FFI-rapport 2014/00943

Towards NNEC – breaking the interaction barrier with collaboration services

Eli Gjørven, Frank T. Johnsen, Anders Fongen,
Trude H. Bloebaum, and Bård K. Reitan

FFI Forsvarets
forskningsinstitutt

FFI-rapport 2014/00943

Towards NNEC – breaking the interaction barrier with collaboration services

Eli Gjørven, Frank T. Johnsen, Anders Fongen, Trude H. Bloebaum, and Bård K. Reitan

Norwegian Defence Research Establishment (FFI)

25 September 2014

FFI-rapport 2014/00943

1312

P: ISBN 978-82-464-2440-8
E: ISBN 978-82-464-2441-5

Keywords

Samhandlingstjenester

Kommando og kontroll

Approved by

Ole-Erik Hedenstad	Project Manager
Anders Eggen	Director

English summary

The Norwegian armed forces intend to reach NATO Network Enabled Capability (NNEC) maturity level 4 within 2030. The realization of NNEC is essential in developing the future tactical Command and Control (C2) systems for the Norwegian armed forces. Such C2 systems include collaboration services, such as chat, video conference, and document sharing, which enable seamless information sharing and collaboration both horizontally and vertically in the military organization. State-of-the-art collaboration services available in the civil domain, provide remote users a sense of presence despite the geographical distance between them. Applied in the military domain, they facilitate collaboration between soldiers which are in different physical locations, thus minimizing the risk related to traveling in the theater.

In this document, we discuss three main challenges of applying collaboration services in a tactical environment:

- Their *adaptability to the tactical environment* with regard to the challenging network situation found in this environment, the necessity of distribution and the mobility of nodes, and the need for services that are simple to use and administer
- Their *interoperability*, i.e. their ability to interoperate with other systems, in particular the systems applied by NATO allies
- Their ability to satisfy *security challenges* particular to the military domain and the tactical environment

We survey state-of-the-art products, both military and civilian, focusing on how they handle the three main challenges named above, to identify emerging trends and research opportunities. The main conclusions from the survey follow below.

Some of the products available in the civil domain, like Microsoft Lync and Google products, offer advanced collaboration services, which could provide high operational value in the military tactical domain. Considering adaptability to the tactical environment, these products are to a certain degree able to adapt dynamically to network parameters such as available bandwidth and packet loss. However, as they have been designed to operate over the Internet, where the bandwidth situation is very different from in the tactical network, their behavior in the tactical domain must be tested. Furthermore, civil systems are commonly based on centralized solutions, which introduce single points of failure and bandwidth bottlenecks into the tactical environment.

The survey also concluded that the intersection between security mechanisms and interoperability requirements is an area that needs more research, in particular when considering the strict requirements of classified information. Furthermore, we observed that emerging trends from the civil domain introduces new types of collaboration services which should be included in the military domain, and in C2 systems.

Finally, we point out the importance of continuing national participation, including FFI's, in standardization work currently carried out internationally and in various NATO forums.

Sammendrag

Forsvaret ønsker å nå Nettverksbasert Forsvar (NbF) modenhetsgrad fire innen 2030, noe som er avgjørende for utviklingen av fremtidens taktiske kommando- og kontrollsystemer (K2-systemer). Slike K2-systemer inkluderer samhandlingstjenester, som for eksempel "chat", videokonferanse og dokumentdeling, og de muliggjør sømløs informasjonsdeling og samarbeid både horisontalt og vertikalt i den militære organisasjonen. Moderne samhandlingstjenester som er tilgjengelig i det sivile domenet, tilbyr brukere som befinner seg på ulike fysiske lokasjoner, en følelse av samvær, til tross for geografisk adskillelse. Anvendt i det militære domenet, muliggjør de samhandling mellom soldater som er på ulike geografiske lokasjoner, og minimaliserer dermed risiko relatert til det å bevege seg i operasjonsområdet.

I dette dokumentet diskuterer vi tre avgjørende utfordringer ved å anvende samhandlingstjenester i et taktisk miljø:

- Muligheten til å *tilpasse tjenestene til det taktiske miljøet* med tanke på vanskelig nettverkssituasjon, nødvendigheten av distribusjon og nodemobilitet, og nødvendigheten av enkelhet i bruk og administrasjon
- Tjenestenes *interoperabilitet*, det vil si deres evne til å interoperere med andre systemer, spesielt systemer anvendt av andre NATO nasjoner
- Tjenestenes evne til å tilfredsstille *sikkerhetskrav* særskilt for det militære domenet og det taktiske miljøet

Vi presenterer en undersøkelse hvor vi har kartlagt produkter som tilbyr samhandlingstjenester, både militære og sivile. Vi fokuserer på hvordan de håndterer utfordringene nevnt ovenfor, for å identifisere fremvoksende trender og forskningsmuligheter. Hovedkonklusjonene er som følger.

Noen av produktene som anvendes i det sivile domenet, som for eksempel Microsoft Lync og Google produkter, tilbyr samarbeidstjenester som kunne gi høy operasjonell nytteverdi i det militære taktiske domenet. Når det gjelder tilpasningsdyktighet, evner disse produktene til en viss grad å tilpasse seg nettverksparametere som for eksempel tilgjengelig båndbredde og pakketap. Imidlertid er disse produktene designet for å operere i en internettomgivelse, hvor båndbreddesituasjonen normalt er veldig ulik den i det taktiske miljøet. Derfor er det nødvendig å teste disse produktenes ytelse under betingelser som likner det taktiske miljøet, for å finne ut hvilken nytte disse kan gi i praksis. Sivile systemer er dessuten ofte basert på sentraliserte løsninger, som introduserer såkalte "single points of failure" og flaskehalser i det taktiske domenet.

Undersøkelsen fant også at skjæringspunktet mellom sikkerhetsmekanismer og interoperabilitetskrav er et område som er interessant for videre forskning, spesielt med tanke på de strikte kravene som gradert informasjon stiller. Videre observerte vi at trender fra det sivile domenet introduserer nye typer samhandlingstjenester som bør inkluderes i det militære domenet, og i K2-systemer.

Til sist fremhever vi viktigheten av å fortsette nasjonal deltakelse, inkludert FFIs, i standardiseringsarbeid som foregår internasjonalt og i diverse NATO forum.

Contents

1 Introduction

The realization of NATO Network Enabled Capability (NNEC), or the Norwegian equivalent Network Based Defense (NBD) (“Nettverksbasert forsvar”), is essential in developing the future tactical Command and Control (C2) systems for the Norwegian armed forces. In [30] NNEC is described as follows:

> The NATO Network Enabled Capability (NNEC) programme is the Alliance’s ability to federate various capabilities at all levels, military (strategic to tactical) and civilian, through an information infrastructure. But the main objective of the NNEC programme, illustrated by the slogan Share to Win, is to initiate a culture change that begins with people. Interacting with each other and sharing information will lead to better situational awareness and faster decision making, which ultimately saves lives, resources and improves collaboration between nations.

The goal for development of NNEC as presented in [21], is that in large, the Norwegian armed forces should reach NNEC maturity level 4 (NML4), called the “Collaborate” level, within 2030. [42] describe maturity level 4 as follows:

> Major organizational and process changes are evident in this level of maturity because of greatly enhanced information sharing, and rich continous interactions between entities allowing vertical synchronization through collaboration and planning and horizontal synchronization through shared situational awareness and understanding of intent.

To be able to achieve this level of information sharing and interaction, a rich set of collaboration services must be available that facilitate seamless interaction across the theater. Commercial products that provide such services are not designed to meet the challenges of the tactical domain, in particular lack of stationary infrastructure, low and varying bandwidth, and security requirements which extend the ones met in a business-like environment.

1.1 Realizing NNEC in the Tactical Environment

Figure 1.1 illustrates the organization and physical layout of a military formation[1]. A military formation is typically hierarchically organized, as indicated by the figure. The chain of command for land forces stretches from the Norwegian Joint Head Quarters, through the brigade level, down to the battalion, company and platoon units. Shared situational awareness and decision making processes require information sharing and collaboration between different levels.

The physical layout of the formation often corresponds with the hierarchical organization; people, physical resources, and infrastructure are clustered in command posts, which are connected by

[1] A military formation as illustrated by the Norwegian Defense “NbF Kampanjeplan”.

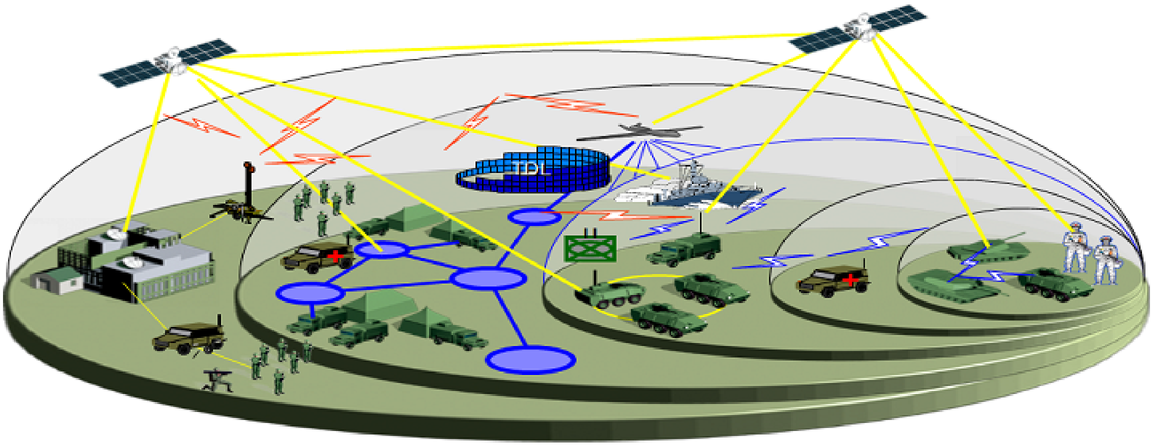

Figure 1.1 The organization and physical layout of a military formation.

communication infrastructure. Units that are on the move, like platoons, squads, or single vehicles or aircrafts, may connect to the command posts and other units using wireless communication like radio or satellite.

Across this complex and heterogeneous environment, NNEC must be established. Technically, NNEC is realized through a Networking and Information Infrastructure (NII)[2] supporting information exchange in the tactical domain. Among many different types of services, the NII includes collaboration services such as e-mail, audio- and video conferencing, and different types of shared applications, such as document editing, presentations, etc. These services provide users with a sense of presence across the theater, as they make transparent the different physical locations of users, and the potentially great distance between them, as we discuss in the next section.

1.2 Operational Value Provided by Improved Collaboration Services

Improved collaboration services enable seamless and transparent information sharing and collaboration both vertically and horizontally between units in the military hierarchy. The added operational value can be summed up as follows.

Presence: Collaboration services provide users with a sense of presence across the theater allowing them to communicate and collaborate as if they were in the same physical location. Different services give different degrees of presence; While the combination of an audio conference and shared presentation slides gives a feeling of sharing a virtual meeting room, a video conferencing service may give the participants a feeling of being present in the same room. A feeling of presence between leaders and subordinates may contribute to better quality of communication, which enables *improved understanding of the leader's intent* and *improved common situational awareness*.

Improved products and decisions: Collaboration services facilitate immediate interaction between

[2] The Norwegian term “Informasjons infrastruktur” (INI) is equivalent to NII

units and levels. Users are able to easily contribute into processes where it would be difficult, sometimes impossible, to participate without such services. Information can be made directly and immediately available to decision makers. Thus, collaboration services may improve the quality of both products, such as intelligence reports, the common operational picture, plans, and "milgeo" products, and decisions.

Minimize time and risk: Collaboration services enable decentralized and parallel planning, and distributed decision making, which speeds up planning and decision making processes. Furthermore, as users do not have to physically move to participate in a planning process, both travel time and risk is minimized.

Less misunderstandings and errors: Collaboration services include a wide range of services suitable for different situations. Being able to choose the most suitable service improves the chances of conveying the correct information. As an example, text messages communicate numbers and letters better than audio and video, because mishearing is avoided. On the other hand, audio and video conferences communicate a more complete picture of the situation a person is in, as audio communicates the tone of his voice, and video communicates his face and body language.

