



# Operational Requirements and Interoperability Challenges

Briefing at the AFCEA Technet  
by  
Director NCSA

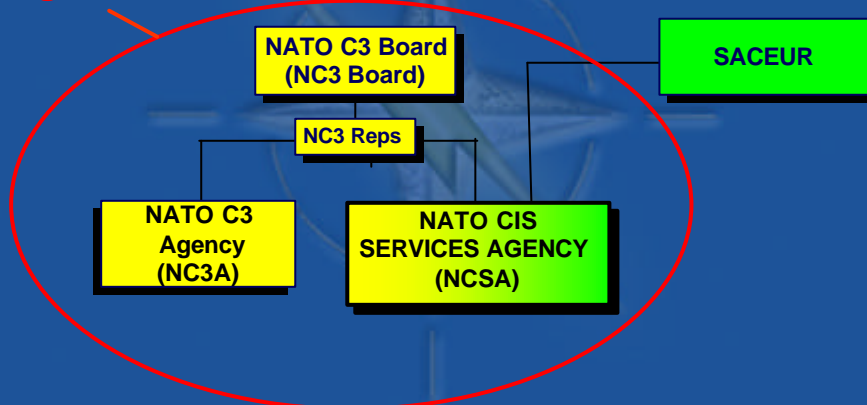
Lieutenant General Ulrich Wolf  
17 Oct 2008

NATO Unclassified



## NATO C3 Organisation

**NC3  
Organisation**



NATO Unclassified



## Outline

- **Priorities**
  - **Support to Operations**
  - **DCIS/DJSE**
  - **CRO CIS Architecture**
- **Challenges**
  - **Evolving Requirements**
  - **Interoperability**
  - **Cyber Defense**

NATO Unclassified



## Modern CIS operations

- **Operational tempo**
- **Information Assurance**
- **Information Sharing**
- **NNEC**

NATO Unclassified  
NATO unclassified releasable to public

This slide illustrates the main characteristics of CIS service provision in NATO and, in particular, to support NATO's operations.

I would like to explain the characteristics of modern CIS operations in more detail:

**Operational Tempo:** The high operational tempo has increased significantly the pressure put on all CIS stakeholders. In 2007, NCSA supported 7 NATO operations, the CIS requirements

of the NRF and over 50 NATO Exercises; all of which required personnel to deploy, support CIS services and be available at short notice.

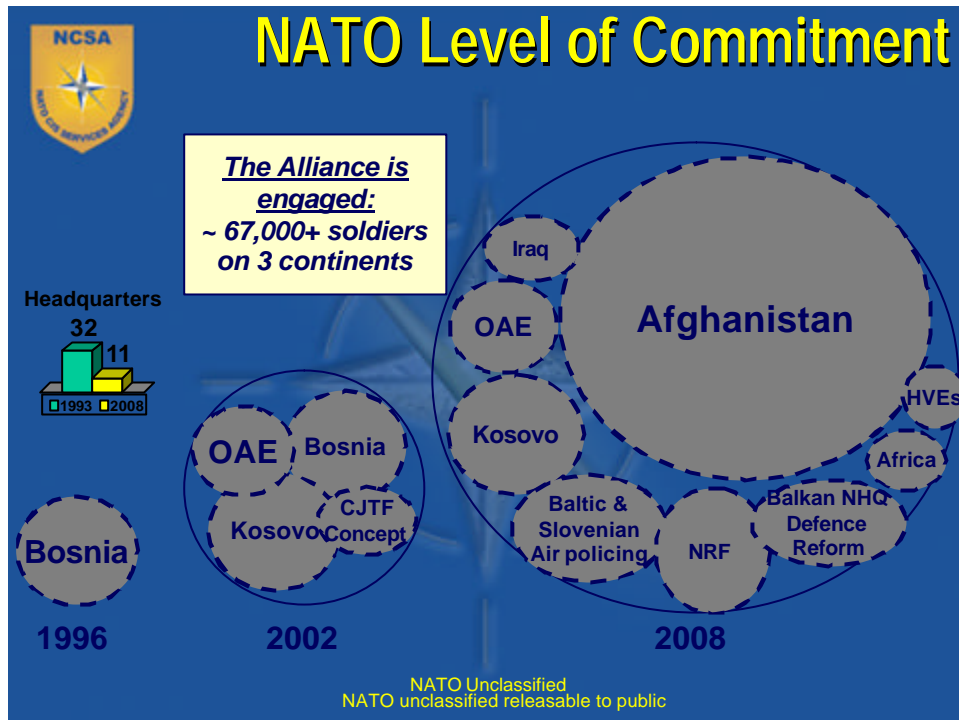
Our greatest challenge has continued to be found in our wide spread CIS service support to ISAF. Since 2006, several interim, quickly developed solutions have become inevitable. In doing this, NCSA has been successfully filling existing capability gaps in theatre. The implementation of Mitigation Plan 4 (MP4) and the provision of CIS to Kandahar Airfield are highly visible instances that demonstrate NCSA's excellent performance. Further, our Agency has been meeting urgent CIS requirements of ISAF within a short period of time. Examples are the delivery of two Limited Interim NRF CIS Equipment (LINC) to give COMISAF the C2 capability to conduct mobile operations; as well as the rapid provision of secure, end to end, voice communication to both HQ ISAF in Kabul and further, across ISAF.

