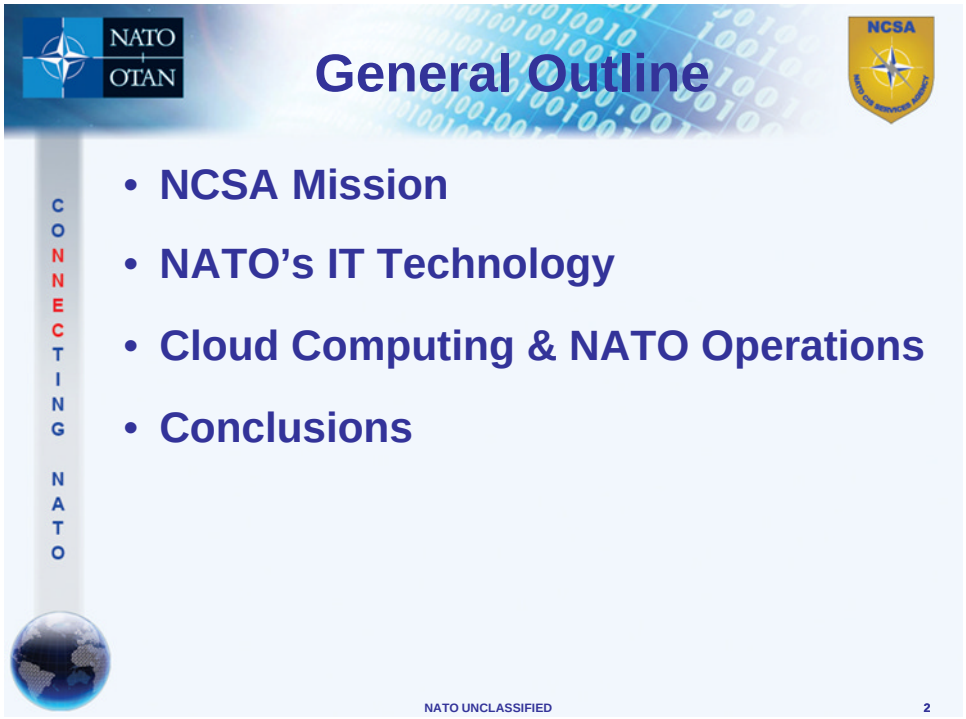
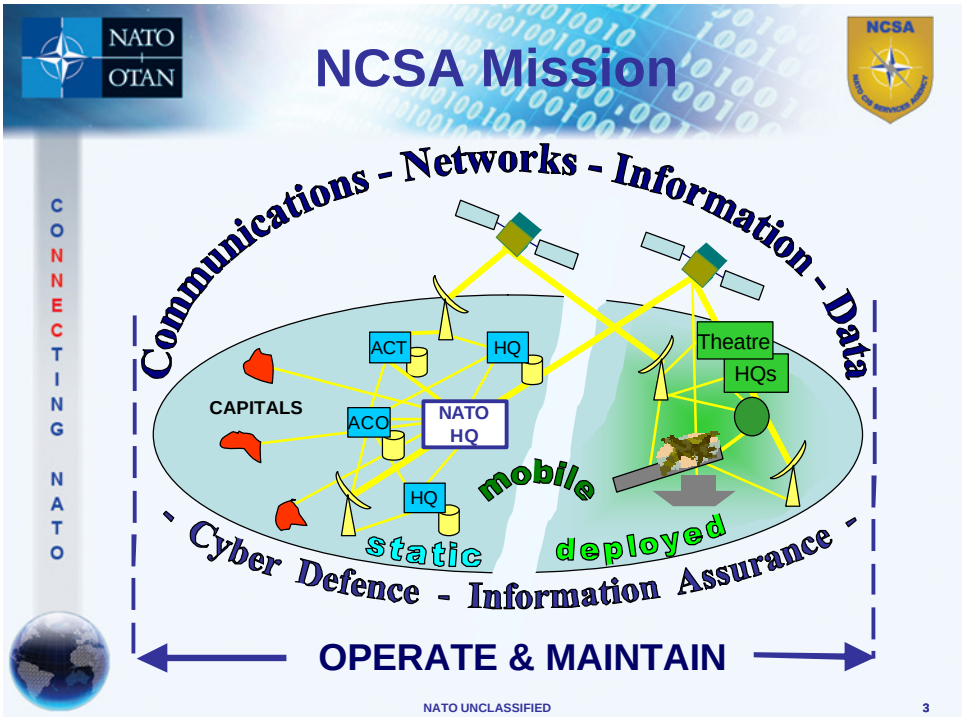
First of all, I would like to thank the AFCEA Europe for this opportunity to contribute in a discussion of **Cloud Computing in NATO Operations**.
Being the Director of Operations at the NATO CIS Services Agency (NCSA), information provision and ensuring integrity as well as the right flow of information in support of our customers are of paramount importance.
Under increased pressure on our financial resources, technologies that can allow us to improve the cost effectiveness of our IT services, and achieve the "famous" **do more with less-paradigm** is certainly of high interest to us in NATO.
As our military operational environment becomes more and more complex while at the same time requiring more and more agility to respond to changing nature of modern warfare, the emergence of commercial technologies (of virtualization, cloud computing, stateless computing etcetera) certainly offers promises of better responsiveness, although non-trivial security issues may limit our ability to exploit them.
Let me turn to a general outline of the topics I will cover.



