Dekelia 15th December 2023

Future of Space Operations

by Dr George Geroulis
Lt General HAF ret.

PURPOSE: *Air Cadets & other students Pre-ideation on the estimated Air Forces future space applications and operations, based on the designed new defense systems' performances and the applied improved innovative technologies, which will update the todays doctrines and Concepts of Operations (CONOPS).*

AIM*: Supremacy of our Air power and dominance in the aerospace area of AF's responsibility*
- *Early perception of upcoming developments,*
- *Appropriate staff training preparation*
- *Timely acquisition of the most suitable air & space means, systems, technologies, & infrastructures*

KEY WORDS

Future: *A timeline of 20 years or more years' timeframe*

Space or outer space*: Is the vast space where all the heavenly bodies move (beyond them and their atmospheres), without a clear boundary between atmosphere and space, due to a gradual decrease in air density with increasing height. The International Aeronautical Federation (FAI) has adopted the so-called Kármán Line, located at an altitude of 100 kilometers / 62 miles, as the practical definition of the separation between Aeronautics and Astronautics. Above 100 km the required speed of an aircraft to fly (produce the required lift) is greater than that required to enter a stable orbit.*

INTRODUCTION

As we try to envisage what air threats we might face in 2040, one thing is certain: maintaining technological supremacy through defense innovation, is a strategic necessity for supremacy of our Air power and dominance in airspace. It is therefore a key consideration within the long-term assessment of the Capabilities Development Plans (CDPs). This long-term strand identifies future strategic factors, related future capability requirements, technological challenges, and opportunities to be considered.

The CDP's Long-Term Capability Assessment of the modern Air Power explores the future capability trends and assesses the standard military tasks over a timeline of 20 years or more years' timeframe. The aim is to provide States' armed Air forces with a wide span of possible factors that may impact future National Air – Space Power[1] (capability requirements) from 2040 and beyond.

---

[1] ***Operations:*** *All the military actions taken place in the aerospace (Defensive & Offensive) plus all the activities held in space (military & nonmilitary) supporting military means & OPS centers*

National Space Power: *The degree of use & utilization of aerospace area and aerospace technology by the state and its agencies. It determines its general power against the rest of the states - neighbors -, acting as a force multiplier in the overall National Power of the country. This is obtained by analyzing the term "**D**egree of **U**se - utilization of space" (Du) by a state in the equation of its total **N**ational **P**ower (P_N).*

$$P_N = P_M \times P_P \times P_O \times P_C \times P_T$$

Where: P_M *= Military power,* P_P *=Political power,* P_O *= Economical power,* P_C *= Coalitions' Power,*

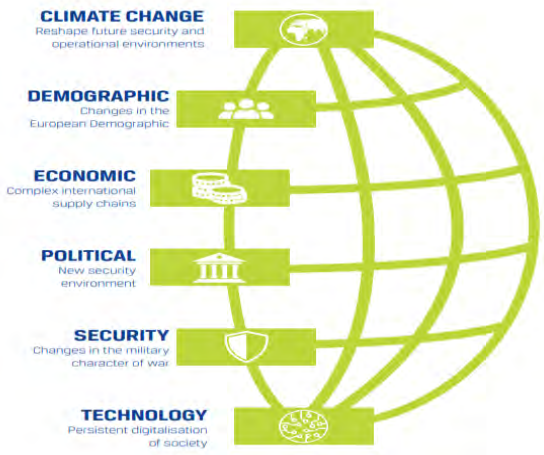
National Space Power is the ability of the state, to control & exploit space or otherwise its ability to control outer space and exploit it for defense or political - national purposes. Undoubtedly, this ability is decisive for the security, independence, and social well-being of its citizens.
This short lecture provides a summary of the factors that will be taken into consideration in the future Space Operations. It also offers a valuable insight into the CDP, whilst also identifying strategic challenges which are likely to shape the operational environment for Air Force beyond 2040.
No one can know for sure what future Air or Space threats & conflicts may arise, but we ought to have the proper capabilities at the ready.

1. FUTURE MILITARY TRENTS ASSESSMENT

To elaborate on this long-term AIR FORCE capability & space operations assessment, the EDA has initiated an evaluation process, according to the CDP short, mid, and long-term periods, is from 2040 onwards.
The assessment process consisted of two main activities, the analysis of the future operational context and the description of the estimated (hypothetical) possible operational scenarios.

1.1 Future operational context

An analysis of the future operational context, considering worldwide geopolitical and socio-economic macro trends, including possible security and environmental challenges is based on a comprehensive review and assessment of official publications and documents, from EU, MS, and NATO relevant entities, referring to strategic and technological foresight in the long term and the identification of specific strategic factor tendencies in 2040 and beyond.



Climate Change: *Climate change could become a possible driver for all remaining trends since the consequences may be exploited intentionally producing significant security challenges.*

Demographic: *The social structure will suffer great changes because of population aging and contracting, the declining power of the middle class, the gender imbalance and uncontrolled migration.*

Economic: *New technologies, along with the higher dependencies on key components, will also have major impacts on employment, demanded skills, and economic opportunities.*

Political: *The growing interdependence of resources between western and eastern states is changing the world balance of power, which is increasingly tilting towards Asia and giving rise to a multipolar international order with greater competition.*

Security: *Social media, propaganda, social engineering, and information control are expected*

$P_T = (P_U \times D_u)$ *= Power of technology (Is the product of the universal technology* P_U *by the State degree of technology use* P_u

to be main drivers of social destabilization, which may be used to promote misinformation, social polarization, distrust, and brain-drain among population.

***Technology** becomes specially relevance in the Grey Zone, driving activities like political and election meddling, cyber threats and attacks, economic coercion, use of proxies, and many other measures – including military action.*

1.2 Changes in the military character of war

Space technologies and hypersonic weapons: Technological superiority is expected to be a major factor in future warfare. The evolution of current technologies and the disruptive nature of new ones will allow significant enhancement of military capabilities but will also pose several challenges for EU armed forces.

*The expected challenge for future technology developments is to reach a **nearly real time situation awareness**. The capability to operate in any domain simultaneously is subject to maintaining a robust cognitive ability and resilience over the adversary, since all actions in traditional domains have effects in the cognitive dimension. As part of the cognitive superiority, it is expected that by 2040 an **enhanced multi-domain operational picture** will be available to develop a nearly real-time narrative unfolding in a particular crisis scenario, as well as to prevail in the clash of truths.*

*Technological advance in **big data analysis** and artificial intelligence driven systems will improve the assessment of the Multi-Domain operational environment and determine how to take and keep the initiative in the 'Battle of the Narrative'. In addition, expected developments in quantum and blockchain technologies should be considered as enablers to create **more robust and resilient communication systems**.*

*An enhanced **cyberspace situational awareness** will be necessary to ensure continuity and early detection of cyber vulnerabilities. The automation of cyber activities, backed by various artificial intelligence algorithms, is an emerging and promising trend that holds immense potential in both the present and the future. The great advantage of this automation over human operators is the **optimization, the self-learning ability, and the speed to handle complex and data-intensive tasks**. Cyberspace situational awareness plays a crucial role in identifying the most effective strategy for utilizing communication and information resources, to generate confusion into the adversary and to minimize the effects of hostile disinformation campaigns.*

1.3 New materials

Technological advances are already occurring at an ever-faster pace. This accelerates the race for technological superiority in many fields such as digitalization, biotechnologies and human enhancement, data management, space technologies, hypersonic weapons, artificial intelligence, new materials, nanotechnologies, manufacturing processes, and quantum technologies.

Increasingly connected and decentralized human networks along with the persistent digitalization of society will bring significant changes to the operational environment. Although the opportunities to access this new digital society are expected to remain unequal, global networks will make instabilities and conflicts more visible to individuals by allowing them to access a wide variety of information about military operations, which may give even more importance to popular opinion.

1.4 Biotechnologies and human enhancement

In the military field, technologies such as human enhancement and new materials will significantly improve the survivability and effectiveness of units and platforms, while the development of novel disruptive weapons (such as hypersonic and directed energy weapons) will bring new opportunities and challenges to the battlefield.

Others, like space technologies, artificial intelligence, nanomaterials, additive manufacturing, and quantum technologies will allow to change the way several military tasks are carried out, including command and control, communications, intelligence and surveillance, engagement, logistics or protection of forces.