To achieve maximum operational value, the choice of collaboration services must be based on the operational needs, not technical limitations. Unfortunately, in a tactical environment, the optimal solution will some times not be available. As an example, video conference will never be able to function when only low-bandwidth military radios are available. However, it is important that the selection of services which are developed and deployed to the theater is not limited by worst case scenarios. The user should be provided with a set of solutions which are *the most suitable solutions available in the current situation*, so that he can select the service that gives him the highest possible operational value at the moment.

1.3 Focus

The process towards maturity level 4 is not only a technology development and exploitation process. It also includes development of culture, competence and organization where such collaboration happens. However, this report focuses on technology development, and in particular development of technologies which contribute to information sharing and collaboration services which will be required to reach maturity level 4 in future tactical systems. The report concludes by identifying the technology areas where more research is required, in order to reach this goal.

Based on general requirements to tactical C2 systems identifies in [41], we focus on the following three technical challenges:

Adaptability to the tactical environment: Collaboration services applied in the tactical environment must be able to adapt to challenging resource situations, due to limited network capacity and mobility of nodes. Furthermore, they must require minimum technical expertise to be manageable for the personell available on the tactical level.

Interoperability: Collaboration services must facilitate collaboration between military forces and a wide range of other actors, such as allied nations, civilian actors, govermental actors, non-govermental organizations, etc. Thus, they have to interoperate with systems applied by these actors, meaning that they need be able to interact with other systems through the use of open standards.

Security: Security properties, such as confidentiality, integrity, and availability, must be supported, in order to handle security requirements of collaboration services running in the tactical environment. In particular, they need to manage the security requirements of all relevant security levels, and information flow between security domains.

This report includes a discussion of how existing systems and services meet these challenges, focused on state-of-the-art civil collaboration products and tools. We focus this study on services that are generic by nature, with respect to the function or work process they support, as opposed to systems and services that are designed for specific tasks, such as operation planning or fire support. However, as we discuss later in this report, this distinction is not always complete; some generic services can be configured and used in a way that makes them more thightly coupled to specific tasks.

1.4 Organization

The document is organized as follows. In Section 2, we describe the collaboration services which are the focus of this document, and the characteristics of such services. In Section 3 we discuss the challenges of adapting collaboration services designed for the civil domain, directly in the tactical environment. In Section 4 we discuss the problems of interoperability of collaboration services in different technical perspectives. In Section 5 we discuss challenges related to the strict security requirements we meet in the tactical domain, and how they apply to collaboration services. In Section 6, we provide an overview of state-of-the-art collaboration services and products, both from the military and civil domains, and we discuss how these services and products satisfy the challenges discussed in sections 3, 4, and 5. In particular, we focus on the applicability of Commercial Off The Shelf (COTS) solutions in the tactical domain. Finally, in Section 7 we sum up conclusions drawn from this work, and we present areas which need more research and development in order to provide state-of-the-art collaboration services in the tactical environment.

This report is part of the background documentation to be delivered in FFI project 1312 ("Taktisk ledelsessystem for landdomenet"). However, the report is also the result of a joint efford between project 1312 and the following projects on FFI, all with a technology focus:

- 1277 ("Informasjons- og integrasjonstjenester i INI")
- 1294 ("IKT-sikkerhet i Cyberdomenet (ISIC)")
- 1343 ("Smart samhandling i det nye informasjonslandskapet")

2 Collaboration Services - Technology and Trends

In this section, we present technology and trends relevant for introducing state-of-the-art collaboration services into the military tactical environments. We give an overview over the collaboration services which are the focus of this report.

2.1 Collaboration Services and Service Orientation

According to [42], NNEC maturity level 4 allows seamless sharing of data and horizontal and vertical interactive collaboration, which is supported by flexible services providing coherent functionality available in the common NII. In the NNEC Feasibility Study [4], Service-Oriented Architecture (SOA) was suggested as the enabling paradigm for building applications, services, and supporting mechanisms, that realize NNEC. There, a service is defined as "a contractually defined behavior that can be provided by a component for use by any component, solely based on the interface contract". When we use the term "service" in this report, we refer to the concept of a service as defined here.

The most important principles of SOA include:

- Explicitly defined interfaces
- Services should be discoverable
- Services should be based on standards
- Loose coupling
- Reusability
- Policy-driven

There are two activities within NATO which are important for the development of service oriented Command and Control (C2) systems between NATO nations.

First, the NATO Consultation, Command and Control (C3) Classification Taxonomy (*C3 taxonomy* for short) [1] is a categorization of the functionality that is expected to be found in the NII. As this report focus on generic collaboration services, the services included in this study corresponds mainly to the services referred to as "Unified Communication and Collaboration Services" by the C3 Taxonomy. However, as some of these generic services can be adapted to certain functions and tasks, they may in some cases develop into services that are more closely connected to one or more Communities Of Interest (COIs), referred to as "COI-Enabling Services", or maybe even "COI-Specific Services", by the C3 taxonomy.

Second, the specification of the standards to be applied by in the services available in the NII. NATO's standardization efforts are instrumental in the development of interoperable systems within the NATO collaboration, and are as such an important subject throughout this report, and discussed in particular detail in Section 4 of this document.

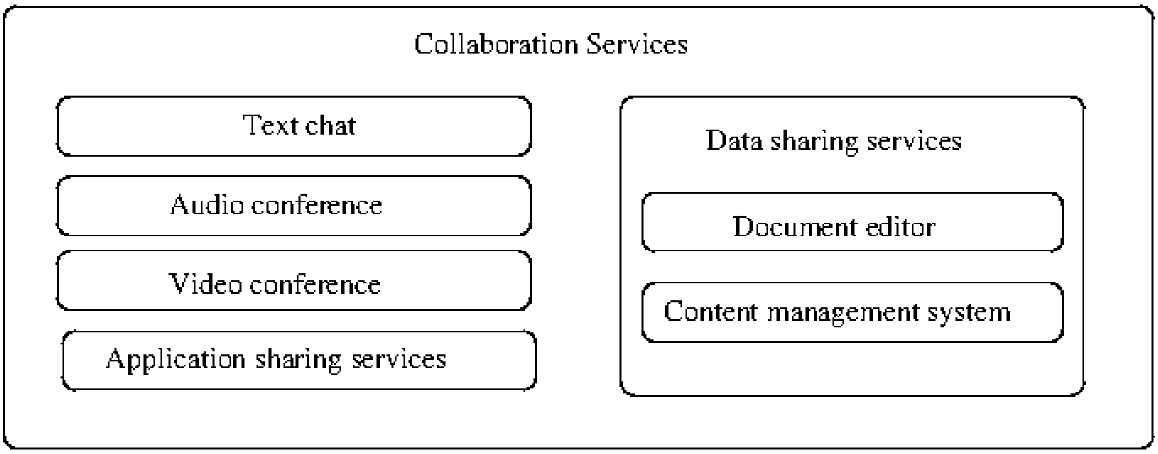

Figure 2.1 The collaboration services included in this study.

2.2 Collaboration Services Overview

In this section, we give an overview over the set of services which are discussed in this report. As illustrated by figure 2.1, the included services are

- Text, audio and video based collaboration services
- Application sharing services
- Data sharing services

These services have been selected because we believe that they will provide high operational value both in short term and in the future, and because they technically span the room of challenges and requirements of many types of collaboration services.

2.2.1 Text based collaboration services - chat

Text based collaboration services, often called chat, allows users to exchange relatively brief text-based messages in near real-time. The messages can be delivered either between two participants (instant messaging), or between several participants (chat room). Popular chat applications are Google Talk in the civil domain, and JChat [32] in NATO.

2.2.2 Audio based collaboration services - audio-conference

Audio based collaboration services provide two-way audio communication between two or more participants, called an "audio conference". Users expect real-time behavior from an audio conference, which means that there should be no perceptible delay. The service must provide an application allowing users to connect to an audio conference. Normally, all participants have the opportunity to speak, but in some cases one may want to mute some of the participants. Examples of applications providing audio conferencing services are Skype and Google Talk.

2.2.3 Video based collaboration services - video-conference

Video based collaboration services provide two-way video communication between two or more participants, called a “video conference”. A video conference normally also includes audio communication. Video conferencing services are similar to audio conferencing services in many respects: Users expect real-time behavior, the service must provide an application allowing users to connect to a video conference, and all or only some participants could be allowed to speak and send video. Many applications are able to support both audio and video conferences, including the above-mentioned Skype and Google talk.

2.2.4 Application sharing services

Application sharing services allow sharing an application user interface over the network to several concurrent users. An example of an application sharing service is a remote desktop application, where an entire desktop, potentially with arbitrary applications, can be shared. With application sharing, all participants should have the same view of the application. Thus, updates in the applications must appear to all the users in near real-time and in the same order, which means that reads and writes to the application state must be synchronized.

2.2.5 Data sharing services

Data sharing services allow several participants to view and edit data elements from different locations. To ensure that users do not overwrite each other’s changes, data access must be synchronized. Among document sharing services, we make the distinction between *shared document editors* and *content management systems*.

A *shared document editor* supports editing of shared documents, where we consider a document to be a single computer file containing text, graphics, pictures, or other types of computer processable content. The editor may support simultanous edits, where several users makes changes to the same document at the same time, and where all users have the same view of the document state at all times. In addition to document editing, a shared document editor often provides basic document management functionality, such as versioning, merging, and rollback. An example of a document sharing service is Google docs, commonly used in the civil domain.

Content management systems supports building meaningful structures of content from several documents, potentially containing different types of data, beyond that of a simple file-structure. As an example, Microsoft’s Sharepoint server contains a web content management system supporting web-site content authoring and publication, and content structure and deployment management. Content management systems can be set up and configured to suit a specific purpose, in which case they can be applied in a similar way as COI-Specific Services.

2.3 Characteristics of Collaboration Services

In this document, we focus on the following characteristics and Quality Of Service (QoS) requirements of collaboration services, which make them challenging to use in the tactical environment:

Bandwidth demanding: Some collaboration services require transmission capacities that are not always available in the tactical environment. In particular, this is true for video-based collaboration services, which may require in the order of hundreds to thousands of kilobits per seconds (kbps). Even though available bandwidth capacity is generally increasing over time, bandwidth is likely to be a limited resource in the tactical environment in the foreseeable future. Thus, particularly bandwidth demanding applications may in some situations have to reduce the rate of transmitted or received data to a minimum, or they may not run at all.

Data delivery requirements: Collaboration services have two different types of delivery requirements:

- *Reliable delivery*: All data passed from the sender is delivered to the receiver. Unless the entire message or file has been delivered, data can not be processed and understood. For example, messaging services typically require reliability.
- *Timeliness*: Data must be delivered within a certain time limit to be useful. For example, audio and video applications typically have timeliness requirements; An audio chat application only works well if audio data is delivered within a time-limit.

When the delivery of data triggers a response from the receiver, the application is also called *interactive*. Interactive applications may become useless if delivery requirements are broken. In the case of audio-chat, the participants will start interrupting each other if the delay becomes large. If the delay becomes too large, it is impossible to have a conversation.

Synchronization: Applications where several users operate on a shared application state, such as a shared document or a shared application, has to provide the application users with a common view of the application state. If the system allows concurrent updates to the same state, it must keep control over concurrent reads and writes, to avoid *consistency problems*. As an example, if several users are editing the same document, the application must ensure that only one user at the time may edit the same content, while different users may edit different parts of the document concurrently. Synchronization requires a yet another type of delivery requirement called *group synchronization*, meaning that data must reach a group of users in the same order. Such delivery requirements may be difficult to satisfy in a tactical environment where communication infrastructure services may suffer from poor and unstable radio links, introducing delays and losses in data transfer.

Non-binary quality requirements: For some services, the quality experienced by the user may vary greatly between a service that is “not useful”, in the sense that the experience is so poor that user may just as well quit the service, to “perfect”, which is the quality that the user would expect in a situation where resources were infinite. As an example, a video in low resolution would often be better than no video at all, but the higher the video resolution is, the better the user experience. The term "non-binary quality requirements" reflects this spectrum of acceptable quality levels where some are better than others. The achieved quality level often depends strongly on the available bandwidth and the delivery characteristics provided by the communication infrastructure.

Service	**Bandwidth demanding**	**Content delivery requirements**	**Concurrency control**	**Non-binary quality requirements**
Text chat	N	R, T	D	N
Audio conference	N	T, R	N	Y
Video conference	Y	T, R	N	Y
Data sharing	D	R, TD	Y	N
Application sharing	D	R, T	Y	N

Table 2.1 Services and characteristics. The letter indicates Y = yes, N = no, D = depending on the application, R = reliability, T = timeliness.

