NATO DIGITAL BACKBONE &
NATO DIGITAL BACKBONE REFERENCE ARCHITECTURE

EXECUTIVE SUMMARY

1. The NATO Digital Backbone (NDBB) will provide the technical means to ensure universal connectivity and data transport across all domains of operations (Maritime, Land, Air, Space and Cyberspace) to share and employ data securely and effectively, to maximise information flow, increase military effectiveness and enhance political decision-making.

2. The NDBB serves as the foundational element connecting the edge to decision-makers and effectors, supporting political consultation and Multi-Domain Operations (MDO). It integrates various data sources and services, enabling large-scale data sharing[1] and exploitation, thus transforming NATO into a data-centric Alliance and enhancing military effectiveness and political decision-making.

3. The NDBB ensures persistent digital interoperability, and delivers resilience through a federation of various information domains and Communication and Information Systems (CIS) services. It supports consultation and decision-making processes while spanning across all operational domains, as well as operations at strategic, operational, and tactical levels.

4. By aggregating individual CIS and CIS federations, the NDBB provides resilient, scalable, and secure digital services, including cloud and edge services[2]. It builds on agreed activities and projects like the “Allied software for Cloud and Edge services (ACE)” initiative. The NDBB relies on multiple service layers, including a resilient transport fabric, Cross-Domain Solutions (CDS), and federated stakeholder clouds. It unifies communications via a common IP network and extends a cloud-first approach to the digital backbone.

5. The NATO Digital Backbone Reference Architecture (DBRA) is part of a family of reference architectures that collectively describe the complete Digital Continuum, governed by the Architecture for Interoperable Digital technologies within the Alliance (AIDA). These reference architectures are organization and implementation agnostic, providing common terminology and facilitating interoperability of organization-specific implementations.

6. In defining nine architectural principles[2], the DBRA aims to harmonize and modernize digital capabilities, supporting capability delivery efforts and minimizing duplications. The key drivers guiding the implementation of the DBRA include adaptability to future military challenges, achieving data superiority, enabling a secure environment, and accelerating agility, resilience, and survivability.

7. The DBRA guides the instantiation of the NDBB, by providing the architectural building blocks for participants to develop target architectures that adhere to common standards and specifications so that their solutions can be integrated and interconnected into a coherent and interoperable NDBB. The first increment of the DBRA includes 35 services[3] spanning across the communications, core, and platform services of the C3 Taxonomy and chosen through consensus within some entities[4] of the NATO Enterprise.

---

[1] Information sharing within the scope of the NATO Digital Backbone shall be in accordance with the relevant NATO policies and procedures [C-M(2007)0118, C-M(2002)49-REV1 and C-M(2002)60], as well as security agreements [AC/35-N(2013)0011-REV2-COR1] as appropriate

[2] Further defined in Annex 2

[3] Services listed in Appendix 1 of Annex 4

[4] Consulted entities include ACO, ACT, NCIA, OCIO, NDS

The NATO Digital Backbone &
The NATO Digital Backbone Reference Architecture (Increment 1)

Background

1. The NATO Digital Transformation Vision (Ref. A) defines the NATO Digital Backbone as a key enabler that "will connect the NATO Enterprise to Allies' national digital capacities to be able to share and employ data securely and effectively in both directions, to maximise information flow, increase military effectiveness and enhance political decision-making."

2. The Digital Transformation Implementation Strategy (Ref. B) expands on this by stating that the NATO Digital Backbone "provide[s] the technical means to ensure universal connectivity and data transport not just across the traditional domains of operations, but also for the new domains of Space and Cyberspace, including Allies and Partners."

3. While the NDBB is conceived so that the Alliance is persistently connected, in support of NATO's missions[1] the NDBB must also make provisions for timely, case-by-case interconnections with entities that are not part of the Alliance. The actual interconnection of any such entity with the NDBB is subject to approval by Allies.

4. Thus, the NDBB supports the transformation from a network- and application-centric Alliance to a data-centric Alliance (DCRA), by providing the means to exchange data at scale and at speed across organizational and national boundaries. The Data-Centric Reference Architecture for the Alliance (Ref. C) positions the NDBB as the Information Communication Technologies (ICT) enabler for data-driven decision-making – see diagram below.

