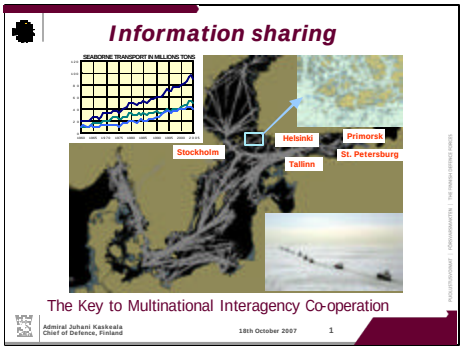
AFCEA seminar in Helsinki 18 October 2007

Information sharing: The Key for Multinational Interagency Co-operation

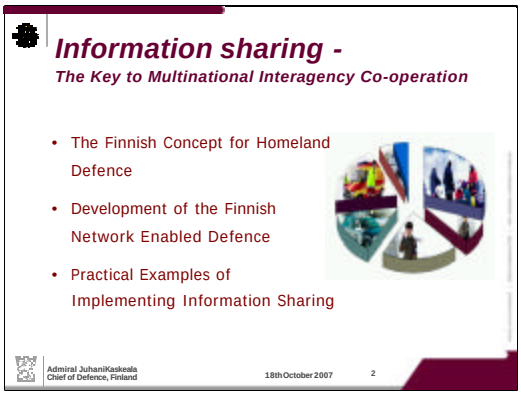
[Slide 0]



[Slide 1]

Mr. Chairman, Ladies and Gentlemen,

I am honoured to address you on the Finnish approach to interagency information sharing and in particular how this concept could be incorporated to multinational and multiagency environment.



-[Slide 2]

- As a background I will present you our concept for homeland defence.

-I will continue with the development plan for the Finnish Network Enabled Defence which describes how modern information technology can support collaboration in complex and unpredictable world around us.

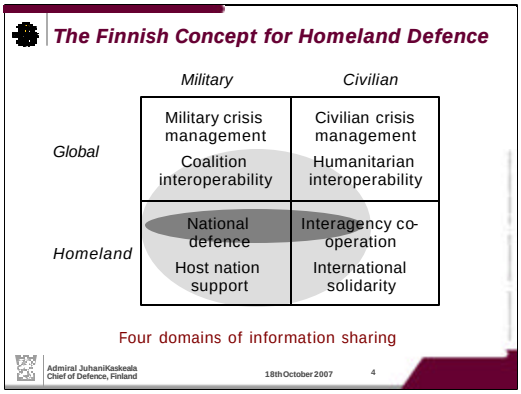
-Finally, I will give you three examples of information sharing and some ideas how these best practises could increase our capability to work together.

[Slide 3]

The traditional Finnish Total Defence concept from the Cold War era has been revised to meet the requirements of today's security environment. The Strategy for Securing the Functions Vital to Society was first approved by the Finnish Government in November 2003. The Strategy was revised in 2006.

This strategy defines the roles and tasks of each Ministry in planning, preparation and execution of crisis management in Finland – including common and agreed threat and crisis scenarios. Co-operation and interaction are common practices today, and even the most difficult situations – also the defence of Finland – are practiced every two years by all necessary authorities in a national wargame.

In principle this mechanism is the Finnish version of the Effects Based Approach to Operations. It does not have all the elements to conduct Effects Based Operations, but it is a comprehensive approach in which all components of national power are brought to bear in a very structured and coordinated way.

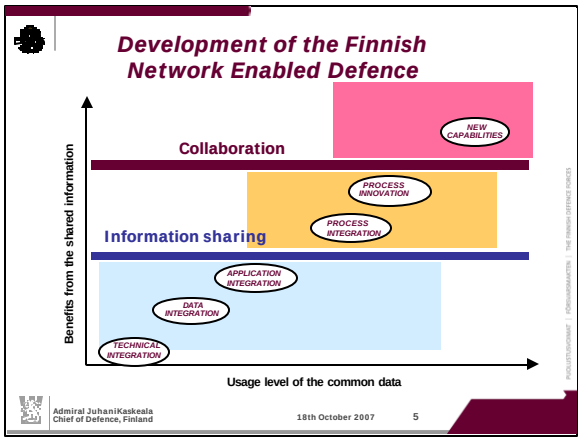


[Slide 4]

One significant capability we need to bring up to date, is multinational interagency co-operation.