Table 2.1 sums up which services have which characteristics.

2.4 Trends in Collaboration Services

In this section, we discuss three emerging trends from civil state-of-the-art collaboration services, namely *data centricity*, *context and semantic awarenessness*, and *composite collaboration spaces*. These trends are particularly relevant for application and data sharing services as described above.

2.4.1 Data centric services

Some collaboration services are characterized by that they concern the facilitation of collaboration *on something*. The main aspect of these services is the collaboration on some product, and less on passing messages or providing media streams. These services naturally lend themselves to a *data centric* architecture as the collaboration supported by these services evolves around sets of data or information products. Among the services listed above in Section 2.2, both data sharing services and application sharing services evolve around the collaboration of data or application products, and are as such examples of data centric services. These services need to maintain shared state of the current product and provide efficient ways to collaboratively work on these products.

As the data centric structure is very common among services found on the Web, the Web and the Mobile Internet are powerful drivers for development in this area. Data centric systems provide simple services on the server side, such as the standard Hypertext Transfer Protocol (HTTP) operations GET, POST, PUT and DELETE. The simplicity of the server side operations allows clients great flexibility to implement different types of business logic on the client side. Thus, data centric systems promote innovative use of the data on the client side, but they are not suitable for restricting the use of data to a certain logic or given business processes.

2.4.2 Context and semantic aware collaboration services

Traditional collaboration services, like chat, audio and video conferences, and shared document editors, primarily support problems of general character. In their basic implementations, most of these services tend to have very simplistic data-models. However, a trend we may observe is the move from general applications and simplistic data-models to more complex applications and advanced data-models that are more tightly coupled to a particular business process; they are aware of the context in which they are being used, and the semantics of the data they process.

Context and semantic aware services are often semi-structured, and they use technologies like micro formats and common ontologies to format and process data, potentially in combination with contextual information. Based on semi-structured information, one may be able to build applications that resembles a web of information pieces, linking to other applications, much in the same way as we have observed with web-pages, going from simple text only documents all the way to complexly linked data and interactive web applications. For example, a service with a document editor may recognize e-mail addresses, names, places, geo-points, URLs or URIs. This information may be used to engage related services, such as e-mail services or map services.

If this trend is continued in the military domain, traditional collaboration services will have to interact with COI services, like situational awareness services and planning services. The challenge of including, presenting and viewing COI data is something future collaboration services may be expected to handle.

2.4.3 Composite collaboration spaces

Civil state-of-the-art collaboration tools combine several collaboration services into composite collaboration spaces, where services can be accessed individually or seamlessly combined, depending on user needs. For example, messaging, forum or streaming services can be combined with voice or video conferencing services into one service. Such combinations may facilitate more efficient collaboration.

Composite collaboration spaces may be set up casually by the end-users, but are more efficient if the services are designed to be aware of each other, and integrate at points with relevance for efficient collaboration. An example of a collaboration service which is collaborative by nature, and therefore naturally in its design, is a virtual world. A virtual world combines different media streams with the ability to share other services within the virtual world, allowing for context aware collaboration [20].

While building composite collaboration spaces has many implications, we emphasize the following which we consider most important:

- As mentioned above, it should be possible to combine different services dynamically, or at least by integrating them into a combined application suite. This implicates that services need to be available on the user's preferred device(s), rather than on separate devices or installations. For example, to be available for integration with other services, a video conference application should be installed on the users laptop or portable device, rather than as a separate video conferencing studio.

- When services are running in the same physical environment, they depend on the same physical resources. Thus, they should be subject to unified service management and control, as the instantiation and configuration of each service impact other services. For example, if the available bandwidth is reduced during a combined video conference and slide presentation, control mechanisms should suspend the transmission of video data, in order to prioritize audio and slides.
- The services should be subject to a unified security regime, with centralized management and single sign on across different security domains, as further described in Section 5.3 in this report.

3 Adaptability to the Tactical Environment

Collaboration services are widely used in the civil domain today. However, the tactical environment is very different from the civil, Internet-like environment in which these services normally are used. Below, we describe certain challenges of the tactical environment wich can make it difficult to reuse civil services directly. We discuss how collaboration services need to adapt to these challenges, to be able to provide the user with a satisfactory QoS also under these difficult circumstances.

3.1 Limited and Varying Network Resources

In the civil domain, and in particular in the business segment, we assume high capacity networks to be available. In the tactical environment, as there is often no static communication infrastructure available, one may have to be established. Normally, this communication infrastructure is based on wireless links. The potentially great distance between units, and the physical and geolographical environment in the area, can make it difficult to establish a reliable communication infrastructure with sufficient capacity. The result may be an infrastructure consisting of very different communication technologies such as satellite communication, mobile wireless broadband (such as 3G, Edge, and 4G), and tactical radios. These technologies have very different communication capabilities. Thus, services running in the tactical environment must be capable of adapting to the currently available network situation at all times, in particular considering

- the *available bandwidth*, which may vary in scale from bytes per second on a narrow-band tactical radio, to megabits per second on a broadband tactical radio or satellite communication
- the *loss of packets*, which is common on all types of wireless links due to distance, obstacles, and interference
- the *delay of packets*, which varies with wireless technology and traffic

Adaptability, and in particular dynamic adaptation, requires that the current network situation is made visible to management functions on the service layer. Furthermore, the protocols which bind services together across the network must be able to signal adaptation related information, such as current service performance characteristics, configuration parameters etc., between participants.

3.2 Distribution and Mobility

In the civil domain, services often rely on local, centralized server components to which one has a reliable connection. Even when a client connects to services over the Internet, the connection to the remote server is normally fairly stable, and provides sufficient capacity.

Units that communicate in a tactical environment can be distributed over a large area, connected by a fragmented communication infrastructure such as described above. Some are mobile units, moving in and out of the coverage of different networks. In the tactical environment, network partitions that disconnect one or several nodes from others, may happen frequently. Systems must be robust against faults and errors that are not likely to happen in the civil domain, but which are likely to happen in the tactical domain, such as jamming attempts, and sudden loss of physical nodes (such as a radio). Rather than relying on the availability of centralized servers to hold global state and synchronize remote nodes, each node has to be able to quickly and seamlessly discover and interact with the nodes that are currently reachable, or operate autonomously if necessary.

3.3 Ease of Use for End-users and Administrators

On the tactical level, it is vital to minimize the need for specialists. Thus, practical use and administration of the system must not be too complex. The system should have a simple user interface, it should not require advanced configuration from its users, and it should not be sensitive to human errors such as incorrect input. For managers and administrators, solutions must be simple and fast to deploy, configure, administer, and maintain.

To relieve users from spending time on administration, configuration, management, and optimization, the tactical system should perform these tasks automatically where possible. Thus, systems needs to be aware of both itself (i.e. able to measure its performance according to pre-defined, and human-defined, criteria) and its environment (i.e. able to measure parameters that affect its execution, such as the available bandwidth or the power status on the device).

3.4 Concluding Remarks

Systems made for the civil domain, based on assumptions about Internet-like network conditions and business environments, will not necessarily function well in the tactical environment. The tactical environment has certain challenges which are quite rare in the civil domain:

- Very difficult networking environment makes it challenging to ensure that collaboration services function in a predictable way, and that QoS-requirements are satisfied

- Due to the distribution and mobility of nodes, one must expect network partitions, making centralized server solutions unsuitable in many cases
- It is particularly important to minimize the dependence on specialist users and administrators on the tactical level

In the survey of state-of-the-art collaboration services presented in Section 6, we discuss if systems and solutions designed for the civil domain are able to adapt to these challenges, and we look at known solutions, in order to identify areas which need more research.

4 Interoperability

Interoperability can be considered as the "oil in the machinery" for NBD. Interoperability can be defined as follows:

> Interoperability means the ability to interact with others to reach a goal.

Interoperability is not necessarily associated with technology. If two people can work together and achieve a common goal through mutual understanding (e.g., same language) — then they are interoperable. Interoperability is a critical capability that must be present in three main dimensions that are complementary: technology (e.g., hardware, systems), processes (e.g., doctrines, procedures) and personnel (e.g., language, terminology, training) [3].

Defense agility concerns the ability to decide and act quickly and rationally as a result of a high degree of interoperability. Seamless interchange and processing of information enables information and decision superiority. Armed Forces network and systems have requirements for interoperable security mechanisms to be able to exchange information and support decision making across security domains, cultures and established social and technical networks without having to translate or affect the ability to process the information.

In accordance with the NATO force goals, the Defense must be able to operate in conjunction with NATO allies. In addition, we need Defense developed interoperability with other coalition partners, and relevant government civilian actors. Moreover, Defense's ability to be interoperable with non-governmental organizations and international organizations is essential.

4.1 Instruments/action

Development of a NBD must support the road-map and architecture that represents methodology and tools for establishing a basis for decision-making. Architecture and road-maps have significant usefulness when instrumenting the necessary interoperability with allies and partners. Actions pertaining to interoperability must be documented, and the solutions must be secured.

Achieving interoperability involves many areas: standardization, training and practice, education,

[3] Refer to the DOTMLPFI lines of development [42]

including cultural understanding, evaluation, lessons learned, multinational development, technical demonstrations, and tests. Relevant authorities must identify and describe actions within the main dimensions for interoperability. An optimal level of ambition for interoperability within and between the main dimensions must be determined through cost/benefit considerations.

To achieve desired effects it is necessary with the implementation of a common framework and standards within all areas of a NBD. Standardization of the technical domain, language, procedures, and framework is essential to achieve interoperability required and the desired maturity level (which, in this case, is NML4).

Interoperability is far more than a technical exchange of information. People must also be interoperable and therefore leadership, operational culture, and education will be developed further so that this is achieved. However, a first step towards interoperability is having interoperable technology in place. Thus, we focus on the technology aspects of interoperability in the remainder of this document.

4.2 Technical interoperability

Technical interoperability, a term used to encompass all the technological aspects of interoperability, focuses on the hardware and software systems that together make up the information systems and infrastructures used to support interaction between humans. Technical interoperability can be seen as the lowest or or most basic level of interoperability, as it is an enabler for other types of interoperability.

In essence, technical interoperability ensures that information can be exchanged between two (or more) pieces of technology. There exists a large number of NATO Standardized Agreements (STANAGs), civilian standards, and de-facto standards that can be used in order to facilitate such information exchange. These standards describe many different aspects of communication, ranging from the lower levels of the communications stack up to data formats, service level agreements and security aspects. We return to the discussion of different types of standards below in Section 4.3.

Composition of different collaboration services (see Section 2.4.3) is inevitably linked to technical interoperability, since services should be able to seamlessly interact with each other where necessary. That is, collaboration services must be interoperable inside a domain as well as across domains.

The first step towards achieving technical interoperability for collaboration services is thus to agree on which standards to utilize for what purpose. However, it is important to note that most standards contain several different alternative or optional ways of addressing an issue. This means that selecting which standards to use is not sufficient in order to ensure interoperability. One also has to agree on how to use the standards — this is commonly done by making interoperability profiles, which describe how to use a standard, or a set of standards in a specific context. To this end, NATO has released the NATO Interoperability Standards and Profiles (NISP) [31] which recommends a set of standards which the NATO allies should implement in their process of reaching C2 interoperability in the transition to NNEC. Also, the TIDE[4] Transformational Baseline 4.0 (currently under development)[5] identifies several important standards related to NNEC. Next, we discuss several groups of standards which are relevant for such standard agreement and profiling by NATO nations.

4.3 Relevant Groups of Standards

As mentioend, there are several groups of standards to consider when developing systems in a military, and NATO, context. Below, we present four groups of standards that we find most relevant in the context of state-of-the-art collaboration services.

4.3.1 Web services standardization

In [4], *Web services technology* was identified as the key enabling technology for realizing NNEC. The Web services technology consists of a family of standards, where Extensible Markup Language (XML), Web Services Description Language (WSDL), and Simple Object Access Protocol (SOAP) constitute the core. In this document, we use the definition of Web services as given by the W3C [45]:

> A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.

Web services are best suited for disseminating discrete, non-real time data. As a consequence, it is currently identified as the technology that should be used to achieve interoperability with respect to machine-to-machine message-oriented information exchange in NII – both for request/response and publish/subscribe. SOAP-based Web services constitute the foundation for an interoperable message-oriented middleware. How this can be realized is further discussed in the SOA Baseline [9].

