AARMS Vol. 22, No. 1 (2023) 23–32.

10.32565/aarms.2023.1.2

Networks Enabling the Alliance's Command and Control

Attila GULYÁS[1]

The Alliance's wide area networks enabling operational command and control (C2) are under continuous revision in order to facilitate the wide spectrum data exchange between NATO Command Structure (NCS), NATO Force Structure (NFS) elements and other key organisations.

The focus is – as always – on the information technology's researches and network-enabled capability development.

It is clear that running the current NATO wide area network has challenges in terms of network management, information security and counter-cyber operations. Therefore, it requires a viable transformation to a wide area network with a higher-level resiliency and scalability.

Having supported by NATO Communications and Information Agency (NCIA), the decade's one of the most important tasks is to re-new, re-design and re-organise the existing classified network domain in support of efficient C2 for the current and future operations.

In this scientific article, I will provide with a short historical background of NCIA's efforts in creation of a more resilient classified domain-net and the needs of core and functional services within the Alliance to introduce the already decided, the viable solution of classified network enhancements.

Keywords: *infocommunications networking, CIS, command and control (C2)*

Introduction

The North Atlantic Treaty Organization (NATO) General Communications and Information Systems (CIS) network (NGCS) was introduced in 1997 in support of NATO Command Structure (NCS) elements (e.g. Supreme Allied Command Transformation SACT, Supreme Headquarters Allied Powers Europe SHAPE, Joint Force Command Brunssum JFCBS, Joint Force Command Naples JFCNP etc.) in the unclassified and classified security domains. In connections with that National Defence Networks (NDNs) and NATO Force Structure (NFS) elements were also required for the interconnections in the abovementioned physical and logical domains in order to provide with the highest level possible multi-connectivity between NATO and national commands. This common

[1] Colonel/OF-5, Director CIS/IT HUN General Staff, e-mail: attila.gulyas@mil.hu

aim has required the establishment of a comprehensive, overarching network structure called NGCS.

The NFS elements have organic support units dedicated for the all-level-support including CIS; however, the NCS principal commands might have no nationally dedicated support units for this purpose. Consequently, this is one of the needs of the establishment of an organisation, which provides the maximum level CIS support in the unclassified and classified, the static domains of CIS networking for NCS and NFS. To accomplish the tasks, the NATO Consultation, Command and Control Agency (NC3A) was formed in 1996[2] embracing the SHAPE Technical Centre (STC) in The Hague, Netherlands and the NATO Communications and Information Systems Agency (NACISA) in Brussels, Belgium. NC3A was part of the NATO Consultation, Command and Control Organization (NC3O) and reported to the NATO Consultation, Command and Control Board (NC3B). In July 2012, re-structuring the NC3A the NATO Communications and Information Agency (NCIA) was established.[3]

One of the key premises of the freshly formed NC3A (later NCIA) was to establish the NATO Core Network (NCN) enmeshing the NCS, NFS and NDN elements connected in the physical domain through gateways, routers and firewalls. In this term, the NC3A has begun to be the organisation embracing both NCS and NFS CIS elements into one comprehensive and scalable network in the unclassified and classified static domains.[4]

NATO Network Enabled Capability (NNEC) initiative promoted the use of NATO classified domain as operational consultation, planning and execution tool across the Alliance providing top-down approach from the principal commands down to national enclaves; meanwhile, the NATO expansions of the late 1990s (Hungary joined NATO in 1999) required new ways for network extensions both in philosophy and materiel.[5] The Connected Forces Initiative (CFI) established the notion of zero-day-connectivity, making that a strategic priority for the freshly joined, connected countries.[6] Zero-day-connectivity enables freshly joined and already existing Alliance members to run core CIS services plus selected basic functional services in order to provide the principal C2 functions with a coherent fundamental networking even before any exercises and operations launch.

Interoperability requires overarching connectivity in terms of Core Enterprise Services (CESs) such as telephony, e-mailing, video-teleconferencing and chat plus selected Community of Interests (CoIs) provided by NCIA primarily, listed in the NCIA Costed Services Catalogue and Service Rates.[7]

NFS and later the Joint Command and Control (C2) Capability (JC2C) initiative led the nations to create NATO Readiness Forces (NRFs) with the need of interconnections into the NGCS. This endeavour turned to high-scale connections towards Multinational

---

2 Károly 2013: 18–21.
3 NCIA official website.
4 NCIA official website (for more information see www.ncia.nato.int/about-us/newsroom/a-history-of-nato-support.html).
5 NATO NNEC website.
6 NATO CFI website.
7 NCIA Costed Services Catalogue.

