Connected Defense:
Vision for 2020

Trusted partner for your **Digital Journey**

Atos

Contents

"Defense is facing a new world of tension where conflicts are on the rise and information dominance is key. Atos is committed to be the trusted global transformation partner in this unique digital journey."

Stéphane Janichewski
Senior Vice President
Defense & Aerospace at Atos

Executive summary

Today defense is facing a new world of tension: conflicts are on the rise and information dominance is key. In this new world, defense decisions need to take into account five levers: collaborative combat, the augmented soldier, tactical communications, data management and cybersecurity.

As an acknowledged expert in these areas, Atos sets out in this white paper how these levers will use digital transformation and how new innovative technologies can meet the challenges of tomorrow's defense.

Indeed, for each of these topics, Atos is exploring new solutions with its customers and is already offering very innovative deployments. This paper sets out concrete case studies of how Atos is addressing market trends to make tomorrow's defense a reality.

Digital transformation of the battlefield allows collaborative combat, ensured by the new generation of Battle Management Systems. This document will explain how: the new digital native workforce can share information and analytics in real time, a revolution for combat doctrine.

The adoption of augmented soldier solutions demonstrates how they enhance information about soldiers or their environment, in order to enable them to do something that was previously not possible.

Tactical communications go further today by using LTE/4G networks management and secure communications with new types of devices in surveillance and combat field operations. Key success factors include meeting the new market request of providing real ATAWAD - AnyTime, AnyWhere, on Any Device capability.

The topic of data is addressed in the context of end-to end data exploitation processes as the new weapon in this market and by leveraging the Internet of Things, artificial intelligence, swarm computing, and quantum technology. Defense approaches today can go further with new capabilities such as predictive intelligence – for instance the ability to offer enemy behavior prediction.

However, benefiting from these, in particular new IT solutions can generate new vulnerabilities. Securing strategic defense assets and organizations is of course a prerequisite. This paper sets out how Atos goes beyond the traditional set of security solutions, deploying advanced technologies such as adaptive security, homomorphic encryption and trusted equipment.

Defense 2020: A new world of tension

Conflicts are on the rise and information dominance is key After the fall of the Iron Curtain, many in the West welcomed the concept of "the end of history",, driving the world to a new era of peace, troubled only by a few remaining crises in failing states. But rising tensions show today that major threats have not disappeared.

Tensions are not only rising in the Middle East and Africa, where civil and interstate conflicts are creating troubles, humanitarian and migration tensions at the doorstep of Europe but there are also threats from terrorism around the globe and increasing tensions in Eastern Europe and Asia, which have the potential to create an undesirable return of conflict to Europe.

In an increasingly multipolar world, defense appears more essential than ever today. While the balance of power and geopolitical alliances are moving at an accelerated pace, there are numerous causes for concern. These include the proliferation of weapons of mass destruction and NRBC (Nuclear, Radiological, Biological, Chemical) weapons as well as, civil and social conflicts due to demographic and urbanization trends in developing countries, global competition for shrinking natural resources, risks of epidemics and pandemics, war and climatic refugees, massive illegal migrations and multicultural tensions.

In this new world, defense is not only essential. It is broader in its scope

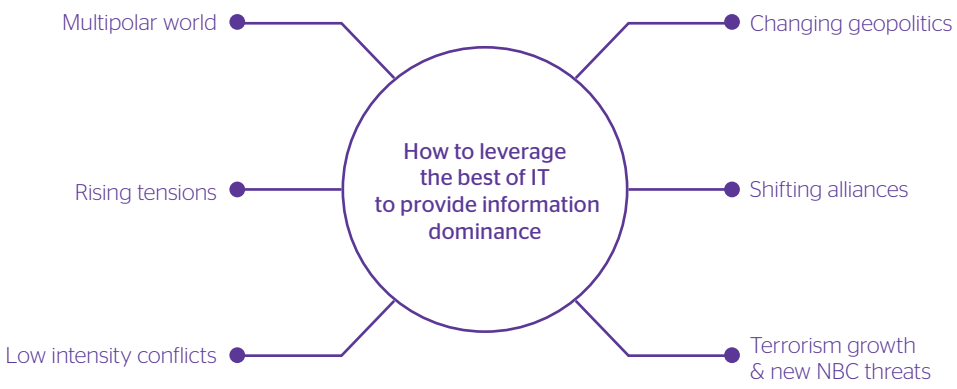
While friends and enemies are merging in an ever more intertwined world, traditional frontiers are tending to fade away. More than ever, defense and security battlefields extend from military to anti-terrorist, economic, financial, mediated and humanitarian grounds on all homeland and foreign territories, with the traditional notion of the "front" extending into a multi-dimensional, ubiquitous chessboard.

These complex defense missions are even strategically hindered as, after having disrupted multiple domains, the digital revolution challenges defense practices themselves. This is happening not only by transforming defense technologies with real-time communications, robotics and automations. It is also transforming the balance of power with the rise of asymmetric and hybrid warfare, as well as opening a new battlefield: cyberspace itself.

New instabilities require a change of paradigm. The defense world faces key new issues: a multipolar world, rising tensions, low intensity conflicts, changing geopolitics, shifting alliances, the growth of terrorism and new NRBC threats.