4.3.2 RESTful Web services

The term *Web services* is also sometimes used to refer to a completely different paradigm than SOA, the so-called *Representational State Transfer* (REST) also known as *RESTful Web services*. REST is an architectural approach that differs from SOA (and then also SOAP Web services) in that it places constraints on *connector semantics* rather than *component semantics*. REST employs a pull-based interaction style (i.e., the client requests data from servers as and when needed). It

[4] NATO consortium supporting the development of Technology for Information, Decision and Execution superiority

[5] Available at *Tidepedia* (requires an account): `http://tide.act.nato.int/tidepedia`

does not support publish/subscribe. Finally, REST is tightly coupled with HTTP, and uses that protocol's defined operations as its "uniform interface" for accessing services. REST is often favored in communities focusing on data orientation (e.g., for semantic applications) rather than service orientation, and has in recent years been identified as a technology of interest by certain groupings in NATO. For example, in TIDE there is some experimentation involving REST in addition to SOAP Web services. For a comparison of the key features of SOAP and REST Web services, see Table 4.1.

SOAP: Simple Object Access Protocol	**REST: Representational State Transfer**
Can use almost any transport	Uses HTTP/HTTPS exclusively
Somewhat complex	Very easy to understand
Industry standard	Lacking in standardization
Based on XML	Can use XML, JSON, etc.
The foundation of a complete middleware	Good for simplistic point-to-point connections
Identified as the key NNEC enabler	Some interest in NATO for certain applications
We refer to this technology as "Web services" in this report.	We refer to this technology as "REST" in this report.

Table 4.1 W3C's SOAP Web services vs Fielding's RESTful Web services.

4.3.3 Military standards

Several groups of standards has been developed in particular for the military domain. NATO has defined a set of *Standardization Agreements (STANAGs)*, which defines processes, procedures, terms, and conditions for common military or technical procedures or equipment between the member countries of the alliance. Also, nations define their own *national standards*, such as the United States Military Standard (MIL-STD), and the British Defense Standard (DEF-STAN). However, many of the military standards build on, and explicitly reference, standards developed in the civil domain.

4.3.4 Civilian standardization organizations

Civilian standards are developed by a number of standardization organizations. Prominent among these is the Internet Engineering Task Force (IETF), which publishes a list of *Internet standards* that are widely used in the civil domain, and which should be preferred also in the military domain.

The World Wide Web Consortium (W3C) aims to lead the World Wide Web to its full potential by developing common protocols that promote its evolution and ensure its interoperability. W3C is designing the infrastructure, and defining the architecture and the core technologies, for Web services.

The Organization for the Advancement of Structured Information Standards (OASIS) is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. The consortium produces more Web services standards than any other organization along with standards for security, e-business, and standardization efforts in the public sector and for application-specific markets.

4.4 Gateways for interoperability in federations

Ideally, every nation in a NATO coalition force should employ the same standards and implement them in an efficient and interoperable manner. This is, however, not always feasible. For example, a standard may sometimes be expressed in an ambiguous manner, leading to a lack of interoperability between products from different vendors. In such cases, a common solution is to introduce a "gateway"; a node which translates between two or more non-interoperable systems.

Using a gateway may be a "quick fix" to overcome the differences between the implementations. Such a route should be avoided, and one should instead pursue further profiling in NATO, thus detailing *how* the ambiguous parts of a given standard should be interpreted. Also, two nations can, for some reason, have chosen two different and incompatible standards for resolving a given capability. In this case a gateway can be used to translate between the two in order to achieve technical interoperability. Yet again it is not ideal, but one cannot expect to be able to dictate each nation's procurement schedule to fit the needs of NATO, and to circumvent this the use of gateways is mandated (for example, the NATO NNEC feasibility study calls such gateways *interoperability points*).

Past and present NATO Science and Tehcnology Organization (STO) groups focusing on the tactical domain and disadvantaged grids in particular (e.g., IST-090 [7], and the currently active IST-118 group) have identified the use of gateways as a tool to get "the best of both worlds": It is possible to make local optimizations in the tactical domain, while retaining interoperability with higher levels through the use of gateways. The overall guideline from [28] is that:

> In general, the infrastructure and services should be optimized for the users without the need to incorporate proprietary, ad-hoc solutions that will ensure tighter coupling between providers and consumers and therefore limit the range of potential partners. Where a protocol is not widely understood in another domain, then gateways should be used to translate from one standard or protocol to another.

4.5 Concluding Remarks

In this section we have discussed interoperability in the context of technology, and we have presented the most relevant standards and protocols which contribute to developing interoperable collaboration services. In particular, we emphasize the importance of national and NATO interoperability requirements and concerns. The main takeaway points are:

- National solutions should be based on NATO standards and approaches where applicable.

- National solutions must be made interoperable with NATO solutions on a technical level using
    - STANAGs
    - Civil standards
    - Service interoperability profiles
    - Gateways to bridge standard with non-standard solutions
- The interoperable solutions must be secure (see Section 5).

In Section 6 we discuss collaboration services in the perspective of these interoperability aspects.

5 Security

Military collaboration involves different use cases and different communication technologies compared to non-military collaboration. Consequently, the security requirement for military collaboration will be different, too. This section presents a short analysis and a set of security mechanisms which can be configured according to the present protection needs.

5.1 Threat and Risks

The threats against the integrity of a military collaborative system can be informally summarized as follows:

- That information is read by unauthorized receivers
- That information is modified undetected
- That information appears to be produced by someone else
- That information is lost (removed)
- That the service is unavailable

These threats will basically be the same as in civilian applications, but they may be weighted differently, e.g., loss of confidentiality may be regarded as a more severe threat.

5.2 Security Requirements in a Military Context

In the general security literature, security properties are often presented along three axes: Confidentiality, Integrity and Availability. These properties can be given the following meaning:

Confidentiality: Information should be read only by authorized receivers. Others should not be able to read the content or possibly not even be aware of its existence. The privacy property is a part of the confidentiality property.

Integrity: Information should be protected against unauthorized and undetected modifications. This requirement also includes the properties of authenticity and traceability, which means that creation and subsequent modifications should be bound to an identified subject.

Availability: Information and processing resources should be available when needed. In the perspective of information safety this property is provided through competent system and network management. From the security perspective, the availability property includes the ability to withstand a denial of service (DOS) attack.

Compared to security requirements in the civil domain, a military operation will set different security requirements and face different threats.

5.2.1 Confidentiality

Confidentiality is normally considered important. The required time to keep information secret depends, however, on the nature of the information. Tactical messages tend to have a short “secret lifetime”, whereas strategic plans and intelligence information should be kept secret for a long time. Since these information categories are handled by different applications it is reasonable to configure the applications accordingly.

A military network will always be a shielded structure, isolated from other networks through dedicated wires, cryptographic protection (of radio links) or through Virtual Private Network (VPN) tunneling. If the confidentiality requirements are to separate users of the network from the rest of the world (which is the case for information classified as RESTRICTED) this shield may suffice. For higher security classification, a separation between the users of the shielded environment is required. This separation must be implemented both on the service level and on the communication level.

Common operating systems will isolate independent activities in the computer, so that processes cannot “spy” on other processes. The robustness of this *process separation* in COTS operating systems is normally not sufficient for military security requirement. For this reason, there exist *multi level operating systems* which offer better separation on the expense of development cost and compatibility with COTS applications.

Privacy is seldom regarded as important in a military context, since all operations need to be individually accountable. Consequently, the suggested privacy protection mechanisms for civil applications are unlikely to be of interest.

5.2.2 Integrity

Integrity is of the highest importance though. *Authenticity* ensures that the sender of a message may be held responsible for the consequences of the message content. A proven origin for every piece of information may be required. In a collaborative environment where an information object may consist of several authors, it may be required that the contribution of each author is indicated. Authenticity mechanisms also seal the information object and protect it from undetected modifications. Establishing the originator of an information object is also instrumental to *authorization* and *access control*.

Related to the authenticity requirement is the problem of *cross domain* operations, a term which designates the authentication of subjects with identity credentials issued by a foreign authority. Although solution blueprints exist to the cross domain problem, it is seldom seen in practice due to a mix of technical and managerial obstacles.

5.2.3 Availability

Availability is of some importance, but the usage pattern of the application will decide the acceptable unavailability period. Battlefield operation may be near-real time and therefore will accept only short durations of unavailability. Since a collaborative service relies on a stack of underlying software layers, the availability demands will include the underlying software layers as well. Since these layers serve several services (not only a single application), their availability is the responsibility of the platform provider, not the service provider. In other words, a collaboration service will rely on the availability of directory services, time service, storage service, identity management services etc., but the design of the collaborative service should not take responsibility for their availability and correctness.

The availability property relies on the inherent robustness to withstand software and hardware faults, as well as deliberate attacks. Some measures will withstand both (like redundancy and fail-over mechanisms), others will be designed to detect and recover from attacks. *Intrusion detection systems* (IDS) are “watchtowers” guarding one computer or a computer network by looking for suspicious activities and taking appropriate actions. An IDS is an essential service in a collaborative environment.

5.3 Applying Security Mechanisms in the Tactical Environment

The tactical environment as discussed in Section 3, offers some challenges to security mechanisms well known in the civil domain.

5.3.1 Connectivity property and security infrastructure services

Certain security mechanisms, e.g., public key cryptography, rely on infrastructure services related to issuance and validation of credentials. Credentials and validity information have limited lifetimes and need to be issued or obtained at regular intervals.

As discussed in Section 3, tactical networks differ from the Internet through the existence of network partitions. Tactical network nodes should therefore not rely on connectivity to services on the main grid at all times.

During a tactical operation, the credentials and validity information may expire and the nodes in the partition are unable to renew them. This situation may cause all authenticated or encrypted communication to fail, which would be safe from a security perspective, but disastrous from an operational perspective; soldiers without the ability to report or receive position information may be victims to “friendly fire” etc.

In a tactical environment, systems should not rely on connectivity to services without a "plan B". Plan B may use other communication channels for vital information exchange, or accept expired credentials/validity information for vital services. In any case, the risk of denying access to services should be weighted against the risk of allowing it. FFI has published research on this problem in [17].

5.3.2 Available bandwidth and latency in tactical networks

Another property of tactical communication discussed in Section 3, is the presence of links with low bandwidth and high latency. Due to this property, protocols used by COTS products may perform poorly and give inadequate communication service to the higher software layers. This problem is addressed in many different context of system design and operation, but will in this section be discussed in the context of security protocols.

Standardized and popular security protocols for handling identity credentials, authentication and access control tend to involve large volumes of transported data. A digital signature from a 2048-bit private key has the size of 256 bytes. An X.509 public key certificate has a typical size of 1200-1600 bytes. Other data elements can be reduced, compressed or excluded, but the size of keys and signatures can not. Lists of revoked certificates can be voluminous too, because they may potentially contain a large number of certificate references.

The same protocols can be observed to create many protocol round trips. Protocols may allow the parties to negotiate over protocol parameters (e.g. choice of algorithms) before authentication and subsequent service invocation, and these actions are all designed to require a protocol round trip. More efficient protocols may easily be designed either by excluding the negotiating phase, using piggyback techniques to do, e.g., authentication and invocation in the same round trip, or to cache previous protocol data for use in subsequent operations. [14]

FFI has studied aspects of scalability and optimization in Public Key Infrastructures and suggested optimization techniques in [16]. Related research at FFI includes the development of an Identity Management prototype for the tactical domain, including efficient security protocols for tactical data links [15].

5.3.3 Usability and system administration

Apart from the technical considerations of information security, aspects of usability and system administration also play a role in the resulting security situation.

Users (end-users and system administrators) seldom regard security mechanisms as essential and tend to find ways to get them "out of their way". Optional mechanisms are likely to be deactivated, and rigorous password policies may cause procedures to be circumvented, e.g. passwords to be written down, shared etc.

A unified system administration may allow security relevant information to be centrally managed.

The security effect of centralized management is that fewer people are involved in sensitive operations like key and rights assignments. Data related to authorization will be stored in one place, less vulnerable to inconsistency problems. Centralized management raises its own interoperability problem though, since a single management console must interface to a wide range of subsystems.

End user software may threat the system security in different ways. The most common threat is the allready mentioned problem of password procedure circumvention. Another common threat is to allow the end user to make policy exception, like accepting a secure connection to a server unable to authenticate itself properly.