**Information Assurance:** We need the proper measures to protect and defend NATO information and NATO information systems by ensuring their availability, integrity, authentication, confidentiality and nonrepudiation. This includes providing for restoration of NATO information systems by incorporating protection, detection, and reaction capabilities.

**Information Sharing:** The political-strategic concept on how to stabilize Afghanistan puts additional burden on NATO's shoulders. NATO knows that military assets are not sufficient to bring stability and prosperity to Afghanistan. We need to closely integrate all available means that is to say: military, economics, cultural and development. Consequently, all players have to coordinate their activities. The players range from the United Nations who are responsible for the coordination of the International Committee's support to the Afghan National Army and National Police. The networked or comprehensive security approach can only work if all players talk to each other and coordinate their activities. Clearly, it is very difficult – if not impossible – to allow International Organizations/Non-Governmental Organizations and AFG national forces access to NATO classified systems. But we do need to pass information to them.

**NATO Network Enabled Capability (NNEC)** operations require flexible, reliable CIS services providing collaboration and up-to-date information throughout the theatre. We need to be able to link NATO's networks with the networks which International Organisations like the UN or the EU have established in theatre.

Sufficient bandwidth and effective cyber defence are essential to accomplish this. As the service provider NCSA is the key enabler for NATO to meet these goals.



## NNEC

**“Need to Know” ⇒ “Responsibility to Share”**

- **NCSA approach to NNEC:**
  - ◆ Seamless information sharing
  - ◆ Collaboration across organisations & theatre
  - ◆ Ease-of-use, net-enabling, interoperable
  - ◆ Secure information exchange

NATO Unclassified

NNEC brings a fundamental change in the way that we work: transforming from “Need to Know” to “Responsibility to Share”. “Need to Know” is based on a hierarchical organisation with pockets of information and knowledge. “Responsibility to Share” is based on cross-collaboration, seamless sharing of information, and theatre-wide constant secure connectivity.

As a service provider, NCSA must be ready to support the operational requirements as they appear. NCSA's approach to NNEC is to provide services that truly are net-enabled supporting:

- Seamless information sharing
- Cross-collaboration across theatre and organisational boundaries
- Ease-of-use, net-enabled, interoperable, and secure
- Allow information exchange with "Responsibility" to share in mind.

To meet this goal NCSA need solutions from industry that support these basic elements. This applies for the services as well as for the tools used by NCSA. Key elements are: service-oriented architecture, interoperability, and industry standardisation. Furthermore, innovations within information sharing, collaboration, and security are needed.

**NCSA**

## Development of DCIS

**Easy-to carry, set-up & use**

**COTS products**

**limit configuration efforts**

**limit training**

**Ro-Ro C-130 ability**

**Scalable to the need**

classified

These slides highlight the requirements to CIS equipment that I have voiced to all, to NATO and to industry.

NCSA succeeded in bringing in these principles into the latest procurement programs that are projected to supplement the Limited Interim NRF CIS (LINC) and to equip the future NATO Signal Regiment.



## Development of DCIS



### **LINC E** (Limited Interim NRF CIS – Extension)

- **All commercial, off the shelf equipment**
- **Assembled and integrated at NCSA depot**
- **Shared logistics?**

NATO Unclassified  
NATO unclassified releasable to public

The LINC E is a good example of NCSA's use of commercial industry to meet a military requirement. The LINC project began as our solution to the problem of supporting the establishment of the NATO Response Force in the face of the long latency that characterizes NATO communications system procurement.

The LINC E equipment introduces newer technologies, yet remains compatible with legacy equipment. New commercial off the shelf technologies such as VOIP are integrated into the LINC-E and this allows us to bring modern telephony standards to the battlefield, ensuring that the battle staff is equipped with services and equipment that he is familiar with from his normal office environment. Similarly, the use of Blade Servers, significantly increase the raw computing power available to deployed users and can reduce the reliance on expensive and scarce connectivity with mainframe computers at the static HQ.