Atos' vision is that, in this new defense context, key players have to gather and leverage data for guiding political and operational decisions. Indeed, good knowledge of the strategic and tactical environment is essential for preventing risks and threats and neutralizing them when prevention has failed. In this new geostrategic context, defense has to adapt its technologies, doctrine, strategies and tactics to reinvent itself as it has done throughout history.

New instabilities require a change of paradigm



Across the mission spectrum, information dominance is key

For millennia, information has been the essence of war. The ancient Chinese philosopher and army general Sun Tzu emphasized the importance of information in the Art of War: “If you know the enemy and know yourself, you need not fear the result of a hundred battles”.

In the defense and security environment, the control of information is a major strategic advantage for any defense outcome. Information dominance requires mastering huge volumes of data and information flowing between frontline and back-office operational and IT sources. It means marshalling the right information at the right moment, in advance and in a way that is superior to the opponent – even in severe environments and in the face of increasing physical and cyber threats.

While defense battlefields, weapons and attacks evolve, core military values do not change: the effectiveness of command, power, agility, endurance, and morale. But one element takes on a new dimension: the mastery of information. If this has always been the heart of defense strategy, it is now more fundamental than ever in today’s hyper-connected, automated, fast-moving world, where allies and enemies, autonomous weapons and critical infrastructures are just a few milliseconds away on digital networks. In a world where military technologies, assets and battlefields themselves become digitalized, information becomes an essential differentiator for victory.

Defense 2020: A new world of tension

New technologies are at the heart of battle management: the network of “connected autonomous bubbles” is a model for the future

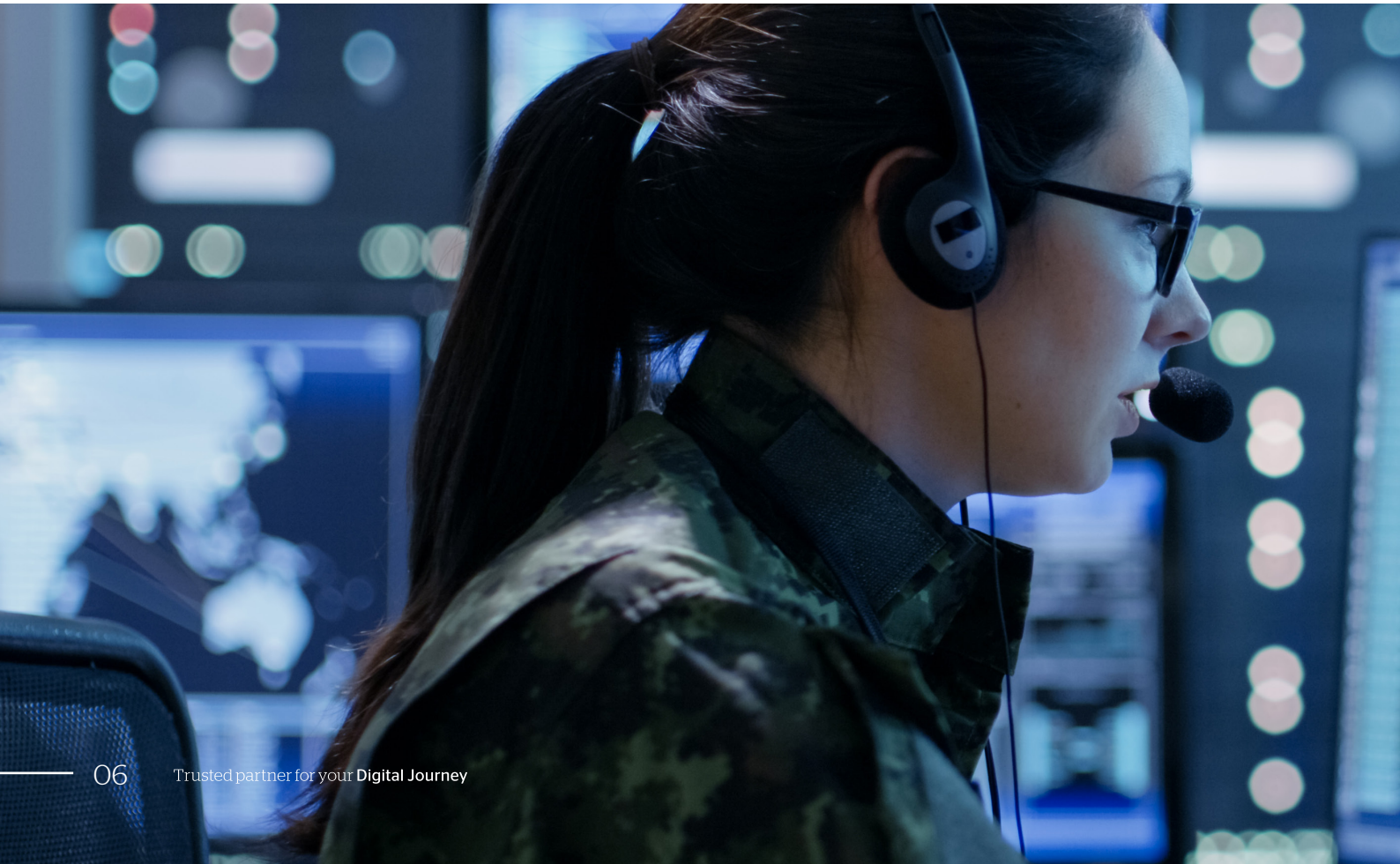
A guiding principle for success is to give each battlefield participant the pre-processed information they need (for example: tactical situation, logistics, weather), in order for them to make the best use of it during the execution of their mission. In this sense, the battlefield is a digitized space where it needs to be possible to collect all the necessary data (some coming from the battlefield, others from elsewhere, e.g. mainland Forces), process it and make it available.

