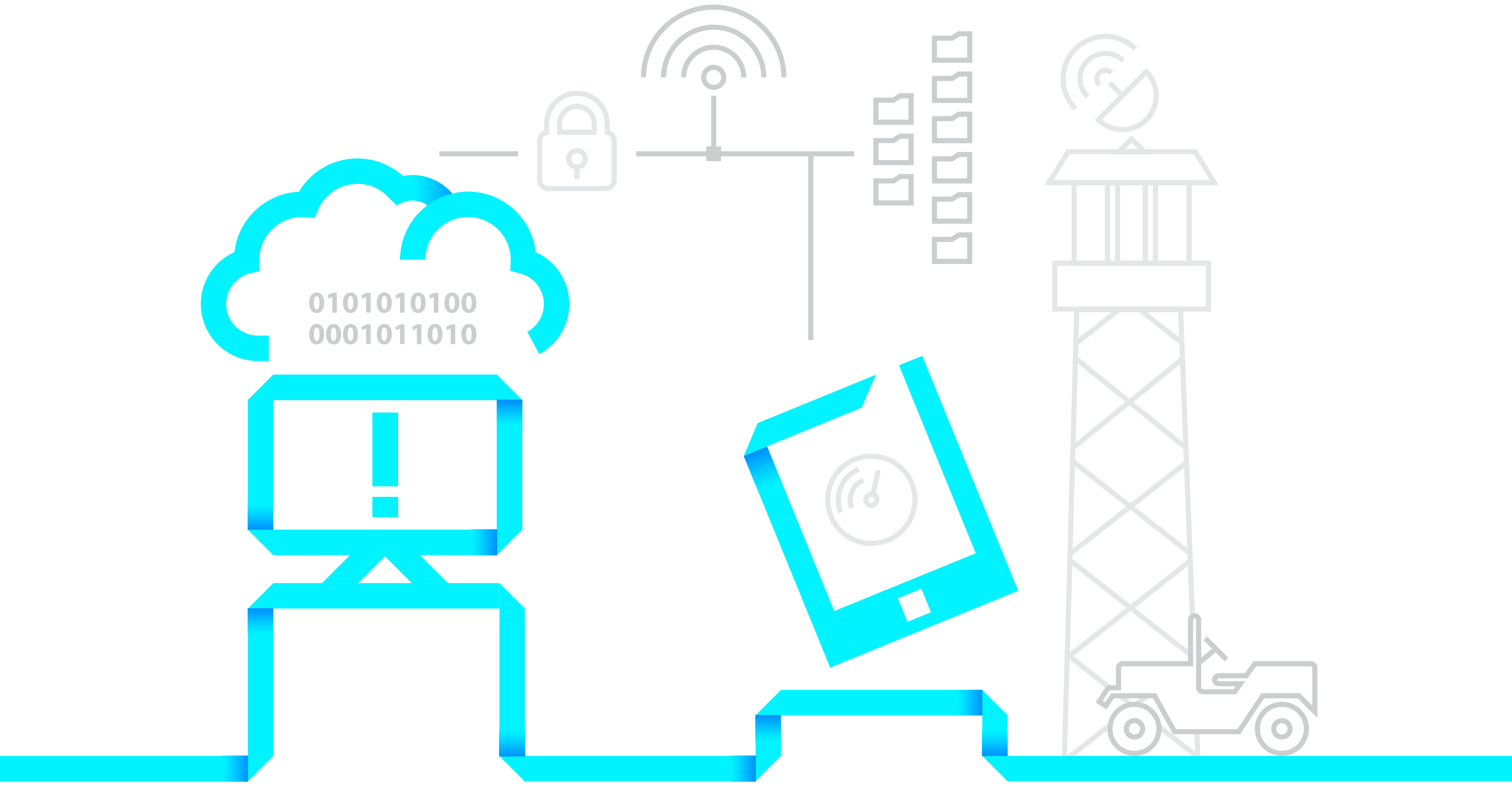
Five trends, one goal

The defense sector is challenged to respond to new types of threat, political volatility and even new combat arenas in the form of cyberwarfare.

As the physical and virtual continue to merge and the borders between them become increasingly hard to define, acquiring new technology capabilities is a non-negotiable strategic imperative. Delivering greater situational awareness and the ability to respond rapidly to unpredictable adversaries require investments in, among others, AI, edge computing, as well as smart and secure connectivity. Today's information architectures will need to be redesigned to integrate with others to share and collaborate quickly, effectively and securely. But technology by itself will not be enough to meet the challenges facing the defense sector.



Today's information architectures will need to be redesigned to integrate with others to share and collaborate quickly, effectively and securely.



Experts

Accenture solves our clients' toughest challenges by providing unmatched services in strategy, consulting, digital, technology and operations.

We partner with more than three-quarters of the Fortune Global 500, driving innovation to improve the way the world works and lives. With expertise across more than 40 industries and all business functions, we deliver transformational outcomes for a demanding new digital world.

ANTTI KOLEHMAINEN

Managing Director, Global Accenture Defense Services

antti.kolehmainen@accenture.com

linkedin.com/in/antti-kolehmainen-14a3042

@anttiKol

DR. VALTTERI VUORISALO

Senior Principal, Global Accenture Defense Services

valltteri.vuorisalo@accenture.com

linkedin.com/in/vvuorisalo

@vvuorisalo

References

1 http://act.nato.int/fmn

2 http://www.newsweek.com/artificial-intelligence-raspberry-pi-pilot-ai-475291

3 https://www.gov.uk/government/policies/armed-forces-and-ministry-of-defence-reform

4 Shacklett, M. (2017, July 21). Edge computing: The smart person's guide. Retrieved September 8, 2017, from http://www.techrepublic.com/article/edge-computing-the-smart-persons-guide/

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

ABOUT ACCENTURE LABS

Accenture Labs incubate and prototype new concepts through applied R&D projects that are expected to have a significant near-term impact on clients' businesses. Our dedicated team of technologists and researchers work with leaders across the company to invest in, incubate and deliver breakthrough ideas and solutions that help our clients create new sources of business advantage. Accenture Labs is located in seven key research hubs around the world: Bangalore, India; Beijing, China; Dublin, Ireland; Silicon Valley, California; Sophia Antipolis, France; Washington D.C.; and Israel.

ABOUT ACCENTURE RESEARCH

Accenture Research shapes trends and creates data-driven insights about the most pressing issues global organizations face. Combining the power of innovative research techniques with a deep understanding of our clients' industries, our team of 250 researchers and analysts spans 23 countries and publishes hundreds of reports, articles and points of view every year. Our thought-provoking research—supported by proprietary data and partnerships with leading organizations such as MIT and Singularity—guides our innovations and allows us to transform theories and fresh ideas into real-world solutions for our clients.

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks. Information regarding third-party products, services and organizations was obtained from publicly available sources, and Accenture cannot confirm the accuracy or reliability of such sources or information. Its inclusion does not imply an endorsement by or of any third party.

The views and opinions in this article should not be viewed as professional advice with respect to your business.