Headquarters following the NATO Readiness Action Plan (RAP),[8] which further cemented the NATO classified domain as one of the foundation pillars of the Alliance's high readiness forces through enabling effective C2 from top to down commands (from strategic to tactical level).

NC3A, then NCIA is to cope with these challenges, has generated mesh networking in the classified domain utilising Mons and Evere in Belgium, Lago Patria (Naples) in Italy as services and data centres/hubs for NATO Enterprise (CES and CoIs) services. Most nations deliver their Information Exchange Requirements (IERs) as priority by simply extending the NGCS down to the national HQs. This means a stovepipe connectivity from the abovementioned data centres run by NCIA down to national HQ (users) challenging the information channels/lines of communications with a broad diversity of threats, requiring scalable measures to guarantee cybersecurity, overall.

Another relevant topic is the finance of Alliance-wide CIS in terms of the common funding/separated (national) funding. Alliance members pay budget to the NATO funds but based on surveys and experiences the rapid expansion of the Alliance, accelerating from the first decade of the 21st century shows that 80% of the actual NGCS footprint was left outside the NATO common-funded capability packages. This means that freshly joined nations were/are not eager to or capable of the improvement of their classified C2-enabling CIS following the NCIA-proposed renewal cycle of hardware and software commonly used in NATO. These results a vast amount of obsolete and cyber-related vulnerable equipment and tools within a mesh networking still designed not to compartmentalise these national extensions. Nowadays, when the cyber challenges are the most demanding threats in our world interconnected, these have been weakening and might compromise the entire NGCS. It is worth noting that the proliferation of nationally managed classified information services' domains, which were designed to individually synchronise their directories (e.g. file servers) and e-mailing (e.g. exchange servers) with the NCIA Automated Information Systems (AIS) domains, the NCIA Enterprise is an indispensable hub for the organisations to communicate with each other.[9]

Therefore, it seems obvious that the currently NCIA-managed NGCS at least the static classified network's domain needs to be revised and re-designed as an important task to give immediate answers to the 21st century's cyber challenges. The relevant counter measures leave great portions of decisions in the hands of organisations (HQs, nations, etc.) to promote their measured, tailored but at least minimum level appropriate actions within the creation of their own network and services.

After this short introduction, this article is to review the ongoing NATO procedures in order to find solutions to the continuous development of network-enabled requirements (Information Exchange Requirements IERs), incorporating the nations and other organisations as information hubs into an Alliance-wide network with embedded and real networking capabilities.

In this article, I will provide with the short descriptions of current researches/trends from NCIA to nations in creation of a resilient wide area network in the classified domain

8 NATO RAP website.
9 NCIA/AFS/2021/050501 – AFS Joining Instructions. 3.

and I will describe the expected steps from nations and other organisations to achieve this higher level of interconnected network of networks.

A viable solution

It is apparent that the Alliance's principal commands (NCS elements) must be supported by NCIA in the future as well. Revolutionary changes can be achieved in the fields of NFS and other organisations' Information Technology (IT) networks, utilising the Federated Mission Networking (FMN spirals)[10] model as a schema in joining the NATO classified static networks. The aim is to create a kind of classified Internet within this relevant domain, giving chance to the nations and organisations through their dedicated host nation and support units to manage their own networking, initially with the heavy support of NCIA.

A possible answer to the emerging challenges is the NCIA initiative Alliance Federated Services (AFS) project. The NCIA has organised the kick off/pilot conference on this topic in April 2019, which was based on the Alliance's Polaris[11] programme. Polaris is a modernisation initiative embracing almost all segments of NATO developments, in order to create an Alliance characterised by cutting age technology within the communications area, scoping on the IT, to provide with resistant and resilient CIS networking, forging the Alliance to comply with the 21st century's challenges. One of the important segments of Polaris is the CIS/IT modernisation led by NCIA, as stated by NATO documentations C-M(2015)0041-REV2 (national/organisations' PoPs), PO(2014)0801 (CIS Security), C-M(2017)0062 (NATO C&I Vision).[12] Surveys and experiences identified that more than 600 Point of Presences (PoPs) exist within the NATO umbrella enmeshing the entire classified static network. To reduce the numbers of NCIA-managed PoPs and involve more the nations and organisations into their management, there is a need to re-design, upgrade/install and manage/maintain as a maximum 2 PoPs per entities, run/supervised commonly by NATO (NCIA) and nations/organisations. Through these PoPs, the entities can utilise the CES and CoIs by NCIA, also they have possibilities to design, operate and maintain their own services (federated services), also to lend or borrow them to/from other NATO nations/organisations (NCIA Business to Business model). It is supported by NCIA migrated services in terms of CES and CoIs utilising cloud services very well-known from the civilian, the private IT environment.[13] The NGCS must transform to a more up-to-date, modern IT network, also it will change the name to NATO Communications Infrastructure (NCI).

