Maritime Line-of-Sight Access Points: Conceptual Design Proposal

Draft – Jan 2025

References:

A. Maritime Line-of-Sight Access Points: An Operational View, White Paper, MARCOM
B. OPERATIONAL REQUIREMENT STATEMENT (ORS) FOR 3486-2023-CFC - DIGITAL ACKBONE - NEXT GENERATION WIRELESS (OTHER THAN SATCOM) SERVICES, SHAPE
C. NATO 5G / Next Generation Networks Vision and Strategy (AC/322-D(2023)0043 (INV))

1. Introduction

The objective of this paper is to define the foundational design elements for the Maritime LOS Access Points (MLOS), taking into account the operational view expressed in MARCOM's White Paper (Ref. A). Essentially, the idea is to stimulate focused discussions amongst the different stakeholders, collect inputs and adjust the course of action in order to maximize the alignment between NATO requirements and National planned capabilities. Such coordination and alignment are paramount to harmonize the efforts and promote synergies discovery, which would pave the way for a more suitable Target Architecture (TA) and cater for more accurate budget customizations for the planned projects in the CPP.

In order to facilitate the foreseen coordination and alignment process, and later the decision-making process, an analysis of limited hypothesis is proposed. It is anticipated that multiple approaches and technical solutions would "solve MLOS", but only a limited number effectively are: (1) fit-for-purpose; and (2) fit-for-ambition. The latter is particularly relevant, since the success of MLOS is correlated with an agreeable level of ambition between NATO and the Nations. Level of ambition consensus, coordination of efforts and synergies are key for the success of any CPP.

In order for this discussion to be proficuous and consequential, a common ground among the stakeholders must be established – building a solid and consensual understanding and context for MLOS is the obvious starting point. Furthermore, a well-defined context will set a number of boundary conditions that should naturally constraint the number of adequate options (i.e. options that are fit-for-purpose).

Then, in order to allow for an adjustment of course, a discussion around a limited number of options, through feedback provided by the stakeholders, should facilitate the agreement on a level(s) of ambition. These discussion options should be fit-for-purpose from the beginning,

but they may reflect different levels of ambition. Ultimately, this informed discussion should pave the way to future TA and CPP scope.

Inevitably, it will not likely be possible to converge to a single option/technical solution that satisfies all stakeholder's level of ambition. In this sense, and if need be, the future TA should be able to accommodate different options/technical solutions (or to allow room for capability growth) – that will correspond to different levels of ambition –, in a way that the delivered capability remains coherent.

Considering the above, this paper is outlined according to the following approach and methodology:

- Collation and interpretation of operational needs and context for MLOS (MARCOM White Paper). This step should allows the reduction of principal components that effectively have an impact on the MLOS solution definition, while setting the criteria for fitness-for-purpose;

- Analysis of Capability Development Challenges and Opportunities. The challenges analysis should identify the most relevant implementation constraints, which inevitably limit the suitable options. This is a refinement of the fitness-for-purpose criteria. On the opportunities side, this step should inform on ongoing activities/concepts/initiatives that influence the definition of the options, such as national capability development efforts, ultimately setting boundaries for the fitness-for-ambition;

- Discussion of Technical Options. In this step, a limited number of options/technical solutions is presented and discussed, based on the boundary conditions (fitness-for-purpose and fitness-for-ambition) previously identified.

2. Operational needs and context

The MLOS is aimed to reduce the overall dependency on SATCOM by complementing BLOS AP capacity and maritime tactical internetworking. The combined effect of both shore based line-of-sight (MLOS) and beyond line-of-sight (BLOS AP) capabilities, which should, together with an ad-hoc networking capability afloat, multiply the possibilities of conduct operations in A2AD and C2D2Es. Bringing different bearers together should enable ad-hoc opportunistic hops – on ships within shore LOS – that may extend range beyond the limits of physics.

Still, the required services support footprint shall be achieved not only through appropriate coverage, but also by adequate transmission capacity and coherent delivery. This means MLOS should be able to: (1) deliver a backhaul capability comparable to SATCOM – i.e. Mbit/s – in order to ensure, under certain limits, a meaningful NATO's Wireless Non-SATCOM alternative to extend the outreach of the NATO Digital Backbone (NDBB); and (2) offer service

coherence and seamless service delivery, whenever is possible to replace the BLOS APs service provision. Such an ambitious manifesto imposes interesting challenges on the services provision model and architecture, as well as, on the orchestration of multinational access networks, with federated capabilities and own management capabilities.

