Look Out 2020+
Industry Trends
Defense

The path to information dominance

Thought Leadership

Atos

Megatrends in Defense: A world of new tensions

"Tomorrow's wars will be radically different. As digital changes the world, it's essential that Defense prepares for information dominance."

Stephane Janichewski
Senior Vice President, Head of Defense & Aerospace, Atos

War has returned. After the fall of the Iron Curtain, there was hope for an 'End of History.' But tensions are rising all over the world, showing threats have not disappeared.

While the balance of power and geopolitics alliances are moving at an accelerated pace, prospects are worrying: terrorism, the proliferation of mass destruction along with nuclear, biological and chemical (NBC) weapons, global competition for shrinking natural resources, the risk of epidemics and pandemics, war and refugees, massive migration and multicultural tensions.

New spectrums of missions

In the new multipolar world, Defense is more essential than ever. It must also broaden its scope. While friends and enemies are merging in an increasingly intertwined world, traditional frontiers are tending to shade away. Defense and security battlefields have grown beyond military into anti-terrorist, economic, financial, mediated and humanitarian grounds in all homeland and foreign territories. The traditional notion of the front is extending into a ubiquitous, multi-dimensional chessboard.

Today's complex defense missions are being hindered strategically by the digital revolution that – after having disrupted multiple domains – is challenging defense practices. The digital revolution is transforming military technologies with real-time communications, intelligent weapons, smart machines and robotics. It is also transforming the balance of power with the rise of asymmetric and hybrid warfare, and also by opening a new battlefield: cyberspace itself.

Reinventing for the 21st century

In this new geostrategic context, Defense must adapt its technologies, doctrine, strategies and tactics, and reinvent itself, as it has done throughout history. In this domain, troop efficiency, operational effectiveness, capacity to support new missions and cyber-protection will be the major challenges at the dawn of the 2020 decade.

Changing geopolitical environments and new digital technologies are not only progressively transforming armies as we knew them but also opening extraordinary opportunities to build the Defense of the 21st century.

#1
Defense spending is at its highest level since the Cold War

37%
increase in defense spending is expected by 2026

$30bn
will be spent on global defense electronics in 2022
$ = USD

+9.8%
more budget was allocated to the US Defense Department in 2018

$108bn
will be devoted to defense IT spending in 2020
$ = USD

$119bn
should be devoted to C4ISR in 2022
$ = USD

2%
GDP is the minimum defense budget recommended by NATO

$16bn
will be invested in smart weapons in 2021
$ = USD

$31bn
will be spent on military robots in 2022
$ = USD

Sources: IHS Markit, Markets and Markets, OTAN, Strategy Analytics, US DOD

Four transformation challenges and opportunities for the future of Defense

1

Augment soldier efficiency

In the digital age, battlefields and their soldiers will be different to those of yesterday. When the **enemy is now mobile and connected**, stealthy with cyberwar and hidden with terrorism, soldiers must stay one step ahead.

What is the best way to **fight in the information and smart machine era?** To succeed, troops need more than **seamless connectivity for exchanges** with their squad and HQ; they need tools for collaborative combat, with **real-time information and coordination** to help them adapt to any tactical situations.

Troops need smart support for assessing threats, risks and their own condition, with **prescriptive assistance** in domains ranging from intelligence to mission and medical assistance. They need to be supported by **smart and connected weapons** along with smart machines such as drones, able to help them optimize tactics in combat.

> **The potential impact is immense. Every human life essential. With digital intelligence and robotics, soldiers can not only make the most of their forces; they can also dramatically minimize the risk of casualties.**

2

Optimize military operations

While war can be won through the superiority of arms, it can also – and is most often – won through the **superiority of intelligence, command, strategies, tactics and logistics**. Only when forces get the right data on threats and the enemy, and the right logistic support, can they optimize their moves and their actions.

In the digital era, this means forces consistently capture and analyze the whole spectrum of communications, signal, human and Open Source intelligence to **detect weak signals that may call for prescriptive action.**

They need to be able to permanently visualize and coordinate all actions in the battlefields across land-air-sea armies' corps. And they need perfectly **coordinated logistics and back office support** to back their every move.

> **Armies are only as strong as their weakest link. This calls for supreme information management alongside seamless operational data flow across the whole chain of command. The result is essential: grasping everything needed for victory.**

3

Take new missions into account

In a changing world, fundamentals of conflicts do not change, but **the forms of war adapt to new environments.** As technologies, demographics, scarcity of energy resources and multipolar geopolitics rapidly transform the world, Defense must evolve its missions.