We thus have a notion of digitally autonomous tactical bubbles, that is to say, those with their own data collection, storage, and processing and distribution capacity, through a BMS (Battle Management System).

The strength of the concept is considering all of these tactical bubbles together, as they can and must exchange processed information. Therefore, theaters of operations and individual combat vessels must have a datacenter, a processing capability and of course an exchange and communication capability both internally and with other bubbles. It goes without saying that the adoption of civil-use technologies can greatly contribute to the development of this concept. For example, IP protocol or datacenters can provide additional efficiency. There remains the essential issue of cybersecurity. Increasingly, we exchange data in “open” systems, which in turn are more and more vulnerable.

This therefore requires the best cyber technology available, for example the need to have a local capacity for predictive analysis in order to predict or deal with cyber-attacks.

Therefore, we believe it is highly beneficial to understand the best ways to deploy IT across defense missions so as to build up these new solutions and provide information dominance.



In this context, Atos' vision is that the power of IT, provided it is adapted to the constraints of the military environment, ensures a decisive contribution to the journey towards fully info-upgraded and info-valued collaborative combat.

In particular, it provides a significant advantage in five pillars:

- Collaborative combat
- The augmented soldier
- Tactical high-performance applications driven communications
- End-to-end data management
- Best of breed prescriptive cybersecurity.

Collaborative combat

Defense, and more specifically the area of future combat/warfare, has unique characteristics, particularly in terms of requirements for strength, security and the constraints of available bandwidth on the battlefield.

Digital transformation of the battlefield is a key issue within the evolution of the defense market

The rapidly changing operational environment demands higher levels of agility, resilience and adaptability, in support of virtual and physical battlefields. Scalability is vital to meet ever-shifting defense and security agendas. Agility and scalability go hand in hand with interoperability, particularly across areas of defense where operations require solutions to be deployed easily, rapidly and seamlessly. The key issues are to get tactical and strategic superiority on land-air-sea by sharing the tactical situation on the battlefield, developing land battle management systems (BMS) and combat management systems for sea and air.

New generation of battle management systems leads to collaborative combat

Collaborative systems must ensure fluidity right across the battlefield in order to share tactical awareness of the combat situation in a very user-friendly way and with the possible use of any communication system.

What is new is that it is possible, in particular by leveraging agile methodology, to develop such systems with a strong interactivity with final users in a short-cycle development time. Instead of having long, costly developments, often turning out to have disappointing outcomes, a new generation of systems can be developed together with the forces, which can contribute to shaping its final content. It is also possible to develop modular architectures and distribution in order to keep improving the system even after it has been deployed.

What is even more important is that it leads to a revolution in doctrine. A simple software system can enable collaborative combat, meaning the real sharing of all available information by all the combat stakeholders and make it possible for all actors to update the situation as needed. Again, the idea is to bring the maximum amount of available information to all actors and to let them use it the best way. It is also to foster a collaborative way of working, in line with what we experience every day in our own private experience.

This is a major shift in the way IT systems are defined, developed and used. It is also a shift in culture and mind-set. Previously, information distribution was top-down on a 'need-to-know' basis and controlled through operational hierarchies. A new generation of digital-native personnel are accustomed to staying connected in real time via social media in a hyper-connected world. Now, we are moving towards a more collaborative model through which anyone can share and view information and analytics in real time. Commanders no longer decide what their troops need to know based on information they have gathered. Instead, they make all information available to their troops who are empowered to select the necessary input to execute their mission.

Case study:

Battle management with a real-time and future-ready system

The French government's DGA's (Direction Générale de l'Armement) aims to equip the French armed forces, to prepare for the future by anticipating threats and risks, to prepare technological and industrial capabilities and to promote arms exports.

The main issues for our customer were to ensure that all the actors of a combat group share the tactical situation on the battlefield and update in real time all relevant combat information automatically and in a collaborative way.

With the Scorpion Combat Information System (SICS), based on our Bull technology Bull BMS (Battle Management System), customers benefit from:

- One single battle information system at the heart of France's Scorpion equipment renewal program
- A user-friendly system, with an interface developed with the French forces thanks to an agile methodology
- A technology-agnostic system, compliant with all types of radio systems
- Readiness to equip allied armies worldwide with a system that is designed for France's combat battalions
- Adaptability of the BMS to each country's operational requirements
- All soldiers on the battlefield, from a private to the battalion commander, can share the tactical situation updated in near real time.