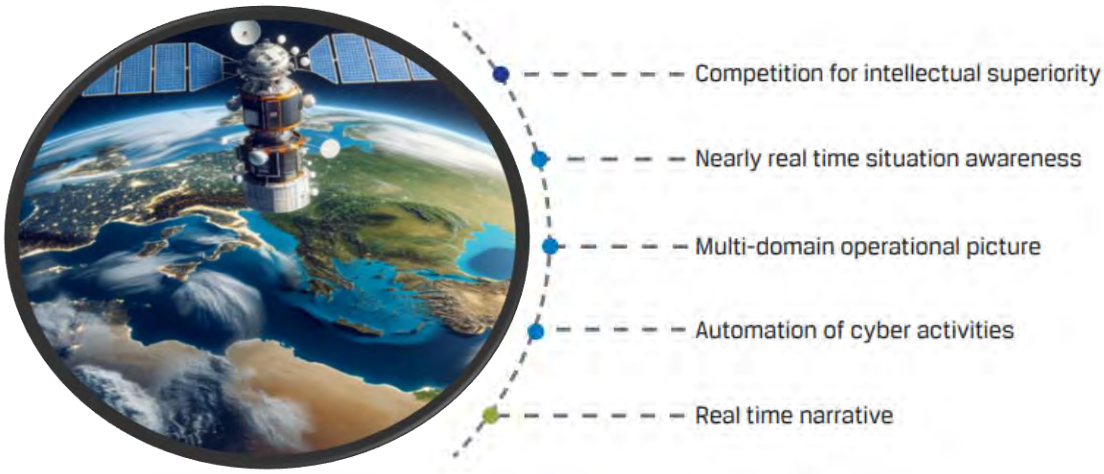
1.5 Quantum technologies

Accessibility and democratization of technology are expected to significantly reduce the technology gap between states and non-state actors, leading military forces, and state actors to ***lose their exclusivity*** *of access to high-end technology and weapons. Non-state actors and even individuals will have greater access to advanced armament and technology, which will open new possibilities for* ***hybrid warfare tactics*** *and* ***increase the risks of confrontations****, even long lasting in the grey zone.*

2. FUTURE CABABILITY TRENDS

The next paragraphs depict the main long-term capability trends identified, describing the associated challenges and the technological leaps. Identification of these capability trends have been driven by the assessment of the need of keeping future military advantage. It is remarkable to note that for these trends to materialize it will be necessary to agree on relevant standardization policies across armed forces and nations.

2.1 Fight for Cognitive Superiority



The extensive use of digital technology and the increasing uncertainty in many fields of society have intensified the competition for cognitive superiority and the conflict over the perception of reality. It will become increasingly important to learn more quickly and constantly ***improve cognitive abilities*** *to gain a significant military advantage.*

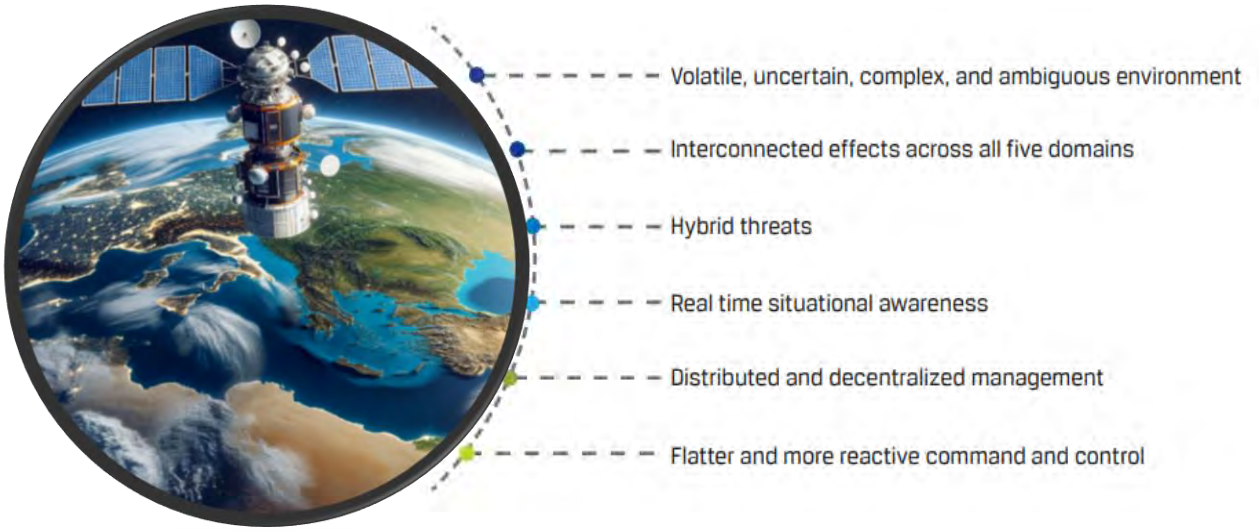
The expected challenge for future technology developments is to reach a nearly real time situation awareness. The capability to operate in any domain simultaneously is subject to maintaining a robust cognitive ability and resilience over the adversary, since all actions in traditional domains have effects in the cognitive dimension.

As part of the cognitive superiority, it is expected that by 2040 an enhanced multi-domain operational picture will be available to develop a nearly real-time narrative unfolding in a particular crisis scenario, as well as to prevail in the clash of truths.

Technological advance in big data analysis and artificial intelligence driven systems will improve the assessment of the Multi-Domain operational environment and determine how to take and keep the initiative in the 'Battle of the Narrative'. In addition, expected developments in quantum and blockchain technologies should be considered as enablers to create more robust and resilient communication systems.

*An enhanced **cyberspace situational awareness** will be necessary to ensure continuity and early detection of cyber vulnerabilities. The automation of cyber activities, backed by various artificial intelligence algorithms, is an emerging and promising trend that holds immense potential in both the present and the future. The great advantage of this automation over human operators is the optimizations, the self-learning ability, and the speed to handle complex and data-intensive tasks. Cyberspace situational awareness plays a crucial role in identifying the most effective strategy for utilizing communication and information resources, to generate confusion into the adversary and to minimize the effects of hostile disinformation campaigns.*

2.2Multi Domain Connectivity "By Design"



*Nowadays, but also further in the future, the operational environment is volatile, uncertain, complex, and ambiguous. These characteristics are accentuated by new technologies and the phenomena of globalization, digitalization, and pervasive connectivity. This defines a competitive environment that goes beyond the traditional domains of land, sea and air and **extends to new domains such as space and cyberspace,** towards actions carried out across all dimensions (physical, cognitive and information).*

*This will also imply the ability to employ forces of different sizes and capabilities, from large scale maneuvers to special operations involving small forces, possibly **unmanned.** Traditional battlefield*

*evolves into a combat situation based on persistent and multi-domain threats, enhanced by **hybrid warfare techniques** and new **high-tech weapons**, to produce interconnected effects across all five domains.*

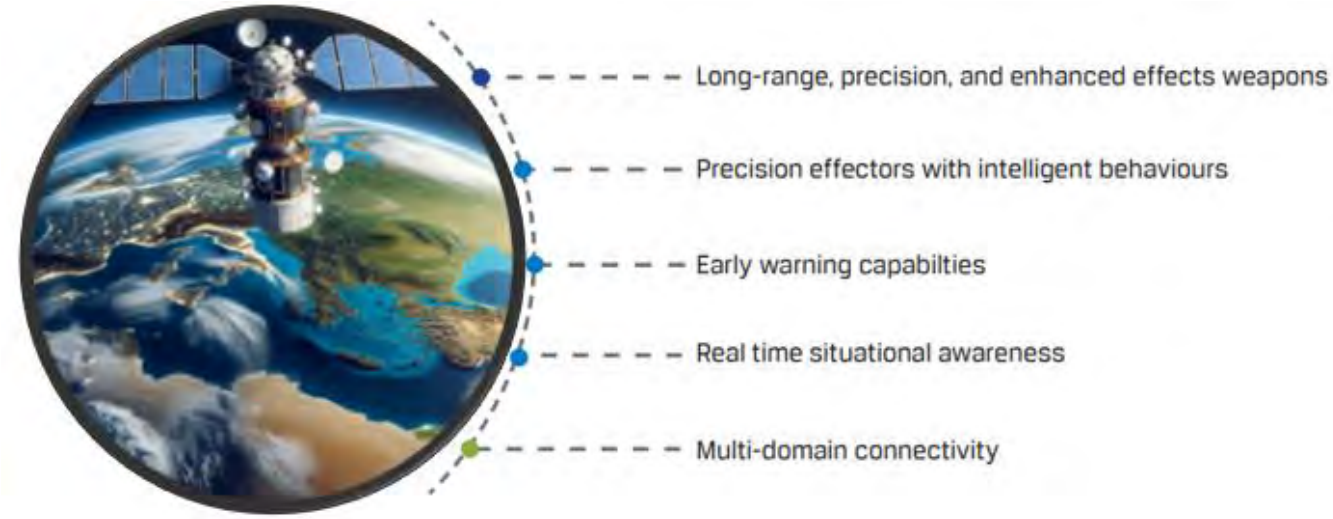
Another relevant element is the possible disuse of the physical frontline concept, in favor of a new type of conflict where actions, including hybrid, take place simultaneously in different spots of the operational theatre, including non-physical domains. In the future, multi-domain operations are expected to be capable of better facing hybrid threats and deterring adversary actions while maintaining initiative and freedom of action.

*Technological developments in the fields of digitalization, communication, and sensors, as well as the ability to analyze, understand, and use data to create actionable information, are expected to require an **enhanced multi-domain operational picture** to keep almost a real time situational awareness. Increasing digitalization of the battlefield will also require strategic and operational planning with decentralized and automated command and control systems to support decision-makers. In this sense, full implementation of the concept of **'combat cloud'**, considering multi-domain and interagency security concerns, will facilitate robust, resilient, and distributed command and control.*

The use of digital technologies for distributed and decentralized management, is currently being implemented in society and will be of standard use in the next decades.