I would like to begin my presentation providing an understanding NATO's operational IT environment. This is intended to set the background of NCSA's involvement in CIS services delivery and help you understand the complexity of the environment we are supporting.

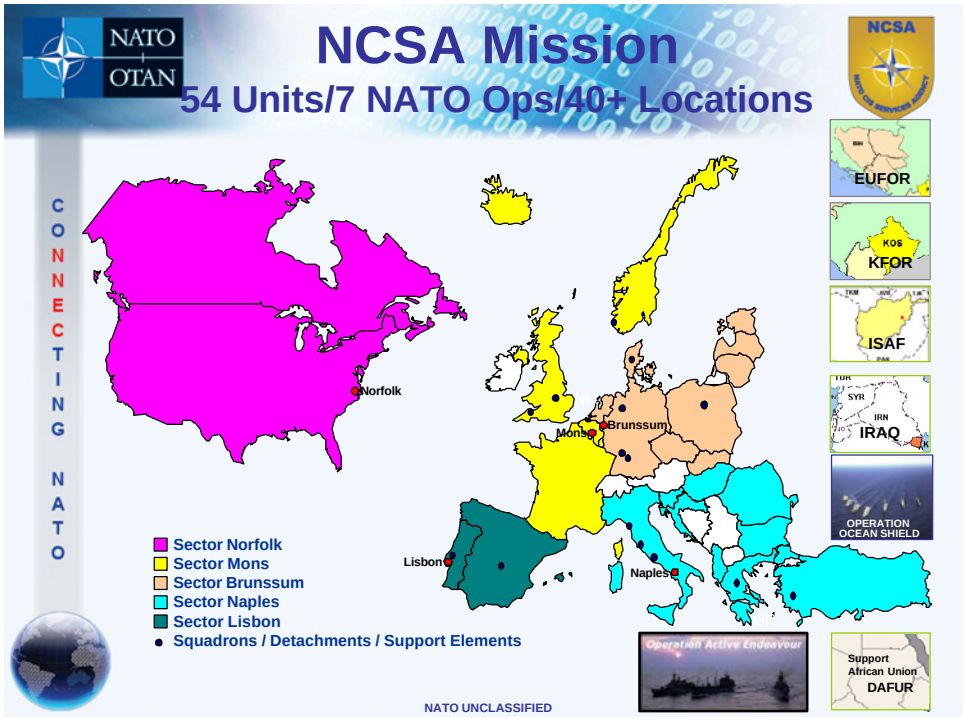
The next part leads us to describe how we in NATO currently see the foundational Cloud Computing technologies fit into our technology roadmap to better satisfy the needs of this operational environment, while minimizing the financial and personnel burden on the nations in the process. Since there are clearly a number of concerns regarding security and reliability issues, there is a clear need to "blend in" a lot of realism into our abilities to work around these concerns (hence the reference to hopes and fears).

And I will finally offer an example of an environment where we currently see the potential for cloud computing technologies to be implemented with good perspectives of rapidly adding value.



NCSA's mission is: To **ensure** the provision of **secure end-to-end CIS services** required for NATO Consultation, Command and Control, **using fielded** Communications and Information **Systems** in the most **cost effective** manner.

