ACADEMIE DE L'AIR ET DE L'ESPACE
AAE
AIR AND SPACE ACADEMY

DGLR

Deutsche Gesellschaft
für Luft- und Raumfahrt
Lilienthal-Oberth e.V.

The Opinions

COLLABORATIVE AIR AND SPACE COMBAT OPERATIONS IN EUROPE

OPÉRATIONS COLLABORATIVES DE COMBAT AÉRIEN ET SPATIAL EN EUROPE

KOLLABORATIVE MILITÄRISCHE LUFT- UND WELTRAUMOPERATIONEN IN EUROPA

2023 AAE Opinion No. 18 | DGLR Opinion No. 4 10€

COLLABORATIVE AIR AND SPACE COMBAT OPERATIONS IN EUROPE

AAE Opinion No. 18

DGLR Opinion No. 4

September 2023

AAE
ACADEMIE DE L'AIR ET DE L'ESPACE
AIR AND SPACE ACADEMY

DGLR

Deutsche Gesellschaft
für Luft- und Raumfahrt
Lilienthal-Oberth e.V.

Legal deposit: November 2023

ACADÉMIE DE L’AIR ET DE L’ESPACE
Ancien observatoire de Jolimont
1 avenue Camille Flammarion
31500 Toulouse – France
contact@academieairespace.com
Tél : +33 (0)5 32 66 97 96
www.academieairespace.com

DEUTSCHE GESELLSCHAFT FÜR LUFT- UND RAUMFAHRT
Lilienthal-Oberth e.V.
Godesberger Allee 70
53175 Bonn – Germany
info@dglr.de
Tel : +49 (0)228 308050
www.dglr.de

Printed by:
EQUINOX
Parc d’Activités Industrielles de Gabor
81370 Saint-Sulpice – France

ISBN 978-2-913331-97-6
ISSN 2426 3931

Cover photo credits: Airbus, Dassault Aviation, Eurofighter, dvids,
photomontage AAE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

"*Does it connect, does it share, does it learn?*" is a question that should be asked of every owner of air and space combat assets in Europe. It is key to enabling collaborative air operations, which provide the best collective response to any threat despite the diversity of national means involved.

Indeed **collaboration**, involving access to the resources of all military assets to achieve a common objective, goes beyond **cooperation**, which only shares the results of some military assets to meet individual objectives.

Collaboration between assets allows for better sharing of onboard resources than simple cooperation. Increasingly, the value delivered by air and space systems comes from collaborative interactions that leverage individual capabilities: the sharing of data collection, storage and processing power allows operational services to be produced and distributed more quickly. Relevant intelligence and timely, secured orders can thus be promptly disseminated, enhancing overall European responsiveness.

Given the **heterogeneity** of European means and assets, and the proximity of potential threats as demonstrated in Ukraine, the success of European operations relies more and more on the ability to:

- network all military assets;
- move from limited cooperation to full collaboration, when mutually agreed.

Nevertheless, a greater openness to accommodate the diversity of assets creates a risk of **intrusion** by enemy forces that must also be addressed. The maximum collaboration level may therefore vary.

Appropriate organization is required to provide tactical agility and reactivity, and all stakeholders must be properly trained.

Of course, collaborative air and space combat operations will support **multi domain operations**[1] through data and information exchanges to deliver joint military action.

Nonetheless the **air and space** domains share some physical characteristics that deserve special attention in the development of collaborative capabilities:

- global reach and unimpeded communications facilitate the movement of material and data through an obstacle-free environment that can support theatre-wide and multi-domain operations;
- limited in-flight resupply (fuel or weapons) necessitates robust collaborative logistics;
- the three-dimensional movements of air and space platforms result in a constantly and rapidly evolving layout of the overall combat system, challenging connectivity.

This opinion paper proposes recommendations on issues that require specific attention in light of the above considerations. Although the implementation of collaboration impacts humans, hardware and software, as well as their interfaces, we will focus on **digital aspects** that are particularly critical in air and space applications. It should be emphasized that some of these may already be taken care of within the EU or NATO environments. Our recommendations will address the various stages of the lifecycle of any procured military capability.

The **recommendations** (detailed in chapter 5) are summarized below.