Robust standardization and validation of processes and procedures will provide full integration between different domains as well as with other institutions or entities, both military and civilian. In turn, the inclusion of autonomous systems, decision support systems or automatic data analysis will make possible to define new organizational structures and a flatter and more reactive Command and Control capability allowing better and faster response.

2.3 Pervasiveness of Multilayer Maneuverable Engagement



*The strong development of long-range, precision, and enhanced effects weapons demands integrated air and missile defense systems, including multilayers and robust attrition capacity, to also address the **growing swarming threats**.*

The combination of existing challenges with the application of emerging technologies under development will make it necessary to enhance the integration and the clustering of fully air and missile defense systems. Ballistic missiles, hypersonic weapons and precision effectors with intelligent and swarming behaviors represent threats which are difficult to counter by traditional standalone

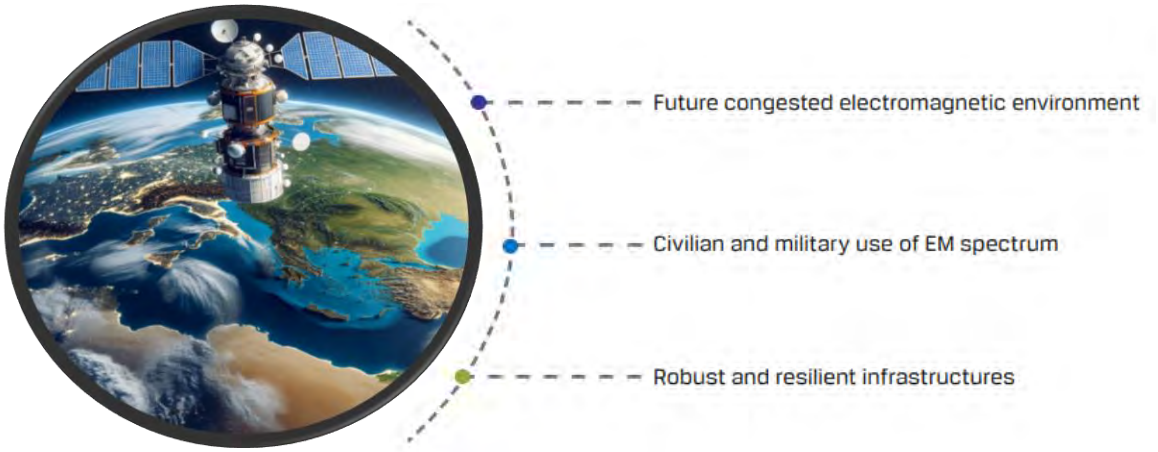
systems. In this sense, aspects such as early warning and the integration of ***advanced sensors****, command and control systems and effectors in extended networks become critical for future protection capabilities.*

Particularly ***hypersonic technology*** *is expected to revolutionize the way air and missile defense is conducted. They strongly expand the attributes of* ***air power (speed, range, flexibility, and accuracy)*** *including maneuverability capacity which could pose a challenge for detection, tracking and engagement. This implies* ***reduced decision time*** *and limited response options. An approach based on multi-domain integrated systems is considered the most advisable strategy to counter this type of threat. A wide* ***network of sensors and assets, including unmanned aerial vehicles, satellites****, and naval and land-based sensors, must act as an integrated data network to detect and react in a timely manner to such threats. The requirements point at the need for a collaborative, integrated and multi-Domain protection network. However, digitalization will also make defense systems more vulnerable to cyber threats and electronic warfare systems.*

Another potential threat is the use of ***drone swarms****. The increasing availability of drone swarms presents a complex threat to counter, due to their size, number, and mobility. This threat has a high potential to evolve considering the low cost and low resource requirement, meaning that both state and non-state actors can gain easy access to this technology.*

The observed general trends exclude a decrease in the likelihood of high-intensity confrontations. In that regard, this trend is of utmost importance to maintain deterrence and the advantage in case of ***peer-to-peer warfare*** *and, to deliver decisive effects on traditional domains (land, sea, air)*

2.4Electromagnetic Spectrum Dominance

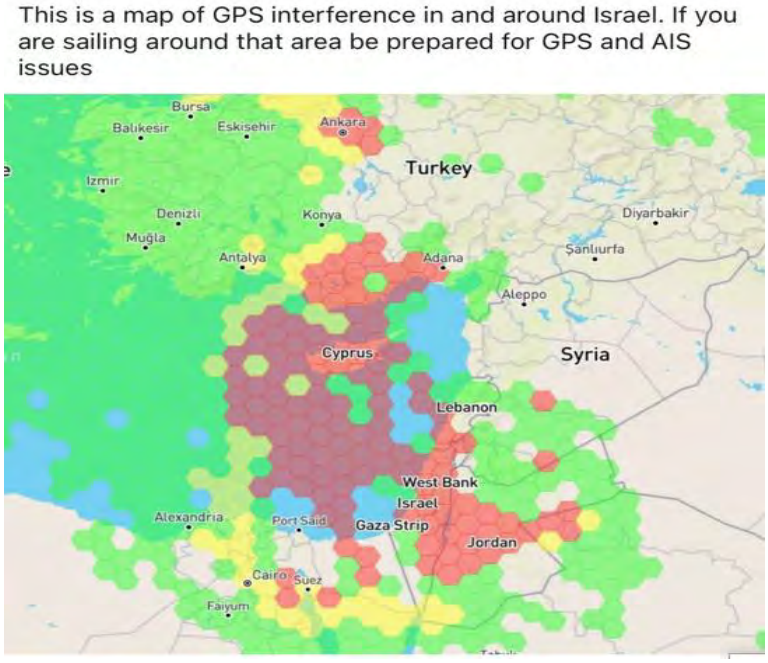


Overall connection and digitalization with an increased use of the electromagnetic spectrum by the military forces constitute a perfect target and ***opportunity for enhanced electronic warfare****. The future congested electromagnetic (EM) environment and its related infrastructure will be even more critical due to the huge increase of data management and communications needs. Consequently, electromagnetic spectrum freedom of use will be a substantial part of future warfare including electronic warfare means, cyberspace situational awareness and resilience of networks, both in the physical and information dimensions.*

Electromagnetic spectrum ***operations (EMSO) have a major enabling role*** *for the planning and execution of military operations in all domains, even increasing its importance and complexity, due to a much more extensive digitized and connected world. Thus, electromagnetic spectrum*

dominance will be a major indicator and a ***paramount component for achieving superiority in all military domains.***

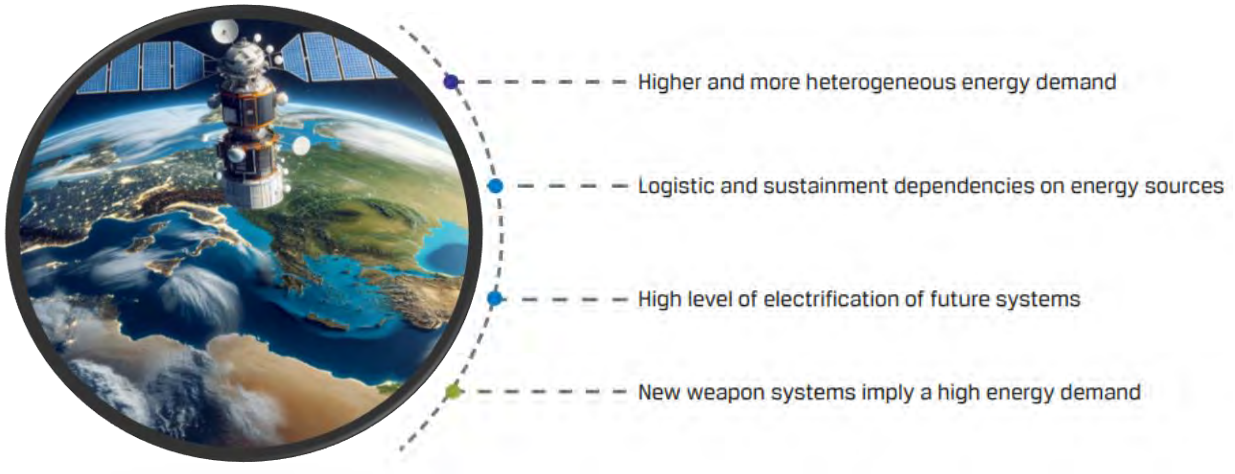
Certainly, the electromagnetic spectrum is used ***for both civilian and military purposes****, sometimes relying on the same assets and infrastructures, and with a growing demand for use. Consequently, the associated challenges for the unrestricted use of electromagnetic spectrum go far beyond the military component, since they affect the whole economic and social development of modern societies.*



Therefore, ensuring electromagnetic spectrum freedom of use is crucial for maintaining the daily activities of modern societies based on a digitized and connected world as well as any military operation.

Consequently, technological developments that allow an advantage over the adversary in the electromagnetic spectrum will be essential. They must succeed in evolving robust and resilient infrastructures able to confront disruptive electronic warfare threats. This should be especially implemented to protect critical infrastructures (including physical and virtual networks). Cognitive superiority and artificial intelligence technologies may improve operations in the electromagnetic spectrum and help managing the complex and highly congested specific environments.