We are living in the information age. Connectivity is the prerequisite for successful political and military engagement in support of peace and stability. A truly comprehensive approach requires network enabled capabilities. NCSA is a major stakeholder in the process in NATO of developing, implementing and operating such capabilities..



Our **areas of responsibility** are shared across five (5) Geographic Sectors as shown on this slide.
Beside the provision of CIS services to the static HQs, the Sectors and the subordinate squadrons they are affiliated to, also operate Satellite Ground Terminals and other transmission stations. The sectors are further regularly supporting deployed operations with personnel augmenting the deployed units according to the principle of **cross-utilization**.
This principle also applies to the depot, the signal school and the headquarter divisions.
With different situations at each sector and squadron, it is clear that only a centralized agency like NCSA is able to provide services wherever needed by having the whole picture of all subordinate units and by the ability to relocate resources.
NATO's overarching CIS services, provided by NCSA, enables operations in Afghanistan, the Balkan region and elsewhere. It provides connectivity and services to around 200 sites and to over 100,000 users who are NATO staff, NATO Nations' staffs and Coalition Partners.

SUPPORTING NOTES:
7 NATO Operations:
ISAF

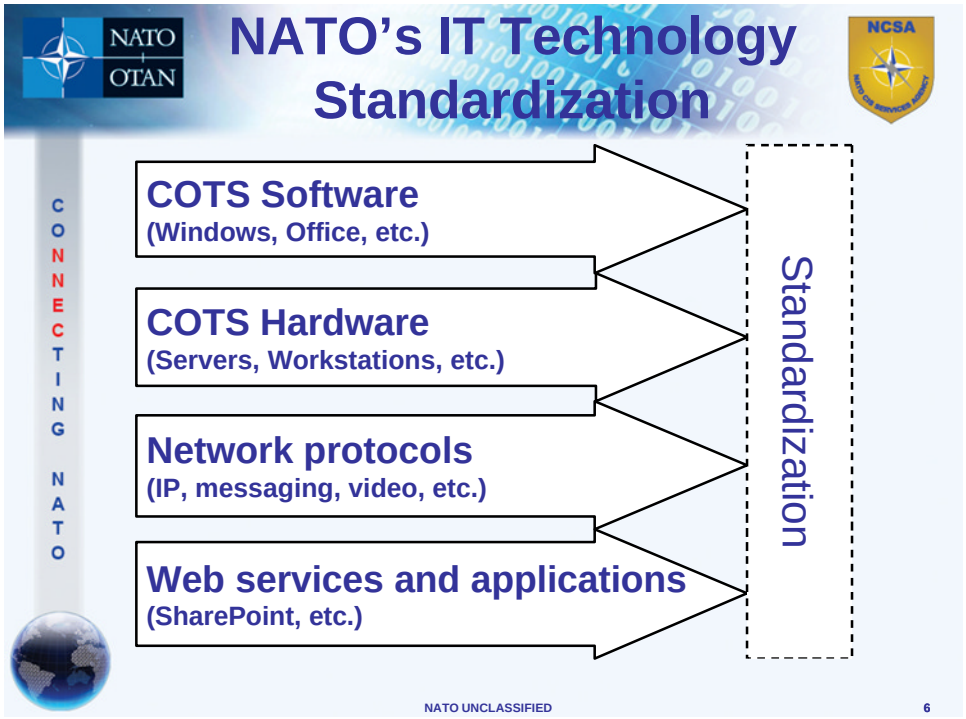
This is the roadmap of the most important technology drivers that we see comprising our future IT services environment in support of NATO's operations.

(Read the bullets or let the audience read them)

The main aims of these capability improvements are the following:

a) To increase the interoperability in our multinational federated IT environment
b) To increase the service levels and user value of our IT services
c) To reduce the cost of ownership to our nations of the IT infrastructure and maintenance