This battle management system is the gateway to collaborative combat.

The augmented soldier

The soldier of the future will be the digital soldier. One of the first goals the digital soldier will want to achieve will be to improve soldier efficiency.

In the digital age, the battlefield won't be similar to those of yesterday. Soldiers will also be different.

While the enemy is now mobile and connected, using cyberwar and terrorism as tactics, soldiers must be one step ahead. How should one combat threats in the information and smart machine era? To succeed, it is not sufficient that troops benefit themselves from seamless connectivity to exchange with their squad and their HQ. They also need the tools for collaborative combat, with real-time information and coordination to adapt to any tactical situations. They must get smart support in assessing threats, risks and their own situation, with prescriptive assistance in domains ranging from intelligence to mission and medical assistance. They must be supported by smart, connected weapons and smart machines such as drones, able to help them optimize tactics in combat. Each human life is essential. With digital intelligence and robotics, soldiers will not only be able to get the most our of their forces, they will also be able to reduce the risk of casualties to the very minimum.

Through connected defense and digital approaches, it is now possible to increase soldiers' capabilities

Soldiers' capabilities can be enhanced by giving them real-time data about themselves and their environment. The digital enablers that make this possible are fast evolving.

With this new information now available, soldiers' skills can be augmented by giving them real-time data that enables them to do, know, understand or feel something they could not previously.

Let's highlight a few examples:

- Augmenting the skill to "do something" by starting or stopping an unknown mechanism (for example, an engine) thanks to a digital enabler such as automatic identification of material, access to a remote knowledge base, or remote support through a camera and augmented reality
- Augmenting the skill to "know something" by obtaining the plan of a building and the best way to reach a point thanks to augmented reality via glasses
- Augmenting the skill to "understand something" by understanding an unfamiliar language thanks to automated audio translation via headset
- Augmenting the skill to "feel something" by commanding a remote robot to dig up and deactivate a mine thanks to gloves with force feedback and augmented glasses.

Case study:

Connected Soldiers
Atos builds the future for connected soldiers

The main issue for our customer access the best capabilities of IT to equip the soldiers of tomorrow, who are becoming increasingly agile and connected.

By carrying out a tactical assessment for our client, the French Ministry of the Armed Forces, we were able to test the performance and relevance of the functional benefits brought about by 4G mobile when used by soldiers. For this, Atos integrated its Auxylium communication system into an ecosystem of mobile technologies and connected military objects.

The customer benefits from:

- A software suite that ensures a consistent flow of information between the various elements of the Auxylium ecosystem, the heart of which is the Auxylium Kit: a smartphone, PTT (Push To Talk) headphones and a Hélium case, which enables seamless connection to civil and military 4G mobile networks provided by several types of mobile bubbles
- A new mobile command post model and civil or military connected objects integrated into the Auxylium services
- Capabilities for soldiers to test assault rifles with connected shot counters, drones which are capable of flying a pre-recorded path, tactile watches that can send an emergency call, and laser sight binoculars
- Military operations orchestrated from a robust tablet where the command can follow events and the location of troops in real time and give orders within moments
- Innovative services including: a wireless communication system, which allows soldiers to continue communication via Auxylium in and out of infantry combat armored vehicles ("on-board and off-board"). A true communications hub on a dedicated military frequency, this solution provides a significant level of protection and is capable of penetrating any type of terrain.

The tactical assessment demonstrated the relevance and effectiveness of all the equipment for the connected soldier in the Auxylium ecosystem, which enables high mobility in the combat zone while reaping the benefits of military or civilian 4G networks.

Tactical communications

In the digital defense world, high-performance application-driven communications are needed. Nowadays, it is essential to ensure tactical management through LTE/4G networks and to secure communications with new types of devices in surveillance and combat field operations.

Tactical communications rely first and foremost on the quality of networks

This quality is particularly acute in terms of resilience and the types of data supported.

As well as wired networks (fibre and copper), connectivity incorporates satellite connections, radio connections, 5G, low-power networks (LoRa, Sigfox), WIMAX and LiFi. These new technologies allow new uses to be supported, in particular connected objects and new coding methods. The Internet of Things (IoT), created as the result of the multiplication of the number and nature of connected objects, is already in service in the area of defense (logistics and maintenance). The IoT will soon reach various users in all areas (GPS, biomonitoring sensors, weapon systems, connected binoculars, light drones, sniper detection sensors, NRBC detection sensors, etc.) right up to the connected soldier, together with strengthened cybersecurity.

Connectivity should be understood as a set of complementary systems, adapted to every need. Users define their requirements (flow, range, mobility, environment, safety, etc.). The wealth of connected objects permits users to propose a vast catalogue of solutions easily adaptable to every need.

In order to avoid the saturation risks of traditionally used frequencies, new protocols and technologies are needed. With edge computing, the calculation is managed at the extremes of the network, at the source of the data.