The ability to communicate with each other and the ability to share situational awareness and understanding make a good start.

In today's crises there are no strict dividing lines between military and civilian - or global and homeland issues. Same tools and procedures should apply to all situations.



[Slide 5]

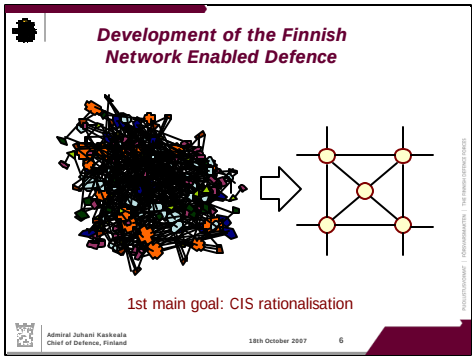
Our Network Enabled Defence development concept is based on our experiences from interagency collaboration both in Finland and in international operations.

The other starting point is our know-how in modern commercial ICT business. We see the Network enabled defence as an evolving concept.

We started our concept development with rationalisation of our current networks. Technical integration and data integration are followed by application integration. The first major challenge is information sharing.

The second challenge we face is mostly cultural – how to collaborate. We need to break the old routines to create new capabilities.

In the third phase we have to find a new way to run the business.



[Slide 6]

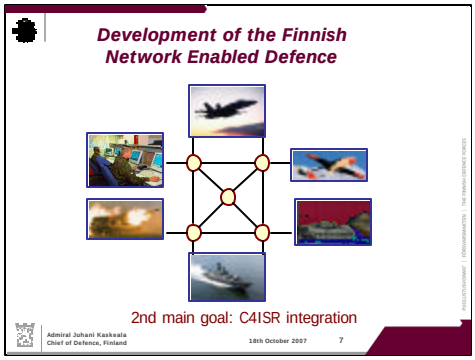
We face the same challenge as most militaries. Our current C2 systems are stove-piped systems developed to support army, navy or air force operations.

Here we see an example of links and interdependencies between different military information systems.

Just a few years ago we tried to map all our communication and information systems. It was impossible. We found over 5500 applications and more than 300 information systems that do not communicate with each other.

So our first main goal is to rationalise current communication and information systems.

The same applies to interagency co-operation since the situation between different authorities and organisations is even worse. In current international operations the mixture of nations and non-governmental organizations multiply the problems.

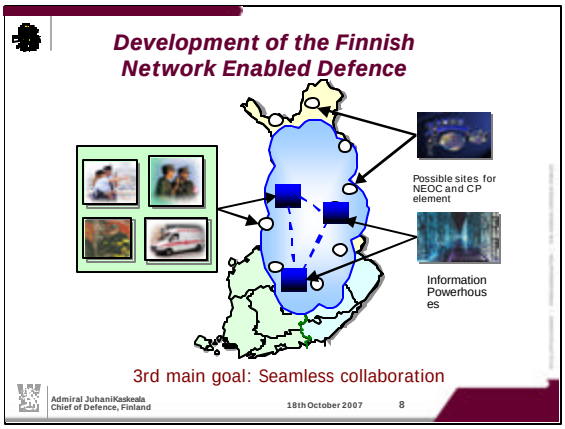


[Slide 7]

Our second main goal is to create a joint and common platform for future operations.

The national information grid will link all sensors, decision makers and shooters to create common situational awareness and enable faster decision making.

This very same principle is also a guiding line when we develop network and services for interagency collaboration. Similar platform is needed for multinational and multicultural environment.



[Slide 8]

The third goal is linked to collaboration: how people communicate and work together.

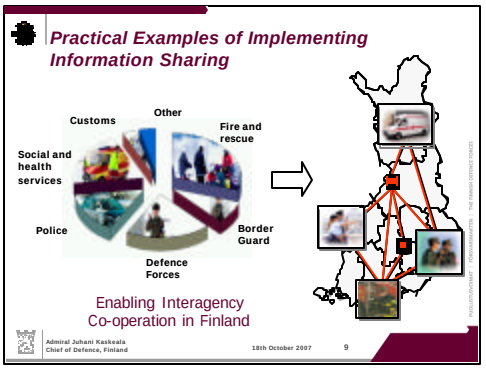
One of our Army Commands was given the task in 2002 to develop and test a Network Enabled Operation Centre (NEOC) concept. After four evolution cycles it has proved to enhance our current capabilities and we have taken it into operational use.