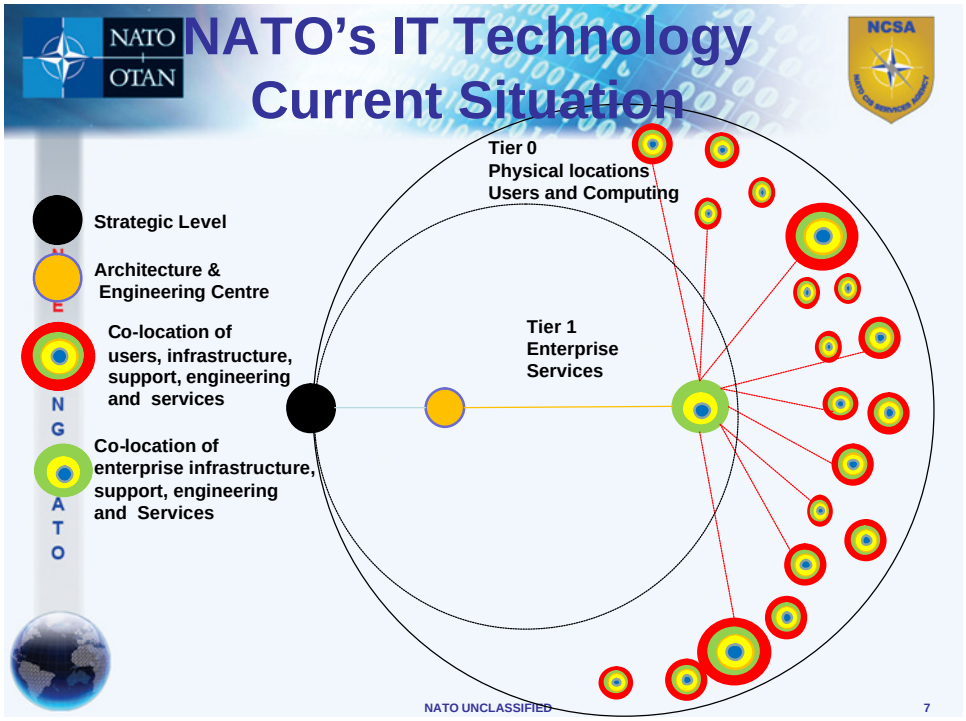
The potential for Cloud Computing technologies to contribute across all of these areas is clear and promising. The next few slides will give some high-level perspectives of the most important of these areas.



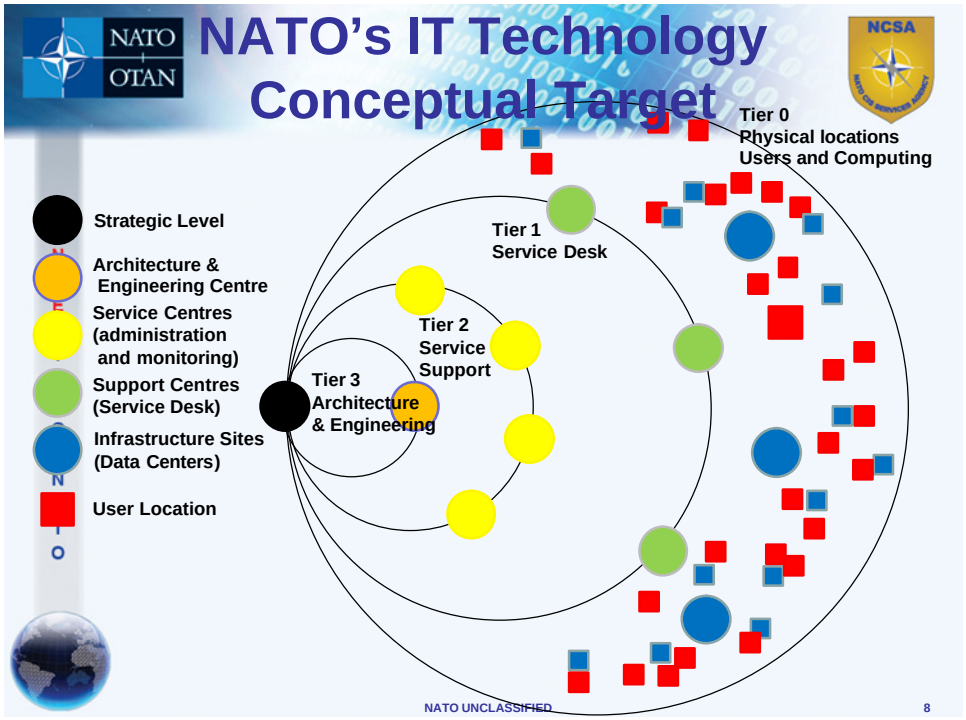
The first step to interoperability is done through the use of standards.
The best way to ensure standardization is:

- not to develop our own software, but use common off the shelf (COTS) software, operating systems, office applications,
- not to fabricate our own hardware, but use COTS servers, workstations, network switches,
- not to re-invent network protocols, but use improved ones, and
- not to re-develop specific user interfaces, but customize those available in the web services and application to meet our needs.