While the frontier between war and peace is blurring, armies must adapt to a changing landscape of threats. While being able to fight conventional hostile armed forces, they must also be able to **detect and fight hostile propaganda, protect critical national companies and manage low-intensity conflicts** inside homelands and allied or hostile territories.

Forces must also be prepared for a **broader set of defense-related missions**, such as anti-terrorism, safe-keeping, hostage rescue, disasters and epidemics management, or even humanitarian relief.

Readiness requires **new forms of engagement** where Defense – while keeping the core expertise of combat – can manage a larger spectrum of missions and **interoperate with the broadest set of authorities**, whether international, national or local.

> **What's at stake for armies: be highly adaptable to win the 21st century's wars in an increasingly complex and networked world.**

4

Prepare for cyberwar

While digitization brings numerous opportunities to Defense, it also opens a **new front: the cyber-world.** Essential for boosting military efficiency, cyber-technologies can also be leveraged as a weapon. Cyber-squads are now active in all modern armies, as many recent and highly **sophisticated cyber-attacks** – such as those from North Korea – have shown. We have not yet felt their full potential.

There are already debates on espionage breaches in defense agencies and the spread of fake news for manipulating elections. But what could the impact of a massive takeover of communication networks be? Or attacks on financial systems? Or misguidance from GPS and transportation systems? Or compromising highly sensitive targets such as nuclear sites or even weapon systems themselves?

This makes **cybersecurity a new critically strategic domain** for warfare, where armies must prepare for both defensive and offensive action.

> **The potential impact is immense. With the annual cost of cybercrime alone expected to range from $ 1 trillion to $ 6 trillion', now is the time to be ready for info-war.**

Building next-generation platforms for next-generation defense ecosystems

"In tomorrow's exponentially growing defense infosphere, next-generation intelligent technologies, and their ubiquitous integration into all defense systems, will be vital for success."

Cyril Dujardin
Senior Vice President Mission Critical Systems, Atos

While battlefields and weapons evolve, core military values – effectiveness of command, power, agility, endurance and morale – do not change. They have even taken on a new dimension: the mastery of information.

Intelligence and communications are more critical than ever in today's hyper-connected world. Digital networks mean allies and enemies, autonomous weapons and critical infrastructures are just a few milliseconds away. **Information dominance is essential for victory in this new world.**

Combining old might with new

For years, the defense industry has worked to build powerful and resilient land, air and sea military and weapons systems. While it has contributed to multiple innovations (the first computers, the Internet, ...), traditional defense R&D processes are now often outpaced by the fast rise of new digital technologies: Big Data, the Internet of Things (IoT), Artificial Intelligence (AI) and next-generation robotics, to name a few.

How can forces combine the strength of traditional weapons systems with the extraordinary new capabilities brought by Big Data for intelligence analysis? By mobile computing for collaborative combat? By prescriptive intelligence for smart weapons and machines?

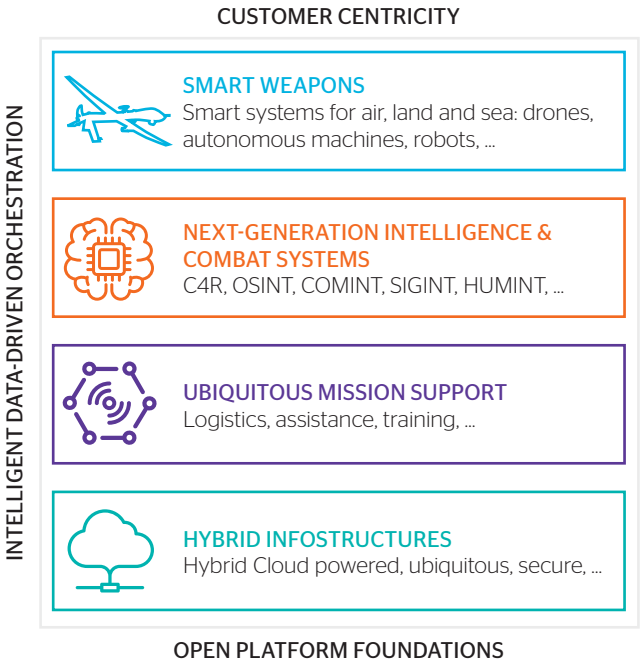
Preparing for the new landscape

Transformation calls for new hybrid development models where digital players bring additional innovation power, enabling agility in the face of changes in threats. To be ready for the future, defense organizations should:

- **Adopt the latest advances in analytics** to detect and react to threats before they impact, outside and within the battlefield.
- **Leverage the power of next-generation IoT and communication systems** to empower operations along the entire chain of command with smart weapons and collaborative combat coordination.
- **Implement the latest cyber-defense technologies** to secure information and operation systems.