Wireless networks will support low latency and future service quality assurance requirements. Creating connectivity bubbles (at a building, site, neighbourhood, or theatre level) will become simpler. Local networks on a remote site allows content delivery even with limited access to the web. Terminals will no longer be personal; they will be reconfigured according to each individual's mission profile. Interfaces will be much more ergonomic and natural (using voice or gesture command, retina recognition, etc.). The cost of the terminals will be lower. The lifetime of the terminals will be extended through optimized predictive maintenance, with ergonomics, weight, sturdiness and autonomy remaining significant challenges for mobility.

Security, value & real-time capability are three main key success factors for developing new tactical communications within defense

To achieve this, application platforms for secure coordination in combat (BMS compatible) or field patrol & surveillance operations have to be developed, aligned with the specificity and the type of data communicated. These platforms provide real-time communication capabilities, and are highly secured.

ATAWAD (AnyTime, AnyWhere, Any Device) enters the world of defense

4G/LTE communications allow anytime, anywhere, on any device, with transparent network switch depending on bandwidth and security level.

This type of platform, ensuring tactical management and secured communications in surveillance field operations, can be deployed by using optimal IT capabilities. For instance, Atos has developed a unique platform offering a secured and customizable platform with COTS technologies which is already supporting French anti-terrorism forces to protect 66 million citizens.

Based on this experience, Atos offers a modular approach capable of delivering end-to-end LTE solutions to military environments and security.

Case study:

Tactical communication with Auxylium Meeting all defense needs in a single custom-made device for the armed forces

The French Ministry of the Armed Forces is responsible for mixed civil and military operations beyond the national French territory, as well operations conducted on national territory, public security missions and military operations. It has been used in the daily fight against homeland anti-terrorism in the streets of French cities, meeting the urgent need for a tactical communication system.

Its main objectives were to minimize the weight soldiers have to carry so that they are able to move around easily, address urgent operational needs and benefit from an industrial solution in development record time (six months).

With the Auxylium solution, Atos offers the customer:

- A tactical, customized, ergonomically optimized, lightweight, reduced energy consumption and ultra-secure smartphone
- A redesign of the Android operating system for native security with a "digital wall"
- Geolocalized imaging of events on maps or satellite photos
- Capability for immediate multicast voice conferencing ("Push-To-Talk")
- Constant availability with the capacity to switch automatically in real time between the military and the civilian 4G network
- Complete encryption of every form of communication.

The Auxylium solution is an end-to-end implementation with a unique co-innovation process and a successful industrialization phase, completed in record time with agile methodologies, 3D printing, and over-the-air regular delivery of new features to deployed systems. The project provides for the establishment of a management and supervision infrastructure for approximately 1,600 terminals.

End-to-end data management
How to transform data into a new weapon

With the explosion in volumes of data and adaptive, self-learning communications, we are just at the beginning of the journey to fully leverage data for defense. The critical capability is to gather, analyze and share data, to use it to predict and adapt to the decisions and movements of opponents, and to turn it into insights that are actionable throughout the chain of command.

The first step is to collect pertinent data

Meta-data is of higher interest and must be dealt with through specific solutions such as data lakes, which pave the way for new applications thanks to big data and analytics.

An important trend in the evolution of sensors and radars is hardware convergence. Tomorrow, communication data and radar data will no longer be received on different hardware. More globally, data from different technological types will no longer need technology-specific equipment to be captured and collected. The intelligence of data capture is no longer in the hardware, but in the software embedded in the sensors.

The future is in computing power through hardware, and in functions through dedicated software.

The world of civil telecoms with 5G has spread to the defense sector and we are witnessing a technological convergence of hardware that is becoming generic, as well as a virtualization of technological specificities thanks to software functional bricks adapted to data specificities.

What is at stake is how to leverage the new technologies that occur in this field: the Internet of Things, artificial intelligence, swarm computing and quantum technology. One can imagine that it will be possible to collect and process a huge amount of data from the battlefield and from back-office entities. The question is how to leverage them in a way that will provide a clear operational advantage.

Atos envisages new digital systems and collaborations that will make processed data and analytics available for everyone on the virtual and physical battlefield. The paradigm is shifting from the traditional hierarchy of information-sharing and decision-making towards a flatter structure in which information is exchanged, analyzed and acted on in real time in order to empower all battlefield and back-office actors.

The new paradigm can be applied to many fields such as intelligence, logistics, combat management, and training. At Atos, we demonstrate the power of such new contributions in the field of intelligence.

Case study:

15 years of collaboration with state-of-the-art solutions for a data-oriented and scalable platform for the air force of a European country

For this client, the main issues were to rely on a reliable and up-to-date source of information to make decisions related to day-to-day air force operations or critical situations and to have the flexibility to regularly integrate new modules within the platform.

Atos developed a solution with many benefits for the customer:

- Effective mission planning with optimal use of currently available resources
- Standardization and optimization of processes at the air-base level
- Presentation of information in real time for each task
- An integration platform to integrate new systems and exchange data
- Flexible and scalable architecture that enables smooth migration of systems.

Atos mainly relied on an agile methodology and used open source products. The first version was developed in 2003, which created strong customer confidence, and a close collaboration with this client, active in the Air Force sector.

End-to-end data management
How to transform data into a new weapon

When it comes to analyzing the data, and to developing predictive intelligence, the goal is to give sense and intelligence to unstructured data

Predictive intelligence requires a deep sector (defense) expertise as well as proven skills in data analysis.