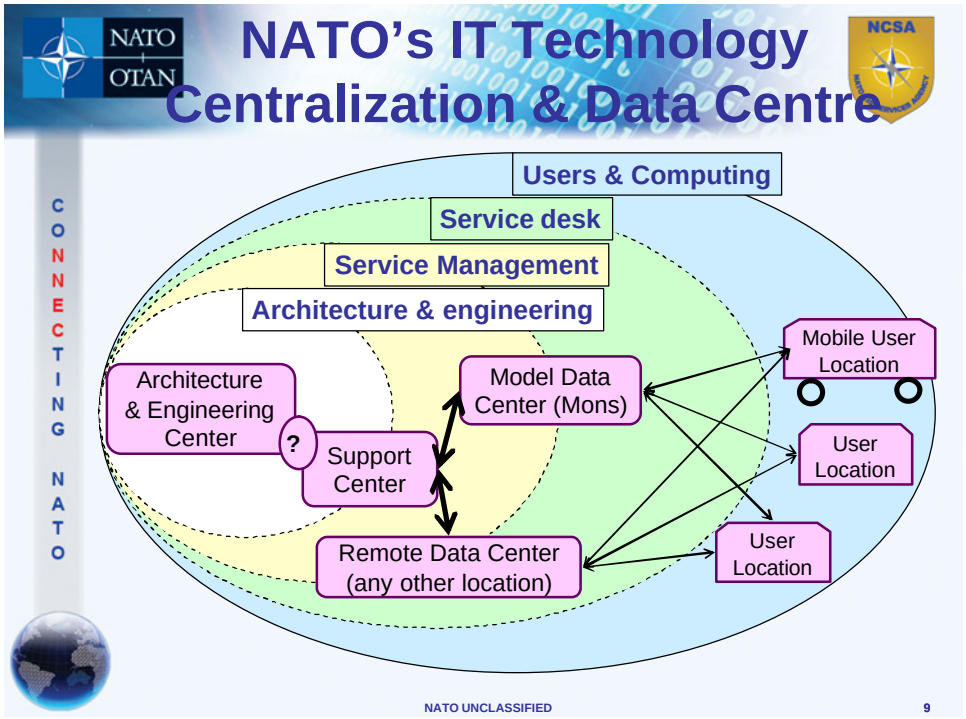
Standardization helps saving resources, manpower and in the end money.
This is the reason why unless the needs are far too specific, standard products must be made working together as much as possible.



Essentially for bandwidth and response time reasons, support had to be close to users, service to support, and infrastructure to service.
This led to small cells, glued together and with users, and able to address all these functions.
Common support and infrastructure could already been unlinked.
Strategic and Engineering levels had no need to stay close.



With bandwidth increase, datacenter technology, remote management tools, things are going to change (have already changed).
Infrastructure sites (blue) can now be "unlinked" and moved away from each other part: the Users (red), the Support (green), and the Service (yellow).
This allow everybody to access any one of the infrastructure resource (according to access rights).
Some infrastructure parts can be regrouped into "lights off" Datacenters, easier to support (power, AC, etc.).
The support level can now be grouped into Support Centers, which can remotely manage the Datacenters.
The services level can be grouped into Service Centers, as is the support.