2.5 Heterogeneous Energy Availability for Operational Environments



Future battlefield, with higher levels of digitalization, presents a higher and more heterogeneous energy demand. Itincludes the ***need to generate, store, transport, manage and distribute energy*** *most efficiently. This will be particularly relevant due to the proliferation of unmanned autonomous*

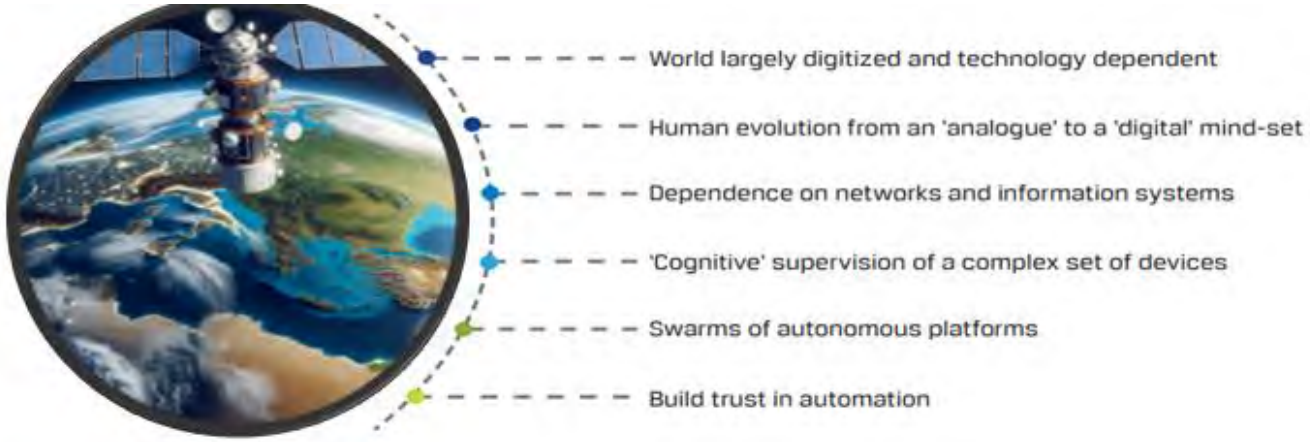
systems, coupled with increasing battlefield sensing, directed energy weapons, and the trend toward platform electrification and other alternative propulsion systems.
This high level of electrification will have an impact on generation, but also on logistics and transportation associated with storage systems. In turn, ***new weapon systems imply a high energy*** *demand at very specific and unforeseeable moments. In the same way, bases and infrastructures in operational environments will need to be more efficient and self-sustainable, also considering climate changeenvironmental disruption and possible widespread shortage of resources.*
Besides efficient and sustainability, other critical requirements refer to ensure energy and power availability and reliability. Power and energy developments, including the overall trend to leverage renewable sources of energy, should cope with future increasing battlefield power demand anytime and anywhere.
As operational energy requirements will be higher and heterogeneous, a comprehensive battlefield energy efficiency,robustness, security, and readiness approach should be implemented. Several technologies will support energy generation solutions (for instance ***new micro modular nuclear reactors and fuel cells****), storage (supercapacitors or advanced high-power batteries among others), management and distribution systems (smart grids and predictive energy management models) will be essential.*

2.6 Extensive Space Capabilities: from Enabling to Shaping the Future Battlefield

The reliance on space capabilities will significantly rise as ***the nature of warfare continues to change****. The development of smaller, cheaper, and easier to deploy satellites will make space an increasingly accessible and contested domain.*
Space assets are foreseen to shape the operational deployment of many capabilities in all traditional domains, such as improved beyond line-of-sight communications, permanent and real-time surveillance, support for precision weapons as well as for sources of fire detection, intelligence and ensuring effective command and control. Future military operations will depend on the expanded use of space capabilities as key enablers for cognitive superiority, intelligence, and high bandwidth communication, and to provide direct effects in all other domains.
In consequence, space assets will have to be robust, reliable, resilient, and redundant to keep high operational availability. Developments in the field of automated self-healing systems as well as higher maneuverability ability can contribute to making those assets more robust.

New launchers *to enable the rapid commissioning of assets will be also paramount to ensure a responsive access to space. Besides, reducing the cost of these launches will increase the specific technological competition, to achieve and* ***keep the strategic advantages*** *offered by this domain.*
Armed forces will ***need to develop the related doctrine, training, tactics, techniques, and procedures to optimize the deployment of space capabilities*** *and to shape military operations in all other domains.*
On the other hand, since space domain will be a field for strategic confrontation, adversary space capabilities constitute a threat, and ***protective measures will need to be developed****. Each asset will be vulnerable to intentional interference and disruption like jamming and spoofing, space debris, intentional kinetic attacks, and a wider range of technological threats. Protection requirements will not be limited to providing better orbiting and maneuver capacities but include passive measures to mitigate the exposure to disrupting or harming the asset performances.*
Another relevant aspect is that the space sector today is significantly impacted by commercial entities. Several companies and organizations are expected to develop new space technologies with high dual-use potential to provide commercial services. Armed forces should adapt their acquisition and services provision processes to maximize collaboration where applicable, keep the technological advantage and secure critical information.

2.7 Coexistence of Analogue and Digital Defense Mindsets

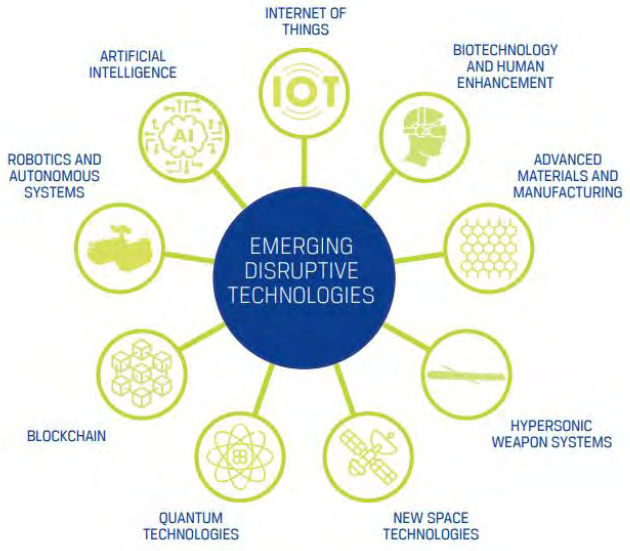


By 2040 and beyond, it is expected that the world will be largely digitized and technology dependent. This will result in a shift between generations' mindsets, with a greater number of people having been raised and educated in a digital environment. This shift will affect the armed forces, with a transition period required to accommodate the ***different basic abilities****. Likewise, legacy military equipment is designed and developed over a long period with co-existing analogue and digital approaches.*
Exploiting all the advantages entailed by technological development requires a gradual evolution from an 'analogue' to a 'digital' mindset, as well as the adequate coexistence of both.
The increasing level of connectivity is producing (with an increasing trend) a strong dependence on networks and information systems. Vulnerabilities associated with possible dysfunctions or intentional actions in the digital environment have crucial relevance.
Another critical aspect refers to society possible evolution, coming from future advances in biotechnology, nanotechnology, machine learning algorithms, and advanced materials, as well as from the significant changes in the ***younger generations' education and attitude towards the digital***

and analogue dimensions. *These technologies will enable a new generation of cognitively enhanced soldiers, more interconnected and with a better understanding of the battlespace.*
Developments in miniaturization, advanced communications, augmented reality, artificial intelligence-enabled systems, or human-machine collaboration will evolve the concept of system operation from a 'manual' control towards a 'cognitive' supervision of a complex set of devices, systems, and swarms of autonomous platforms. Armed forces must be adapted to this changing situation and develop a culture that embraces digital technologies but enables personnel to understand benefits and potential associated risks and hazards.
Regarding autonomous systems, the risk of overwhelming reliance on their use must be considered before developing military capabilities highly dependent on autonomy. Armed forces must develop the appropriate tools which allow them to build ***trust in automation****.*
Finally, it is essential to maintain operational readiness and capacity in degraded environments. As the global security situation continues to evolve and become more complex, military forces must be prepared ***to respond to threats in a variety of environments and conditions****. To do so, they must be capable of rapidly adapting to all fast-evolving operational environment.*

3 TECHNOLOGY IMPACT ON FUTURE MILITARY CAPABILITIES

The following sections are introduced by a short description of the EMERGING DISRUPTIVE TECHNOLOGIES (EDTs), as the main purpose is to look at them from the capability development perspective, to describe possible military applications and next challenges to be considered as part of the future battlespace.



3.1 Internet of Things

The concept of the Internet of things exploits the deployment of numerous sensors allowing the real-time information collection and analysis of the environment, as well as the persistent monitoring of systems and platforms. The primary objective of this approach is to enable the remote supervision and management of devices, providing valuable insights into the surrounding environment, which facilitates informed decision-making.