[10] Low 2021.
[11] NCIA official website: *Polaris programme*.
[12] Trouvé 2021.
[13] NCIA/AFS/2021/050501 – AFS Joining Instructions. 8–9.

The way to the optimum

Based on the FMN[14] concept,[15] the new AFS model must utilise the following layers' federations (in accordance with C3 taxonomy[16]).

- Network layer
- Core (enterprise) services layer
- Cybersecurity layer
- Information Technology Infrastructure Library (ITIL) layer
- CoI layer
- Verification and validation layer

Once the NNG interconnections completed thus the layering, the layers' federations might be the key for success. After defining the federated layers, it is worthwhile to deep-dive into the levels of network layer in order to overview then identify the real needs and tasks to nations, organisations to re-set their connectivities. In Table 1 are to be found the pre-planned federation initiatives focusing on the network layer.

Table 1: Federation initiatives

Type	Definition	Explanation
Type 0	Currently NGCS PoPs	Might be transformed to NCI node
Type 1	CoIs extensions mostly for NCS	For a specific organisation/need/ requirement; planned to be guided and supervised by NCIA only
Type 2	This layer is for NFS, HQs and other organisations	N/A
Type 3	Alliance and national C2 elements without direct NCIA supervision	N/A
Type 4	All which are not in the abovementioned levels and are not supervised by NCIA	N/A

Source: NCIA AFS Conference report 248-4/4/2019/NATO as of 02 April 2019.

The target of this modernisation effort is to bring the focus to Types 2–3–4, designing a new network layout, exchanging the hardware (PoPs), re-design the Internet Protocol (IP, currently IPv4) addresses, develop the Service Management (SM) including Quality of Service (QoS) measures.

Therefore, it appears obvious that join AFS first and foremost must be a national effort for all Alliance member organisations (NCS, NFC) and other HQs, national extensions. It also seems evident that the highest profits and benefits will be at the national or organisation level with this re-structuring once they have their state-of-the-art, newly constructed network extensions with the bright possibility of further enlarging, with the re-organisation of CES and CoIs to other Alliance members, organisations.

---

14 Károly 2020: 571–586.
15 NATO SACT Future Mission Network (FMN) Concept FCX 0010/TT-8523/Ser: NU, October 2012.
16 Károly–Németh 2019: 55–67.

Design principles

As I have already flagged out the current NNG (border router with border protection services BPS) will connect directly to the organisation, nation's border router. The NNG can be commonly managed by NCIA and the respective nation; however, the management of national gateway (e.g. edge routers) and BPS must be the role and responsibility for the nation. In other words, boundary protection mechanism (can be local and/or centralised) will be placed by the respective nation.[17]

Also, border protection measures are the clear interest of each nation. Figure 1 shows the possible solution depicted the current network situation forward to the near future visions.