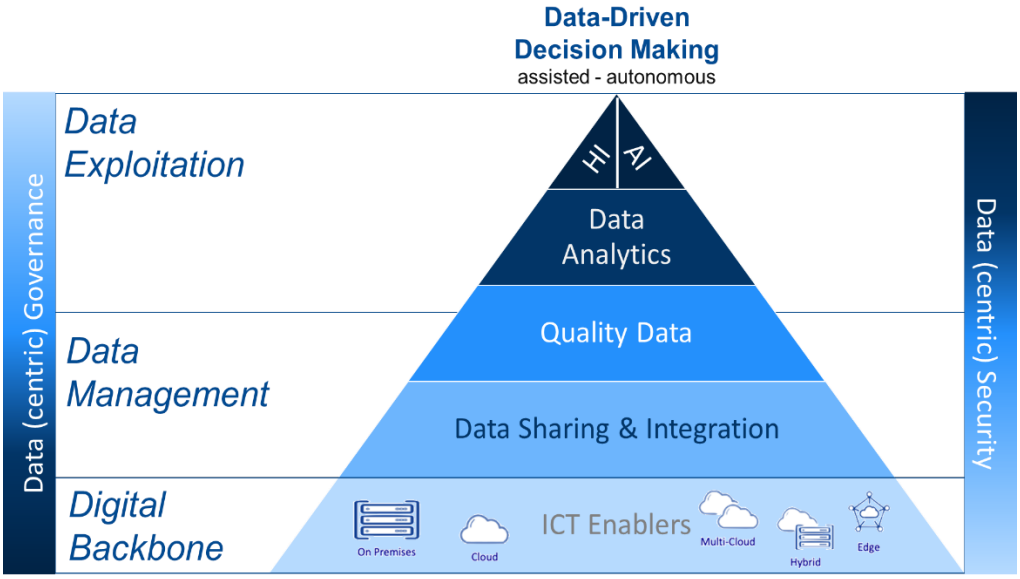

Figure 1 – Data-Driven Decision-Making Diagram[2]

[1] In accordance with C-M(2007)0118, NATO's missions include NATO operations, projects, programmes, contracts and other related tasks.

[2] Within the diagram Human Intelligence is abbreviated as HI and Artificial Intelligence as AI.

Aim

5. The aim of this document is to provide the foundational elements of the NDBB and its Reference Architecture (DBRA). In doing so, the document specifically:

5.1 Clarifies the differences between the NDBB and DBRA, provides definitions, scope, principles, cloud aspects (such as Cloud to Edge), and links with other workstrands;

5.2 Presents the NDBB as part of the Digital continuum,[3] made of building blocks, actors, and enabling CIS stack;

5.3 Outlines how the NDBB will be developed and governed, including compliance to existing policy and development of new policies;

5.4 Establishes the first increment of the DBRA with considerations for both Allies and the NATO Enterprise;

5.5 Define the architectural principles and the scope of the DBRA within the Alliance through its objectives, dimensions and context;

5.6 Define the minimum service provision and service federation frameworks, and service interoperability points and profiles for Allies and the NATO Enterprise;

5.7 Provide a baseline for further considerations on the topic.

Definitions

6. As defined in the first version of the DCRA for the Alliance, the NDBB is *"a federation of networks and systems, that provides the technical means for a resilient, scalable, and secure digital service continuum including cloud and edge services. This federation connects sensors, decision makers, actors and effectors, across the various organizational, national, operational and security domain boundaries, supporting the full range of political and military activities in peacetime, crisis and conflict, including maximum level of effort[4]."*

7. In support of this definition, the DBRA is an independent product that provides the architectural building blocks, principles and elements for participants to contribute to and interconnect with the NDBB. The DBRA structures the NDBB services and relationships, providing a set of templates for developing target or solution architectures. To this end, the DBRA is an evolving and growing product, of which Increment 1 instantiate only 35 services of the C3 Taxonomy creating blueprints for an initial development of the NDBB.

THE NATO DIGITAL BACKBONE

Vision, Scope and Goals of the NATO Digital Backbone

8. The vision of the NDBB is to enable and assure persistent interoperability across the Alliance, and throughout one or more episodic coalition mission networks at day-zero. It shall provide multiple layers of resilience, resulting from a full and dense federation of

[3] The concept of "Digital continuum" is a conceptual model that ties Digital Products to Digital Services in order address issues of ownership, access, control and co-creation.
[4] Maximum level of effort equates multiple joint operations conducted simultaneously in different geographical areas.

NATO Enterprise, national and multi-national CIS, which can host Community of Interest (COI)-specific services.

9. The scope of the NDBB spans across several dimensions, including:

9.1 All operational domains defined by NATO;

9.2 The Alliance (Allies and the NATO Enterprise) and the preparedness for timely, case-by-case interconnections[5] with entities outside the Alliance;

9.3 Static, deployable and mobile postures;

9.4 Political and Military Consultation

9.5 Strategic, Operational and Tactical C2;

9.6 All classification levels up to NATO Secret;

9.7 Baseline Activities and Current Operations, and Crisis Response Operations;

9.8 Common Funded, Multinational and National funding mechanisms;

9.9 Communication, Core and selected COI-enabling Services;

9.10 Tier 1, 2 and 3 Networks.[6]

10. The end goal that the NDBB is enabling to achieve one single and globally-accessible environment for information sharing, from the political realm through all three levels of command, and spanning across multiple participants, multiple operational domains, and all the COIs within. The sharing of information shall be possible irrespective of, and compatible with, the degree of compartmentalization endured by the underlying CIS infrastructure.