Shipboard systems counterpart are not part of MLOS investment component, but are key elements to frame the capability development. Ideally, MLOS should be based on deployed technologies afloat to speed-up the implementation processes, but, unfortunately, the MC-195 does not include any capability that would fit the purpose. Therefore, the end-user infrastructure has to be developed, from scratch, as well. In that sense, MLOS has to be designed and implemented in such a way that it shall be straightforward to adopt and implement on board the maritime platforms. Mostly, two aspects are key to consider: (1) real estate for installations, particularly exterior above-deck space; and (2) electromagnetic compatibility/coexistence with incumbent shipboard systems. These constraints reduce the candidate options for the technical solutions.

Furthermore, in the current strategic context, time-to-operation is a key success factor for a capability deployment. Therefore, MLOS should aim for an Initial Operating Capability (IOC) that shall be based, largely, on readily available products and services that can provide a foreseeable evolution and flexibility to accommodate future improvements. Additionally, it is paramount to consider not only the interoperability amongst different vendors' implementations, but also the radio frequency (RF) spectrum availability to operate with such products. Hence, MLOS shall not aim for sophisticated Electronic Protection Measures (EPM) for an IOC, as this would certainly conflict with the initial priorities of interoperability (through standardized technologies), time/complexity of deployment; and complexity of shipboard installations. Obviously, these shall not preclude future evolutions towards more sophisticated features, including EPM.

Finally, the coherence between NATO and National efforts is paramount for a successful MLOS capability development. While not representing an operational requirement, synergies should reduce implementation costs and risks, particularly for infrastructure that is deployed on National territories. Several Nations have their own programs on MLOS equivalent capabilities to support other-than SATCOM broadband littoral coverage, which include/plan the usage of public and non-public relevant infrastructure. Potentially, such an overlap between NATO and National initiatives enables joint ventures, with obvious benefits for all parties.

3. Development Challenges and Opportunities

In practice, the constraints imposed by the operational context reduced the technical options for MLOS deployment to an IMT based solution. Nevertheless, such circumscription should not necessary lead to any limitations on the final delivered capabilities, because the Next

Generation Networks (NGN), such as IMT/5G, not only satisfactorily respond to the MLOS specific requirements, they also leverage opportunities for partnerships between NATO, Nations and Public providers. The latter are particularly important to address challenges such as extensive coastlines coverage, RF spectrum availability and time-to-deploy. Ultimately, NATO and Nations shared visions and strategies, as in Ref. C, identified NGN, and particularly 5G, amongst Emerging and Disruptive Technologies with high potential for transformation of NATO capabilities and MLOS has been often presented as potential scenario.

IMT/5G based technologies fulfil the MLOS requirements for interoperability, capacity, time-to-operation, long term evolution and sustainability. However, their most remarkable characteristic is the practical deployment aspect, which ultimately influences the operational relevance of a capability: availability and coverage. NGN are highly scalable, flexible and enable multiple levels of integration between public and non-public networks, which opens a wide range of opportunities to architect a solution based on diverse existing infrastructure, rather than developing everything from scratch. The implementation effort can then be centred in the critical elements of the capability, while partnerships with public and non-public providers would ensure the delivery of the complementary components. In other words, the deployment of MLOS should be focused on the development of military/information sensitive elements, while taking advantage of the synergies that would resolve complex, costly and risky areas, such as implementation of own infrastructure − including radio stations to ensure appropriate coverage − and RF spectrum management.

Paradoxically, such flexibility and diversity opportunities pose the most significant challenges for MLOS design. In practice, the MLOS final solution has to harmonize a multitude of combinations of public and non-public infrastructure components, which result from identified synergies with National capabilities implemented under different views and ambition levels. While approaching Security, Complexity, Investment and Functionalities, Nations may have significant disjoint perspectives, so a lack of correlation, between NATO and National approaches towards MLOS capabilities, would force an implementation of NATO Common Funded alternatives and add a variable to the problem. Moreover, one should not expect a clear picture, with respect to National intentions, available at MLOS design phase, so the final architecture shall accommodate such uncertainty, as well.