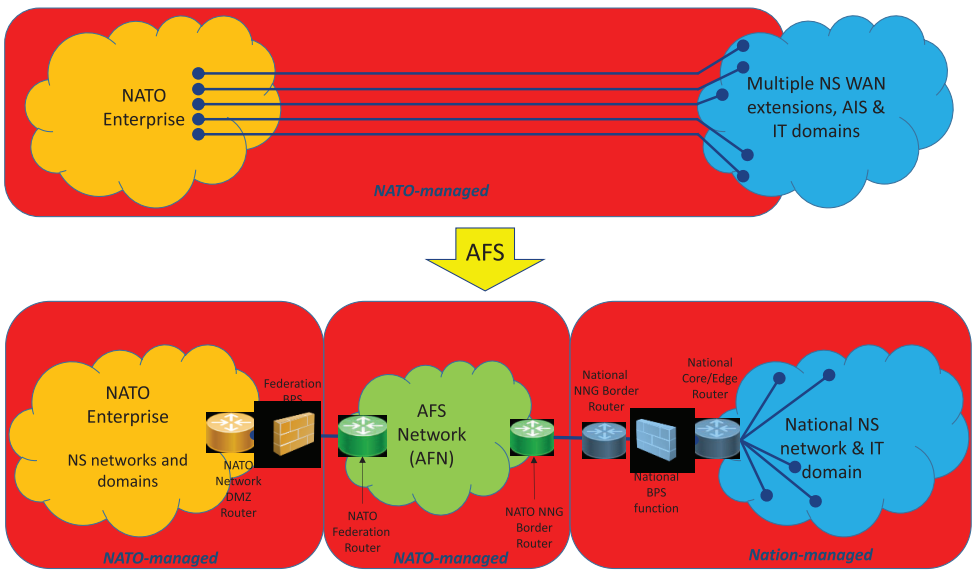

Figure 1: Current and future static networking environment

Source: Defourneaux 2021

Figure 1 clears that the new networking allows the Alliance to operate in the entire network as classified Internet (IP routing and Domain Name Services DNS) with the essence of the national efforts for building blocks of it. National networks might have, might receive services from NATO Enterprise; however, each of them are highly encouraged to develop their own Alliance Federated Networking (AFN) capabilities in terms of Core Enterprise and functional (CoIs) services brokered by/with/under direct support and supervision of the NCIA, who still governs the entire NATO classified static networking.

[17] NCIA/AFS/2021/050501 – AFS Joining Instructions. 7.

NCIA will also support the national IPv4 private space allocations, establishing the NCIA Naming and Registration Authority (NRA).[18] It is recognised that during the last decades NCIA and nations/organisations have less care of proper IP-spacing and like in the civilian environment, as demands require, the IPv4 must be exchanged to IPv6, the migration of the IP-spaces[19] is inevitable and vital in building a cyber-resilient classified network.

Road to success

The NCIA has designed the steps of any organisation to re-transform their obsolete network to federated static networking.[20] As I have stated already, this is an NCIA-led initiative therefore, the Agency offers viable steps to achieve the full connectivity. Here are the most important, the required actions by any nation, organisation as follows in Table 2.

Table 2: Steps for federation

Steps	Actions
Step 01	Upon invitation by the respective nation or organisation, NCIA gets a common view of the NS extensions, IT services (DNS, Email and Directory) and IP space.
Step 02	The nation, organisation has the decision, which extensions are to migrate and which ones would remain end-to-end managed.
Step 03	The nation, organisation and the NCIA NRA agree on the final delegated IP space available for the entity to manage.
Step 04	The nation, organisation takes over and uplifts the legacy assets (gateways, routers, BPS) used for the migrated extensions, where required.
Step 05	The nation, organisation or NCIA commissions the NNG and national NNG Edge Routers.
Step 06	The nation, organisation aggregates connections or networks behind the national NNG Border Router (this is national responsibility), then develop and maintain the IT services.
Step 07	The nation, organisation provides security accreditation for this freshly formed network, including the elements inherited from the legacy extensions.
Step 08	NCIA migrates the national NNG Border Router connection from the legacy NGCS router to the NATO NNG Border Router.

Source: Compiled by the author based on NCIA/AFS/2021/050501 – AFS Joining Instructions. 16–17.

Having accomplished the steps above, obviously the nations and organisations' benefits would be that the respected entity has the full control and management of her entire classified static network with the possibility of future extensions including enlarging the current classified static web with deployable (mission) networks or elements implemented in a coherent and scalable, resilient way. That is the vital point when static and deployable classified networks – utilising the FMN compliant networking principles – shall be

[18] NCIA/AFS/2021/050501 – AFS Joining Instructions. 8.
[19] Murdock 2021.
[20] Friedrich–Janinez 2021.

federated in terms of layers then CES and CoIs.[21] All this means that this freshly formed cloud would be outside the NATO Enterprise footprint; therefore, it has the full individual management of IP space assigned to it by NCIA NRA. Nations and organisations can create new network nodes, change the network topology (extend or reduce) and upgrade network appliances as well as deploy new applications and services. In another approach, this federated method gives the nations, organisations free hands to run their classified network business as they wish, more importantly as the operational requirements, changings enforce.

Summary, conclusions and the way ahead

As it apparent, the currently used NGCS cannot be managed any more due to specific reasons defined by NATO strategic and operational documentations. There is a need for transformation, there is a requirement of urgent network upgrade utilising the FMN principles in the NATO classified, static networking as well. NCIA has initiated the AFS project in 2019 to answer the challenges of the 21st century clearly identifying the needs then setting the rules, roles and responsibilities by NCIA itself, NCS, NFS and other elements, especially nations and organisations how to re-design that obsolete classified static networking currently called NGCS.