The use of extensive networks of sensors deployed in all domains, devices and platforms will offer a ***decentralized environment*** *that provides a common operational view of the situation and will provide valuable data to support decision-making once analyzed. Combined with others, these technologies will also provide greater supply chain visibility and* ***improve supply and maintenance operations****. Real-time information about status, position, speed, fuel, and other parameters of equipment, systems, armament, and ammunition will help to improve sustainment and reduce the costs associated with deployment and mobility.*

For air defense systems, the use of extensive sensor networks that provide real-time information will help to detect and counter new airborne threats such as autonomous systems, swarming threats or hypersonic missiles that have different attack vectors from traditional platforms.

From the soldier's perspective, one of the most significant applications is the use of portable devices in support of ***health monitoring and medical treatment****, making use of technologies such as biometric monitoring or augmented reality. This will have a direct impact on the way operations such as combat search and rescue or medical evacuation are conducted.*

Internet of things provides ***support for military training and education****, monitoring personnel either in operational or remote environments. Together with other technologies, such as big data or augmented reality, it also helps to recreate complex environments based on real data offering more efficient, fast, and realistic training in secure environments.*

On the other hand, the main concern regarding internet of things refers to cybersecurity. It makes systems more vulnerable to cyber-attacks, and the need for high-capacity wireless networks will require a better protected use of the electromagnetic spectrum. Another significant challenge refers to the need for interoperability among the different connected devices. Many suppliers, technologies, and protocols demand that interoperability standards must be established to ensure proper implementation and performance.

3.2 Artificial Intelligence

Artificial intelligence-based systems are valuable tools with multiple applications in the military context. Over time, artificial intelligence is expected to take over some parts of decision-making processes. Appropriate verification and validation measures are critical to ensure the effectiveness of the decisions taken by these algorithms.

Certainly, one of the main uses of artificial intelligence is its applications for autonomous systems. Some existing systems are already capable of autonomous maneuver and decision-making. The eventual application of autonomy to the entire engagement chain has ethical and legal implications which must be addressed in terms of clear rules of engagement and definition of the human role in the decision-making process (i.e. in the loop versus on the loop).
The necessity to maintain an effective response to the use of such autonomous system by adversary will drive the conversation in the future. Artificial intelligence applications are envisaged in cyberspace due to its ***ability to analyze data and identify weaknesses, to allow cyber offensive and defensive actions.***
From a strategic perspective, it can have a significant impact on ***strategic deterrence****, such as the ability to detect and collect information related with strategic weapons, which can change the geopolitical landscape and affect nuclear deterrence postures. Together with other technologies, such as additive manufacturing and the use of digital twins, it will have a significant impact on military logistics, improving efficiency in the supply chain and equipment maintenance.*
In addition, artificial intelligence will also improve human cognitive capabilities, such as translation and native language understanding: it will also play an important role in analyzing unstructured information to improve intelligence capabilities, including applications such as managing disinformation campaigns and identifying fake news. It should be noted that a critical challenge is identified in the lack of adequate standards and procedures for proper verification and validation of artificial intelligence-based systems.
Finally, it must be underlined that a gap in the development of this type of technology might represent a significant threat to security and Defense.

3.3 Biotechnology & Human Enhancement

One of the key applications of biotechnologies and human enhancement technologies is the ***ability to monitor the combatants and their surrounding in real time****. This will enable more accurate diagnosis of their health, mood, and general status as well as help to provide a better situational awareness. Multiple sensors can be integrated into the soldier's clothing or equipment, to monitor various parameters and automatically recommend actions. Regarding the soldiers monitoring, the* ***use of micro-sensors or augmented reality technologies will help to use real-time information and to better control the mission accomplishment.***
The use of unmanned systems requires effective integration of human capabilities with robotics and autonomous systems while non-invasive devices will allow for easy implementation of human-machine collaboration. More invasive integration connecting the brain and/or nervous tissue with computers does not seem feasible in the short to medium term.

Nevertheless, in the long-term these interfaces will allow increased situational awareness and optimization of decision-making processes. Neurostimulation and pharmaceutical technologies could be considered to improve training and instruction, and brain interfaces could be used in the future to stimulate and enhance relevant areas of the human abilities. These technologies enable remote advanced medical treatments that were previously only possible in specific medical facilities. This is possible thanks to technologies such as telemedicine, robotic-assisted surgery, biomaterials, or additive manufacturing.

The use of novel materials and biotechnologies in the military domain presents challenges that must be addressed before their application, including legal and moral implications and the toxicity of nanomaterials. Finally, in addition to ethical and legal concerns, these technologies still present some technical challenges, especially regarding the physical constraints surrounding the engineering of metamaterials with acceptable mechanical, thermal, and environmental properties safe enough for human health.

3.4 Robotics & Autonomous Systems

There are many possible applications of autonomous systems in Defense as these systems are being rapidly incorporated into military capabilities. It is expected that this process will accelerate in the coming years. Their use will be greatly enhanced for information acquisition, surveillance, and intelligence analysis, as well as in routine tasks, such as border surveillance with minimal human supervision.

The use of autonomous systems allows for improved combat capability as the systems are not conditioned by human physical and psychological limitations. The use of such systems in combat could contribute to reduce the risk of losing combatants.

Another application refers to improving transport capacity by automating the transport of cargo and personnel to optimize operations. A combination of manned and autonomous means for transportation allows for redesigning supply networks and achieving better integration between strategic, operational, and tactical transport, and moving towards the concept of ***'on-demand' logistics****. In the future, these systems are expected to play an important role in logistics.*

Israeli C-130J: Supplies dropping in front line of Gaza ops with auto remote parachutes.

They will have an impact on system maintenance and repair using automated management and distribution of supplies across domains, as well as on operational medical support. Both, in combat and in-field hospitals, autonomy will enable faster healthcare tasks and reduce the need for specialist doctors to be physically deployed.

Autonomous systems can also ***be used in electronic warfare tasks to protect the military assets by detecting and neutralizing threats*** *in the electromagnetic spectrum and to perform offensive actions such as signal jamming. The main challenge presented by these systems, beyond the technological development, is determining the appropriate level of autonomy to be provided. This will depend on several factors, including the adaptation of doctrines to ensure their safe employment and compliance with applicable laws and regulations. In particular, the ethical concerns concerning the use of robots in the entire engagement chain and autonomous systems in military operations is a critical challenge that requires in-depth analysis and the development of the necessary legislation and regulation.*

3.5 Advanced Materials & Manufacturing

Advances in new materials and manufacturing techniques have a major impact on military capabilities, and their application in Defense covers a wide range of areas, from new metals and production techniques to synthetic biology, nanotechnology, and stealth designs.

The use of metamaterial-based communication systems in future systems will provide advanced communication capabilities that will make better use of the electromagnetic spectrum. In addition, metamaterial-based antennas will increase power output, improve directionality, and extend the frequency range, making them ***useful in both offensive and defensive electronic warfare****. Metamaterials also enhance the performances of optical and infrared sensors, enabling higher fidelity and wide-area coverage for increased detection and identification.*

In addition, these materials also offer protection from a variety of threats, such as chemical, biological radio and nuclear agents, kinetic impacts, weather conditions, and stealth capabilities for survivability and protection. On the other hand, in CBRN defense field, nanotechnology and self-decontaminating surfaces offer advanced solutions for identification, protection and

decontamination against modern chemical, biological radio, and nuclear threats, enabling the detection of dangerous particles with minimal energy consumption, as well as providing additional active protection.

These materials also enable the development of more enduring equipment or clothing for extreme environments, including ***underwater or for outer space****. They also allow for the modulation of visible, infrared, radar, and acoustic signatures, enabling the reduction of signatures to allow stealth capabilities. Highly efficient batteries and energy solutions benefit from new material developments, enabling the extensive use of electric and hybrid platforms in a wide variety of applications, from portable devices, vehicles, command and control, sensors, and weapons systems.*

Finally, additive manufacturing could transform logistics and supply chains by enabling remote production of parts, components, and supplies, including spare parts for vehicles, weapons, ammunition, and medical supplies. It is important to assess the level of maturity of the technologies in this field, as many of them are still in the early stages of development and are not expected to be effectively applied in the medium term.

3.6. Hypersonic Weapon Systems

Hypersonic weapons are a major challenge due to their different behavior compared with traditional armament and munitions. The specific advanced and revolutionary performances, in terms of speed, maneuverability and trajectory, ***require the development of new detection systems*** *and countermeasures that modify current approaches to air and missile defense concepts and architectures.*

The main advantage of this type of weapon is the ability to hit long range targets quickly and accurately while hiding from detection systems, limiting the adversary's ability to react and countering anti-access capabilities. The incorporation of nuclear capabilities by some actors could be a paradigm shift in ***strategic deterrence*** *and* ***increase the instability*** *of the strategic environment by*

rethinking current nuclear strategies. In consequence, the development of more sophisticated and effective defiance systems is needed at both the tactical and strategic levels. Due to the short response times to such threats, early warning and detection are considered as the foremost enabler to ensure effectiveness of countermeasures.

To enhance detection, it is necessary to establish extensive sensor networks able to detect during the launch phase, with the interconnectivity and interoperability of defense systems across multiple domains.