11. In the political realm, the NDBB is to:

11.1 Support faster and timely political consultation by providing a digital collaboration and communication platform where meetings can take place more often with minimum restrictions;

11.2 Enable trustworthy and auditable connection to data spaces[7] hosting political or diplomatic relevant data needed for consultation; and

11.3 Contribute to augmenting insight for political consultation and accelerating the access to trustworthy data and AI models.

12. At the Strategic level of command, the NDBB is to:

12.1 Support the Military Decision process by providing a platform that fully supports the interface between political consultation and military decision;

---

[5] Systems and services are designed to enable seamless connection when needed, even though they are not actively connected under normal circumstances. The actual interconnection of any such entity with the NDBB is subject to approval by Allies. This approach ensures that systems can be swiftly and effectively linked when needed.

[6] Current networks identified in scope include, enduring networks such as the Alliance Federation Network (AFN), the Alliance Protected Core (APC), the common-funded NATO Enterprise Core Networks (ECN), and the Alliance COI Networks (ACN) as well as episodic mission networks which may include authorized non-NATO entities.

[7] Further information can be found in the International Data Space Reference Architecture Model at: https://internationaldataspaces.org/

12.2 Enable an information environment that drives Multi Domain Operations and Political Military Assisted Decision Making; and

12.3 Contribute to improving SACEUR's Area of Responsibility (AOR).

13. At the operational level of command, the NDBB is to:

13.1 Deliver the digital services required by ACO for the orchestration of effects across operational domains in the context of MDO;

13.2 Enhance ACO's warfighting readiness by providing modern and resilient digital infrastructure and services, dynamically tailored to current and future operational needs;

13.3 Improve Situational Awareness and enable data-centric decision making across ACO commands;

13.4 Increase the survivability and resilience of digital capabilities assuring ACO's mission; and

13.5 Guarantee national stakeholders' connectivity to operational decision makers through dispersion of points of presence.

14. At the tactical level of command, the NDBB is to:

14.1 Provide the integration access points to nations in order for their fog and tactical edge components to connect to NATO operations and missions and enhance the exchange of data and information; and

14.2 Enhance the capability of reconfiguring command post in a very dynamic environment by addressing nomadic and mobility scenarios.

15. As an example, to visualize three core dimensions of the NDBB, one should consider a notional cube that integrates different axis such as 'Operational Domain', 'Security Classification Levels as well as non-classified information', and 'Level of Warfare', and enables data flows and collaboration across these dimensions. (Figure 2).

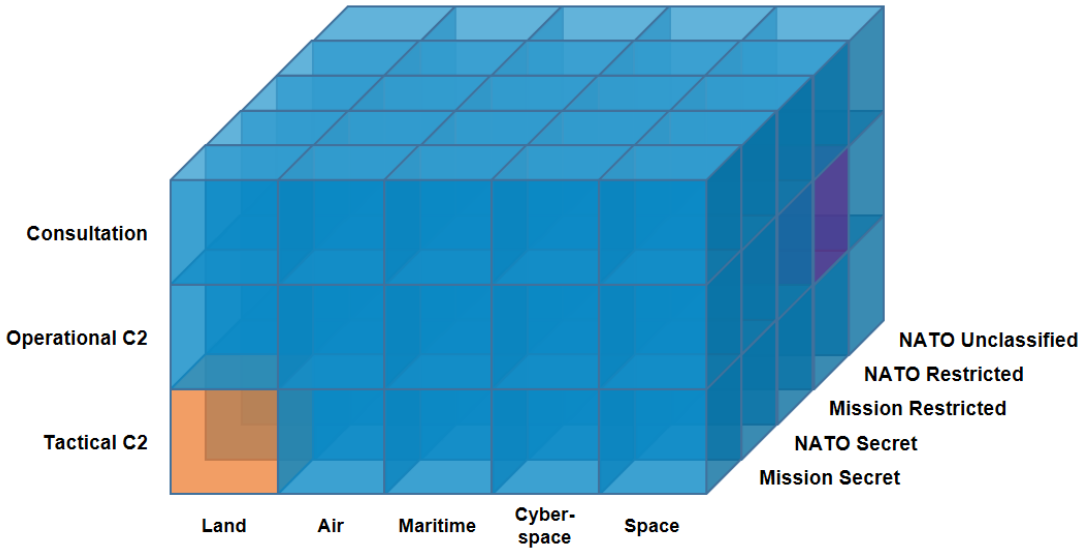

Figure 2 NATO Digital Backbone Dimensions

16. In the example, the dataflow will connect any cell of the cube to another, independent of their position. This connectivity is envisioned to be automated, fully auditable, resilient and supported by data pipelines which transform and refine the source data, while being adapted to support data profiles and policies for data integration. While most of these data services will be enabled by the data-centric platform residing on top of the NDBB, different types of data pipelines and dataflows will need to be supported. As an example, these include:

16.1 Batch processing – for large quantities of data sets for input into C4ISR and SA Services;

16.2 Data integration – for feeding data from multiple source into a single unified service such as a Machine Learning algorithm; and

16.3 Streaming data – for incoming flows of data provided by edge devices, such as GMTI[8], friendly force tracks, full motion video.