R1: Enhance the current hardware-centric combat model with a data-centric combat model (“Software defined combat”) taking advantage of the benefits of the aerospace environment to achieve local and temporary air and space superiority and support multi domain operations.

R2: Develop a complete set of operations according to foreseen scenarios and step down to each global actor: linking intelligence means with ground related assets, global and national Common operating pictures (COP), all current and future piloted aircraft (such as NGWS, Tempest-GCAP, NGAD...) and drones, working with respective national owners, allied armies and navies and special forces.

[1] *Air, space, cyber, land, naval plus information and electromagnetic spectrum.*

R3: Build, use and maintain a complete simulation lab, a “Digital Twin” adapted to all possible allied operations, in order to check the efficiency of all functions needed in each of the strategies envisaged.

R4: Draw up a list of requirements, technical specifications and standards for European air and space collaboration based on EU and NATO initiatives: dual by nature because they include links with non-military structures that can provide valuable data to defence services.

R5: When collecting information on European-based assets (for force generation or capability development), always list interfacing capabilities (technical and procedural) and assess them against the above requirements.

R6: Explore the possibility of a digital platform to manage air data exchanges (Data traffic management), capable of adapting to a variety of coalition situations. Establish relevant governance/decision-making principles for each operation.

Red thread example

Use cases are recommended to illustrate the potential improvements of collaborative air and space combat operations.

The use case detailed hereafter is to detect and neutralize a convoy of long-range surface-to-surface missiles moving from a storage location to a launch site at an unknown time, using contributions from air, space and ground players. It represents a persistent concern because success or failure has strategic implications.

COLLABORATIVE AIR AND SPACE COMBAT OPERATIONS IN EUROPE

1- THE RATIONALE OF COLLABORATIVE AIR AND SPACE COMBAT OPERATIONS

1.1. The war in Ukraine

This war has demonstrated that a collaborative organisation can mitigate factual military inferiority.

"*Everything seen, risks being destroyed*[2]". This sentence illustrates the importance of combining knowledge (*what*) with precision (*where*) and timing (*when*), so that military means, limited in numbers, are not targeted by the enemy and are then directed against legitimate targets, avoiding collateral damage. It has involved combining collaboration in:

- **human** aspects (technical training, solidarity and motivation);
- **material/hardware** aspects (ability to effectively mount and use different physical assets like US-procured missiles on Russian-designed aircraft, standardized plugs for batteries, etc.);
- **virtual/software** aspects (data analysis and correlation by allies, circulation through different networks, cross-cueing target location and identification, radio frequency encryption, strategic communication on social networks…).

1.2. Collaboration or cooperation

Collaboration is understood hereafter as going beyond **cooperation**.

Cooperation means sharing a **result** (e.g. intelligence on a target) with other interconnected entities. This result is obtained by an entity through its internal resources. These entities may or may not pursue the same objective, but they do have a common interest in sharing a result to achieve their own **separate goals**.

Collaboration means sharing **resources** internal to an entity (e.g. sensors), by granting other entities access to them on request or even by publishing availability of those resources. This usually implies that all share a common enough objective to allow external control over their internal resources. It

[2] *Gen. Thierry Burkhard, Joint Chief of Staff, France, January 2023.*

allows maximum exploitation of existing resources but also raises the question of who decides on priorities when resources are limited: e.g. an external request for an internal resource of an aircraft may have higher priority than its current internal use by its pilot. The pursuit of a **common objective** shared by all is therefore important.

Collaborative combat allows **greater effectiveness** than cooperative combat but requires a strong technical and organisational setup.