4. Design Constraints

In addition to the operational requirements, several other factors contribute to shape the MLOS final design. Amongst others, security, mobility/authentication, coverage and investment/O&M seem to be the most critical. The balance and trade-offs between such factors would dictate an optimal solution that fulfils the operational requirements in a cost-effective way, without jeopardizing future evolutions. Security is probably the most notorious factor

when it comes to IMT/5G networks; and it is closely linked with complexity and cost of the adopted solutions; typically, increased levels of security required more complex and standalone systems with obvious cost penalties. Mobility, authentication and roaming, in the case of MLOS, involve a strong orchestration and management component. Coverage is coupled with the RF spectrum usage and geographic distribution of radio stations (gNBs). Finally, different deployment models (e.g. public, private or hybrid) require varying levels of investment; public networks typically have lower upfront costs but higher long-term O&M costs, while private networks require significant capital investment in infrastructure.

Notwithstanding, the MLOS operational context, with its intrinsic information security context, imposes a number design constraints that are driven by security (ex: accreditation). The adoption of standardized technical solutions prescribed in the STANAGs 5637 and 5640 shall deliver state-of-the-art protection with respect to COMSEC and INFOSEC, as Protected Core Networking (PCN) is widely adopted in Alliance Federation Networks/Services. However, in the case of IMT/5G Public Networks − considered untrusted bearers − additional measures shall be considered to ensure the protection of NATO user's metadata. The (obvious) first step would be the logical segregation (virtualization) of the NATO-assigned physical infrastructure, i.e. Network Slicing; such a solution would logically isolate both the Control and User Planes and consequently the processing of metadata. However, depending on the level of trust on a specific Public Provider, Security Accreditation Authorities may find the logical segregation insufficient to ensure a proper protection of NATO metadata and require additional physical segregation of Control and User Planes. In that case, an IMT/5G Non-Public Core for MLOS might have to be considered. However, for Nations operating an IMT/5G Non-Public network, the concern would be addressed with the assignment of a Network Slice for NATO usage.

Furthermore, security-driven design constraints are also applicable to international mobility and identity management processing. IMT Public Providers often use Roaming Service Providers to manage the roaming between Nations providers. These third-party Brokers are responsible, amongst other things, for authentication and mobility management. Hence, similarly to the national IMT/5G Public Providers, these Brokers will mostly process NATO metadata in the same physical infrastructure, as any other user. Again, if such arrangements are not acceptable by Security Accreditation Authorities, an alternative solution must be found to ensure that a trustful Broker will process NATO metadata in a dedicated and physically segregated infrastructure.

Naturally, the necessity to deploy non-public infrastructure to ensure security accreditation of MLOS solutions has a direct impact on investment and O&M costs. However, as the metadata is processed in the Control and User Planes, logical separation (Network Slicing) is still likely to be acceptable in the Radio Access Network (RAN), which represent the most relevant component on the MLOS cost structure. In other words, despite the envisaged necessity to implement physical segregated NATO Roaming Service Provider (Broker/Core) and most

likely National 5G Control and User Planes (Cores), the radio stations (RAN) are expected to be leased as a slice of National IMT/5G Public Providers' RAN. While the former is impacting the investment costs, the latter is significantly reducing it by transferring the costs to O&M.

Finally, consideration shall be made to the impact of coverage requirements, which are not specified in the [OR-6] of Ref B. Therefore, assuming Nations will lease RAN Slices from their IMT/5G Public Providers, there are two approaches towards MLOS offered coverage: (1) best effort, based on existing infrastructure from national IMT/5G Public Providers; (2) full coverage of national littoral waters, through complementally deployment of private RANs to fulfil the coverage gaps. Again, the latter option would have impact on investment/O&M costs.

5. Conceptual Approach

At this stage, it is difficult to anticipate a unique approach towards MLOS implementation. Nations have different perspectives and plans towards the usage of IMT/5G for maritime applications, so practical deployments are far from being synchronized. In some cases, there are significant efforts to explore private 5G in the tactical domain (5G bubbles), with interesting experimental results demonstrating the operational relevance of NGN, while in other cases the appetite seems not to go beyond morale and welfare applications. Therefore, the conceptual design shall capture the different understandings and offer a solution that is fit-the-purpose and able to accommodate different views.

The starting point is the overall MLOS high-level communications concept, represented in Figure 1, which reflects the foundational requirement for MLOS: National (MLOS) components shall integrate with the Alliance Federation Services (AFS) and provide connectivity between Coloured Clouds (CC) hosted in maritime platforms and NATO infrastructures. Considering the PCN concept, this requirement translates into National MLOS components being part of a National Protected Core Segment (PCS) that integrates with the wider AFS Protected Core (PCore). This approach achieves two goals: (1) transport of CCs' traffic through the PCore, enabling any business/functional service within the CCs; (2) ashore-to-afloat continuity of a protected transport network (the AFS PCore), which implements a subset of security features to the CC traffic.