The LINC family is built to be scalable and allow for flexibility to meet the end user's requirement, from a small forward command unit to a major HQ, we are looking to be able to provide the soldiers in theatre with a 'building block' set of equipment that can be tailored as required

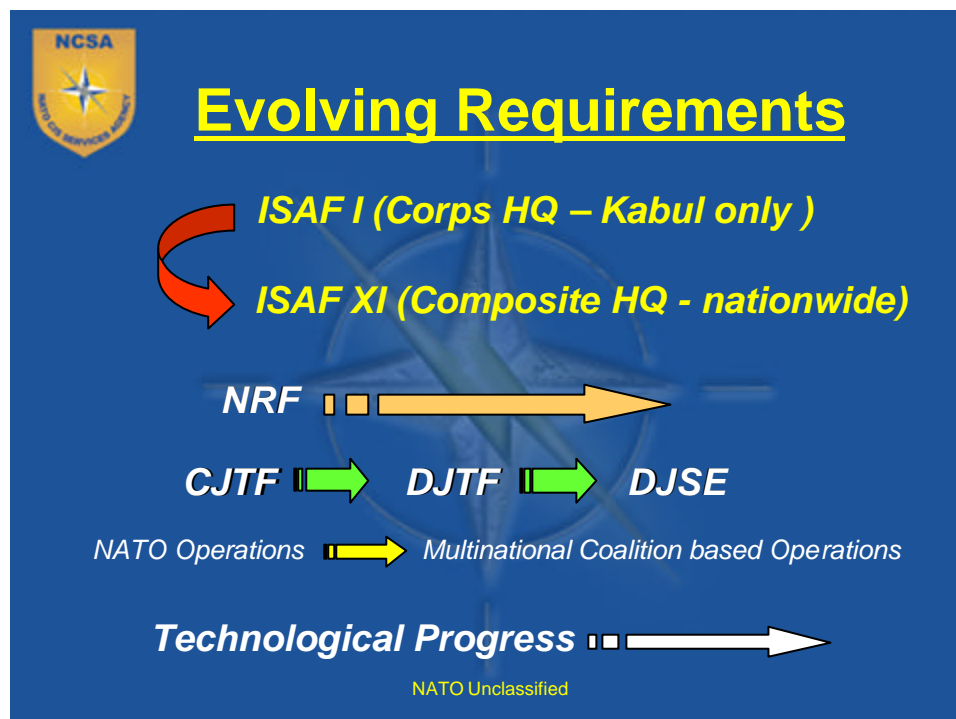
Instead of limiting our capability to a set number of end users we have created a flexible equipment set that can provide customer support from 24 to an almost limitless number through the addition of more interoperable modules

Much of the LINC E will retain the same equipment set as was fitted in the original LINC program. With this in mind we have in a sense created a 'family' of CIS equipment that allows for better logistical management:

- Less variety of equipment to be procured and held as spares
- Less of a training burden because much of the equipment remains the same, so courses do not require to be designed from scratch

Through the judicious application of use of new technology and by involving NCSA staff and their operational experience gained in the field from the outset, we have been able to reduce the amount of boxes that must be used to house this kit making it smaller, lighter and easier to easier to deploy and operate.

Commercial of the shelf equipment offers us exciting possibilities for rapidly increasing our capability, capacity and deployability, but we must ensure that the operational experience gained by our personnel in conflict zones is also included in our future equipments Shared CIS logistics between NATO and industry is another area where NATO could gain effectiveness and efficiency in maintaining NATO's deployable equipment pool. This needs to be further investigated.