1.3. The digital transformation

Digital technologies have brought a new dimension to collaboration. They have enabled a massive increase in information collection, transfer and processing for the purposes of situation awareness, disseminating orders, reporting actions and assessing situations:

- they allow for information collection from a variety of **heterogeneous sources**, some of which did not even exist three decades ago (e.g. social networks);
- through standardized sampling, coding and exchange protocols (like Internet protocol – http/IP) they create a sort of **universal digital language**, capable of **translating** every piece of information (text, sound, images...) into a digital file in order to **transfer** it through a global network of terrestrial or radio links;
- processing speed, massively parallel computations and "Big data analytics" have dramatically increased the capacity to **extract on-time relevant intelligence** from the mass of collected information, when the latter is properly "mined" and "tagged";
- "**Artificial Intelligence**" (AI) can provide a "digital partner" to improve the relevance of options offered to the crew, and thus the effectiveness of human actions. It could be used in the case of non-lethal operations, to assist data synthesis and exchanges for managing cyber data, post actions status data…

A need is emerging for **co-learning** within this new Human-Machine team, as well as a demand for explainability and traceability of the provided information and **trustworthiness** of recommendations that will trigger decisions. Human accountability and responsibility are at stake.

1.4. The focus on the air and space dimension

This stems from their physical characteristics and associated impact on collaboration:

- air and space provide an **obstacle-free** environment favouring radio or optical transmissions. Operations take place in a seamless, homogeneous environment, offering global access and reaching interconnecting nodes and unhindered data transfer, which are all at the core of collaborative operations;

- the permanent **3D motion** required for airborne objects makes it challenging to interconnect assets in the air, given high velocities, 3D movements and external limiting factors (clouds, probability to detect and intercept, denied environments);
- also challenging is **access to platforms in flight** and physical transfer between them (e.g. air or space refuelling). Propulsive energy and ammunition are thus limiting factors of airborne operations to maintain air superiority. Collaborative planning and execution can optimize resource sharing between participating countries and mitigate those limitations. Extensive preparation must go into procedures (air refuelling rendezvous or cross servicing), compatible hardware interfaces (connectors, attachments points) and interoperable software technologies to ensure seamless bi-directional data transfer between aircraft and smart (guided) ammunition.

1.5. Enhancing key air and space capabilities

The military effect can be better tuned and controlled by enlarging the spectrum of all EU and NATO accessible means:

- fast detection and reaction from space and air, from very low to very high altitude, by means of intensive information sharing and data enabled services;
- high readiness and availability of assets, through effective supply and logistics, which allows cross usage and servicing of all European and NATO operated assets.

Red thread

- *Cross checking information from a variety of sources with technical eavesdropping indicates high probability of a convoy being launched. Open-source intelligence collects pictures posted on social networks, supported by AI-enabled identification software.*
- *Satellite-based infrared/radar monitoring can detect and transmit the threat data by data link to armed aircraft.*
- *Target engagement is delegated to an on-scene commander, supported by contributing, duly identified assets, authorized to join a dedicated data loop.*
- *Self-guided armaments can be reprogrammed in real time, and/or guided through laser beam designation by drones on mobile targets.*
- *Cyberattacks can disable integrated air defence systems, supported by escort jammers and air-to-air fighter to counter opposing air defence means.*
- *Attack on the convoy is triggered by the on-scene commander, closest to the situation.*

2- THE STAKES

The effectiveness of air and space operations always depends on the technological state of the art. It may dramatically vary depending on different threat types and for a changing context, but operations should always consider the following key principles:

2.1. Credibility and legitimacy

These two principles support and drive a collaborative combat system in Europe based on the founding principles of its nations:

- credibility comes from the ability to deliver military effects where and when required against any target, considering one's own self-protection and the presence of opposing forces ("No place to hide");
- legitimacy comes from the controlled use of disruptive but strictly sufficient power against recognized targets, avoiding unnecessary collateral damages and following a traceable, accountable and auditable decision-making process ("No mistake").

Effective collaboration between stakeholders can actually enhance these principles.

2.2. The heterogeneity of European means and assets

Diversity of means can compromise the success of operations within Europe:

- success relies more and more heavily on the capability to interconnect the different assets and move from limited cooperation to full collaboration when and where jointly agreed;
- at the same time, being more open to the diversity of assets creates a risk of intrusion by enemy forces that must be addressed;
- human, hardware and software aspects should also be addressed.

The proximity of potential threats as illustrated in Ukraine calls for strong, collective reactivity based on collaborative assessment and actions: air and space play a key role in this.

2.3. The impact of emerging paradigms

The effects of these new paradigms must be considered on the envisioned air and space collaborative schemes:

- "New Space" assets and services, which can enhance and speed up access to information collection and dissemination;
- new propulsive means (sustainable aviation fuels, electrical propulsion…) and climate related constraints, particularly on training operations.