NCIA provides the comprehensive Joint Membership and Exit Instructions (JMEI) as well, to any entities across the Alliance to read, digest, utilise and finally act for the maximum effort. That is the evident account of the network transition initiative, following the steps guided by that document, nations, organisations can achieve their successful and rapid joining into this freshly defined and formed networking.

Hungary has also stepped forward on this way establishing the core network planning team of our classified static networking. At this phase, this board's primary task is to review the current HUN NATO S*cret Network's (HUN NSN) layout and nodes, PoPs than create an upgrading plan, a viable solution with the proper timeline to the decision makers, how and when, most importantly with whom can the HUN NSN be transformed first, then federated with, in accordance with AFS principles.

The challenge is given now. I strongly believe, soon HUN NSN shall turn into a new classified network organised in accordance with AFS principles.

List of abbreviations

AFS	Alliance Federated Services
BPS	Border Protection Services
C2	Command and Control
CES	Core Enterprise Services
CIS	Communications and Information System

[21] Athanasiadis 2022.

CFI	Connected Forces Initiative
CoIs	Community of Interests
DNS	Domain Name Services
FMN	Federated Mission Networking
ITIL	Information Technology Infrastructure Library
JC2C	Joint C2 Capability
JFCBS	Joint Force Command Brunssum
JFCNP	Joint Force Command Naples
NACISA	NATO Communications and Information Systems Agency
NC3A	NATO Consultation, Command and Control Agency
NATO	North Atlantic Treaty Organization
NCI	NATO Core / Communications Infrastructure
NCIA	NATO Communications and Information Agency
NCS	NATO Command Structure
NDN	National Defence Network
NGCS	General Communications and Information Systems (CIS) network
NFS	NATO Force Structure
NNG	NATO and Nation Gateway
PoP	Point of Presence
RAP	NATO Readiness Action Plan
SACT	Supreme Allied Command Transformation
SHAPE	Supreme Headquarters Allied Powers Europe

References

Athanasiadis, Christos (2022): *Transition of MND-C to AFS as a Nation AFS and NNG Update.* Brussels: NCIA HQ, NCIA – HQ MND-C workshop, SME presentation, slide No. 13.

Defourneaux, Gilles (2021): *AFS Joining Instructions Who? Why? What? How?* AFS workshop. Brussels: NCIA HQ.

Friedrich, Gernot – Janinez, Deflet (2021): *Alliance Interoperability Architecture Federated Mission Networking, and Alliance Federation Services.* AFS workshop. Brussels: NCIA HQ.

Károly, Krisztián (2013): Szövetséges erők követése az afganisztáni hadszíntéren. *Honvédségi Szemle*, 141(3), 18–21.

Károly, Krisztián (2020): Automatizált erőkövetési képesség megvalósításának lehetőségei a Magyar Honvédség híradó-informatikai rendszerében. In Pohl, Árpád (ed.): *Biztonság és honvédelem. Fenntartható biztonság és társadalmi környezet tanulmányok II.* Budapest: Ludovika Egyetemi Kiadó. 571–586.

Károly, Krisztián – Németh, András (2019): The Possibilities of Supporting the Public Functions with Fleet and Force Tracking Systems. *AARMS*, 18(3), 55–67. Online: https://doi.org/10.32565/aarms.2019.3.5

Low, Warren (2021): *Protect Core Networking – Workshop Introduction/Context.* Brussels: NCIA HQ.

Murdock, Aidan (2021): *IP Addressing.* AFS workshop. Brussels: NCIA HQ.

NATO CFI website. Online: www.nato.int/cps/en/natohq/topics_84112.htm
NATO NNEC website. Online: www.nato.int/cps/en/natohq/topics_54644.htm
NATO RAP website. Online: www.nato.int/cps/en/natohq/topics_119353.htm
NCIA/AFS/2021/050501 – AFS Joining Instructions.
NCIA Costed Services Catalogue. Online: https://dnbl.ncia.nato.int/Pages/ServiceCatalogue/Services.aspx
NCIA official website. Online: www.ncia.nato.int/
NCIA official website: *Polaris programme.* Online: www.ncia.nato.int/what-we-do/nato-consultation-command-networks/polaris-programme.html
Trouvé, Pascal (2021): *AFS Contribution to Polaris programme.* AFS workshop. Brussels: NCIA HQ.