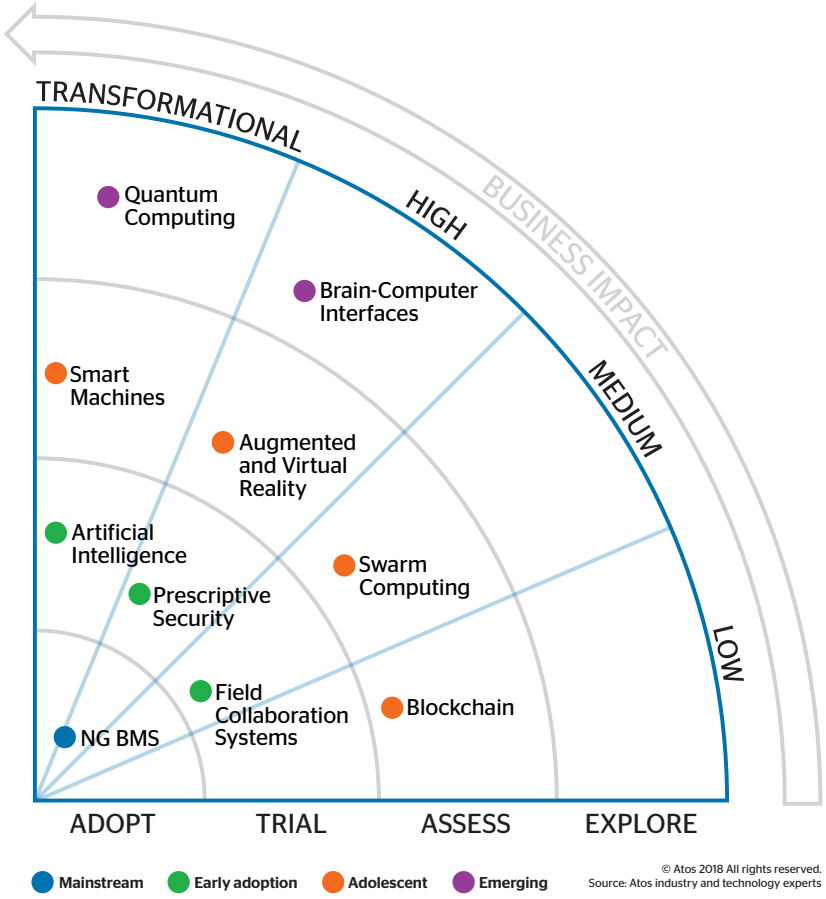
Military players should adopt the latest digital technologies, leveraging not only traditional defense providers but also innovations brought by digital specialists.

Next-generation technologies for the future of Defense



This is just the start of the journey. Defense needs to prepare for more disruptive technologies that are just emerging today and will turn out to be transformational in the years to come.

10 disruptive technologies that will shape the future of Defense



Source: Atos industry and technology experts

Defense Look Out 2020+ Radar: 10 key technologies set to impact Defense companies over the next 5 years.

Want to know more? Examine the Look Out 2020+ Global Technology Radar to get deeper insights into these 10 strategic technologies and many more: **atos.net/lookout**

Next-Generation Battle Management Systems are unified C4ISR systems for land, air and sea battlefields that streamline information flow between all levels of command. A cornerstone for info-dominance, they simplify sharing the tactical situation and orchestrating actions between connected HQ, vehicles and combatants, turning data into knowledge and knowledge into action.

Artificial Intelligence promises to second human cognitive capabilities with virtual assistants, knowledge engineering and smart machines. From intelligence & reconnaissance to computational military reasoning or autonomous combat systems, military applications are numerous. Defense players must experiment with the most mature use cases now.

Prescriptive Security uses real-time dark web monitoring, AI and automation to detect potential threats and stop them before they strike. Applications range from cyber-protection to connected military equipment security. Defense players should integrate it into their information and operational Security Operation Centers.

Field Collaboration Systems are an ecosystem of 4G mobile technologies and connected military equipment (rugged tablet, connect assault rifles, drones, tactile watches, laser sight binoculars, ...) enabling teams to share and collaborate easily for missions in mobile tactical bubbles. They must be at the heart of connected forces strategies.

Smart Machines are promising to revolutionize military environments, with potential applications such as Autonomous Weapons Systems (including unmanned aerial, surface and underwater vehicles) as well as military robotics and cruise missile. While some technologies are just adolescent, defense players must assess military applications now.

Augmented and Virtual Reality are blurring real and virtual worlds, allowing combat and defense forces to get augmented information within the context of their current environment. Defense players should test use cases in wargaming, training, information management and combat assistance.