2.4. Freedom to choose EU, NATO or a coalition of the willing

Collaborative air and space combat operations within European assets must be accessible whatever the context of operations. As stated in the Strategic Compass[3]:

- "*A stronger and more capable EU in the field of security and defence will contribute positively to global and transatlantic security and is complementary to NATO, which remains the foundation of collective defence for its members*".
- "*The transatlantic relationship and EU-NATO cooperation, in full respect of the principles set out in the Treaties and those agreed by the European Council, including the principles of inclusiveness, reciprocity and decision-making autonomy of the EU, are key to our overall security*".
- "*Boost cooperation with bilateral partners that share the same values and interests such as United States, Norway, Canada, UK and Japan*".

[3] *"Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security", approved by the European Council, 21 March 2022.*

3- IMPLEMENTATION

Collaborative air and space combat operations enhance effectiveness in the following domains.

3.1. Operational military domain

Exchanging information at every stage, from initial requirement to actual employment, is a key to federating existing assets of the aerospace domain:

- preparation of air and space capabilities: collaborative forces must share information when dealing with equipment requirements, development and production of assets (aircraft, air defence, radars...), and education and training of personnel;
- Collaborative Situation Awareness (CSA) in crisis or war time: collaborative forces must share information to establish both friendly and enemy Air Order of Battle in real time:
    - who is where,
    - what/who is threatened by whom (e.g. detect incoming drones, enemy artillery positions, predict and advise potential targets);
- collaborative planning and conduct of operations: who is best placed to counter a threat at a given time considering, for example, enemy movement or firing. Collaborative C2 is essential, defining and delegating tasks and authority amongst coalition assets;
- collaborative assessment of the effectiveness of actions: the sooner the situation is updated, the more relevant the next decision/action cycle.

3.2. Strategic and political domain

Collaboration within all European available assets, whatever the country of origin of their manufacturers, will help keep all options open for European decision-makers to use existing EU or NATO frameworks or to set up *ad hoc* coalitions. This covers:

- the planning and conduct of air and space combat operations using all European available assets, whatever the agreed format, in accordance with political decisions;
- the choice and inclusion of partners in coalition operations;
- the pooling and sharing of resources to develop European capabilities (e.g. connecting R&D facilities, sharing information/specifications through common working environment and pooling and/or sharing data sets for machine learning);
- understanding whether collaborative combat actions are and will remain possible whatever the coalition is. This implies the standardization of interfaces (physical and virtual) and its impact on the performance of the concerned asset. Note that abiding externally defined standards may restrict overall performance.

3.3. Economic domain

Non- or less-collaborative assets will suffer under commercial competition, particularly when technical standards are defined by competitors:

- abiding standards and protocols may negatively impact business modifications of products for companies facing competition. This covers the participation and engineering costs involved to define and promote the standards;
- defining standards and then selling products that meet these standards brings a clear competitive advantage, and often provides more functionalities.

3.4. Technological sovereignty in Europe

- Ensure control and European synergies within key and developing technological areas (quantum when available, AI, cyber, electronic warfare…).
- Define with others, and protect the independence of standardization processes. These processes should not impair Europe’s freedom to set up coalitions and conduct air and space operations: all European nations should be guaranteed access to hardware or software interfaces involved in standardization, whether their provider is in the coalition or not.

4- RECOMMENDATIONS

Executive summary recommendations summarize the more detailed ones below which have been ordered in accordance with the different lifecycle phases of the product. Beginning with "basic principles" that should be considered along the whole process, recommendations are grouped under the headings "pre-acquisition phase and requirements", "project and acquisition phase", and "operations and employment phases[4]". The rationale is first explained and drives the recommendations.

4.1. Basic principles

A collaborative air and space combat system in Europe will not be set up in one go. The following gives some guidance as to the different steps of the development process.