Architectures based on space sensors, unmanned systems, radars, as well as algorithms based on artificial intelligence or quantum computing to process information in real time need to be deployed. Regarding interception, integrated and layered defence systems are needed for the interception of hypersonic weapons, and ballistic missile attacks.

***Non-kinetic effectors should also be considered as an effective solution**, including electronic warfare systems, directed energy weapons or electromagnetic pulses, especially in saturation attacks. Moreover, such missile defense systems require extensive geographic coverage in tight response time, therefore the cooperation will be decisive to deploy effective capabilities to counter this challenging threats.*

3.7 New Space Technologies

*Reduced technological gaps and decreased production costs are driving the rapid growth of space services, with increased participation of state, non-state, and commercial actors in this domain. The commercial space sector has great potential for growth, offering services traditionally provided by government entities. **Space provides critical services needed during military operations**, such as communications, observation, and sensing, which are enhanced by the development of space technologies, leading to a significant improvement in the planning, execution, and assessment of operations.*

Space based Communications enhance surveillance, intelligence and C2, and enable multi-domain operations while relying less on ground infrastructure. Observation enhances early warning and target analysis services, enabling real-time and comprehensive threat and damage assessment on the battlefield.

*The strong growth in the use of space by multiple actors means that this domain is becoming an environment of confrontation, where the competition for space dominance, as well as the access denial to potential adversaries, is an emerging reality. **Space assets equipped for engagement**, surface systems able to engage space assets, or even space debris' risks,* are current and future threats *that require the development of appropriate protection measures. Maneuvering capabilities, protection and redundancy are required to minimize the possible loss of a platform in service.*

*On the other hand, commercial entities, enhanced by increasing private investments, are leaders in developing new space capabilities. To **ensure autonomy in the use of space services** from a military perspective, regulatory requirements related to rights of use, and coordination of space activities need to be addressed.*

3.8. Quantum Technologies

Quantum technology exploits the principles of quantum physics in technological applications, and its impact has been observed in several fields, such as computing, sensors, and communications, improving data collection, processing, encryption, and transmission. Quantum technologies may ***be employed for defensive and offensive operations in cyberspace****, enabling new attack vectors and increasing the effectiveness of traditional hacking methods.*

The transmission of information and the security of communications will benefit from quantum technologies, which will enable secure connection and interoperability between military systems and devices on the battlefield, such as drones, aircraft, ships, soldiers, and command and control systems.

Concerning command and control, the combination of artificial intelligence and quantum technologies will offer advanced decision support tools, enabling the development of more effective and distributed command and control capabilities, to allow a more responsive assessment of the fast-changing operational environment.

They will also improve surveillance, reconnaissance, and multi-domain intelligence by providing higher accuracy, sensitivity, and data processing capabilities. In the underwater environment, these technologies will enable better target detection and effective sub-surface communications.

The maturity of these technologies can vary depending on the specific applications in different domains and specific implementation challenges related to resilience and robustness of systems. One of the main challenges is to implement them gradually without revolutionary requirements changes, thus avoiding unfulfilled expectations and mitigate the associated risks. A major challenge to consider is the impact of quantum encryption on legacy systems with outdated cybersecurity protection. These legacy systems may not be compatible and require significant upgrades. Furthermore, these weak points of the military networks could hamper their use and compromise the overall security of the operations.

3.9 Blockchain

Blockchain allows information to be recorded in a distributed and secure way, creating immutable digital records applicable in transactions, communications, and supply chains, to ensure

privacy and data integrity. The use of this technology for Command and Control ensures the authenticity of information and the proper transmission of orders, leading to more accurate, agile, and automated execution.

Regarding ***cyber defiance, it provides an additional layer of security****, enabling authentication and validation of data in real time and making it difficult to manipulate or detect by potential adversaries. It also improves the efficiency and security of logistics and supply chains by enabling visibility of the entire supplier network, guaranteeing the origin of parts, and facilitating traceability. It also enables the identification of the entities involved in the whole maintenance process, as well as the certification of parts and components.*

On the other hand, the implementation of blockchain-related technologies faces different challenges, including scalability, energy consumption and regulation update. Regarding scalability, it should be noted that blockchain has certain limitations in terms of computing and storage requirements. This is certainly a technological challenge that will need to be addressed, since it will be crucial for the uptake of these technologies into effective military capabilities. Energy consumption is also a current factor to be considered and it is necessary to work on the development of more sustainable and energy-efficient blockchain solutions. Within the defense sector, it is necessary to adapt the appropriate policies for implementation and use of blockchain, as well as assess the impact it has on doctrine and procedures.

4 FUTURE REQUIREMENTS FOR MILITARY CAPABILITIS

4.1Command Capabilities

Command capabilities are mainly influenced by those technologies related to information management and communications. Thus, technologies such as Internet of things, machine learning or blockchain will be critical for this capability area where cyber capabilities will be used both for defensive and offensive purposes. ***Future communications will enable proper interagency coordination****, where an* ***integrated network will be crucial*** *to facing misinformation campaigns.*

Big data and data processing will contribute to assessing the information and framing a robust combined and cooperative combat cloud. Future armed forces will need cyber resilient networks that offer dedicated, integrated, and continuous command and control (C2) applications, data services, and communication during Multi-Domain operations. Command capabilities will require a strategic and operational planning with automated and decentralized C4I (Command, Control, Communications, Computers, Intelligence) to support the decision-making process.

Future command and control systems should apply a distributed approach, resilience towards electronic warfare and cyber threats, as well as adaptability to fast emerging concepts and doctrines. The congested environment will be affected in the future by technological developments, especially those in the fields of EDTs such as new space technologies, autonomous systems and robotics, human enhancement, quantum and blockchain.

***Space domain footprint and redundancy, in particular, will contribute to enhance communications** to enable better interagency coordination among stakeholders. New advanced sensors based on quantum technologies will collect more available data and gain an advantage through situational understanding.*

Therefore, support from quantum computing and automated data processing will be needed to help strengthen the decision-making process. Command, control, and communications will need to be supported by quantum and blockchain technologies to ensure and enhance communication security. Blockchain applications could improve Big data management and strengthen cyber defense, as well as secure defense supply chains and reinforce the resilience of communications.

4.2 Inform Capabilities

Information and cognitive superiority will be a key aspect in the future operational environment, characterized by an ultra-digitized and connected society with vast amounts of information to be shared. Being capable of collecting, processing, analyzing, and transmitting all this data timely and securely will be essential for military intelligence activities. Several technologies will be the drivers of future information capabilities, particularly those related to communications, connectivity, big data management and analysis, and digitization.

*In the future battle for information, **space and cyberspace domains are expected to be the main providers of situational awareness for armed forces.** Cyberspace will be the main channel for storing and transmitting data managed by military forces, as well as the host for all the information shared by society on digital media, which will become increasingly important for cognitive warfare. On the other hand, space will be an increasingly contested domain due to the use of satellites and other space assets to conduct surveillance, provide communications, and collect intelligence. In this field, cooperation with civilian and private sectors will be paramount since they are expected to play*

a crucial role for the technological development in this specific domain. Other technological developments will also bring new opportunities for intelligence gathering, transmissions, and data analysis, such as unmanned and autonomous systems, advanced sensors, internet of things devices, artificial intelligence, and blockchain.

Developments in sensing technologies will allow the collection of higher-quality data by using miniaturized, low-cost, and quantum sensors. Data security will benefit from blockchain technology and quantum cryptography to secure data storage and transmissions, while internet of things applications will create extensive information networks across all domains to improve situational awareness and provide common operational pictures to the commanders on the battlefields. Artificial intelligence will be the key enabler of future data fusion and analysis systems, which are expected to be capable of rapidly analyzing vast amounts of data, extracting valuable information, and disseminating it without human interaction.

Likewise, AI enabled systems will have a significant role in information control and counterintelligence activities, which will also be increasingly important to maintain cognitive superiority over adversaries. The importance of the battle of narrative must also be mentioned since the information from military operations and conflicts are expected to become increasingly available to the public. Cyberspace is expected to be exploited for future misinformation campaigns and propaganda, aimed to alter public opinion, and possibly contribute to destabilize societies. Military forces will need to leverage social media and other relevant media channels to conduct information and psychological operations, as well as to protect population from adversary's influence and misinformation campaigns.

4.3 Engagements Capabilities

Engagement capabilities will be improved thanks to the development of a new generation of weapons and platforms that will produce great changes in the confrontations. Likewise, the use of hybrid warfare tactics, information warfare, and psychological operations will play an increasingly important role on the battlefield.

The implementation of technologies such as new materials, better sensors, and artificial intelligence, among others, will allow the development of smart munitions with greater precision, power, and range. It is expected that the use of this weaponry will allow for faster engagement, at greater distances, and with less risk of collateral damage. Improvements in energy production and storage will enable the development of directed energy weapons (DEW) with increased range and power, allowing their use for a wider range of purposes across all domains. These weapons, both lethal and non-lethal, are expected to be a powerful means of countering several emerging threats, such as drone swarms or hypersonic missiles. Electronic warfare and cyber offensive means will play a major role in controlling the heavily congested electromagnetic spectrum of future battlefields, which will be critical to achieve military superiority.