Swarm Computing or 'hive computing' are massively distributed, self-organizing systems of intelligent systems that work collaboratively towards a strategic objective. Promising applications include fleets of Unmanned Air Vehicles for reconnaissance, strike or jamming. Armies must assess their potential now.

Blockchain is a potential game-changer for conducting or auditing exchanges with parties without prior trust relationships. In the defense field, it may apply in domains such as secure messaging, resilient communications or trusted logistics support. Defense organizations should begin to explore use cases.

Quantum Computing promises to break traditional combinatory analysis limitations, bringing in disruptive advances in cryptanalysis, simulation, Big Data and intelligence capabilities. Defense players must start preparing for both quantum computing and quantum-safe cryptography.

Brain-Computer Interfaces promise to leverage neural sciences to establish a direct communication pathway between humans and digital devices or machines. While yet prospective, these technologies could have disruptive applications in telepresence, robotic augmentation, warfighting and also mind control. Defense organizations should start exploring them.

A glimpse into the future of Defense: Expert views on best practice for digital transformation

Stephane Janichewski
Senior Vice President,
Head of Defense & Aerospace, Atos

Philippe Duluc
Senior Vice President, CTO,
Big Data & Security, Atos

What could Defense look like in five years?

In the face of growing threats, we expect to see Defense in the coming years securing a more multipolar and complex world, animated by rising geopolitical tensions. **Cyberspace will probably join today's land, air and sea battlefields** as a strategic defense issue, with information a key target.

In this more dangerous, more connected world, we are convinced **information dominance will be the mother of all battles.** It is already emerging today with autonomous machines, connected weapons and augmented soldiers. It will be even more critical tomorrow as digital and physical worlds converge through the Internet of Things (IoT) and Artificial Intelligence (AI) to enable **info-valued battlefields and ubiquitous intelligence systems.**

The supplier landscape will probably evolve: less fragmentation between tier one integration players, combining digital and defense expertise while leveraging innovative start-ups. These complex, fast-innovation-driven ecosystems will require new methodologies in strategic defense planning and procurement.

As innovation accelerates, **the gap between the digitally transformed and the late followers will widen.** Those left behind will be at risk.

Which driving forces will help them succeed?

The race for info-dominance will change defense strategies. We think that there will be three key factors for success.

The first is an ambitious strategic vision for defense digital transformation and agile roadmap for adapting to the fast-changing technology landscape where traditional rigid programs fall behind. Atos is helping defense organizations drive these.

The second is next-generation defense systems for a connected world where massive overarching, rigid universal systems may be counterproductive. **Defense organizations will need to work in collaborative ecosystems,** constantly interconnecting and interoperating between divisions, armies and partners. Each entity should also operate in **'autonomous info bubbles' to drive agile decisions in the field.**

The third is avoiding information saturation from the connected world's immense flows of data. Critical challenges will be intelligently filtering to **extract the right contextual insight for action and providing it in a user-friendly way.** Managing this last mile is at the heart of our defense innovations.

> "Artificial Intelligence, Smart Machines and Cybersecurity will be critical domains for tomorrow' warfare. To succeed, armies must prepare now."

What should defense players do today?

The three strategic pillars in defense are: the right intelligence for defining priorities, agile operations and freedom of maneuver – adapting in the field, independently of other forces. We think that info-mastery is at the heart of these pillars and this is what our defense clients strive for. At Atos, we help them in five strategic domains:

- **Collaborative combat** with unified C4ISR battlefield management systems, enabling real-time coordination of forces for intelligent warfare. We notably deploy these strategic technologies for the whole French Army, within the Scorpion program.
- **Augmented soldier,** with drones, connected weapons and intelligent communications. We collaborated with armed forces to develop Auxylium, a very mobile user environment that coordinates defense missions in the field, in autonomous and interoperable bubbles.
- **New-generation applications driven and tactical communications systems** leveraging the latest LTE digital technologies in all missions, homeland security, anti-terrorism and more.
- **Next-generation intelligence systems** leveraging the latest Big Data and Artificial Intelligence technologies to analyze all sources from the exponentially growing infosphere (OSINT, HUMINT, IMINT and SIGINT) and anticipate and prevent threats.
- **Cybersecurity** to mitigate cyber-threats with AI-powered prescriptive security.