The initial aim with the demonstrator was to improve survivability of Army HQ's by dispersing them to small elements, and to enhance information management with modern information technology.

What we discovered was that we could conduct centralized planning in a distributed environment through collaboration tools and new planning processes.

The NEOC concept enables also interagency collaboration since we can co-locate our partners, such as Police, Search and Rescue Services etc., into the net computer.

Now we can physically co-locate a planning element with them, and at the same time virtually connect with other elements of the HQ.



[Slide 9]

In 1997 the Finnish government made a decision to develop a national mobile communication system for all security authorities based on tetra-technology.

This Tetra-network has been in nation-wide operation for some years. Good experiences in using commercial technology encouraged us to use same approach also in international operations. The basic idea was to use proven COTS-products and solutions in an innovative way that is acceptable to most users – to meet the minimum information exchange requirements.

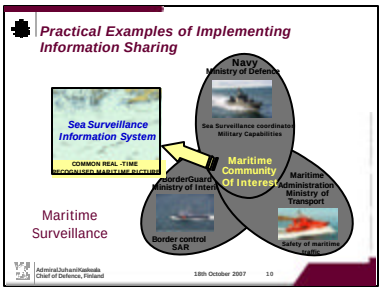
Our next step is to develop a common information environment for all security authorities. To avoid duplication we shall share the Defence Forces communication networks with our key governmental partners.

Ladies and Gentlemen,

The theme for this event is from weather to warfare. All authorities need weather forecasts. In the Defence Forces we used to have different weather messages for air, maritime and ground operations. Today all these messages to military as well as to other authorities are provided by the Finnish Meteorological Agency.

Creation of joint data model for weather messages was one of the first integration steps.

Another step is security authorities' joint positioning system based on Tetra cell location system already in use by the police.

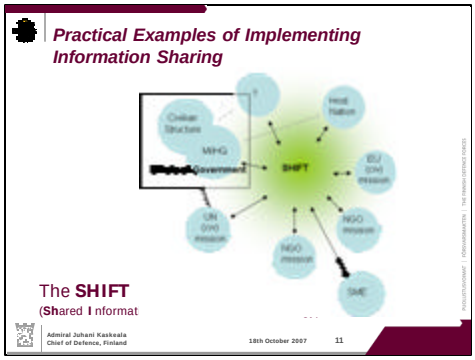


[Slide 10]

Another new key area of interest is Maritime Security. On my first slide there was an illustration of the Sea Lines of Communication in the Baltic Sea. In early 90's all Finnish maritime authorities used to have their own information systems and sensors. The Finnish government decided that there should be no duplication or multiplication of efforts. So all relevant agencies were forced to cooperation by new legislation and a small start-up investment funding.

The Sea Surveillance Information System which compiles and presents the Recognized Maritime Picture is in operational use among all Finnish maritime actors. It also enables electronically integrated information exchange with Sweden. Each participant is given access to the level of their own information requirements. The System has recently been upgraded to fulfil NATO standards.

Based on our experiences with Maritime Surveillance cooperation Finland leads the European Defence Agency's Maritime Surveillance (MARSUR) project. In the US Joint Forces Command-led Multinational Experiment 5 Finland contributes to Maritime Security Awareness (MSA) by linking together pictures of our own Maritime Surveillance system and NATO's Baseline for Rapid Iterative Transformational Experimentation (BRITE).



[Slide 11]

In the MNE5 exercise Finland leads one of the Limited Objective Experiments named Shared Information Framework and Technology (SHIFT).

The SHIFT promotes transparent information sharing among all participants in International Operations. In essence SHIFT is not a system but ability to exchange information between different information domains.

Our intention is to prove that a pool of common security information, that is provided by a trusted party and accessible to all, would benefit everyone taking part in the operation.

[Slide 12]

Finland is one of the first nations to use service oriented architecture and Commercial–Off–The-Shelf technology to build a military command and control system.

We know that are always risk's to be in the avant-garde group but we did not have many options. Most our current command and control systems will be outdated quite soon. We simply can not afford to rely on legacy systems.

On my last slide you can see Gartner's Industry Report's estimate of military Service Oriented Architecture -related development. Our integrated C4I –program is ranked among the top four.

As one of the world's leading IT-analysts Gartner's estimates have been self-fulfilling. I truly hope they have it right also this time.

END