- Collaborative operations rely on **human, physical**/hardware, and **virtual**/software interactions. These should be **checked technically** and operators **trained** before any real engagement.
- Any European air and space asset should be able to be introduced **seamlessly** into existing air and space operations. These assets should be able to replace similar ones and should be used without jeopardising continuity and thus the effectiveness of the overall operational chain.
- Considering current variability in assets interoperability, **different levels** of collaboration should be defined, from limited transmission of information to full participation in the integrated processes of collaborative air and space combat operations systems.
- **Diversity should be turned to advantage** (human, material/hardware, virtual/software) in terms of resilience, by enabling controlled and secured interactions despite different internal design.

Different assets may address the same issue in different ways, thus making the overall system more **resilient**. This is true as long as they are interoperable

[4] *As currently defined by ISO/IEC 15288. Retirement phase is not dealt with here.*

and exchangeable in the value chain. They deliver **operational services**, which are combined together concurrently or sequentially to carry out air planning and achieve objectives.

Such services are usually **platform agnostic** (e.g. “detect a military truck in a certain area”) but require **formatted** inputs (e.g. search area perimeter and desired timing) and output (images and/or vehicle ID, coordinates…) in order to fit into a more global process of intelligence gathering.

- **Someone must be placed in charge** at every step and at any time, to **validate access of accredited stakeholders** to the collaborative processes, whether as service provider or consumer.

Priority 1

R: Ensure that platforms from different countries can exchange and relay data by **free use** of existing standards and procedures, with no technical constraint due to the absence of one nation in a “coalition of the willing” type of operation.

R: Build on existing initiatives to set up a European operated **digital twin** of air operations to spot weaknesses that hamper the overall decision-making process, and foster and fund initiatives to remedy them.

R: Identify **potential bottlenecks** when moving data and and/or material resources necessary to air and space operations.

Priority 2

R: Implement the **CARD**[5] recommendations dedicated to “simplifying procedures, increasing information sharing and providing more specific priorities” to participating Member States (pMS).

R: For some key crisis management or war missions, identify **available services** delivered by air and space platforms in Europe, their **input/output requirements**, and check whether they can be seamlessly called for in a combat situation.

[5] *CARD: “2022 Coordinated Annual Review on Defence Report”, Nov. 2022.*

Priority 2 (cont.)

R: Prepare **portable connectivity** means to be produced and distributed at large scale.

R: Analyze appropriate connectivity of military assets to leverage **civilian clouds and social networks'** redundant data transfer capabilities.

Red thread

Collect European available asset models that could and should participate in the convoy attack and implement their models in the digital twin. Run simulation checks for data exchanges and collaborative software releases to check and analyze:

- *target characteristics, military effects and services required to detect, stop, neutralize the convoy;*
- *which assets will deliver them;*
- *through which channels and whether connectivity is in place;*
- *overall feasibility and risk level of the mission.*

Ensure command authority is clearly attributed and can be practically exercised at all steps of the operation.

4.2. Pre-acquisition phase and requirements

Collaboration begins with the agreement to proceed towards better pooling and sharing of aerospace resources. It should involve governmental and industrial stakeholders to set up appropriate requirements:

- **Governance** options (multinational, EU, NATO...) should be defined for the setting up of relevant data exchange **architectures**.
- Political choices on how to organize forces, how to delegate or how to Control and Command (C2) should not depend on rigid technical choices of the architecture and interfacing standards; **the participation or absence** of any nation or Member State should not prevent implementation of effective collaborative actions through air or space connectivity nodes.

Priority 1

R: Build on NGWS/EDF and other experiences to standardize interconnexions and set up **common working environments** for sharing design and development models and simulation with appropriate security levels.

R: Enable message formatting standardization and cloud computing to circulate timely and relevant information (orders and situation awareness) among **duly authorized** participants.

Priority 2

R: Develop **lessons learned** from Ukrainian conflict "from the danger of cell phones to the importance of a quick-moving industrial base[6]", where combatant citizens using a wide range of unmanned air assets managed to survive and defeat massive attacks.

R: Test scenarios through **wargaming** and **digital twins** to spot vulnerabilities in data and/or material and human circulation when conducting air and space operations involving European forces using existing simulation systems built for previous definitions of operations and functions.

R: Assess **Internet access** requirement, including space-based back up.

Red thread

When developing a new multinational aircraft intended to detect/attack a convoy, circulate among participants the envisioned sensor, airframe and antennae models to check their fields of view once installed.