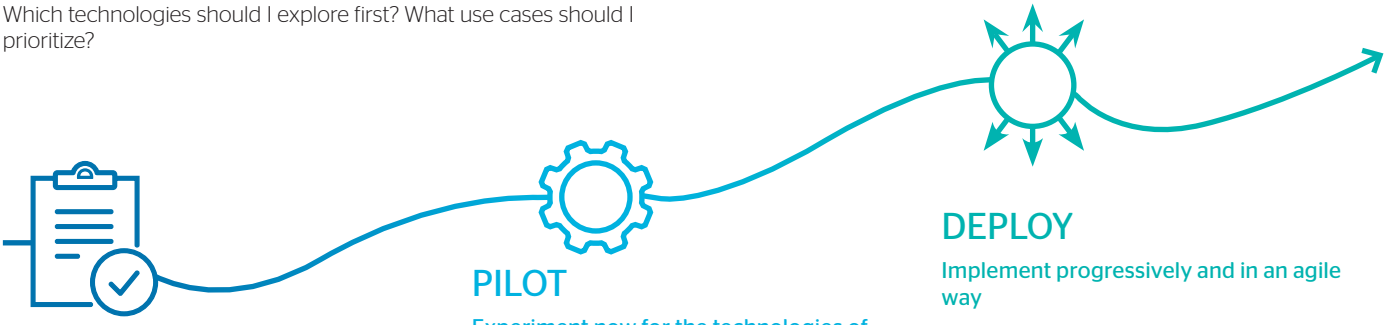
We are convinced combining the best of military and civil tech innovation will be key, unifying electronic and digital technologies strengthened for military use while leveraging the largest ecosystem of partners to provide effective, user-friendly innovation. This is what we strive to do for defense forces.

Creating your own Defense transformation journey

With the battlefield transforming, you must drive your organization forward. Faced with a rapidly changing defense ecosystem, the questions you will be asking is not 'Why change?' but 'Which direction?' and 'How?'

The first step is **building your strategic vision for defense digital transformation.** This overarching view will drive the initial steps, defining the overall direction your technology roadmap will take. Which technologies should I explore first? What use cases should I prioritize?

Having painted that strategic picture, you must next define a roadmap. Your roadmap must be agile; it must allow you to adapt as new tensions and novel threats emerge. We have drawn up a three-step approach to help you on your journey.



PLAN

Explore where you want to go

Define an agile roadmap for success. Begin with technologies such as **NG BMS, Field Collaboration Systems, Augmented & Virtual Reality, Prescriptive Security and AI.**

PILOT

Experiment now for the technologies of tomorrow

Explore the upcoming potentialities of **Smart Machines, Swarm Computing, Blockchain, Quantum Computing or Brain-Computer Interfaces.**

DEPLOY

Implement progressively and in an agile way

This will help you manage the ever-broader spectrum of missions and interoperate with authorities at whatever level required.

Throughout these phases, an open approach to innovation, such as the **Digital Business Continuum** approach developed by Atos, will be paramount to success. In an ecosystem world where information dominance wins wars, openness is the best way to capture collective intelligence. As armies strive to transform, **open innovation labs** – such as the Atos Labs on Artificial Intelligence – will provide an ideal environment for bringing new ideas and new concepts to life – and creating military strength for tomorrow.

Where should you begin?

As the Trusted Partner for your Digital Journey, Atos can help. Meet our experts and stay one step ahead by getting hands-on experience of new disruptive technologies.

ENGAGE in a co-innovation workshop at one of our Business Technology & Innovation Centers.

Get off to a quick start with a personalized workshop. Ask for a meeting:
> atos.net/btic

EXPLORE how the latest technologies can boost your own practice.

Leverage our experts and labs to build POCs tailored to your own business:
> atos.net/defense

STAY TUNED with the latest trends and best practices in digital transformation.

Keep yourself informed. Follow the latest insights from the field on:
> atos.net/blog

This is an extract from the full Atos Look Out 2020+ report, which provides an in-depth analysis of the emerging megatrends, business transformation opportunities and technologies that will drive innovation in the years ahead.
Explore the full report on **atos.net/lookout.**

About Atos

Atos is a global leader in digital transformation with approximately 100,000 employees in 73 countries and annual revenue of around € 13 billion. European number one in Big Data, Cybersecurity, High Performance Computing and Digital Workplace, the Group provides Cloud services, Infrastructure & Data Management, Business & Platform solutions, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies, digital expertise and industry knowledge, Atos supports the digital transformation of its clients across various business sectors: Defense, Financial Services, Health, Manufacturing, Media, Energy & Utilities, Public sector, Retail, Telecommunications and Transportation. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline. Atos SE (Societas Europaea) is listed on the CAC40 Paris stock index.

Find out more about us
atos.net/lookout
atos.net/defense

Let's start a discussion together

CT_180511_AS_LOOK-OUT-DEFENSE