The role of a *Single Sign On* system (SSO) can be regarded in the same perspective. SSO allows the user to login once for a group of services, and offers an opportunity to maintain one high quality password which is set and changed once for the entire service group. Users may have less incentive to choose poor (easily guessed) passwords since they are less frequently typed in.

5.4 Secure Communication Patterns for Collaboration Services

Collaborative applications apply several types of communication patterns, which need to be secured to satisfy the security requirements described above. In particular, the communication pattern applied affects cryptographic techniques in different ways.

5.4.1 Many-to-many communication pattern

Some collaboration services, e.g., chat, and video and audio conferences, allow many-to-many conversations. Public key cryptography is not well suited for this communication pattern.

While public key cryptography has proven to be very useful for protecting one-to-one communication in message format, it is not always suitable for the “many-to-many” communication pattern. Public key encryption uses the key of the intended recipient and the content cannot be read by anyone else but the recipient. This leaves two alternatives for the many-to-many case: (1) unicast messages encrypted with each receiver’s private key, or (2) multicast messages encrypted with a key known to the entire group. While the former solution is bandwidth expensive, the latter solution introduces the cost of group key management.

Although several solutions to multicast protection have been proposed, no well established standard exists.

5.4.2 Stream encryption

While encryption of request-response communication is well understood and standardized, video and audio conferences require *streaming* of audio and video data. Since digital signatures cannot be applied to streams in the same way as they can be applied to finite objects, authentication of ongoing streams must make other arrangements. Standards for encrypted and authenticated datagram traffic exists, called Datagram Transport Layer Security (DTLS) [34], and can be used for stream protection. It is not known, however, if implementations are interoperable or if stream security still relies on non-standardized solutions.

5.4.3 End-to-end security

Collaboration services may require *end-to-end security*, which means that intermediate servers or proxies cannot tamper with or eavesdrop on the information content. End-to-end security is normally a privacy enhancement in the case where the servers or infrastructure is not trusted. There are several ways to achieve this. A commonly used solution is to use the Secure Sockets Layer (SSL) [18] and the Transport Layer Security (TLS) [10] protocols, which provide encrypted and authenticated transport connections between computing processes. End-to-end encryption will (if the server allows encrypted traffic) exclude the server from any value added services like malware protection, translation, formatting, merging etc. Furthermore, end-to-end encryption may interfere with QoS optimizations (such as cross-layer optimization, see [23] for further details) in intermediate nodes.

Conclusively we state that the different communication patterns and nature of the information flow have strong influence on the security technology that may be applied. Solutions which are found sufficient for request-response mechanisms are not necessarily sufficient for collaborative services.

5.5 Aspects of interoperability and COTS products

Standards for application protocols seldom include security mechanisms sufficient for military purposes. Necessary security mechanisms must often be retrofitted through extra protocols layers, which may affect the interoperability properties of the service.

A typical feature of security standards is the abundance of optional features, which may be implemented differently between products. Solving interoperability problems in well established standards like IPSec can involve a surprisingly large effort. For Web services, NATO points to standards like WS-Security, SAML, XACML, and WS-Federation for supporting different aspects of security related to message-oriented middleware and web applications. This is currently a work in progress, as interoperability profiles are being developed through TIDE as well as put in the NATO Federated mission network implementation plan (NFIP). In other areas functionality is sparingly defined and has relatively low ambitions, and if one leverages private solutions then interoperability will be limited, or perhaps not to be expected at all.

COTS products are ready to use, but offer little adaptability and have little room for modifications. Different COTS products tend to implement similar security mechanisms in different ways, so that their configuration and management cannot be unified. It is, e.g., common for COTS programs to have separate storage of keys and certificates, so trust anchors, personal keys and certificates have to be managed separately for each COTS product. Also, they may choose different protocols and protocol parameters. As an example, the two web browsers Internet Explorer and Firefox have different requirements to a public key certificate during an SSL connection, so it is possible to issue a server certificate that is accepted by Firefox but not by Internet Explorer [13].

5.6 Concluding remarks

The design of the collaborative service must meet the security requirements which are naturally solved at the service level. These requirements are likely to be:

- Confidentiality above the RESTRICTED classification. The implementation of the necessary confidentiality protection will be built on top of OS process separation and access control, on encryption libraries and services for key distribution, validation and management.
- Authenticity of most type of messages, with individual identification of the author. The implementation will be built on top of libraries for digital signature generation and verification, and on services for key distribution, validation and management.
- Availability of the service level, provided that the underlying software is working as expected. The implementation of a collaborative service must be robust and rigorously tested so that attacks through the ordinary service interface are unlikely to succeed. The underlying intrusion detection system can be expected to detect and eliminate non-functional attacks (like blunt DOS attacks).

While security mechanisms for discrete data, such as messaging and file transfer, is well understood, we have presented open issues related to communication patterns used by collaboration services, such as media streaming and many-to-many communications. In particular, with regard to interoperability, current COTS products normally rely on non-standard solutions.

Finally, we note that the deployment of a collaborative service must ensure that the underlying software components have the necessary robustness and correctness to support the security requirement of the collaborative service.

6 Overview of State of the Art

In this section, we provide an overview of state-of-the-art collaboration services and products. We discuss how these services and products satisfy the challenges discussed in previous section, namely their ability to adapt to the tactical environment, their interoperability and use of open standards, and security issues. With regard to products, we include both military and civil products into our discussion, but we place main focus on civil collaboration products that we at the moment find in the military domain in a limited degree, and we discuss the concrete problems of introducing them into the tactical environment.

6.1 Tactical Chat Solutions

Instant messaging, often called "chat", is an important aspect of collaboration because it is a fast, efficient, and non-intrusive way of communicating, it consumes little resources, and is easy to use. Chat may also provide a presence service, as well as simultaneous communication between many people. These characteristics have made chat services very popular on the Internet, and there exists a large number of different chat services. Examples are IRC (Internet Relay Chat), Google Talk, Jabber, Windows Live, and ICQ. Since communication is essential within C2, chat services have also become popular in the military domain. Chat services have been used in military operations on several occasions (one example being Operation Iraqi Freedom [11], where chat was also used in special operations). The fact that NATO addresses chat in both the NNEC Feasibility Study [4] and through the Core Enterprise Services Working Group (CESWG) [9] shows that chat has become an essential C2 tool.

6.1.1 Adaptability to the tactical environment

Common for popular chat services on the Internet is that they are server-based, i.e., all clients must connect to a server, which in turn relays the message to the recipient(s), possibly via other servers. Also, chat services depend on reliable delivery of messages. For all such connections, the Transmission Control Protocol (TCP) [8] is the prevalent protocol on IP-based networks. This poses no problems in wired networks, which provide stable topologies and high bandwidths. For mobile ad-hoc networks (MANETs), on the other hand, end-to-end TCP connections can be difficult to establish and maintain due to the limited bandwidth and frequent packet loss. In the tactical environment, we need solutions that can deliver the messages reliably and bandwidth-efficiently, without relying on a centralized server infrastructure.

Limited and varying network resources

Multicast is an efficient means of distributing one message to many recipients. In particular, link layer multicast on a wireless link exploits the characterististics of the wireless link, which is inherently a broadcast medium. However, also higher level multicast (IP multicast and application layer multicast overlays) may reduce the bandwidth usage by transmitting each message only once between several routers, or between application layer nodes.

As an example, the ChatWAN application, built on the DoDWAN middleware [26], supports communication in disconnected MANETs through the use of broadcast on the wireless link. ChatWAN implements a subset of the IRC protocol [24], enabling clients to connect using standard IRC clients. Other chat applications that use multicast-based solutions are discussed in [3], a solution which support secure group chat, and in [25].

Distribution and mobility

Multicast can also be leveraged in order to decentralize a chat application and do away with the central server. When using multicast, the delivery success rate and bandwidth use depend on the efficiency of the protocol. Reliable multicast protocols can be leveraged, such as NACK-Oriented Reliable Multicast (NORM) [2]. Previously we have created a decentralized chat mechanism, called *Mist-CHAT*, at FFI. Mist-CHAT has its own reliable distribution mechanism and does not rely on underlying routing or multicast mechanisms. Experiments have shown that this solution significantly outperforms competing applications in networks with disruptions due to high node mobility [39].

However, if there is a need for a node to go into radio silence, Mist-CHAT will not work. Ideally, we want a node to be able to receive messages even if it is currently in EMCON[6] and does not transmit anything. This led us to investigate other possible solutions besides Mist-CHAT as well. In our most recent attempt, we have chosen to focus on the ACP142 protocol [43] for reliable multicast, because it has been designed specifically for use in tactical networks. It is a highly configurable protocol that, unlike other reliable multicast solutions we are aware of, can function under EMCON as well. A team at NTNU has built an experimental chat solution on top of ACP142 under supervision by FFI. This solution has been successfully tested in an emulated networking environment, and the implementation of both ACP142 and chat application are freely available as open source.[7] The work has been performed in context of NATO STO/IST-118 "SOA recommendations for disadvantaged grids in the tactical domain". This current solution, as well as our previous Mist-CHAT, are both being considered by the NATO STO/IST-ET-070 exploratory team for tactical chat.

6.1.2 Interoperability

NATO has chosen to standardize on the eXtensible Messaging and Presence Protocol (XMPP) [36, 37] for instant messaging in its JChat [32] solution. XMPP is server-based, making it ill-suited for use in a tactical environment where a central server constitutes a single point of failure. This has led to an increased research focus on developing chat solutions that are adapted to the tactical domain, as well as a shift from the previous focus on IRC to the current focus on XMPP. Thus, it is important to choose solutions that are either compatible with XMPP, or that can be made compatible with XMPP through a proxy or gateway solution.

From the literature overview provided above, we have identified three approaches that are commonly used when attempting to implement chat in tactical networks and that retain interoperability with XMPP on some level. Figure 6.1 illustrates these three approaches, from left to right: 1) Attempting to use XMPP directly, but with certain optimizations, 2) Using a proprietary solution in the dynamic environment, but using gateways to achieve interoperability with COTS XMPP clients and servers, and 3) Proprietary client and optimizations, but using a gateway for interoperability with an XMPP server in the backbone network.

[6] *EMCON* is short for *emission control*, also known as *radio silence* where a node has entered a state where it may receive but not transmit data.

[7] We have released our Java implementations of the chat solution and the ACP142 protocol (also known as P_MUL) as open source. They can be obtained from `https://github.com/libjpmul/pmulchat` (the chat application), and `https://github.com/libjpmul/libjpmul` (the ACP142 protocol).

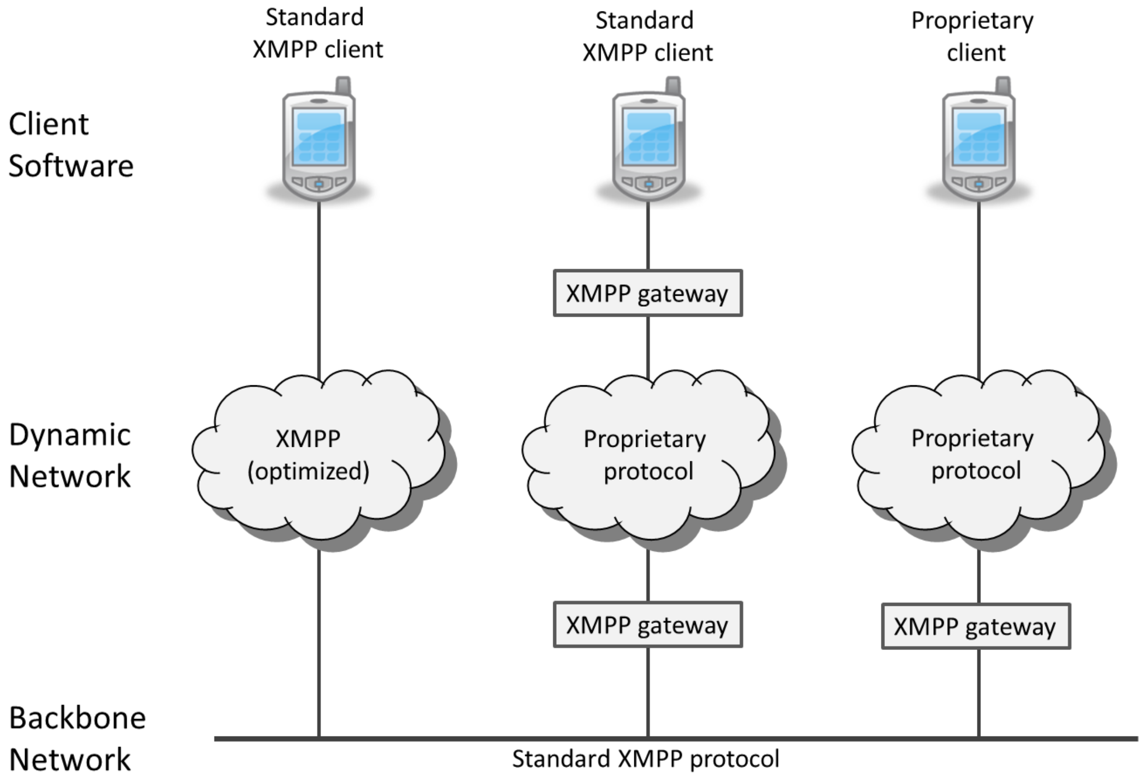

Figure 6.1 Chat solution approaches to retaining interoperability with XMPP

The abovementioned chat applications [3] and [25] are both XMPP-based chat applications which use proxies and gateways to achieve XMPP compatibility. Also, the abovementioned Mist-CHAT mechanism can achieve interoperability with XMPP through a gateway. To this end, Mist-CHAT was presented as input to NATO STO/IST-090 "SOA challenges for real-time and disadvantaged grids" and was a part of the group's final demonstration at MCC 2011 in Amsterdam, Netherlands.