Run simulations in the digital twin to identify connectivity needs with other stakeholders, define latency and data bandwidth requirements, authentication and approval processes, reporting processes, etc.

[6] *https://breakingdefense.com/2023/02/what-pentagon-leaders-say-they-have-learned-from-a-year-of-observing-the-battle-in-ukraine/, accessed March 13, 2023.*

Extend **ammunition** with two-way connectivity to receive and transmit data (usually collected by the target seeker device).

Increasing ammunition stocks costs time and money. Increasing the effectiveness of each missile avoids multiple firings on a single target and averts collateral damage. Improved, up-to-date target data information transmitted to the shooter and munition reduces emission needs and increases stealth.

Priority 1

R: Ensure that **interfacing standards** (physical and virtual) exist **for guidance and feedback** between shooter/guider and ammunition, and are under European control. If this is not possible, create them so that an aircraft from one nation can guide and collect information from a missile fired from another nation's platform.

R: Also address the risk highlighted by the Ukrainian "wake-up call" on **armament shortages** of "increasing fragmentation and non-EU dependencies".

R: Check and ensure the continuity of the **ground supply and logistics** chain, so that goods or data can be delivered throughout Europe.

Red thread

Estimate munitions type, accuracy and numbers to neutralize a ballistic missile convoy:

- *which aircraft can fire and guide them;*
- *where to store and mount them;*
- *how to ensure positive identification of the trucks;*
- *risk of collateral damage…*

4.3. Project and acquisition phase

Collaborative aspects must be kept in mind when running the procurement, development and production phase of the project. Air collaborative combat in Europe begins with industrial collaboration when developing new assets. Competition for budgets and markets, as well as Intellectual Property Rights (IPR) management, can hamper the success of multinational undertakings.

Business issue: digital transformation reduces, even eliminates entry barriers. IPR have to be re-examined to maintain fair competition.

Priority 1

R: Create an ***ad hoc*** **working group** to examine how to manage IPR in multinational projects with strong digital content.

Air collaborative combat involves exponential data and service exchanges that must be addressed in many different contexts and will evolve over time. We need tools to address the complexity of designing a system of systems[7].

Priority 1

R: Update and use digital twins of the European air and space system of systems to check **standardization and availability** of European owned platform models. Run simulations to check the proper interactions within the system.

R: Define **accreditation processes** to allow login as a recognized participant to the air collaborative system.

R: Develop an inherently evolutive, **service-oriented architecture** (similar to existing commercial models) to collect and match a service offer by a provider to a service request by a consumer.

[7] *SoS criteria: operational independence, managerial independence, evolutionary development, emergent behaviour, geographical distribution (Maier, 1998) + interdisciplinarity, heterogeneity, networked systems (De Laurentis, 2005).*

Priority 2

R: Implement **joint Model-based system engineering** (MBSE), including industries and military collaborating in single shared models and applied to systems of systems.

In particular, the mass of data and the complexity of interactions could saturate and slow down decision-making. This is leading to the development of AI-based exchanges and manœuvres between air and space assets.

Priority 1

R: Define a standard **of data sets**, so that they can be shared easily in crisis (notably those used to train machine-learning algorithms), and **trustworthiness criteria**.

R: Ensure traceabilty and trustworthiness of **algorithms** to maintain and demonstrate certification of assets and legitimacy of air and space actions.

R: Anticipate a European coordinated inclusion of new **data processing** tools that are emerging, such as quantum computing and sensing, reinforced machine learning, microchips, photonics.

Red thread

Detecting and attacking a protected ballistic missile convoy on the move at very short notice will require strong collaboration between a variety of European military assets. When developing a new aircraft, its capacity to integrate this collaborative network (as a consumer and/or provider) is paramount and should be envisioned and checked at every step.

4.4. Operations / Employment phase

This phase covers the concrete implementation of collaborative capacities developed in previous phases. Direct information flows of relevant time and position information lead to decision and actions that allow air and space operations to deliver **appropriate, legitimate and credible** military effects.