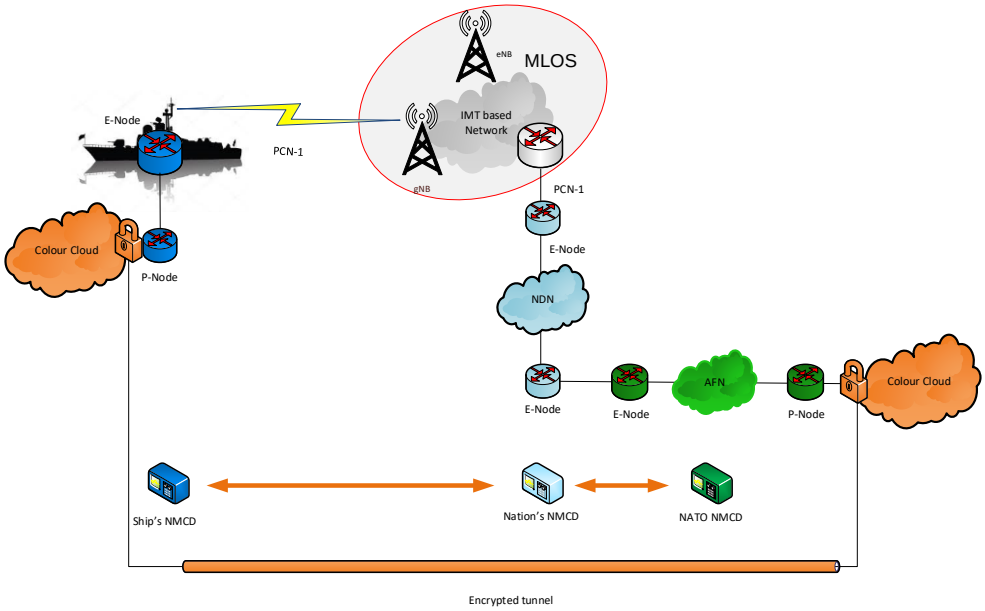

Figure 1 – Overall MLOS high level communications concept.

Eventually, the challenge becomes the definition of IMT/5G based networks that compose the National components of MLOS. Indeed, security will be the driver for most design decisions. As a mobile edge of the AFS PCore, MLOS will handle platform and CC traffic metadata, which may pose challenges for security accreditation: (1) IMT User Equipment (UE) metadata, such as UE identity, data sessions, geographic location and mobility management data; and (2) CC's and PCS traffic metadata, such as network addresses, protocols and traffic patterns. Despite being unclassified metadata pertaining to UE, routers, firewalls and other edge network devices, an opponent can leverage these metadata to infer on platforms' identity, location and networking activities.

On the other hand, considering the advantages associated to existing deployed commercial IMT providers' infrastructure – namely existing RAN footprint –, a wide range of implementation options (i.e. levels of synergy between Nation and IMT providers) can be identified and assessed. Hence, it is sensible to conjecture on Nations' approach towards MLOS deployment – highlighting the metadata viewpoint – and group them into the following two cases.

5.1 Use of untrusted/uncontrolled infrastructure

The use of **untrusted/uncontrolled infrastructure** for MLOS bearers consists of National MLOS implementations that have no ownership or control of any IMT/5G infrastructure; therefore relying on a turnkey service provided by the IMT commercial provider. The only relationship between the Nation and the service provider is through consumer-grade data plans enabled with international roaming. In this case, visiting (foreign) platforms would utilize the MLOS service through the same consumer-grade data plans (through the Host

Nation or international roaming), with no specific need for a-priori coordination. Figure 2 illustrates this case and approach, where the MLOS service would just yet be another consumer-grade user of the IMT provider's infrastructure.