Context of the NATO Digital Backbone

17. The context of the NDBB encompasses a digital continuum that connects the edge to the decision makers and the effectors. Political consultation as well as the hybrid nature of MDO will require that the Digital Backbone provides an entry point for public data spaces and for other non-military actors that will be acting as data sources, providing data to the Digital Backbone.

18. The Alliance Data Sharing Ecosystem[9] (ADSE) pilot aims to demonstrate the connection between data spaces to share and exploit data at scale, from external stakeholders (e.g., Academia and industry) to internal ones (e.g., Digital Ocean, Alliance Future Surveillance and Control). In doing so, challenges of data integration and exploitation must be addressed through a federation model for data exchange and compliance. Secure access to non-NATO public data-spaces will be enforced by the security services of the NDBB.

19. Services hosted in non-NATO public data-spaces will need to be closely integrated with framework services providing gateways and API based access points to the backbone. Further, data platform services and federated fata fabric services[10] handling the lifecycle, persistence and processing of data for political consultation and military decision will have to be on top of the NDBB.

[8] Ground Moving Target Indicator
[9] PO(2024)0316.
[10] Change requests submitted to ACT for inclusion in the C3 Taxonomy

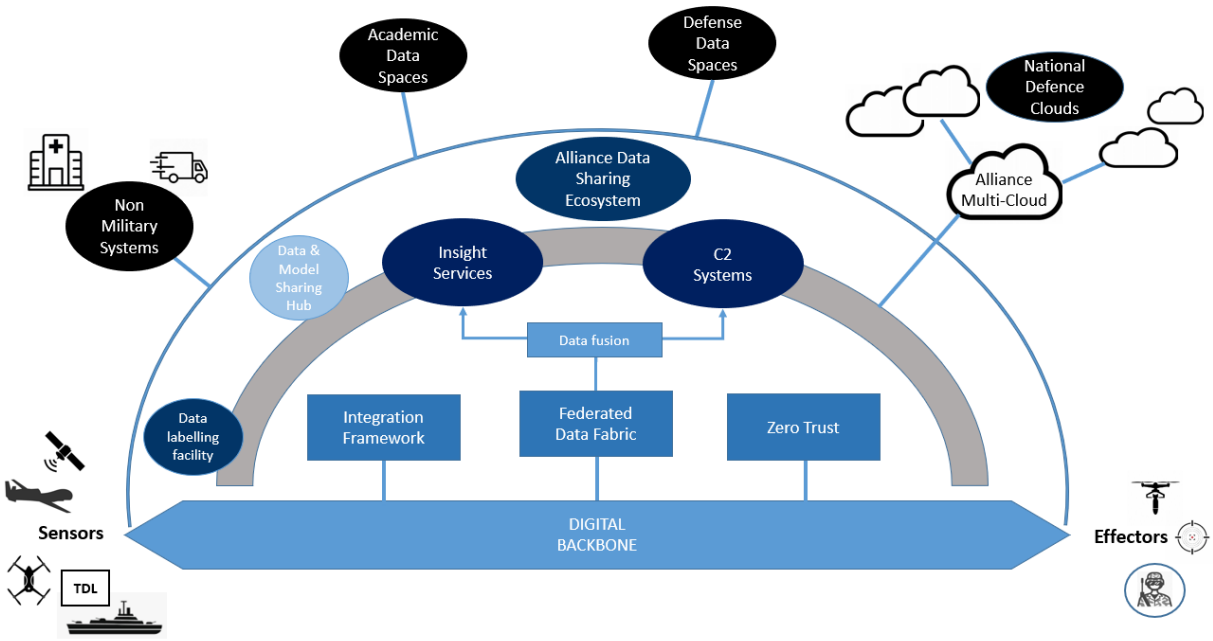

Figure 4. Context of the Digital Backbone

20. The NDBB enables the digital continuum that federates the different CIS, connecting various forms of data sources that will be consumed based on a publication-subscribe pattern. The following list describes the entities that will permanently contribute and consume services from the NDBB. The list includes:

20.1 The NATO Enterprise entities;[11]

20.2 The Allies' Armed Forces and any national-led multi-national forces; and

20.3 Non-Military Entities engaged in civil-military cooperation (CIMIC) as well as those in the wider spectrum of public services (e.g., safety, medical, border control), non-governmental organizations, all means of mass communication (e.g., broadcasting, publishing, and the internet).