6.1.3 Security

Some but not all standardized and experimental solutions address security. Such security mechanisms are often at the level of user-name/password security towards a central server (as in XMPP), possibly accompanied by SSL/TLS, discussed in 5.4, as well. This may be inadequate for tactical use, and requires further consideration. Furthermore, a security solution needs to leverage current NATO approaches to single sign-on issues.

6.1.4 Concluding remarks

Efficient and robust chat applications in the tactical environment can be implemented, for example through the use of multicast overlays. However, such solutions do not always follow the standards NATO identify. Indeed, the SOA Baseline [9] identifies XMPP for instant messaging, meaning that at some level a national chat solution must be compatible with XMPP for participation in NATO coalition forces. Non-standard approaches can be made compatible with XMPP through for example a proxy or gateway solution.

XMPP can be combined with known security mechanisms. However, there are challenges related to the application of such security mechanisms in the tactical environment which were discussed in Section 5.

6.2 Audio and Video Conferencing

Audio and video conferencing gives users the fastest means to communicate situational awareness, namely direct, live communication through voice and picture. In civil life, different types of audio and video conferencing applications are much used. For informal conversations between friends and colleagues, desktop applications like Skype and Google Hangout have become quite popular. In the business segment, solutions integrated into the computer platform used by the business, are often selected, such as Microsoft's collaboration application suite, Lync[8]. In large private and governmental organizations, including the Norwegian Defense, more advanced video conference studios are being used. These studios, consisting of rooms including screens, microphones, and suitable interior, and the necessary servers and infrastructures, are delivered and installed in the organization by companies like Cisco and Polycom.

Below, we discuss if and how the challenges of the tactical environment as described in Section 3 are met by state-of-the-art audio and video conferencing applications, as for example those mentioned above. However, even though video and audio data are technically quite similar, video data is by far the more resource demanding, and as such, more challenging in the tactical environment. Thus, we focus this section on video conferencing applications and video data. Similar techniques as those described below can be applied to audio data.

6.2.1 Adaptability to the tactical environment

Video conferencing applications consist of continuous streams of picture frames which are digitally encoded and compressed, efficiently reducing the size of the stream in order to transport it over networks. Making such applications adaptable to the characteristics of the tactical network, and the physical and logical distribution of the application and its participants, while keeping the application simple to use and administer, is a challenge.

Limited and varying network resources

As the available bandwidth in the tactical environment may vary from extremely poor (for example as provided by tactical radio) to quite good (for example as provided by satellite communication), adaptation of video streams is absolutely necessary in the tactical environment, in order to scale the stream up or down to a bit rate that is feasible to communicate through the network. Video adaptation means adapting the bit rate and quality of a stream by adjusting the parameters of the encoder producing the stream:

[8] In 2011 Skype was purchased by Microsoft, and it can now interoperate with Lync.

- The *number of frames per second (fps)*, i.e. the *smoothness* of the video, as more frames per second requires a higher bandwidth.
- The *size of each frame*, i.e. pixel resolution, as larger frames generally require more data than smaller ones.
- The *quality of each frame*, i.e. the *clearness* of the pictures, as clear pictures require more data than blurred pictures.
- Combinations

Finally, as different encoders produces different quality relatively to bit rate, it is important to select an efficient encoder.

The characteristics described above spans an adaption space consisting of different video encoder configurations that satisfies different bandwidth limitations and timeliness requirements. COTS products does exploit this space for civil applications, both for stationary and mobile. As an example, Microsoft's collaboration tool Lync provides a video conferencing application which performs automatic bit rate adaptation[9]. However, as such solutions have been designed for the enterprise environment, more experience with applying COTS products in the tactical environment is needed. Solutions targeting the tactical environment in particular have also been proposed. For example, [6] discusses how video streams can be adapted to tactical devices by applying transcoding, and presents a prototype of such a tactical device. The work presented in [6] is focused on broadcast applications, and not interactive applications.

Video stream adaptation as described above, can be applied in the end nodes to hide the effects of varying bandwidth from the user. However, such adaptation can not hide data loss, which may happen frequently on a wireless network. Due to the timeliness requirements of audio and video conferencing services, the usual mechanism for repairing packet loss used in the Internet, packet retransmission, cannot be applied. A more suitable solution for media streaming is Forward Error Correction (FEC) code, where the sender encodes a little bit of redundant data into the media stream to allow reconstruction, rather than retransmission, if some of the packets are lost. FEC is normally applied in wireless networks in the lower layers (physical or link), but recent cross-layer approaches propose improving FEC by combining it with application layer mechanisms [22, 35]. According to available documentation, Lync do use FEC to improve quality for users that connect through a unreliable network. For further discussion of cross-layer optimization for video, see [23].

One must accept that in some situations in the tactical environment, the network conditions are so poor that it is not possible to communicate video, or even audio, streams. In this case the application must seamlessly fall back to a service with QoS-requirements that can be satisfied despite the difficult bandwidth conditions, such as chat, or stop the application completely.

Distribution and mobility

[9] Some official technical documentation on Lync can be found on `http://technet.microsoft.com`. Unofficial documentation can be found on various blogs, such as `http://blog.schertz.name`

COTS video conferencing applications are often managed by a centralized server called a Multipoint Control Unit (MCU), which processes the audio and video streams before transmitting them to receivers. This centralized component may become both a resource bottleneck in the system, and cause client connection problems in the case of network partitioning. A decentralized architecture, both with regard to video data processing and stream distribution, improves scalability and tolerance for network partitions.

The original Skype protocol had a decentralized architecture. The protocol was not standardized and "closed source" - its implementation was not known to the public - , but it has been analyzed and re-engineered by several project [5, 27]. The original protocol used an overlay peer-to-peer network with super-peers both for signaling and media streaming. Peers communicated directly or through a super-peer. The user directory and presence information was distributed among the peers. However, according to [27], Skype did use a centralized login server to enable authenticity and privacy. Still, the decentralized architecture of the protocol did to a certain degree avoid the single-point-of-failure problem of centralized architectures.

Ease of use

As discussed above, video in particular spans a large adaptation space which can be quite complex to understand and exploit. Both end users and administrators need to be supported by automatic configuration mechanisms in handling the large number of alternative configurations that may be available for such applications. Ideally, users should be allowed to set high level policies expressing their requirements and preferences, which are mapped by automatic configuration to specific system configurations.

Some COTS systems support such automatic configuration. According to available documentation online, both Microsoft's above mentioned video conferencing tool, Lync, and Google's video chat solution, Google Hangout, are able to automatically adjust the video quality depending on the available bandwidth [19, 29].

As mentioned earlier, COTS solutions are designed for an Internet, or even business, environment, where the network conditions are quite different from the tactical network. Thus, algorithms supporting automatic configuration may be based on assumptions that are not true in the tactical environment. Such solutions need to be tested in the tactical environment, to evaluate their performance under those conditions.

6.2.2 Interoperability

As discussed in Section 4, interoperable systems are capable of interacting with others to reach a goal. For audio and video collaboration systems, being interoperable means that even systems which are delivered by different providers, installed and configured independently in different organizations, are able to

- initialize audio and video streaming services between users, including user presence

discovery and user address lookup (often called a "catalog service"), and negotiation of media (audio and video) formats and quality
- encode, transport, decode, and present media streams to users in a meaningful and predictable way
- dynamically adapt the system configuration, including the parameters of the media streams, as discussed above, in order to maintain service quality as far as possible
- perform the above tasks while maintaining security properties

Systems must facilitate such interoperability through the use of open standards and media formats, rather than proprietary solutions. The standards applied by audio and video conferencing systems are first and foremost protocols that define *media session initiation*, *media compression format*, and *data packetization and transport protocols*. Below, we present a few of the most used protocols in existing audio and video conference applications.

For *session initiation*, COTS systems normally support the *Session Initiation Protocol (SIP)*, or H.323. SIP is a signaling protocol for audio and video streaming applications on the Internet maintained by the Internet Engineering Task Force (IETF) [10]. SIP can be accompanied by the *Session Description Protocol (SDP)* supporting negotiation of media format and quality. H.323 is a recommendation from the ITU Telecommunication Standardization Sector (ITU-T) defining a set of standards addressing call signaling, media transport and control, and bandwidth control for audio and video conferences [11].

Considering *media compression formats*, two of the most commonly used video formats at the moment is H.264[12] and VP8[13]. H.264 is developed and standardized by the ITU-T Video Coding Experts Group (VCEG) together with the ISO/IEC Moving Picture Experts Group (MPEG), while VP8 is owned by Google. While H.264 contains patented technology, and therefore requires licenses, Google has released VP8 under a royalty-free public license.

The prevalent protocol for *data packetization and transportation* of media streams on the Internet, is the Real-time Transport Protocol (RTP) [38]. As the above-mentioned transport protocol TCP is not suitable for data with strict timeliness requirements, RTP is often combined with the unreliable protocol User Datagram Protocol (UDP) [33]. RTP is accompanied by its own signaling protocol, RTP Control Protocol (RTCP), which is used to monitor the real-time traffic, signal Quality-of-service related information, and synchronize streams that are related. Thus, RTCP can be used by adaptation mechanisms to signal QoS-related information from a receiving end-point to a sender. RTP and RTCP are standards developed by the IETF.

The above-mentioned standards are only a few of many standardized protocols and formats available for audio and video streaming systems. The NISP [31] mentioned in Section 4.2, refers to the standards which are the recommended solutions when implementing NATO interoperable

[10] http://www.ietf.org/html.charters/sip-charter.html

[11] http://www.itu.int/rec/T-REC-H.323/

[12] https://www.itu.int/rec/T-REC-H.264

[13] VP8 is part of the Open Web Media project http://www.webmproject.org/code/specs/

streaming services. Most of the above-mentioned standards are mentioned by the NISP. It is crucial that chosen solutions follow guidelines such as the NISP, in order to be able to reach NNEC maturity level 4.

Existing COTS systems do claim to follow open standards. However, according to experience reports available on the Internet, as these products still apply extensions to and dialects of protocols and formats, there is still a need for gateways to make such systems interoperate in practice [14].

6.2.3 Security

The main security issue for video (and audio) conferencing applications is confidentiality; ensuring that only authorized users knows about and receives a video conference. The two most important mechanisms for maintaining confidentiality are authentication of users, and encryption of content. Some issues that were discussed in Section 5 related to secure communication applies here.

First, authentication can be realized by users presenting identity credentials to a login server. However, with COTS solution, the login server is centralized, and may suffer the problems of centralization mentioned above. Also, COTS solutions for managing credentials, certificates etc, are not optimized for the tactical networking environment.

Second, once users are authenticated, communication between them must be protected by cryptographic mechanisms. COTS solutions do support cryptographic protection either between each client and a centralized application management server, such as the MCU mentioned above, or end-to-end. Protection between client and server means that if the server is compromised, so is every video stream under its management. This solution is still used by COTS solutions such as Lync [15], but some COTS solution, such as Cisco Webex[16], advertise that they now provide end-to-end encryption. Still, as pointed out in Section 5, stream security often relies on non-standard solutions, and may not interoperate well.