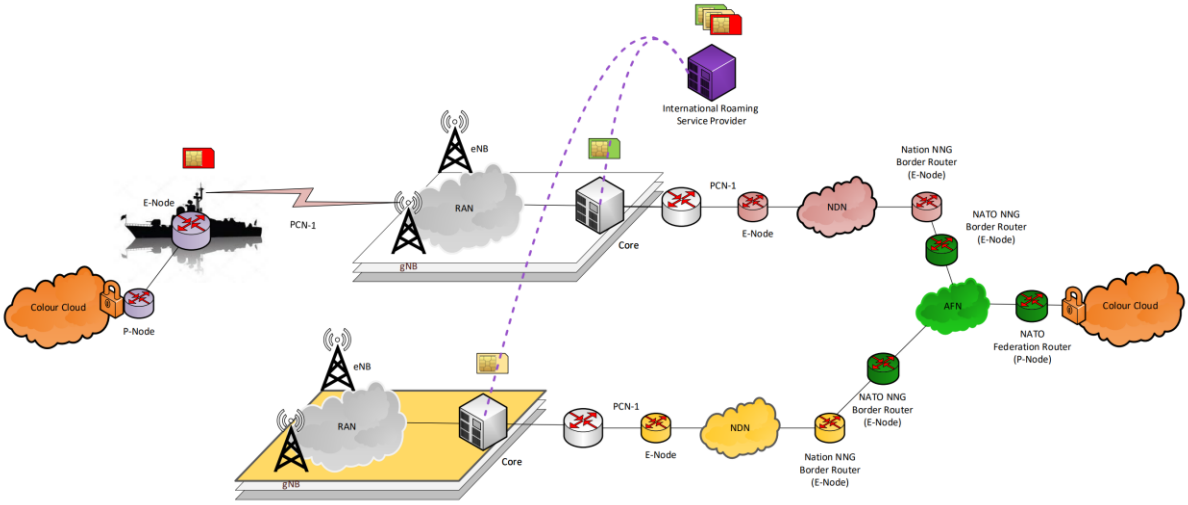

Figure 2 - Untrusted bearer/IMT operator case.

Regarding CC/PCN metadata, in addition to the exposure to the IMT provider's infrastructure, they will likely be exposed to the Internet links enabling the interconnection of MLOS to the National PCS. While defeating potential simplicity, scalability and cost benefits of this approach, enterprise agreements with select IMT providers – for the provision of dedicated backbone links to the PCS – may mitigate and avoid the exposure of CC/PCN metadata to the Internet.

Concerning the IMT-related metadata, this approach exposes platform UE metadata to the IMT commercial providers, including any international roaming provider/broker involved in the service provision chain. These providers will have visibility on UE location, mobility and identity data, which can pinpoint sensitive attributes of the host platform itself. This effect is emphasised within the operational context of maritime platforms, which operate in a reduced traffic density terrestrial environment (when compared to land terrestrial networks), making maritime platforms more vulnerable to metadata exposure.

All in all, IMT and Internet service providers – which can be untrusted service providers or trusted service providers whose infrastructure has been compromised – will handle sensitive platform (IMT and CC/PCN) metadata, as there is no isolation between the MLOS infrastructure and the provider infrastructure. When assessing this aspect as a security risk, Security Accreditation Authorities shall factor the technical constraints of this approach and MLOS' operational usage context, the latter amplifying the sensitivity of metadata.

5.2 Use of trusted/controlled infrastructure

The use of **trusted/controlled infrastructure** for MLOS bearers may be realized in different flavours and approaches; that is, the Nations can leverage a palette of "infrastructure leasing agreements" with IMT commercial operators (e.g. network slicing), which can provide different levels of infrastructure segregation, ownership and control. Additionally, aspects related to service provisioning (e.g. SIM card issuing or roaming) can be realized in a distributed (handled by each Nation independently) or centralized fashion (through a NATO broker). Figure 3 illustrates a notional set of cases leveraging this approach. The most common cases within this approach consist of: network slicing; RAN sharing; standalone private networks; and hybrids/combinations of the previous.