21. For each of the entities described, the NDBB will provide different functions:

22.1 For the NATO Enterprise, the NDBB is the sole bearer of the NATO Digital Workplace, as well as the provider of multi-cloud connectivity, supporting initiatives such as Protected Business Network (PBN);

22.2 For the NATO Force Structure (NFS) entities, the NDBB will provide access to the CIS applications, and will enable NFS entities to contribute with applications and services; and

22.3 For Allies' Armed Forces, NDBB will integrate any CIS contribution in support of Alliance permanent tasks, as well as provide the gateway and integration points to connect C4ISR and C2 systems to take part in NATO operations, missions and trainings.

[11] As described in AC/322-D(2015)0014-REV4 (INV), and including both Entities and Points-of-Presence. The NATO Force Structure Entities not included in the document will be considered part of the NDBB when supporting Alliance Operation Missions – when served by their own, NFS-organic CIS – that would then federate with the NATO Enterprise CIS.

The layers of the NDBB

22. The NDBB relies on multiple layers of services (Figure 3) where the foundation unifies the communication layer on an IP-based protocol at the network layer. A secondary federation capability is provided by a Multi-Cloud approach that enables edge to Cloud connectivity to deploy data services and standard profiles down to integration points at the tactical edge.

23. The core of the NDBB is based on a ubiquitous and resilient transport fabric that unifies all communication with a routable IP network, meaning that all traffic and all data exchange is based on IP routing.

24. On top of this transport fabric, there is a layer dealing with Cross-Security Domain Solutions (CSDS) that provides a controlled interface to control the access and flow of information**.** CSDS allow network domains to exchange information with other domains based on relevant policies, either one-way or bi-directionally.

25. The Network Centric Security Compartmentalization provides the mechanism to compartmentalize information and separate different COIs. This segmentation is software-defined and cryptographically enforced and aims to be augmented by DCS and Zero Trust in a future iteration of the NDBB, while still respecting relevant policies.

26. The Multiple Federations of NDBB Stakeholders' layer is where different stakeholder's clouds integrate, transform and exploit data. To do so, these stakeholders require common security services such as Federated Identity and Access Management.