This includes the transfer and processing of data, and real-time conversion of data into useable information, without jeopardizing operation security through unauthorized access. This requires an adapted data traffic management system similar to civil Air Traffic Management. It may lead to synergies while respecting military and civilian specificities.

Priority 1

R: Design and empower a **"data traffic management" authority** to coordinate and match, where and when agreed, data-related service providers and consumers, enabling C2 planning and conduct[8].

Priority 2

R: Federate European satellites to set up **a collaborative cloud**, defence oriented.

Europe has a finite number of heterogeneous assets : superiority, even if only local and temporary, requires the most efficient usage of these assets through a maximum of synergies and optimized resource management to reach full situation awareness (SA) covering: collection, comprehension, projection[9].

Priority 1

R: Each European air operated asset with crew should feature a unique **authentication proof** to join and qualify as collaborative service provider and/or consumer.

R: Exploit **Open source intelligence** (OSINT) capabilities, for instance the use of social networks as demonstrated in Ukraine.

[8] *European Air transport command is a good example when dealing with material transfers: it matches contributed aircraft availability with freight or passenger movement requests to deliver hardware mobility services.*

[9] *Endsley, M.R.: "Toward a Theory of Situation Awareness in Dynamic Systems", Human Factors Journal 37(1), 32-64.*

Priority 2

R: Update and disseminate in quasi real time **identification, RF jamming and cyberdefence** algorithms.

Move to Cloud-based command and control (CBC2) through dynamic delegation, exploiting the effectiveness of posting on social networks a requirement to attack a target with pictures and coordinates, and requesting permission for any well-placed shooter to engage it, through a very short decision-making loop.

Priority 1

R: Build on recent combat situations to **pre-identify distributed** C2 delegations and check whether corresponding **data flows** can be secured and authenticated.

Red thread
A very large number of contributors from different countries will be involved, in order to detect, track, target and engage the missile convoy in a timely way despite opposition and decoys, and then to assess and demonstrate the result, and provide feedback to political authorities.

5- CONCLUSION

Enabling collaborative operations is a major challenge considering the variety of air and space assets in Europe. One cannot wait for wartime situations to develop, but should implement concrete measures to build collaborative capabilities in Europe: from the initial requirements and throughout the whole lifecycle, whatever the nationality of the equipment maker.

Notwithstanding the importance of hardware compatibility and seamless human interactions, we focused on data and information circulation among stakeholders. Exchange possibilities have dramatically increased in the last decade: organizing them is critical to efficient and effective collaborative operations, at every step of their preparation and implementation.

This is the rationale of the above recommendations, which deserve full attention in our opinion.

ANNEXES

Members of the working group (AAE and DGLR)

- Claude-France Arnould
- Jean-Georges Brevot
- Georges Bridel
- Bruno Depardon (Secretary / Secrétaire AAE)
- Jean-Pierre Devaux
- Gérard Fouilloux
- Philippe Koffi
- Keith Hayward
- Tobias Heiss
- Winfried Lohmiller (Secretary / Secrétaire DGLR)
- Franco Malerba
- Bruno Mazzetti
- Jean-Paul Palomeros
- Thierry Prunier
- Yves Robins
- Louis Roche
- Claude Roche
- Bruno Stoufflet
- Michel Troubetzkoy
- Antonio Viñolo
- Paul Weissenberg

Interviews conducted for this Opinion

- European Defence Agency, NATO International Staff, Eurocontrol, NGWS and FCAS Teams
- Dassault Aviation, Airbus Defence and Space, Thales, MBDA
- Air Defence Commander, Space Commander, Special Ops Commander (Joint Staff), Special force Brigade (Air Force)

ACADÉMIE DE L'AIR ET DE L'ESPACE
Ancien observatoire de Jolimont
1 avenue Camille Flammarion
31500 Toulouse – France
contact@academieairespace.com • Tel: +33-(0)532 669796
www.academieairespace.com

DEUTSCHE GESELLSCHAFT FÜR LUFT- UND RAUMFAHRT
Lilienthal-Oberth e.V.
Godesberger Allee 70
53175 Bonn – Germany
info@dglr.de • Tel: +49 (0)228 308050
www.dglr.de

9 782913 331976

ISBN 978-2-913331-97-6
ISSN 2426 3931

10 €