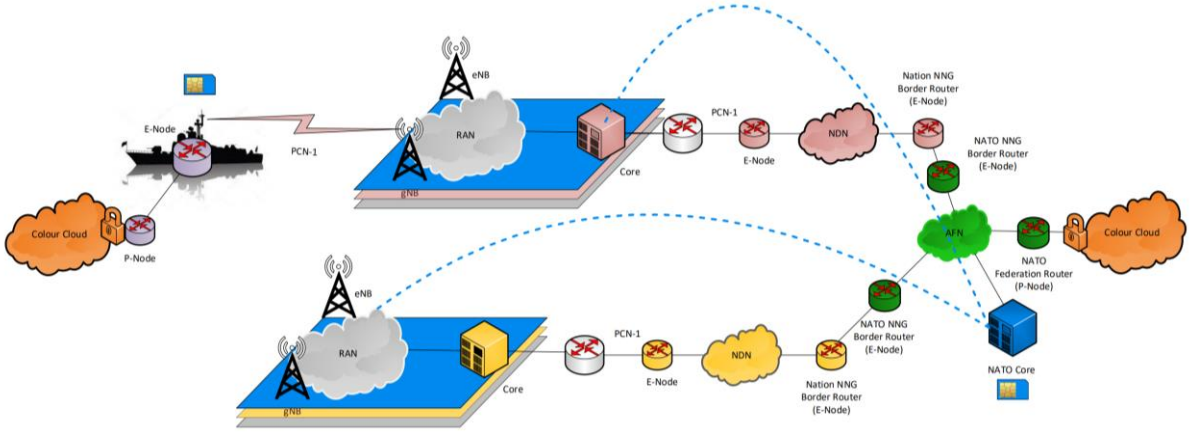

Figure 3 - Trusted bearers notional cases.

As any of the variants within this approach presumes the use of segregated and/or dedicated transport links, CC/PCN metadata should not be mixed with other IMT traffic nor exposed to Internet links enabling the interconnection of MLOS to the National PCS. Also from this perspective, specific Quality of Service (QoS) measures may be agreed with and implemented by the IMT operator to improve the MLOS service.

Network slicing realizes the logical and/or physical isolation of critical functions, particularly those handling UE identity and mobility management data. Still, network slicing entails a dependence on the operator's infrastructure, which can further be reduced with alternative RAN sharing solutions. Through RAN sharing, Nations may operate sovereign private Core Networks, while only leasing the RAN from the IMT operator. Finally, Nations may still complement the operator's RAN with a private RAN, which may be needed to achieve the required MLOS footprint. In the end, any slicing/sharing solution should provide a level of isolation from the provider that is far superior to untrusted/uncontrolled approaches: UE/CC/PCN metadata should never be mixed with other operator's traffic. Whether slicing or RAN sharing are sufficient, depends on the specific security accreditation risk assessment.

Finally, the use of trusted/controlled infrastructure represents a challenge for the MLOS provisioning model. As Nations may opt for specific implementation solutions, either a distributed or centralized service management approach should provide MLOS service coherence and continuity (including roaming). While a centralized service management approach – e.g. through a NATO Core Network and using the AFS PCore as roaming network – should provide seamless roaming operations and provisioning (e.g. NATO SIM card issuing), a distributed service approach means less integration and less automation with provisioning. In the end, the final solution will be influenced by National appetite to automate roaming and provisioning aspects.

6. Final Remarks

This paper highlights and discusses foundational MLOS capability development elements, such as requirements, operational context and ongoing NATO/National efforts. These are essential to determine the solution (or family of solutions) that should enable the MLOS capability. The analysis of limited hypothesis converges into a coherence with the AFS services provision model and architecture, while the operational context/requirement (e.g. footprint and early IOC) reduced the technical options for MLOS deployment to IMT-based solutions.

With the metadata in the centre of the discussion, the focus of MLOS capability development activities shifts to security risks and to the security accreditability of IMT-based solutions. While COMSEC and INFOSEC concerns are easily addressed through the adoption of PCN design principles and alignment with AFS, there are not NATO (or known National) policies or doctrine that can drive solutions to protect NATO metadata.

It has been argued that untrusted/uncontrolled infrastructure offers several flexibility, scalability and cost of ownership/operation advantages, but with no/little guarantees as to the protection of platform (IMT/UE) and network (CC/PCN) metadata. In the specific operational context of maritime platforms served by MLOS, this should represent a significant operational risk, which shall be factored by Security Accreditation Authorities in the specific security accreditation risk assessments.

Finally, it has been discussed that trusted/controlled infrastructure, which can be realized by different sharing/leasing synergies with operators, should realize potential (security accreditation) acceptable levels of metadata segregation and protection. Network Slicing or RAN Sharing are prime examples of state-of-the-art enablers that can contribute to the protection of NATO metadata. It is not, however, without a complexity penalty that segregation and protection of metadata are achieved. MLOS service continuity and provisioning requires service management solutions, which can be distributed or centralized. For the latter, the use of NATO Core Network and NATO transport backbones (AFS) to automate service management and provisioning is a matter to be considered.