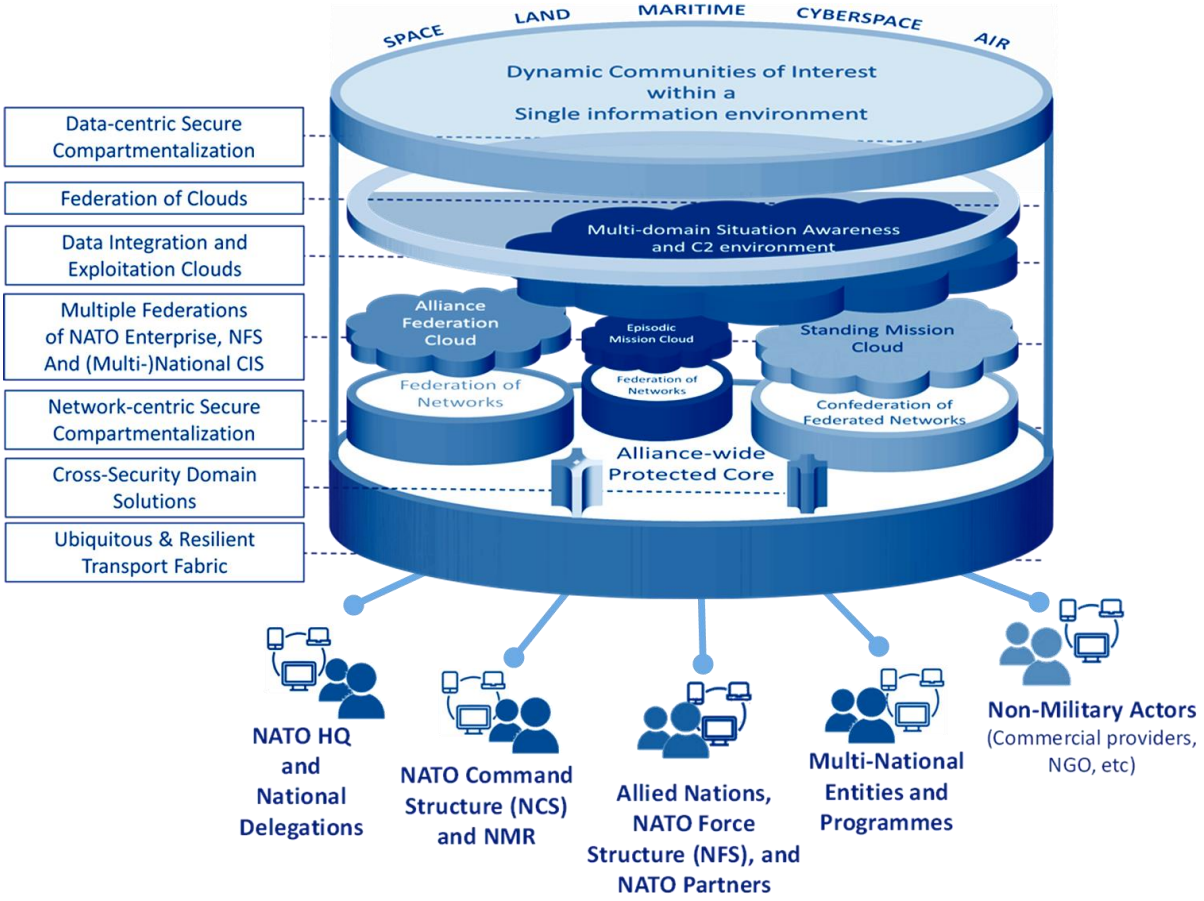

Figure 3: NDBB layered view of the Context Diagram

27. Unifying communications via a common routable IP network and extending today's instance of the digital backbone by modernizing it with a Cloud-first approach are key first steps introduced by the NDBB. In this context, the NDBB is an integral part of the cloud-fog-edge ecosystem across the Alliance, with private cloud instances being part of various federated CIS[12].

Federated model of the NATO Digital Backbone

28. Federations with the NDBB will ultimately occur across the full digital infrastructure. From the infrastructure and platform layer (federation of clouds infrastructure), communications access layer (federation of network Coloured Clouds) to the communications transport layer (federation of protected core segments, resulting in the Alliance-wide Protected Core). At the bottom of the stack, the NDBB shall rely on networks identified in scope. These include:

[12] Under the multinational cooperation for the development and fielding of "Allied software for Cloud and Edge" services, (Ref AC/322-WP(2023)0096-REV6, 10 May 2024).

28.1 the Alliance Protected Core (APC)[13], acting as a resilient and ubiquitous underlying transport fabric, serving multiple network Coloured Clouds[14]. Through NATO Enterprise, national and commercial contributions, the APC, hereafter referred to as the Protected Core, will be able to scale in capacity, reach and resilience, on demand;

28.2 Network Coloured Clouds will initially exist and operate under the current network-centric security model. In the future they will incorporate Data-Centric Security (DCS), with the corresponding reduction of the number of Coloured Clouds. Besides connecting the CIS infrastructure together, network Coloured Clouds will provide access to external entities connecting to the NDBB, enabling their interaction with services hosted and distributed across the NDBB infrastructure. To that end, Coloured Clouds will enable both enduring and episodic federations of independent networks.

29. In general terms, the NDBB is intended to aggregate a range of CIS and CIS federations that operates in different information domains. Within the NDBB information exchanges shall occur both bilaterally, multi-laterally, or upstream, towards any environment aggregating information across domains and operational areas. Further, information exchanges shall occur seamlessly and yet being subject to data sovereignty and releasability constraints.

30. The NDBB will enable nomadic operations in response to changes in the strategic and operational environment. To that end, the NDBB will provide interoperability points for the tactical domain, to connect and exchange tactical domain specific data with services available and residing on the backbone. As a principle, data needs to be provided outside of its original context, and can be exchanged leveraging the NDBB as a peer-to-peer communication service.

31. All in all, and through the widespread adoption of the federated model, the NDBB is intended to provide an Alliance-wide information highway, over which the NATO Enterprise, national and multi-national CIS can operate and share information.

THE NATO DIGITAL BACKBONE REFERENCE ARCHITECTURE

Defining the Reference Architecture

32. A Reference Architecture (RA) is used in an Enterprise Architecture (EA) context to provide a template or a blueprint of the architecture for a particular field of interest. It provides a common language to discuss and drive design decisions for related solution architectures or particular implementations. It promotes adherence to common standards, specifications and the patterns and underlying services that compose the Reference Architecture.

33. A reference architecture is agnostic of individual organisations, specific infrastructure or services and implementation programmes or projects. Actors and capabilities shall be

[13] The Alliance-wide Protected Core was introduced in the Core ACT/CAPDEV/CAP/TT-3768/SER:N*:, NATO Enterprise Wide Core Communications and Multimedia Access Services CPP, Programme ID: 9A3001, October 2022.

[14] AComP-5637, Edition A Version 1 December 2019, para 1.5.5. d

proven compatible, and able to evolve, with the architecture views and blueprints described within the RA.

34. In this context, the DBRA structures the NDBB services and relationships, providing a set of templates for developing target or solution architectures. To that end, Annex 3 places all the actors and capabilities in their current and foreseeable contexts, by describing a first instantiation of those blueprints.