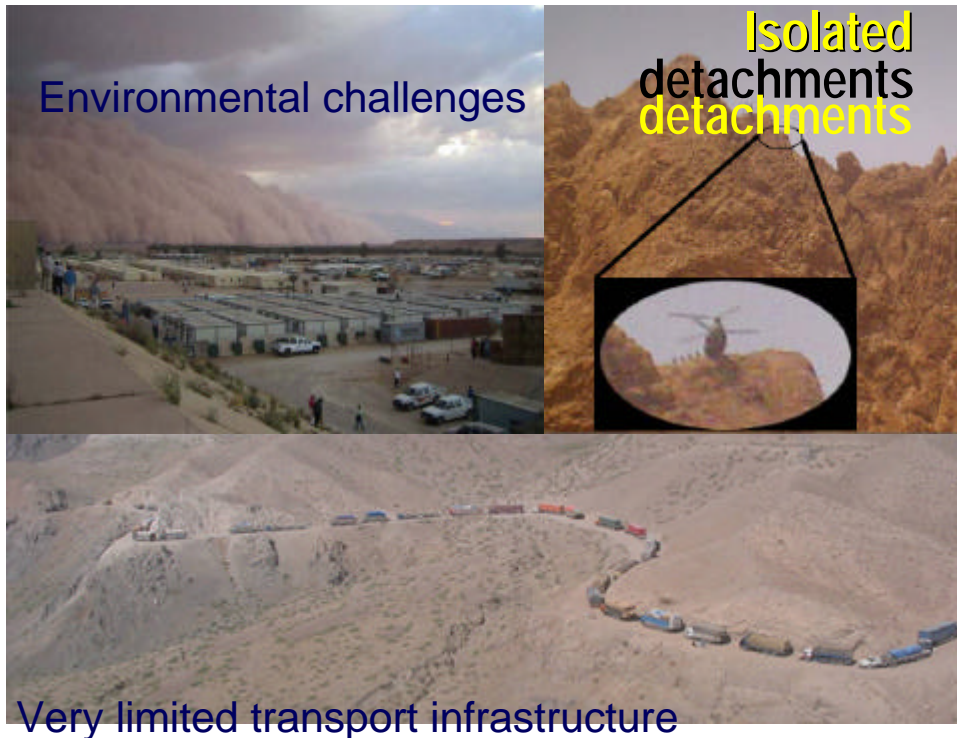
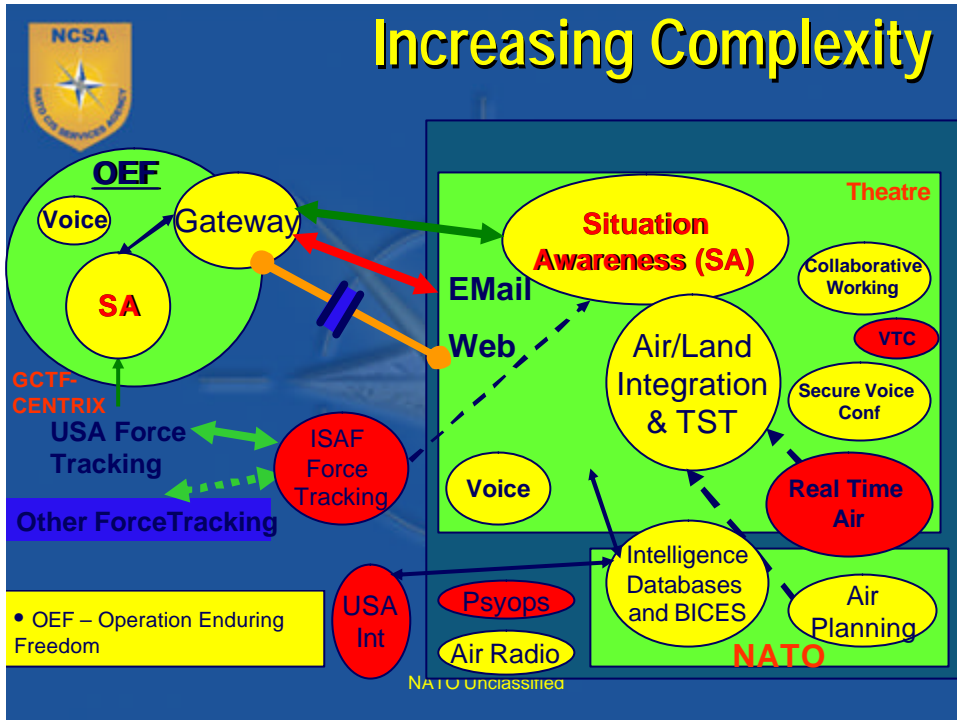