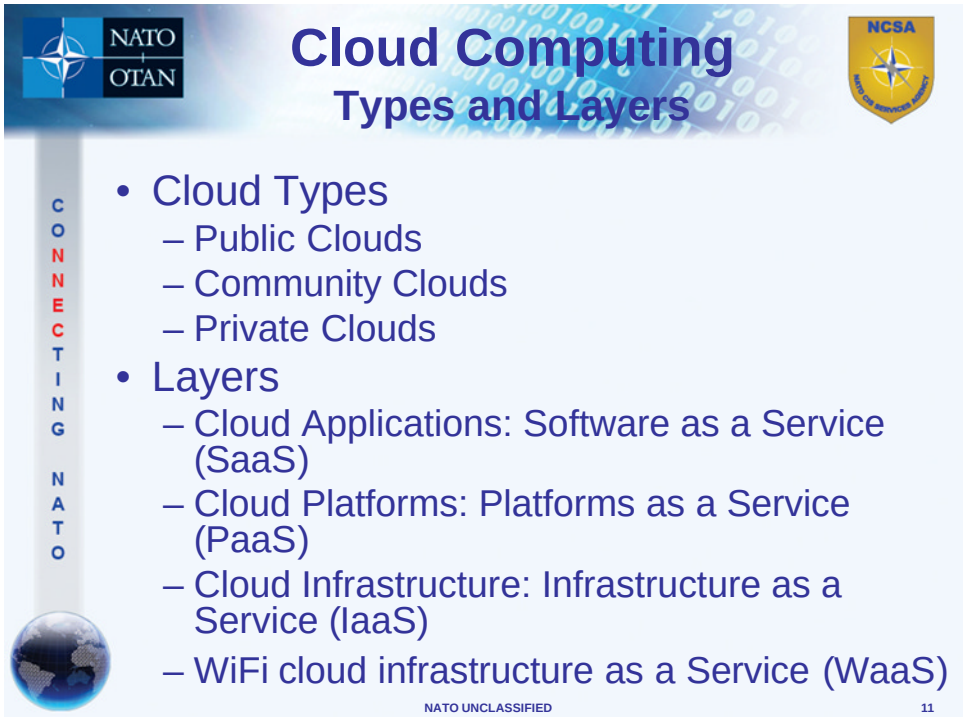


But, besides systems and infrastructure, it is the whole support which must be shared.
This is the reason why the concept of a consolidated Data Center (DC) was created. It provides a capacity to Host Services, Resource Provisioning (Infrastructure as a Service) and Well defined Processes and procedures for Operation, Management, Provisioning and Funding.
These services are provided by Service Management to Users through Service desk.

The Model Data Center (MDC) has to be located on both Service Desk and Service Management in order to insure the best level of service.
It has to be backed up by a Remote Data Center (RDC), used as a spare in case of any type of incident. The RDC must be fully operational in order to reduce the loss of service to the minimum acceptable to users.
The first part of this project is to build the MDC from the existing infrastructures and centralized services, to implement resource provisioning through virtualization and to set up liable processes and procedures. Once the MDC is up, running and liable, the RDC site is to be build , the connectivity between both DC to be enhanced.

The next part leads us to describe how we in NATO currently see the foundational Cloud Computing technologies fit into our technology roadmap to better satisfy the needs of this operational environment, while minimizing the financial and personnel burden on the nations in the process. Since there are clearly a number of concerns regarding security and reliability issues, there is a clear need to “blend in” a lot of realism into our abilities to work around these concerns (hence the reference to hopes and fears).

And I will finally offer an example of an environment where we currently see the potential for cloud computing technologies to be implemented with good perspectives of rapidly adding value.



Private Clouds (suitable for NATO) – Services and resources are made available to only those who have been granted permission and have passed security checks.

Also, in some degree, we are using presented layers:

- For example, applications fully under control of NCSA;
- Key parts of the infrastructure and platform layer is provided to customers in order to have: access control, portal functionalities, and integration facilities

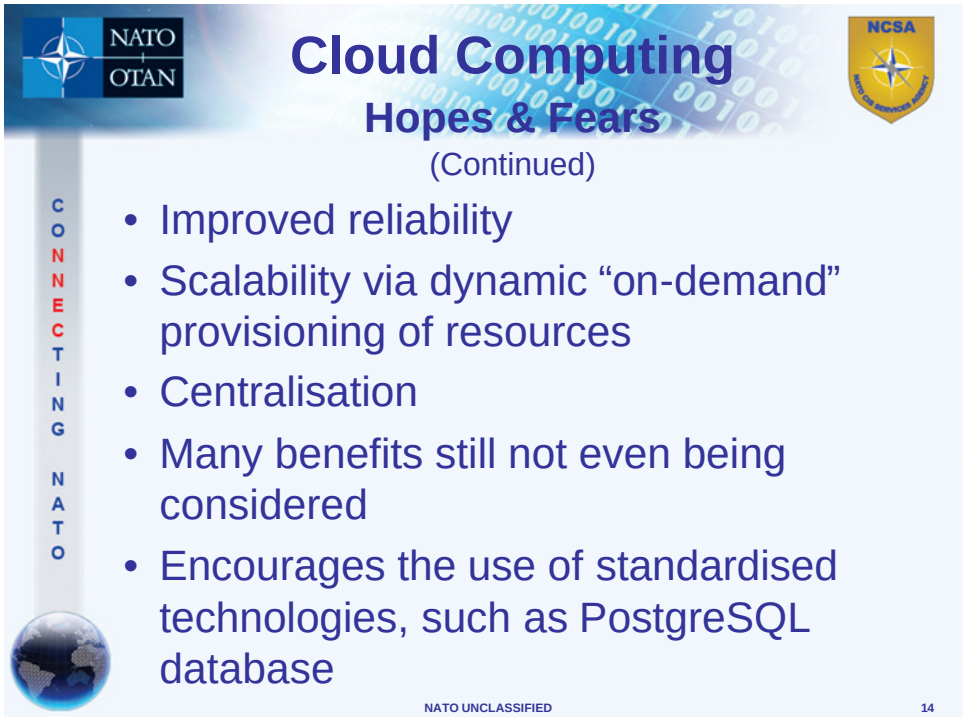
Generally, NCSA realizes the benefits of using Cloud Computing, but we are also aware of the fears related to it.