The development of enhanced and inexpensive sensors will significantly improve electronic warfare systems, which will be a powerful effector against critical infrastructures, communication

networks, platforms, and other critical assets. Likewise, cyber-attacks will be used to disrupt or degrade adversaries' assets remotely and even anonymously, which will bring several possibilities and challenges for military forces. Robotics and autonomous systems will be broadly integrated into military units, performing a great variety of functions in several missions. Autonomous platforms, manned-unmanned teaming, and the related adaptation of tactics will bring several challenges to force protection but will also present new opportunities to carry out missions with less risk to human life.

Human enhancement could also be a disruptive factor for engagement capabilities. Technological developments in the fields of exoskeletons, wearable sensors, brain-computer interfaces, AI-driven systems, augmented and virtual reality devices (AR/VR), and synthetic biology devices will enable significant improvements to soldiers' physical and cognitive abilities.

4.4 Protect Capabilities

Future operational environment challenges and threats will call for major improvements in force protection for personnel, vehicles, infrastructures, facilities, and all military assets. The use of novel materials will enhance physical protections, such as vehicles' armor, personal equipment, and infrastructures, among others. Advanced materials will also enable the development of new medical equipment, such as synthetic biology devices, and better protection tools against CBRNE agents. The effects of climate change must also be considered for physical protection.

Equipment, materiel, platforms, facilities, infrastructures, personnel, and particularly electronic systems will need to be capable of operating in evermore extreme and fast changing environmental conditions. Since the cyber domain is expected to be the place where a vast amounts of critical information for military operations will travel, cybersecurity will be one of the pillars for ***future force protection****. Leveraging new technologies, such as quantum cryptography, AI enabled or driven systems, and internet of things (IoT), will be necessary to protect digitized assets and information networks from cyber-attacks. Cryptography and active cyber countermeasures will also be key to protecting communications and avoiding unwanted interception of data transmissions.*

The extensive use of robotics and unmanned systems is expected to be an essential part of future force protection, since their use in all kinds of missions will reduce the risk to human lives. However, these automated and digitized assets also entail the challenge of their vulnerability to cyber-attacks, electronic warfare, and directed energy weapons. Also, enhanced use of autonomous systems entails the threat of swarm tactics, which will call for enhanced defensive measures capable of dealing with significant numbers of autonomous assets.

Artificial intelligence enabled systems will be capable of automatically generating responses and exposing adversaries' deceptive behaviors and influence, including through social engagements, news reactions, messages, publications, reports to decision-makers, warnings, etc. Likewise, artificial intelligence will allow the coordination of detection systems, automated weapons, and active

protection systems to engage potential threats without human intervention and provide better protection to platforms, facilities, or lines of communications.

Different degrees of automation for security measures will also improve anti-access/ area-denial capabilities with the use of new effectors, weapons, and non-kinetic means, including directed energy weapons, electronic warfare, cyber means, and increased range artillery. ***Advanced sensing means, such as quantum sensors, space assets, extensive detection networks, and miniaturized sensors, will detect possible threats*** *with increased precision and at larger distances. These improvements will be essential to detect and engage advanced stealth platforms, small assets, and fast-moving threats in all domains.*

4.5 Deploy Capabilities

It is expected that future deployment activities will be highly impacted by developments in the field of artificial intelligence, robotics and autonomous systems, human enhancement, as well as the overall digitized and interconnected world.

Readiness and rapid deployment capabilities will be necessary to ensure the capacity to react and confront fast shifting conflicts in an operational environment with increased tempo. Individuals, equipment, infrastructures, logistics lines, and platforms must be prepared for rapid commanding, mobilizing, and deployment, to ensure they are fully operational upon arrival at the theatre.

This will call for more resilient, flexible, and affordable platforms, infrastructures, and installations. The exploitation of hybrid warfare and grey-zone tactics will make surveillance capabilities evermore important in detecting and excluding hostile presence from the theatre.

*Using autonomous systems****, space assets****, and surveillance networks, along with civilian and commercial infrastructures, will be critical to conduct persistent control of adversary movements and identifying possible threats. Interaction with civilian entities will also reduce the number of military facilities dedicated to deployment and ensure the ability to exploit host nation aerial, maritime, and land transport infrastructures, as well as hubs and reception-staging infrastructures.*

In addition, using ***modular and scalable multi-role platforms*** *will be necessary to maximize the tasks of all vehicles and minimize dependence on specific-purpose units. It will reduce the dependence on special purposes platforms, improving opportunities for collaboration, and decreasing the related logistic footprint. In order to improve freedom of movement and safety, most assets, and platforms (ground, maritime and aerial) will need to have sufficient defensive and concealment capabilities to ensure their security and minimize their dependence on external security resources.*

This will call for units suited with detection systems, active and passive protection systems, and more firepower. Using innovative materials, such as nanomaterials and self-healing materials, will allow the development of platforms with reduced weight and improved mobility. Besides, using alternative fuels, such as biofuels or even exploiting electric and hybrid propulsion, could also improve the efficiency of those platforms.

4.6 Sustain Capabilities

The future operational environment will call for major improvements and changes in military sustainment capabilities. Future tactics and technology developments will change many aspects of sustainment tasks, though they will also bring several challenges to logistics and supply chains. Several technologies, such as robotics and unmanned systems, internet of things, and artificial intelligence, among others, will have major impacts on how sustainment tasks are planned and conducted. The wider use of robotics and autonomous systems in logistics will allow to improve overall efficiency while reducing sustainment risks and personnel needs.

These systems could carry out several logistic tasks, including medical treatment, transport of supplies, maintenance, equipment recovery, and support in humanitarian missions and disasters, among others. Particularly, using robotics for medical tasks could improve combatants' survivability by providing the ability to treat personnel remotely and assist them in shorter response time. Improving the efficiency and traceability of sustainment tasks will require cloud-based data networks supported by artificial intelligence models, to provide real-time information to decision-makers, as well as to monitor and plan units' requirements and services. Using these data networks, the logistic systems could take advantage of artificial intelligence enabled systems to manage stocks, plan certain services, and predict specific needs, such as spare parts, medical supplies, personnel services, etc.

Monitoring the status and needs of all platforms, units, facilities, and stocks will also require advanced connectivity and high-bandwidth communications capable of providing real-time information to sustainment decision-makers (internet of the things). In addition, virtual representation technologies such as digital twins and augmented reality devices could be useful tools to improve sustainment services as well, including maintenance tasks, personnel services, or telemedicine.

Likewise, 3D printing, and Additive Manufacturing are expected to be a powerful enabler to reduce logistics footprint with the ability to produce specific components locally, including synthetic biology devices for medical tasks. It will have a significant impact on mobility, therefore on the survivability of the ground-based assets. Another factor to be considered is the impact of climate change on the operational environment, such as natural disasters and fast-changing extreme weather conditions. Supply chains will need to be adapted to the demands that these conditions will bring, such as maintenance services and readiness to also perform an increasing amount of possible humanitarian missions and civilian evacuations.

5 SPACE COMMUNICATIONS

In an era where information dominance is pivotal to national security, satellite communications (satcom) stand as a cornerstone of modern defense strategies. This section explores the intricate technical aspects of satcom and illustrates its strategic importance in national defense, offering a roadmap for leveraging these technologies to bolster military capabilities.

5.1 Technical Aspects of Satcom

Satcom's efficiency is further enhanced through advanced modulation, encryption, and orbit selection strategies. Spread spectrum and frequency hopping techniques mitigate risks of jamming and interception, crucial in maintaining operational security. Geostationary (GEO), Medium Earth

Orbit (MEO), and Low Earth Orbit (LEO) satellites are chosen based on required communication latency and coverage area, optimizing the strategic use of these assets.

Satcom operates across a spectrum of frequency bands, each tailored for specific applications:

- *C-band (4-8 GHz): Balancing bandwidth with resistance to weather interference, C-band is key for stable maritime communications, a vital component in naval operations.*

- *X-band (8-12 GHz): Reserved primarily for military use, the X-band's high resistance to rain fade and secure communication capabilities make it ideal for tactical operations in diverse environments.*

- *Ku-band (12-18 GHz): Favored for its higher bandwidth, Ku-band supports data-intensive applications, including UAV control and real-time video, although it's more prone to atmospheric interference.*

- *Ka-band (26-40 GHz): Offering the highest bandwidth, Ka-band is employed in high-throughput satellite systems but requires advanced error correction techniques due to its vulnerability to weather conditions.*

- *L-band (1-2 GHz): Known for its reliability and obstacle penetration, L-band is used for satellite phones and GPS systems, ensuring constant communication and precise navigation.*

- *S-band (2-4 GHz): Utilized for satellite telemetry and near-Earth communications, S-band is integral to space-based operations and satellite maintenance.*

Satcom's efficiency is further enhanced through advanced modulation, encryption, and orbit selection strategies. Spread spectrum and frequency hopping techniques mitigate risks of jamming and interception, crucial in maintaining operational security. Geostationary (GEO), Medium Earth Orbit (MEO), and Low Earth Orbit (LEO) satellites are chosen based on required communication latency and coverage area, optimizing the strategic use of these assets.