Third, to support bandwidth efficient many-to-many video conference, there is a need for secure multicast. As pointed out in Section 5, no well established standard for secure multicast exists.

6.2.4 Concluding remarks

The area of audio and video conferencing applications on the Internet has matured over the last decade. However, we are not aware of research that documents how COTS products function in the tactical environment. We have concerns related to the set-up and configuration of audio and video conferencing systems, which should be tested and evaluated in the tactical environment to gain more knowledge about their performance and reliability when exposed for poor and varying

[14] `http://imaucblog.com/archive/2014/03/03/understanding-the-lync-video-interoperability-server-vis/`

[15] `http://blog.csnc.ch/2014/01/lync-top-5-security-issues/`

[16] `www.webex.com`

available bandwidth, frequent losses, and network partition. In particular, it is important that the service degrades in a controlled way.

Furthermore, there is still a lack of standardized stream protection mechanisms, and there a need to document standards compliance and interoperation between products. The use of gateways and proxies should be avoided if possible, as they complicates systems, and may interfere with security and QoS mechanisms.

6.3 Application and Data Sharing Services

In Section 2.4, we discussed some high level trends in collaboration services which are particularly relevant for application and data sharing services. Thus, in this section we discuss application and data sharing services together, in the perspective of these trends.

Application sharing services

An application sharing service is able to share a local application, running on one computer, with multiple users on different computers. An example of such an application is the Remote desktop application, which allows users to connect to a remote computer and operate the desktop of this computer together with the local user. Application sharing is an example of a data centric service which supports distributed collaboration while staying unaware of the semantics of the shared content or product. It shares the application window and gather user input like keystrokes and mouse movements from all involved users, but is unaware of the content of this input.

Application sharing services make applications designed for single-users available to multiple users. Nowadays, it is common to address collaboration and multi-user functionality when developing new applications, which provides more efficient solutions for multi-user requirements such as reliable and timely data delivery to all users, and concurrency control. Still, application sharing provides a tool for improvised solutions in lack of more specialized solutions.

Document sharing services, content management systems and web application frameworks

Current data sharing services become increasingly semantic aware, and they may provide a composite collaborate space able to handle different types of documents and media in a uniform way. Current solutions often combines content management systems with *web application frameworks* to provide a easy-to-use and easily adaptable solution for the publication of web content. Further, these frameworks also provide an environment for web applications within the context of the framework.

An example fo such a framework is the Sharepoint solution mentioned in Section 2.2. Another example is MediaWiki (the software of Wikipedia[17]), which lets users collaborate on documents by organizing them into an interlinked and structured shared document collection. These frameworks let the users build meaningful structure around the documents by, for example, inter linking

[17] http://www.wikipedia.org/

documents or reference pictures or videos within the collection. The documents themselves, or sub-collection of documents, may become quite complex as with questionnaires, forums, dynamic lists and even small applications. The document collection, and its organization, will by itself be a product, such as article on Wikipedia, and the documents should be referenced within this context. The features of such frameworks and “wikies”, are discussed in [12].

6.3.1 Adaptability to the tactical environment

We now discuss how the features and qualities of web applications and data centric collaboration services can be adapted to the tactical environment.

Limited and varying network resources

Generic collaboration services which are unaware of its shared content, such as an application sharing services, must communicate both the output (desktop or window image) and input (key presses, mouse movements, and touch gestures) reliably and with little latency between the participants. Consequently, they are generally resource demanding, especially in terms of network usage. On the other hand, as context and semantic aware services often consist of pre-defined data models and functions, they are able to communicate more efficiently. Thus, they may be easier to optimize for the tactical environment than general purpose services. Furthermore, knowledge about the relative importance of content can be used to prioritize resources like bandwidth, storage and processing by applying techniques such as intelligent caching, synchronization of data, and graceful degeneration. Thus, context and semantic aware data centric services with well defined APIs is an promising approach to building more specialized collaboration services adaptable to the tactical environment.

The data centric approach combined with context information and semantic awareness facilitates the development of different clients for one service, to support different use-cases and varying resource situations. For example, a soldier in the tactical environment who is normally connected to a low bandwidth network, or is off-line, should be offered a different client than the staff officer with a broadband connection, even though they access the same data. *Responsive design* is an approach much used with modern web sites and web applications where the layout of a web application is adapted to the resources available on the current device at run-time. For example, an application may choose one layout when viewed on a smartphone, and a different one on a PC-monitor.

Finally, developments related to the mobile Internet brings more robustness into commercial applications built for mobile and wireless devices. Users connect to services over mobile wireless networks, such as 3G, 4G, or Edge, which provide varying network characteristics similar as in tactical networks, and service providers implement their services accordingly. For example, to handle disconnected periods, many web applications support off-line mode and caching on the client side. Such techniques can be applicable for applications running in the tactical domain as well.

Ease of use

In contrast to military systems, which are normally managed by the military organization, modern web applications are developed with the assumption that the user's terminal is physically and organizationally out of the administrators reach. Users connect to services with different types of devices over which the service provider has no control, and they use commercial networks where the service provider has no jurisdiction. Thus, automation and easy administration of client software are paramount to keep costs down.

As an example, to simplify administration, Web applications are often pulled from the server when the service is first addressed and used. Updates to client software is installed on the server, and pulled by the client when it revisits the service. However, while this approach is easy to administer for the user, the performance of such behavior depends on how well it adapts to the tactical environment.

6.3.2 Interoperability

In this section we discuss standards with particular relevance for application and data sharing services. As the development of standards related to application and data sharing is mostly concentrated on standard applied on the web, we focus the discussion on web standards such as HyperText Markup Language (HTML), HTTP and REST.

Web applications and HTML5

To many of the commercially available collaboration services, the web-browser is now the preferred application framework. The high availability resulting from cross-platform qualities, combined with the attractive distributed management model, has shown to be extremely powerful with the Internet. For HTML-based web applications, HTML 4.01 is the current recommended NATO standard identified by the NISP [31]. However, clients developed to companion data centric services are increasingly built using HTML5 and the HTML5 related Javascript APIs. These clients run in a HTML5 capable web browser or rendering engine.

A transition from HTML 4.01 to HTML5 as the recommended standard will bring some issues, especially since HTML5 is a collection of different standards; the HTML5 markup and a collection of related Javascript API standards [44]. While web applications based on HTML 4.01 often require the use of plug-ins and a "companion technology" to constitute an adequate application environment on the client side, the HTML5 standards are bringing new capabilities to the web-browser. The environment of an HTML5-capable browser is similar to the application environment found in traditional operating systems. The HTML5 Javascript APIs improve on storage, computing/parallelism, networking, and the user-interface with 2D/3D capabilities, touch gestures etc. HTML5 applications are in many cases becoming genuine alternatives to native applications.

As the HTML5 standards has not been designed with the challenges of tactical networks, as discussed in Section 3, in mind, adaptations to the tactical environment may be necessary. Nevertheless, it is likely that within the 15 years scope of this report, HTML5 and related Javascript APIs will be included in the recommended NATO standards.

HTTP and REST

HTML and resources for web applications are commonly delivered using HTTP, or mechanisms that builds on HTTP, such as REST services as discussed in Section 4.3, and combined with the Javascript Object Notation (JSON) format. The simplicity and characteristics of REST and JSON, indicated by Table 4.1, are often preferred before Web services, SOAP and XML by many developers of web-applications. For data centric applications, these protocols have become a defacto standard, and adherence to the standard HTTP operations does contribute to interoperability among such systems. With well designed data centric services is it possible, with little effort, to support multiple interfaces, based on these rather simple protocols and standards.

The standard mechanisms of HTTP, like GET, POST, PUT, and DELETE, combined with version control and conflict resolution on the server, is often sufficient for many collaboration services to function well. To be able to provide real-time collaborative communication, many of the new services use different high-level transport mechanisms. For example, the popular Javascript socket.io library uses mechanisms like WebSockets, Adobe Flash Sockets, AJAX long polling, AJAX multi-part streaming, Forever Iframe, and JSONP Polling. However, these mechanisms has been designed with Internet environment in mind, and are based on maintaining transport connections between the client and server over some time [40]. Thus, their performance in a tactical network, with unreliable and low bandwidth, and network partitions, is unknown.

Web Distributed Authoring and Versioning (WebDAV)

For document editing, the WebDAV[18] is an extension of the HTTP protocol. WebDAV adds methods and headers to facilitate distributed authoring, but not simultaneous authoring of the same document. However, to provide close to real-time collaborative editing, other transport protocols, like the ones mentioned above, are required.

6.3.3 Security

Few of the commercially available collaboration services are developed with classified information in mind. Most offer some degree of protection and they commonly use SSL/TLS to carry HTTP (HTTPS) to improve confidentiality. Further, oAuth [19] 2.0 is becoming a popular protocol to facilitate authorization. Such solutions is sufficient to provide end-to-end confidentiality of unclassified information. However, for classified information, we refer to the discussion of secure collaboration services as discussed in Section 5.

The SINETT projects at FFI (projects 1084 and 1189) have been working under the hypothesis that satisfying the higher classification levels may not be cost-efficient in many situations. To

[18] `http://www.webdav.org/`

[19] `http://www.oauth.net/`

be able to start using emerging collaboration services, one should, where possible, constrain the communication to unclassified information, to be able to use advanced collaboration services. When communication of classified information is required,one must fall back to simpler (with respect to collaboration), but more secure services like the messaging services.

Finally, we observe that it may not be feasible to maintain the essential qualities and characteristics of certain collaboration services while satisfying the constraints of higher classification levels systems. For example, the *need to know principle* is in contradiction with the very essence of a service like a wiki. Such collaboration services could be unsuitable and inefficient for classified information.

6.3.4 Concluding remarks

Technological progress linked to the Internet, the Web and the mobile Internet are drivers for new collaboration services. The area is in rapid development, both in the adoption of services and with new classes of services being formed. In this section, we have discussed how civil trends on this area, namely data centricity, semantic and context awareness, and composite collaboration spaces, is relevant for collaboration services in the tactical domain. The discussion can be summed up as follows:

- The consensus within the web application domain around the HTML, HTTP and REST protocols, does provide a level of interoperability within this area
- Data centric services allows much flexibility to the client side implementation considering the use and presentation of data
- Context and semantic aware services may be easier to optimize for low bandwidth tactical networks as context and semantics does not have to be communicated over the network
- Services developed for mobile devices and networks do handle limited and changing network resources availability which may be reusable to a certain degree in the tactical domain.
- Security mechanisms, which is normally based on SSL/TLS, but are not applicable for classified information.

Finally, we find it likely that HTML5 and related Javascript APIs will be included in the recommended NATO standards. Thus, it is important that issues related to, in particular, tactical adaptations and security, are identified.

7 Conclusions and Research Opportunities

In this document, we discussed three challenges of introducing state-of-the-art collaboration services into the tactical environment:

- Adaptability to the tactical environment

	Chat	**Audio and video**	**Data-centric Collaboration services**
Adaptation to the tactical domain	Solutions are known and tested	Known solutions work well in civil domain, but must be tested in tactical domain. Depends on centralized components.	New trends in the civil domain barely introduced to the military domain
Interoperability	Agreement on XMPP, but tactical adaptations and security protocols not standardized	Good coverage of standards, but not entirely interoperable in practice	Well established standards in the civil domain, but these have to be adapted to the tactical domain
Security	Known mechanisms can be applied, but open issues related to tactical adaptations and interoperability	Interoperability issues related to streaming and many-to-many communication. Cross-domain is challenging.	No support for classified information. Largely based on SSL/TLS security.

Table 7.1 State of existing solutions to collaboration and communication in the tactical environment.

- Interoperability
- Security

We surveyed state-of-the-art solutions that meet these challenges in different degrees, to uncover where there are open issues and potential for future research. The results of this survey are summed up in this section, and presented in table 7.1. The colors of the cells in the table indicate the state of available solutions and products. The green cell in the figure indicates that, even though there may still be open issues, this area is well covered by current solutions. The yellow cells indicates that there are known solutions with which we have some experience, but there are still some open issues which needs to be further addressed. The red cells indicates that in this area there is a definite need for more research. There are open issues and problems that we do not yet know how to address.

Research opportunities related to the challenges of adaptability to the tactical environment, interoperability, and security, are summed up in short below.