JOIIS exhibits some of the characteristics of *cloud computing* such as the use of web services.
In the future, it will be possible to scale horizontally by interconnecting different JOIIS servers so that a request from a client can be serviced by any cloud member.
CNAFS is fully web-enabled and centralized. All data is stored and processed on the NCSA datacenter. The system is provided as a service (SaaS); the footprint onsite is limited to standard workstations. The user community doesn't have to worry about installing any new client software, new hardware (server). All CNAFS services are provided centrally as soon as the user is connected to the system.
While we do have some examples of cloud computing in NATO operations, it is generally difficult to implement cloud computing in current NATO operations because many of them are not pure NATO operations, but are "coalition" operations that involve non-NATO entities. Because of this, NATO's legal and security regulations limit the scope of cloud computing utilization.

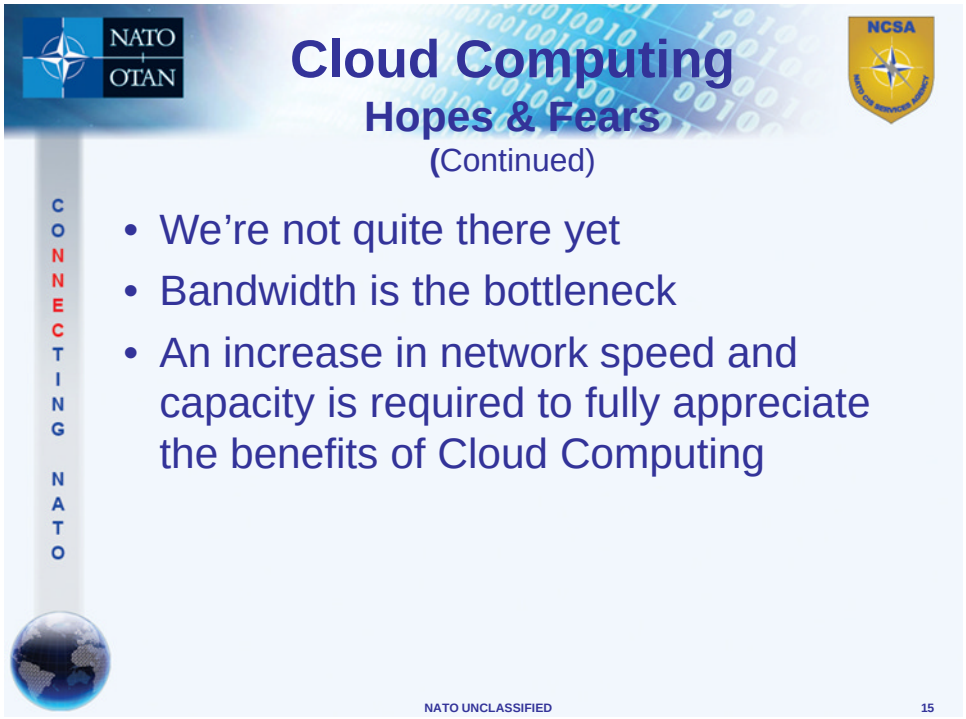
SUPPORTING NOTES:
JOIIS - A situation monitoring and assessment tool. Its primary use, enabling Intel and OPS users to view and analyse the current battlespace objects.