5.2 Strategic Importance in National Defense

Satellite communications (satcom) are fundamental to national defense for several reasons, each correlating with the unique capabilities that satcom systems offer:

- *Enhanced Command and Control (C2) Capabilities: Satcom facilitates instantaneous, global communication between commanders and their forces. This capability is crucial for the coordination of complex military operations across multiple theaters. In modern warfare, where timely decisions can have significant implications, the ability to rapidly disseminate orders and gather feedback is invaluable.*

- *Robust Intelligence, Surveillance, and Reconnaissance (ISR): Satcom enables real-time data transmission from reconnaissance satellites and UAVs. This includes high-resolution imagery, electronic signals intelligence (ELINT), and other forms of data critical for maintaining situational awareness. In scenarios like counter-terrorism operations or monitoring hostile territory, the importance of such real-time intelligence cannot be overstated.*

- *Precision Navigation and Timing (PNT): Satcom systems, particularly those involved in global navigation satellite systems (GNSS) like GPS, provide critical PNT services. These services are essential for the accurate deployment of forces, navigation of vehicles (both manned and unmanned), and guidance of precision-guided munitions.*

- *Interoperability in Coalition Operations: Modern defense strategies often involve multinational coalitions. Satcom allows for seamless communication and coordination among allied forces, irrespective of geographical constraints. This interoperability is key to executing joint operations effectively.*

- *Rapid Deployment and Flexibility: Military operations often require rapid deployment in regions without established communication infrastructure. Portable satcom equipment can be quickly set up, providing immediate communication capabilities in remote or austere environments.*

- *Enhanced Cybersecurity and Resilience: In the face of growing cyber threats, satcom offers a secure communication channel, often incorporating advanced encryption and anti-jamming technologies. This resilience is crucial for maintaining operational security and effective command and control under adverse conditions.*

5.3 Roadmap for Leveraging Satcom in National Defense

To fully exploit the advantages of satcom in national defense, a strategic roadmap should be considered:

- *Investment in Cutting-Edge Technology: Continuous investment in advanced satcom technologies such as laser communication links, high-frequency bands, and next-generation encryption methods is essential. This will ensure superiority in communication capabilities and resilience against emerging threats.*

- *Building Redundancy and Resilience: Developing a diverse array of satellite assets across different orbits (GEO, MEO, and LEO) can provide redundancy, ensuring communication continuity in case of the loss of certain satellites. This approach also mitigates the risk of ASAT (anti-satellite) capabilities of adversaries.*

- *Integration with Terrestrial Networks and Emerging Technologies: Leveraging the integration of satcom with terrestrial networks and emerging technologies like 5G, IoT, and edge computing can enhance data processing and distribution capabilities, crucial for modern military operations.*

- *Training and Simulation Programs: Implementing comprehensive training programs for personnel to handle advanced satcom equipment and deal with potential cyber and electronic warfare threats is essential. Regular simulations and drills can prepare the forces for a range of scenarios, ensuring operational readiness.*

- *Strengthening International Partnerships: Developing and maintaining strong international partnerships for satcom resources can enhance global coverage and interoperability. This includes participating in joint satellite programs, sharing intelligence, and aligning communication protocols with allies.*

- *Regulatory and Policy Frameworks: Establishing clear regulatory and policy frameworks to guide the development, deployment, and operation of satcom systems in the defense sector is necessary. This includes addressing aspects like frequency allocation, orbital slot management, and international cooperation.*

- *In conclusion, the strategic importance of satcom in national defense cannot be overstated, offering unparalleled capabilities for command, control, communication, and intelligence. By following a comprehensive roadmap for leveraging these technologies, nations can not only enhance their defense capabilities but also maintain strategic superiority in the increasingly digitized and interconnected realm of global security.*

6 CONCLUSIONS

We tried to envisage what air – space threats we might face in the long-term period, considering worldwide macro trends. We analyzed the future operational context, and we assessed the future military capabilities, focusing on space operations in a new more competitive environment that goes beyond the traditional domains of land, sea and air and extends to new domains such as space and cyberspace.

The assessment is based on the identified specific strategic factor tendencies and technological foresight in 2040 and beyond.

We anticipate changes in the military character of war due to expectations of the technological superiority. Space technology improvements, hypersonic weapons, nearly real time situational awareness, enhanced multi domain operational picture, big data fast analysis, more robust and resilient communication systems, enhanced cyberspace situational awareness, higher speeds of handling complex and data-intensive tasks with new artificial intelligence applications will mainly support upgraded doctrines for air & space superiority and supremacy.

Hybrid warfare techniques, digital technologies for distribution and decentralization, automated C2 systems supporting decision makers and new concepts of "COMBAT CLOUD" and growing swarming threats with high-tech weapons and air and space platforms, manned and unmanned, will compose the new threat environment.

Electromagnetic spectrum operations will have a major enabling role for the planning and execution of air-space operations in all domains. In consequence, space assets will have to be robust, reliable, resilient, and redundant to keep high operational availability. Developments in the field of automated self-healing systems as well as higher maneuverability ability can contribute to making those assets more robust.

New materials, biotechnologies and human enhancements and quantum technologies will change the existing way of carried out many operational military tasks, including C4I, Intelligence, engagement, force protection and logistics.

Significant operational advantages will be gained with rapid learning and constantly improve of cognitive abilities. Multi domain connectivity "BY DESIGN" will be capable to cover the future offensive, defensive and supporting military needs worldwide.

Internet of things, Artificial intelligence, biotechnology & human enhancement, robotic and autonomous systems, advanced materials & manufacturing will enable the development of more effective, more enduring, and reliable equipment - military systems. New space, quantum and blockchain technologies will provide critical services needed during military air operations in cyberspace.

Space domain footprint and redundancy, in particular will, contribute to enhance communication to enable better interagency coordination among stakeholders. Space and cyberspace domains will be the main providers of situational awareness and cyberspace will be the main channel for storing and transmitting data managed by military forces, as well as the host for all the information shared by society on digital media, which will become increasingly important for cognitive warfare. On the other hand, space will be an increasingly contested domain due to the use of satellites and other modular and scalable multi role platforms and space assets to conduct surveillance, provide communications, and collect intelligence.

Engagement capabilities will be improved thanks to the development of a new generation of weapons and platforms that will produce great changes in the confrontations. Likewise, the use of hybrid warfare tactics, information warfare, and psychological operations will play an increasingly important role on the battlefield in conjunction with AI. Engagements, Force Protection & Deployment, using autonomous systems, space assets, surveillance networks among with civilian and commercial infrastructures will be critical to conduct persistent control of adversary movements and identifying possible threats.

However, all the above mentioned assessments for the future military capabilities and operations with emphasis on the space activities and technological events consist a real challenge for the new blood of the tomorrow Air Forces officers to understand and to contribute with their active participation to the new AIR SPACE TRANSFORMATION from the present to the future with a simple PRINCIPLE DOCTRINE " AIR SPACE SUPERIORITY & SUPREMACY FOR EVER"

Sources:

1. *EPSTEIN,J (1989) Measuring Military Power. N.Jersey, Princeton University Press*
2. *ΓΕΡΟΥΛΗΣ,Γ (1915) ΠΟΛΙΤΙΚΗ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ, ΑΝΑΓΚΑΙΟΤΗΣ ΕΥΦΥΟΥΣ ΠΡΟΣΑΡΜΟΓΗΣ ΓΙΑ ΧΑΛΕΠΟΥΣ ΚΑΙΡΟΥΣ (Τεχνικο-Οικονομική Προσέγγιση Έξυπνης & Ευέλικτης Αντιμετώπισης της Οικονομικής κρίσης και των πολλαπλών προκλήσεων) Ακαδημία Στρατιωτικών Αναλύσεων, Κείμενο Εργασίας Νο 13/ ISSN: 2407-9863*
3. *ΓΕΡΟΥΛΗΣ,Γ (1917) ''Επιπτώσεις της Εθνικής Αμυντικής Στρατηγικής και της Πολιτικής Προμηθειών στην Περιφερειακή Στρατιωτική Σταθερότητα'' ΕΤΗΣΙΑ ΕΠΙΣΤΗΜΟΝΙΚΗ ΗΜΕΡΙΔΑ Α.ΑΚ.Ε., 2017*
4. *Kolovos, Alexander, "**The European Space Policy - Its Impact and Challenges for the European Security and defense Policy",** European Space Policy Institute, ESPI Perspectives 27, p.18, September 2009.*
5. *Νιζάμης Κωνσταντίνος, **«Το Μέλλον του Πολέμου: Υπερ-υπερηχητικά Οπλικά Συστήματα»,** Αεροπορική Επιθεώρηση, Τεύχος 119, Αύγουστος 2020.*
6. *European Defense Agency, (2023) QU-07-23-206-EN-N, ISBN: 978-92-95075-77-1, DOI: 10.2836/360180*
7. *ΓΕΡΟΥΛΗΣ, Γ «**Αεροδιαστημικές Επιχειρήσεις – Χαιρετισμός»** Αεροπορική Επιθεώρηση, Τεύχος 127, Απρίλιος 2023, ISBN 1105-5960*