Information is key. Therefore, future information solutions must converge toward a better and quicker understanding of the situation to optimize and shorten decision times. We can distinguish three different aspects: collecting the information, analyzing the data and exploiting the information.

Thanks to the technology, data is correlated and transformed into information usable to understand the enemy.

Once data has been transformed into information, the next step is to exploit and use it efficiently. And the challenge is not only to know, but also to understand and even to predict enemies' reactions. Therefore, the technology must become a real-time support for decision makers. This real-time support implies understanding the actual situation, the enemy's goals, and anticipating its next moves and decisions.

The next step is information sharing and access: once the information is available, the first priority is to communicate it. With the overwhelming flow of information, the information must be relevant for each group of people in need of it. With too much or incorrect information, it becomes useless; with too little or inadequate information, decisions could become irrelevant. So technology must be able to structure the way the information is presented in order to make it useable and understandable to stakeholders. The solutions must be smart enough to filter, analyze and anticipate as much as possible what information is to be displayed, to whom and when. This must be as smooth as possible, whatever the complexity of the battlefield and the size of the coalitions.

It must be stressed that communication in wars is also highly dependent on reliable networks. As the size of information increases with almost no limits, modern armies need networks with more and more bandwidth, and of course security, resilience and easy deployment.

To give another predictive example, weather prediction errors or technical errors are also no longer acceptable, since the use of data makes it possible to avoid such errors and to ensure virtually flawless prediction. A focus can be made on this specific predictive application: analytics can predict enemy behavior and provide swift decision support, hence the need to gather data to automate processing. Access to data is often the biggest hindrance. The geographical tracking of profiles makes it possible to identify changes in behavior. For example, monitoring is reinforced when the curve of behavioral normality of individuals does not return to normal or when these individuals intersect. The interest of a predictive approach is, on the one hand, to avoid monitoring too many individuals, and on the other hand to answer the question: when will they go into action?

The threat is now globalized and military personnel are poorly aligned with surveillance requirements, so only the democratization of computing and large computing powers make it possible to monitor this threat. 100 new analytic algorithms are developed every year. They are used for mission preparation, mission execution, and mission summary reports.

The enemies are no longer nation states, but mafia-like groups. A target is no longer just a building, a ship or a tank. In fact targets are classified on the basis of their impact. For example to deprive a region of electricity it is sufficient to wreck an electrical tower, which is also less costly than bombarding an entire electrical plant. A defined target must be reached in a very precise way, as new solutions no longer give the possibility for imprecision. To develop such precise systems, seamless extraction actionable insights from multiple sources and types of data have to be gathered and correlated. Intuitive, event-driven and rule-based alerting and analysis have to be provided. Well-timed actions are enabled thanks to deep data analytics and massive computer power (HPC – High Performance Computing).

Data is at the heart of Atos' strategy

The Codex Defense solution, the most powerful and highly secure platform on the market, is one of the four priority growth areas defined by Atos Chairman Thierry Breton. Atos investment in R&D is over 150 million euros. Atos controls the entire value chain, thanks to business partners chosen by Atos. The platform is sized to add algorithmic modules and scale them up. It is redundant on several locations. Atos' 40 years of experience in electronic warfare, its airborne and naval equipment, its intelligence and battle management know-how has led to a natural growth of expertise and these solutions are among the most advanced on the market.

Tactical smart and cognitive cyber physical systems can also learn from data & from their environment

Finally, besides the capture of electromagnetic data to perform strategic analytics, predictive or proactive actions, in the defense market we must also mention the development of tactical, smart and cognitive systems that can learn from their environment and act autonomously in specific time limits and sporadic connectivity with a datacenter. These so-called cyber physical systems see their intelligence develop thanks to big data, and independently detect an event in an environment, analyze the information alone in a cognitive mode, and then take the decision of what action is to be carried out in a few milliseconds. Only the intelligence of these sensors is capable of measuring the impact of this action, which can be for example to send a countermeasure to jam a signal, or go as far as piloting an armament system. After a learning phase of analytics, these cyber-physical systems are autonomous. And of course they can become more efficient when connected to either a network or a datacenter.

Illustration:

Artemis
A sovereign infrastructure, centered on the use of data, for the service of defense.

The Artemis project is a vital issue for the French Ministry of the Armed Forces.

The partnership with Atos will provide an infrastructure focused on big data usage. Many uses could be developed.

The customer's key challenge is, in the context of the defense market, to maintain its military positioning of France at the highest technological level, enabling new defense uses to be accelerated.

The client benefits from:

- A new architecture that will enable it to cope with the constant increase in the volume of data it must process to accomplish its various missions.
- The ability to support any type of data, from any source, in real time, to accelerate decision making
- A geographical distribution of Artemis platforms that does not hinder communication between the different servers, such as a global virtual infrastructure
- A commitment to a very high and unique quality of service and availability rate
- The implementation of a cybersecurity policy adapted to the nature of the platforms, data and users
- A development detached from any software constraint, linked to the choice of open source
- A user-friendly interface, which can be taken in hand immediately by users.