Architecture Vision

35. The architecture vision of the DBRA is to provide guidelines and direction to harmonize and modernize current digital capabilities, in a continuous and iterative approach. The DBRA shall provide the specification of the required services, through multiple iterations of the architecture. The *Architecture for Interoperable Digital technologies within the Alliance* (AIDA) will cohere the DBRA aligning and negotiating conflicts with other Reference Architectures, such as the DCRA, the upcoming Zero Trust Reference Architecture and NATO Digital Interoperability Framework. Future iterations of the DBRA should consider other reference architectures such as the NATO ISR Interoperability Architecture (NIIA),[15] the NATO Intelligence Systems Architecture (NISA), the AirC2 Reference Architecture to ensure that NDBB fully enables these COI-specific services and capabilities.

36. The DBRA provides a blueprint, from which specific capability-level architectures can be derived by Allies and the NATO Enterprise. It is intended to serve the following two main purposes and audiences:

36.1 It provides an initial technical description of the NDBB building blocks (e.g., principles, users, goals, constraints, etc.); and

36.2 It instantiates the NDBB by providing a first increment of services in the context of existing and programmed capabilities, aiming at supporting capability delivery efforts, while minimizing duplications, gaps and inconsistencies.

DBRA Specifications, standards, policies

37. The DBRA is defined in accordance to the following specifications, standards, policies and Reference Architectures:

37.1 The **Alliance C3 Strategy** and the C3 Regulatory Framework, to ensure coherence with policies and directives;

37.2 The **AIDA,**[16] to ensure coherence with other Reference Architectures;

37.3 The **Data-Centric Reference Architecture for the Alliance** (Ref. C) providing data platform and services required for capturing, labelling, transforming, and routing of data through the NDBB while managing the lifecycle of data assets;

37.4 The principles set by Allies in **the NATO Zero Trust Policy** (Ref. J), NATO Zero Trust Strategic Plan and derived technical and implementation guidance and directives to ensure information security across the NDBB;

[15] AEDP-02, NATO ISR Interoperability Architecture
[16] AC/322-WP(2024)0087-REV5

37.5 The **NATO Architecture Framework (NAF)** (Ref. K) as the standardized way to develop architectural models and artefacts that are compatible with the two meta-models used by Allies and the NATO Enterprise;

37.6 The **C3 Taxonomy** Baseline 6 (Ref. G) as the model representing CIS concepts and relationships, as well as providing a common language to synchronize activities; and

37.7 **Federated Mission Networking (FMN)**, as the governed framework for planning, preparing, establishing, using, and terminating mission networks in support of NATO's missions.

Drivers

38. Drivers that define the goals of the DBRA are the adaptability to meet future military challenges, the achievement of Data superiority, secured environment to exploit classified data, accelerate agility, resilience and survivability:

39. **Adaptability to future military challenges** - At its core the NDBB will modernize political and military decision making. Such a vision is embodied in the MDO concept, which builds upon the principles of unity, creativity, agility, and interconnectivity. Realizing the NDBB, the DBRA is one of the key enablers to interconnect forces, platforms and systems both within the NATO Enterprise and also with C3 systems of Allies.

40. **Achieving data superiority** - In military operations, timeliness in the decision process is a distinctive key advantage. In order to achieve information superiority and data-driven decision making at all levels, the DBRA must drive the service interoperability and data standardisation required by other efforts like the DCRA and the ADSE.

41. **Enabling a secured environment** - Ubiquitous connectivity and adopting cloud service models blurs the security perimeter and diminishes its effectiveness. Zero trust is the prevailing approach to address CIS security threats, and it requires:

41.1 The enablement of a Federated Identity management across the Alliance in order for nations and national resources to gain access to resources on the NDBB; and

41.2 The enablement of multi-level security access to adequately address the security model and reduce the risk of operational disruption, while protecting the cloud-fog-edge continuum.

42. **Data Centric Security** - Data Centric Security goes beyond perimeter defence, protecting access to data and metadata through attribute-based access control. Metadata is used to describe and categorize data, *"DCS applies another layer of defence-in-depth by directly protecting the data, both at rest and while in transit. Along with this enhanced protection, DCS offers a greater level of control for data and improved sharing through facilitating better data management, identity management and more fine-grained access management*"[17].

43. **Accelerate agility, resilience and survivability** - The DBRA will accelerate the federated approach to Communications and Core Services across the Alliance, supporting NATO becoming more agile to respond a dynamic changing environment. Notably:

[17] PO(2024)0275, Data Centric Security Implementation Plan, 26 July 2024

43.1 The DBRA will need to deconflict agility and resilience requirements of established and foreseen capabilities. In achieving this, cloud computing can propose the built-in mechanism to address agility (i.e. variable computational power and agile deployment process via Dev-Sec-Ops and DataOps) while providing resilience and survivability. This will be achieved by establishing distributed data centres combined with airgap environments;

43.2 The DBRA needs to provide a template to federate existing capabilities (e.g. through Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)). Cloud-native and cloud computing model will also facilitate this federation by providing on-demand access to a shared pool of CIS resources that is already designed and provisioned when needed; and

43.3 The DBRA will harmonize the NATO CIS landscape evolution with a cloud-first service model, harmonising and driving a single operating model across the Alliance, enabling convergence between static and deployable environments.