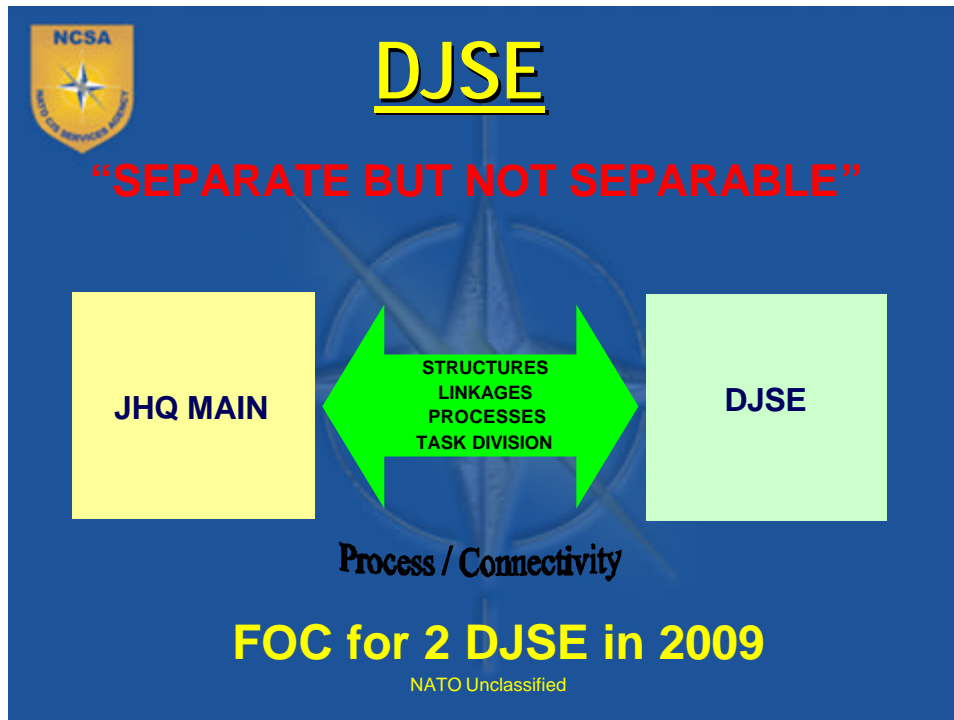
Now I would like to continue with the challenges NCSA has been facing.

Changes in LOA and the philosophy of how NATO will conduct expeditionary operations has had, as a side effect, a detrimental effect on coordination and planning of CIS capabilities.

- ISAF has changed significantly in both size and complexity from the NATO initial deployment.
- A Commander may place differing emphasis on the role of the CRO and wish to change the direction of some programmes due to be implemented during his tenure.
- Strategic documents changes based on variation/expansion of the mission.
- NATO is increasingly looking to non-NATO nations to act as coalition partners. As a consequence, NATO CIS (that includes information management) must be re-aligned to enhance coalition command and control. Currently the focus is on providing information downwards. Recent ISAF experience shows an increased use of nationally provided information, especially in the ISR domain.
- The rapid evolution in technology from the time of the requirement definition until capability implementation (may take up to 18 months) can result in requests for changes/upgrades.

All these makes the governance so difficult but also so important.





The next major project in which NCSA has been involved is the DJSE (Deployable Joint Staff Element). This concept is an operational level HQ element designed to be in the theatre as the deployed joint staff for an operational level commander.

The new concept of the DJSE may facilitate the way ahead towards a standardised NATO HQ for CRO.

I would like to shortly highlight the operational background of the DJSE concept to facilitate the understanding of its CIS challenges.

New quality: Delineation of responsibilities with no overlap, same information in both, HQ Main as well as in the forward elements.

CIS prerequisite to implement this concept: Collaborative Tools / secure links / bandwidth.

Current capabilities sufficient to support 2 DJSE. To support the required 46 PoPs of 6 DJSE, NCSA needs the 3rd Bn.

Challenging timelines: LCC HD and MD to reach DJSE IOC (DEC08/Jun09) and FOC (Jun09/DEC09).

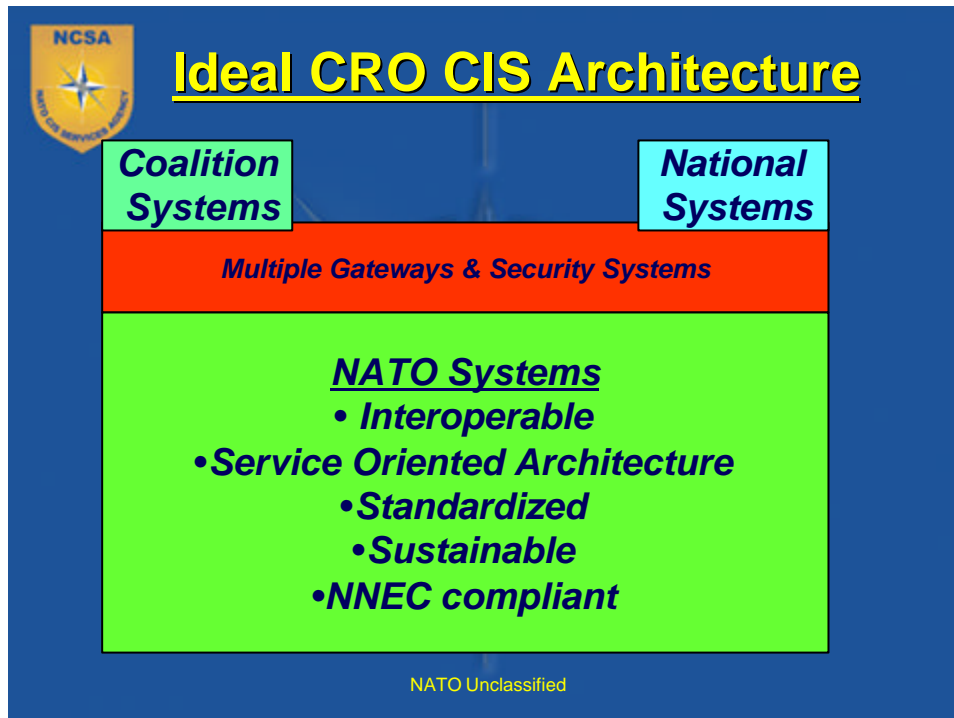
In order to meet the challenging timelines, the CIS support for DJSE has been organized in a way that is different from the past:

Fast Track:

NCSA has taken lead to develop in close coordination with NC3A and NAMSA CIS solutions to enable LCC HD and MD to reach DJSE IOC and FOC using existing capabilities and also a limited set of experimental / commercial products/tools.

Long term:

The Bi-SC DJSE CIS Implementation Team (CIT) is to develop with support of NC3A and NCSA a broad conceptual, experimentation and spiral approach of CIS to match DJSE FOC. The approach has to reflect and support the IOC and FOC solutions developed by NCSA.

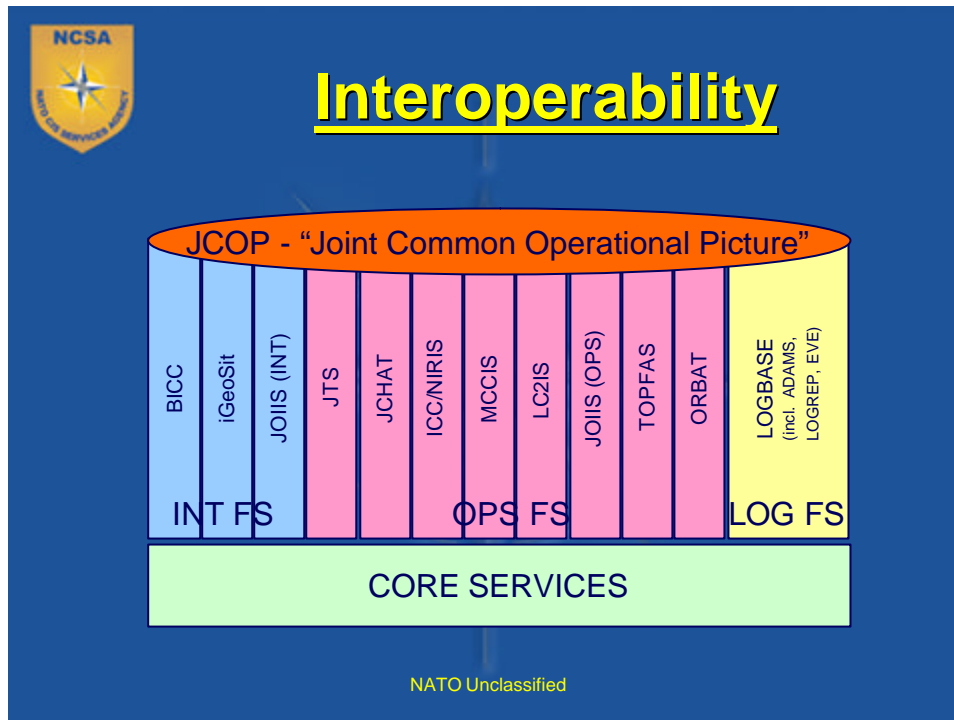


What could be the ideal CIS architecture?

From the CIS perspective, you will see the multiple security domains that need to exist under a NATO led CRO. This includes enterprise wide Cyber Defence. We can assume Non NATO Troops Contributing Nations (NTCN) and then the additional National C2 systems provision. NATO, coalition and national systems are integrated and work together.

The ideal CRO HQ should be based on the Bi-SC programme modified by ISAF experience, and on the Service Approach Architecture that enables for sharing of information between different systems. There should be no duplications and minimized overlaps of functionality. And the HQ must be sustainable from the CIS point of view. Final goal is NNEC compliancy.