Atos has built on its expertise in the use of agile and DevOps methods in order to develop Artemis. Atos brought in user experience specialists from the defense ecosystem during the design phase. It should be noted that the R&D is French, stemming from Atos, which has partnered with an ecosystem of start-ups and outstanding university research laboratories, to ensure the best service for this project and to benefit from the best of innovation.

Cybersecurity
The core of connected defense

Securing defense strategic assets and organizations is not only about deploying existing solutions and products. It is also concerned with managing cybersecurity, identity and access management, IoT and communications security, and adaptive cybersecurity protection. More particularly, a robust cyber defense strategy requires a combination of technical solutions as well as organizational solutions such as educating public sector servants against cyber threats to mitigate and reduce the weakest links in the security chain: technical vulnerabilities and people.

Atos has a well proven Return On Experience regarding prescriptive threat detection, instantaneous remediation, and weak signal detection by analyzing massive amounts of data and threat-detection before it happens. At that stage, the analysis of risk and impact from all domains will allow the automation of the adaptive response. Consequently, a cybersecurity approach is quintessential to thwart targeted and sophisticated cyber warfare techniques. When dealing with motivated and skilled enemies, and to protect public organizations and citizens in this increasingly unpredictable world, combining a defensive and deterrence approach will achieve the most adaptable, agile and effective results.
An interconnected battlefield offers as many opportunities as it does risks. It is a truly vulnerable cyberspace.

A strong cybersecurity national strategy is essential

As the cyber threat landscape is rapidly changing, and given the diverse profiles of cyber enemies (from nation-sponsored threats to cybercriminal gangs to hacktivists), national security will also depend on a cyber defense strategy.

Any national cybersecurity strategy will need to understand the cyber threats environment and appropriately measure the impacts and counter measures necessary to secure the survival of the nation's economic, military and civil infrastructure.

The following elements should form the key focus of a national cybersecurity strategy:

- Cyber Resilience: protecting and defending the national defense communication and operations from any type of cyber aggression
- Critical National Infrastructure: protecting and defending critical national infrastructure against cyberattacks
- Active Cyber Defense through threat detection and sharing cyber intelligence with key public sector organizations to keep abreast of the emergence of new threats and technology developments, thus pre-emptively protecting and defending the nation
- Regional and International collaboration with partners (nations and the private sector) to reinforce cyber defense mechanisms and improve detection and deterrence capabilities.

Beyond these best practices that should be implemented today, it is of paramount interest to look at the promising new technology that will reinforce cybersecurity in this field

Defense is certainly the sector for which advances and innovations in cybersecurity are most beneficial and should be the subject of rapid Proofs of Concepts. Innovations in cybersecurity include self-adaptive defense, homomorphic encryption, or the management of trusted equipment.

To implement self-adaptive security solutions, more attention must be paid not to protection but to real-time detection and response, so that available defense mechanisms can adapt immediately to detected attacks. It is a question, for example, of detecting whether a presence in the network is legitimate, has the access rights provided for and whether the actor's behavior is completely normal. As mentioned earlier, it is still the techniques of big data that allow this type of solution to be designed, given the mass of information to be processed in real time. These new techniques will thus develop supervision devices, with self-learning machines and predictive analysis capacity, as well as access control or network security devices, which will thus be able to adapt dynamically.

Personal protection technologies (PETs: Privacy-Enhancing Technologies) are technologies that protect or hide personal data in order to comply with the corresponding regulations and ensure trust between individuals. The protection of such personal data requires traditional technologies such as access control or encryption, and technologies that ensure that the use of the data is limited to the intended applications. Recently, new encryption techniques (such as SHM: Somewhat Homomorphic Encryption) have been developed that allow efficient evaluation of certain simple and specific logical functions. Homomorphic encryption is a privacy technology solution that represents an exciting innovation in the field of cybersecurity.

Of course, data can be encrypted before being sent to the server, but to be usable again, it will have to be decrypted, and therefore made vulnerable again. It is this weakness that homomorphic cryptography corrects by allowing calculations to be made on the encrypted data and then to access the final result, which is identical to that which would have been obtained by directly analyzing the unencrypted raw data. Data remains encrypted throughout the data usage process. The Cloud works blindly on the encrypted data and returns the final result to its recipient, who is the only one capable of decrypting, because he has the decryption key. We understand that when it comes to analyzing data stored on a cloud, conventional cryptographic methods are no longer appropriate and that homomorphic encryption provides an answer because it allows operations on encrypted data without ever having to decrypt the latter.

In these much more open environments than before, terminals must have a higher degree of trust. Through its Bull technologies brand, Atos has embarked on the design of ultra-secure terminals. The most sophisticated device is equipped with a biometric sensor, but above all, as for the entire range, its hardware generates encryption keys that protect voice and data communications. As for downloadable applications, these must be validated by Atos engineers: in the Android world, 4,000 applications have so far received the green light, including Shazam or those of Air France or SNCF. The communications ports of the devices are also protected, which is not the case with conventional smartphones. Orange, in this case Orange Cyber defense, which has signed a partnership agreement with the manufacturer, will complete the system with a specific application for encrypted e-mails. This has natural applications in the defense sector with everything connected to battle management or the digital soldier.