CNAFS - Part of the Logistics Functional Services Capability Package (LOGFAS CP), it provides the following functionalities: Financial Control, Budget Management, Purchasing & Contracting, Accounting, Treasury, Disbursing, Travel Management and Audit.

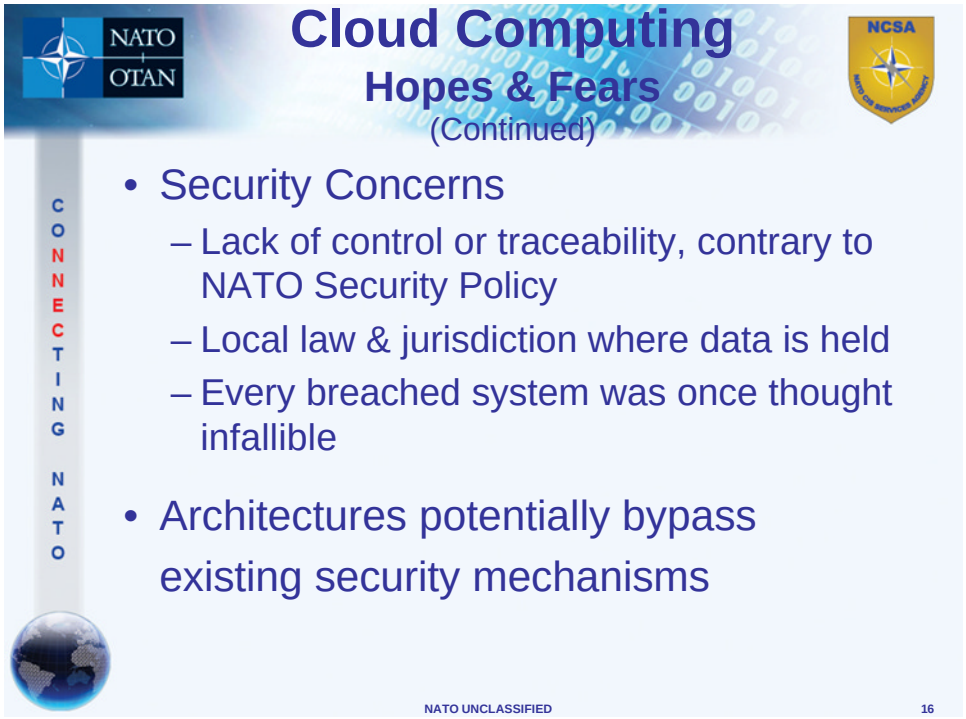
Cloud computing can help to provide huge advantages to NCSA, some of which are being realised already.
Costs are greatly reduced as hardware resources are shared between groups of users and reduced manpower is required to maintain the cloud and the services it provides.
Utilisation and efficiency – Many systems are ‘idle’ much of the time while other servers are at peak load. Within a cloud, load balancing is used to distribute work load to improve performance. Departments do not need their own dedicated hardware. Each server within the cloud can do the same job(s) as any of the others.



Improved Reliability – Multiple redundant sites can be used to avoid a single point of contact and to aid in disaster recovery.
Scalability via dynamic “on-demand” provisioning of resources on a fine grained self service basis, approaching ‘real time’ without users having to engineer for peak load periods.
An NCSA Cloud could be used to centralise all training documents or to enable remote learning resulting in reduced training costs.
Many benefits still not even being considered.



We`re not quite there yet.
The increased usage of Cloud Computing within NCSA would require an increase in network bandwidth. Even the most powerful 'cloud' imaginable is only as fast as the connection speed between the client machine making the request and the cloud itself.
The bottleneck in cloud computing will always be the bandwidth and the quality of the network connection.



As can be seen from the previous discussion there will be very limited use of the outsourced public/ commercial cloud models in our NATO environment, due to issues of security, cyber defence and physical protection

It is, however, expected that solutions to overcome the current security issues will eventually be available, allowing the shared use of data storage and CPU capacity from commercial cloud service providers

What is already now very clear is that “privately” owned and operated networks and datacenters will allow NATO to make full use of a number of the opportunities offered by the technologies delivered by cloud computing products.

A plea to our security “accreditors” and developers of trusted solutions could be to ask for the software that separates the virtualized domains to provide enough trust in the separation to allow the same hardware resources to operate simultaneously with different security levels.