Architectural Principles

44. The Architectural Principles[18] (Table 1) define the underlying general rules and guidelines for the use and deployment of resources and assets related to the NATO Digital Backbone, and complement those described in the Enterprise Architecture Policy.

Table 1: List of principles employed by the DBRA

Principle	**Statement**
Governance and Compliance	Establish clear governance and management mechanisms, including compliance frameworks, to govern the behaviour of participants, ensure regulatory compliance, and enforce agreed-upon policies and standards.
Data Sovereignty	Respect data sovereignty and national regulations, ensuring that data is collected, processed, exploited, and stored in compliance with agreed NATO policies, directives, and standards and respective national laws and regulations.
Federation of CIS Services	Implement a federation model of Communications and Information Systems (CIS) services across the Alliance with day zero connectivity. This federation should be designed to allow for expansion when required and authorized. It should include federated Identity, Credentials, and Access Management services to enable authentication and authorization for accessing systems, services and data available across the federated CIS.

[18] A detailed description of the Architectural Principals is described in Annex 2 of this document.

Principle	Statement
Federated Cloud Computing	Implement federation, based on a “Cloud-first” approach, to provide flexibility, reliability, scalable capacity and performance and efficiency of CIS services provisioning across the Alliance. Open architectures should be preferred to leverage Open Cloud stacks and industry best practices and standards (to be adopted by NATO).
Leverage Existing Capabilities	Implement a federation model that, whenever and wherever possible, leverages capabilities that already exist across the Alliance.
Security by Design	Ensure that security underpins the design, testing and implementation of the CIS. Data Centric Security and Zero Trust are two examples of concepts that follow this principle and aim at protecting CIS assets and resources, of which data and information are the most valuable.
Interoperability by Design	Ensure that all systems, services and data adhere to standards that are either open, NATO agreed, or NATO adopted to ensure seamless communication and interoperability between participating parties.
Resilience and Redundancy by Design	Implement redundancy and fault-tolerant mechanisms to enhance resilience against failures and disruptions, ensuring continuous availability and reliability of critical services.
Scalability and Flexibility by Design	Develop architectures to accommodate dynamic changes in demand, allowing for scalability and flexibility in resource allocation and service provisioning.

Architecture Description

45. From the business perspective, and beyond its focus on enabling MDO, the DBRA serves as a reference to develop digital backbone architecture(s) serving the NATO Enterprise, the Alliance and Alliance-led Coalitions. From the strategic decision making down to selected tactical environments, and across all five operational domains, these entities will use the backbone to establish, operate and consume services.

46. The DBRA builds upon the governing notion of multiple and diverse interoperable CIS being interconnected and exchanging information products. These interconnections exist, within and between different information domains, in order to enable the sharing of information, both cooperatively and reciprocally, using four different mechanisms:

46.1 Plain access to information products residing in a given information domain (without involving federation), e.g. by natively hosting the requesting user within that domain.

46.2 Exchange of information products within a given network and information domain, enabled by the federation of services, federated identities, adhering to FMN specifications, and following the network-centric security models.

46.3 Exchange of information products, between two different network and information domains, based on enhanced labelling, releasability policies, and their enforcement and the domains’ boundaries;

46.4 Data sharing, across information domains, based on clearance-based and attribute-based access control to cryptographically-protected data packages, following the data-centric security (DCS) model.

References

A. PO(2022)0405, NATO's Digital Transformation Vision, 04 Oct 2022.

B. PO(2023)0191, NATO's Digital Transformation Implementation Strategy, 31 May 2023.

C. AC/322-WP(2024)0087-REV5, A Data Centric Reference Architecture for the Alliance – Version 2, 14 Nov 2024.

D. AC/322-N(2023)0019, NATO Digital Transformation in Support of Multi-Domain Operations – Bi-SC Inputs to NATO Digital Transformation Implementation Strategy, 16 Mar 2023.

E. Enclosure "E" to C-M(2002)49-REV1, Security of Information, 20 Nov 2020.

F. C-M(2002)60, The Management of Non-Classified NATO Information, 11 Jul 2002.

G. ACT/DIR/DIV/TT-6492/SER:NU:1394, C3 Taxonomy Baseline 6, 9 Dec 2022.

H. AC/322-WP(2022)0043 (INV), NATO Digital Backbone/Transformation Vision, 19 Aug 2022.

I. SH/CYBER/J6/DB/24-016090, Allied Command Operations Digital Backbone Vision and implementation strategy, 10 Apr 2024.

J. AC/322-D(2023)0063 (INV), NATO Zero Trust Policy, 30 Nov 2023.

K. AC/322-D(2018)0002-REV1, NATO Architecture Framework Version 4, Jan 2018.