We need to get a better grip on evolving requirements by developing a template for a generic CRO HQ with standardized packages of CIS systems (hard- and software). Developing the DJSE concept, we see a huge potential in achieving a generic, more standardised solution for CRO HQs.

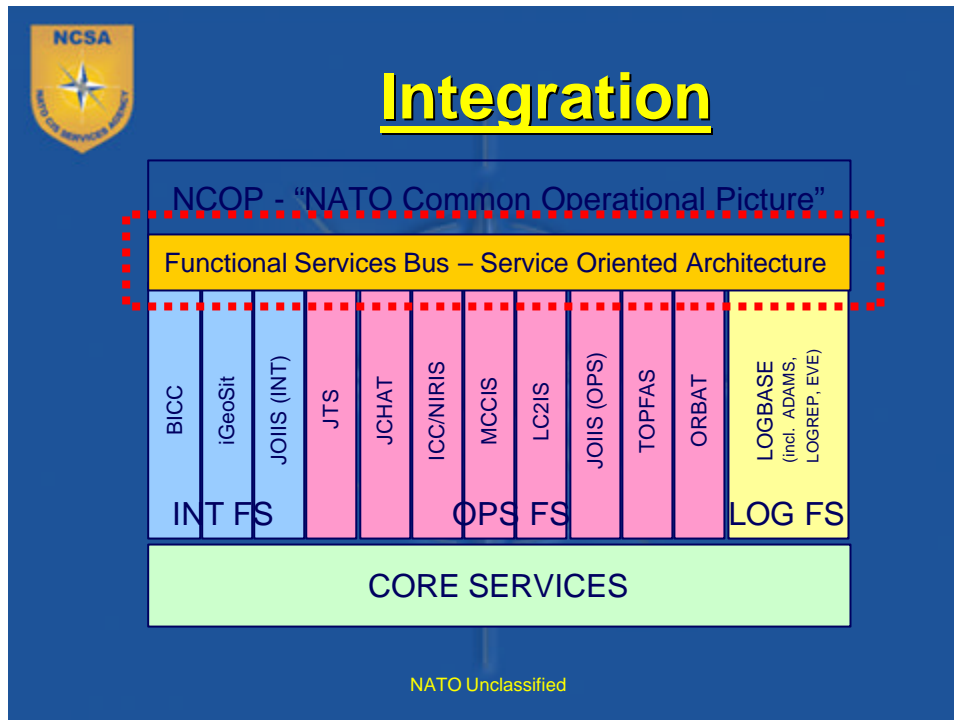


A major challenge to CIS service provision is caused by the **stovepipe approach to Functional Services** such as OPS, INT and LOG.

Land systems (e.g. LC2IS) do not “converse” easily with maritime/air or INT systems. Current systems are built using different technologies, are stove-piped and may not be interoperable. Therefore, software interfaces need to be developed to produce combined land/maritime/air or friend/foe representations for the Commanders. Interoperability challenges occur whenever systems are procured or evolve in isolation.

The complexity of this is illustrated with **JCOP** – by just the sheer number of systems and consequent interconnections. The **JCOP** prototype was developed as quick win to interface the stove piped information sources. This is an interim solution, working currently with NATO’s various FAS’s in the static structure. If it is to be implemented in ISAF it must be augmented with ISAF specific interfaces (such as JADOCs and C2PC).

This slide shows how complex the integration of different systems is and why it takes significant resources and time.