Case study:

Cybersecurity with homomorphic encryption
A proof of concept jointly developed by Atos and CEA (Commissariat à l'énergie atomique) to demonstrate the capability to secure industrial digital systems and create autonomous biometric systems

For CEA, a key player in technological research, **the main issues were:**

- To get hyper connected with confidence
- To share sensitive data with an ecosystem without disclosing its content
- To make identity controls with smartphones and smart cards without deciphering biometrics data at any time.

They benefit from:

- A secure industrial digital platform, by sharing sensitive data with an ecosystem without disclosing their content
- Autonomous biometric systems, by enabling identity controls with smartphones and smart cards, without deciphering biometrics data at any time
- Mathematical operation on ciphered data
- Unveiling of data in a hyper-connected world with infinite applications each time it is needed to securely share data in trust, protecting its value at any time.

The cooperation with CEA, which is investing strongly in this area, is a unique opportunity to be ahead of the competition in deploying this technology that will become key in any hyper connected market such as defense.

Main findings and conclusion

The overall trend is clear: military organizations are opting to move towards "infovalued" combat management to benefit from information dominance and maintaining efficiencies and credibility.

Moving to "infovalued" combat management requires a true digital journey and this is not an easy move.

To achieve success, the following three factors need to be actioned :

- Defining a real digital journey roadmap involving all stakeholders and giving in a timely manner all the different tasks to be executed by all actors.
- Proceeding pragmatically with open and flexible architectures: the concept of tactical bubbles mentioned in this document is an example of this pragmatic approach, which can be implemented by proofs of concept and by all tactical battle units as needed in a standalone but interoperable way.
- Being aware of an uncontrolled process of data deluge: the objective is not to saturate all actors with too much information but to make them able to access to all of it in a more user-friendly way. This requires some continued work on the data dashboard of each actor as well as relying more on artificial intelligence to discharge all actors from useless tasks. More data is an opportunity but also a challenge to tackle.

It is therefore obvious that the evolution of information systems requires the adoption of information technologies, well controlled by IT world actors. They work at the cutting edge of technology information trends and have the track record and know-how to manage the transformation they generate in all concerned organizations. They also know how to partner with pure defense system suppliers in order to build up end-to-end solutions.

It is time to give more responsibility to IT world players in the field of information dominance development.

In addition to their general know-how about digital transformation, they know how to develop industrial solutions with these new development methodologies, such as agility, which allow full interaction with end-users throughout the development process. This interaction generates a full adaptation to user needs, as they evolve through a better knowledge of what is developed and is possible. These new methodologies enhance the need to change the old paradigm of procurement. The question is no longer about selecting a supplier on a rigid specification, but rather about selecting a trusted partner that will bring value and innovation all along the development and run cycle phases.

Atos is fully committed to be the trusted partner in this journey, and through all its assets and deep knowledge of the constraints of the military environment, to bring the maximum value to its defense customers.

Why Atos?

With more than 4,500 security specialists worldwide, unique security technologies across the whole IT/OT chain, and fourteen 24x7 Security Operations Centers across the world, Atos offers unique expertise to support the defense sector in building a resilient and effective cybersecurity strategy.

Our track record demonstrates European roots, global capabilities and cyber expertise in defense sector pain points:

- Atos offers "best of breed" security services and products across the spectrum as we develop our services based on the leading security solutions independent of the hardware layer and our own specialized cybersecurity product suites (Encryption, Identity & Access management, Secure Smartphone).
- Our cybersecurity products are commercialized under the brand Bull, Atos technologies and built on Bull expertise in cybersecurity. Our products hold certifications from European national agencies and are developed in Europe.
- Atos has over 14 Security Operation Centers (SOCs) worldwide and 9 SOCs in Europe.
- Atos has a core set of global customers and proven know-how in managing security environments for its customers. Atos has end-to-end capabilities to address all customers' needs from managed security services and consulting to project integration which is cost-effective for our customers.
- Atos security experts have developed extensive expertise in the security field and are committed to sharing their expertise with the customers.

Atos is committed to innovation and has been leading security innovation programs for the European Union for the past decade through the Atos Research & Innovation organization.

Digital transformation: the journey to Connected Defense

Atos' services portfolio (Battle Management Systems, Hoox for Mission, Auxylium) are illustrations of solutions that harness the power of digital technologies to support the armed forces to achieve their goals.

We propose a bigger digital transformation journey to connected defense, to enable, empower and protect the defense community from the frontline to the back-office.

Roadmap to digital transformation

The roadmap is to have a consistent introduction/timely evolution of the systems to take into account this new technology and progressively move to the old generation of systems to the new digital generation of systems.

This must be managed and achieved progressively to avoid disruption.

It may take up to five years to achieve a radically changed environment to bring the very the best of digital and information technologies into defense and security environments.

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. The 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

Let's start a discussion together

For more information, contact:

Stéphane Janichewski
Senior Vice President
Defense & Aerospace at Atos
stephane.janichewski@atos.net
+33 6 80 74 84 11

CT_1847_180507_RY_B_CONNECTEDDE