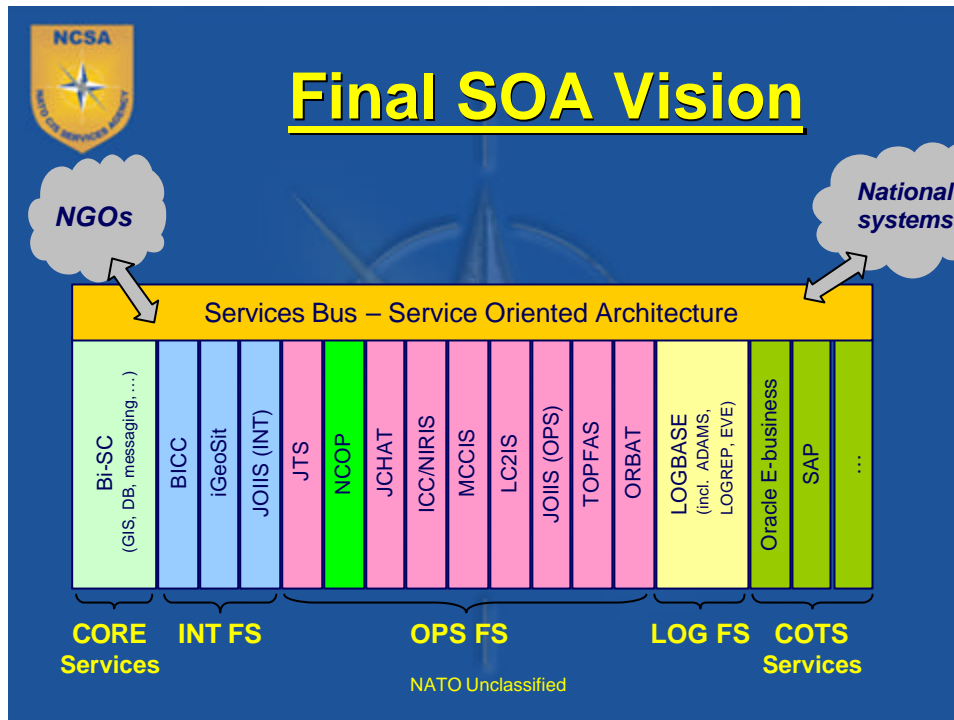


In order to overcome the stove piping of the systems, the existing Functional Services are to be adapted in order to support information sharing through well defined system interfaces. The structured information can then be made available and shared by existing systems on the basis of a **Functional Service Bus**.

This approach will allow seamless exchange of standardized data between the existing systems. Because existing systems are a mixture of different technologies, only a **Service Oriented Architecture (SOA)** approach that is in synchronization with the NATO Network Enabled Capability/Concept (NNEC) will be able to provide a solution. Also this SOA implementation must be in line with industry recommendations and commercial best practices.

JCOP will eventually be replaced by a fully industrialised NSIP based NCOP solution that will provide a reliable common operational picture and enhanced situational awareness capability to military commanders. The NCOP NSIP project has already been authorized and all experience gained from the JCOP usage during NATO exercises (Steadfast Jackpot, Steadfast Jaw, Steadfast Joist, Steadfast Cathode, Steadfast Juncture and also CWID 2008) will be fed into this implementation.

We need to overcome these interoperability problems – not after the systems are fielded but already in the definition and development phase of the delivery process. ACT has been heavily involved in leading efforts to migrate to an SOA approach and there has been a significant effort in terms of both development (ACT) and implementation (NCSA), with NC3A in close support for “solutioneering”.



As a customer NCSA wants to be able to

- Choose the best solutions on the market
- Plug'n'play COTS & Core services

The “Final SOA Vision” combines the plug'n'play vision with the need to reduce integration/interoperability complexity. In the “Final SOA Vision” is to implement a SOA architecture. The services bus is the integration point of all services from all functional services to the Core/COTS services. The service bus also services as integration point for national systems and NGOs. The service bus must have a few standardized interfaces that supports NATO’s needs to reduce (or even remove) the interoperability challenge. Services can be built from other services enhancing re-use e.g. NCOP is built from the core services and some COTS services. Finally, it should be possible to plug'n'play services and COTS.

All of these ideas are based on the promises of service-oriented architecture (SOA) set by industry. NATO encourages industry to meet these promises by:

- Agreeing on standards for SOA implementation approaches.
- Truly provide COTS services that can integrate across providers – getting away from today's situation with COTS products that are difficult to make work together.
- Make the SOA promise of easier plug'n'play become reality.
- Example: Why can Oracle E-business only work with Oracle DB?



## Cyber Defence

- **Cyber War is ongoing**
- **Enemy has the advantage**
- **Attacks are getting more:**
  - ◆ **Sophisticated**
  - ◆ **Proficient**
  - ◆ **Pervasive**

A visualization of a cyber attack, showing a globe with various colored lines and dots representing network connections and data flows, with some areas highlighted in red and yellow to indicate active or compromised nodes.

As I have mentioned, NATO's CIS infrastructure is complex, far reaching and is absolutely critical to its daily business.

NATO is fighting a war that rarely gets a mention in the public sector. We fight it every minute of every day. Defending and protecting our networks.

We have encountered a range of adversaries from the script kiddie sitting in his or her bedroom, organised criminals, hackers and even nation-sponsored attacks.

These attacks range from being troublesome or embarrassing through to being potentially very damaging. And we see things getting worse. Make no mistake, the attackers have the advantage. They need to find just one vulnerability to exploit while we need to always strike the balance between securing the network but enabling effective use of the network.

And the attacks themselves are growing More Sophisticated, More Proficient and More Pervasive.

Accordingly, we must align and strengthen our defences. This is even more important if we continue the path to NNEC and plug and play of COTS in the SOA.