7.1 Adaptability to the Tactical Environment

One of the most, if not the most, limiting factor for the use of collaboration services in the tactical environment, is bandwidth. However, at the time of writing, the bandwidth situation in the tactical environment is moving from *always poor* to *varying between poor and decent*. In the Norwegian army, 3G (4G next), Satellite modems and broadband wireless are taken into use on the tactical level, scaling up the available bandwidth to megabits per second. However, bandwidth is still a very limited resource when these high capacity links are not available, and off-line periods will be a problem one must be ready for in the foreseeable future. Collaboration services need to tackle these challenges while staying interoperable, and while maintaining security properties.

The success of collaboration services depends on that solutions are able to use the resources available at any time; Scale up when the bandwidth situation improves, and degrade as gracefully as possible when it is poor. Civil solutions today are capable of such dynamic adaptation to resources. To our knowledge, their performance in the tactical environment is not well known and documented. Thus, they should be tested and evaluated, to see if they can be adapted to the characteristics of the tactical network, and under which circumstances and conditions.

Another concern with COTS products, is that they commonly depend, partly or entirely, on centralized architectures and algorithms. Centralized solutions introduce single points of failures and bandwidth bottlenecks. Solutions for decentralized signaling and data distribution exists, such as multicast overlays and peer-to-peer techniques, but are to our knowledge not used by current collaboration service providers.

Emerging trends within collaborative applications in the civil domain are turning towards context specific services, where users collaborate about some specific task or content. As the type and layout of data is known to the service, there are great opportunities for optimizations, which can be crucial for their applicability in the tactical domain. It is important to find out which role such applications play within the future collaboration services.

7.2 Interoperability

It is imperative for current and future systems to stay interoperable with NATO. Interoperability is realized through consequent use of IP, STANAGs, civil standards, and service interoperability profiles. The state of interoperability for existing collaboration services is uncertain at best

- Some services can, with little effort, be fully interoperable by careful selection and employment of relevant standards - protocols and formats (e.g., text based messaging, audio and video conference)
- Some services employ standards that are suitable in infrastructure networks yet unsuitable for the tactical domain. For example solutions based on TCP or other connection oriented protocols which assume low delays and that network partition rarely happens. Here further research is needed to bridge the two.
- Some services lack current standardization in the military domain and need further research. Such as collaboration services, where new trends emerge.

One may see interoperability as a “buyers argument”, in a market of suppliers which may have incentives to lock customers to their solutions. In order for interoperability to become a reality, customers must be very focused on specifying that products should comply to open standards, and they should verify that the products actually do so. In this respect, the ongoing standardization work carried out internationally and among our NATO allies is important. FFI participates in international arenas where standards are defined, and where products are compliance tested and evaluated. While it is an important contribution to promoting interoperability, it also provides an opportunity to influence the development of these standards.

7.3 Security

The security requirement for a collaborative system is quite similar to any other information system. Some distinguishing factors exists however, which should be addressed in any collaborative development activity:

- The information may be subject to streaming, which require different mechanisms for encryption and signatures than ordinary messages. Interoperability of existing mechanisms has to be verified.
- The communication parties may belong to different security domains, raising the need for cross domain solutions. Cross-domain solutions exists, but are not much used due to technical and managerial obstacles.
- The communication pattern will include many-to-many communication, which need different mechanisms for protection than one-to-one communication. Currently, no well established standard for many-to-many communication exists.
- Collaboration in tactical networks requires prudent security protocols that minimizes network load. Civil protocols often perform poorly in the tactical network due to low bandwidth and high delay.

Finally, standards for secure communication used in the civil domain is often not sufficient for classified information, in particular above the RESTRICTED classification. Thus, applications that are considered secure in the civil domain may have to be further secured by mechanisms accepted by military authorities.

References

[1] NATO C3 Classification Taxonomy. http://tide.act.nato.int/tidepedia.

[2] B. Adamson, C. Bormann, M. Handley, and J. Macker. NACK-Oriented Reliable Multicast (NORM) Transport Protocol. RFC 5740 (Proposed Standard), November 2009.

[3] T. Aurisch and P. Steinmetz. Securely connecting instant messaging systems for ad hoc networks to server based systems. The 16th International Command and Control Research and Technology Symposium (ICCRTS), Quebec City, Canada, 2011.

[4] P. Bartolomasi, T. Buckman, A. Campbell, J. Grainger, J. Mahaffey, R. Marchand, O. Kruidhof, C. Shawcross, and K. Veum. NATO Network Enabled Capability Feasibility study Volume I: Overview of NATO Network-Centric Operatioal Needs and Implications for the Development of Net-Centric Solutions Version 2.0. NATO.

[5] S.A. Baset and H.G. Schulzrinne. An analysis of the skype peer-to-peer internet telephony protocol. In *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, pages 1–11, April 2006.

[6] B. Bennett, D. Bussert, R. Pham, and B.A. Hamilton. Transcoding content for tactical mobile computing devices. In *Military Communications Conference, 2005. MILCOM 2005. IEEE*, pages 128 –132 Vol. 1, oct. 2005.

[7] Trude H. Bloebaum, Norman Jansen, Frank T. Johnsen, Peter-Paul Meiler, Ian Owens, Leon Schenkels, and Joanna Sliwa. Soa challenges for real time and disadvantaged grids, final report of the nato cso ist-090 research task group. Submitted to NATO STO 29.4.2013.

[8] V. Cerf, Y. Dalal, and C. Sunshine. Specification of Internet Transmission Control Program. RFC 675, December 1974.

[9] Consultation, Command and Control Board (C3B). CORE ENTERPRISE SERVICES STANDARDS RECOMMENDATIONS: THE SOA BASELINE PROFILE VERSION 1.7. Enclosure 1 to AC/322-N(2011)0205, NATO Unclassified releasable to EAPC/PFP, 11 November 2011.

[10] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard), August 2008. Updated by RFCs 5746, 5878, 6176.

[11] B. A. Eovito. The impact of synchonous text-based chat on military command and control. in 11th ICCRTS Coalition Command and Control in the Networked Era, Cambridge, UK, Sept 2006.

[12] Mikael K. Fidjeland, Bård K. Reitan, Bjørn Jervell Hansen, Jonas Halvorsen, Tor Langsæter, and Hilde Hafnor. Semantic wiki - collaboration, semntics & semi-structured knowledge. FFI-report 2010/00496.

[13] Anders Fongen. Optimization of protocol operations in a public key infrastructure. Technical Report 2010/02499, Forsvarets Forskningsinstitutt, 2010.

[14] Anders Fongen. Scalability analysis of selected certificate validation scenarios. In *IEEE MILCOM*, San Jose, CA, USA, Oct 2010.

[15] Anders Fongen. Federated identity management in a tactical multi-domain network. *Int. Journal on Advances in Systems and Measurements*, Vol.4, no 3&4, 2011.

[16] Anders Fongen. Optimization of a public key infrastructure. In *IEEE MILCOM*, Baltimore, MD, USA, Nov 2011.

[17] Anders Fongen. Validation of inferior identity credentials. In *8th international conference on communications and information technology*, Tenerife, Spain, January 2014.

[18] A. Freier, P. Karlton, and P. Kocher. The Secure Sockets Layer (SSL) Protocol Version 3.0. RFC 6101 (Historic), August 2011.

[19] Google. https://support.google.com/hangouts.

[20] Hilde Hafnor, Bård Karsten Reitan, and Dinko Hadzic. Virkelig (sam)arbeid i en 3d virtuell verden. FFI-report 2007/02588.

[21] Forsvarssjef Harald Sunde, General. Forsvarssjefens plan for utvikling av et nettverksbasert forsvar Del II - Plan. Forsvaret, June 2011.

[22] Hai Jiang, Weihua Zhuang, and Xuemin Shen. Cross-layer design for resource allocation in 3g wireless networks and beyond. *Communications Magazine, IEEE*, 43(12):120–126, Dec 2005.

[23] Frank T. Johnsen, Joakim Flathagen, Mariann Hauge, Eli Gjørven, Terje M. Mjelde, and Frode Lillevold. Cross-layer design and optimizations. FFI-report 2014/00985.

[24] C. Kalt. Internet Relay Chat: Client Protocol. RFC 2812 (Informational), April 2000.

[25] R. Lass, D. Nguyen, D. Millar, W. Regli, J. Macker, and R. Adamson. An evaluation of serverless group chat. IEEE Military Communications Conference (MILCOM), pages 1639-1644, Baltimore, ML, USA, 2011.

[26] Y. Mahéo, N. L. Sommer, P. Launay, F. Guidec, and M. Dragone. Beyond opportunistic networking protocols: a disruption-tolerant application suite for disconnected manets. `http://extremecom2012.ee.ethz.ch/papers/1-extremecom2012-Maheo.pdf`, Extremecom, 2012.

[27] Ouanilo Medegan. Skype reverse blog. http://www.oklabs.net/category/skype-reverse/.

[28] Peter-Paul Meiler, Francesca Annunziata, Burcu Ardic, Christoph Barz, Graham Fletcher, Trude Hafsøe, Novo Ignacio Hernandez, Norman Jansen, Frank Trethan Johnsen, Daniel Marco-Mompel, Jonas Martin, Ian Owens, Betul Sasiogly, Leon Schenkels, Joanna Sliwa,

Jens Stavnstrup, and Akif Tokuz. An overview of the research and experimentation of ist-090: Soa over disadvantaged grids. In *Military Communications and Information Technology: A Comprehensive Approach Enabler*. 2011.

[29] Microsoft. http://technet.microsoft.com/.

[30] NATO. NNEC Web Page. http://www.act.nato.int/subpages/nnec.

[31] Command NATO Consultation and Control Board (C3B). NATO Interoperability Standards and Profiles. `http://nhqc3s.nato.int/architecture/_docs/NISP/PDFcoverdoc.html`.

[32] NCIA. Joint Tactical Chat (JChat). `http://tide.act.nato.int/tidepedia/index.php?title=Joint_Tactical_Chat_%28JChat%29` (access requires a Tidepedia account).

[33] J. Postel. User Datagram Protocol. RFC 768 (INTERNET STANDARD), August 1980.

[34] E. Rescorla and N. Modadugu. Datagram Transport Layer Security Version 1.2. RFC 6347 (Proposed Standard), January 2012.

[35] Brent Rickenbach, Peter Griffin, Jason Rush, John Flanagan, Brian Adamson, and Joseph Macker. Adaptive data delivery over disadvantaged, dynamic networks. In *MILCOM 2011*, 2011.

[36] P. Saint-Andre. Extensible Messaging and Presence Protocol (XMPP): Core. RFC 6120 (Proposed Standard), March 2011.

[37] P. Saint-Andre. Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence. RFC 6121 (Proposed Standard), March 2011.

[38] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RTP: A Transport Protocol for Real-Time Applications. RFC 3550 (INTERNET STANDARD), July 2003. Updated by RFCs 5506, 5761, 6051, 6222, 7022.

[39] Magnus Skjegstad, Ketil Lund, Espen Skjervold, and Frank T. Johnsen. Distributed chat in dynamic networks. IEEE Military Communications Conference (MILCOM) 2011, pp.1651-1657, 7-10 Nov. 2011, Baltimore, MD, USA.

[40] socket.io. Introducing socket io. http://socket.io/#browser-support.

[41] Åshild Grønstad Solheim, Ole-Erik Hedenstad, Jan Erik Voldhaug, Frode Lillevold, Bjørn Jervell Hansen, Raymond Haakseth, and Ole Ingar Bentstuen. Helhetlig taktisk ledelssystem for landdomenet - forslag til målbilde. Technical Report 2013/00825, Forsvarets forskningsinstitutt (FFI), Mars 2013.

[42] Harald Sunde. Forsvarssjefens plan for utvikling av et nettverksbasert forsvar: Utgivelse av del i – strategi, og føringer for det videre arbeid for utvikling av et nettversbasert forsvar (NbF): Del i – strategi. Forsvarssjefen fastsetter FSJ plan for utvikling av et nettverksbasert forsvar (NbF) Del I – Strategi til bruk i Forsvaret, Oslo 19. mai 2010.

[43] The Combined Communications-Electronics Board (CCEB). P_MUL – a protocol for reliable multicast messaging in bandwidth constrained and delayed acknowledgement (EMCON) environments. `http://jcs.dtic.mil/j6/cceb/acps/acp142/ACP142.pdf`, December 2001.

[44] W3C. Html5 - w3c candidate recommendation. http://www.w3.org/TR/html5/.

[45] W3C. Web services glossary W3C working group note 11 February 2004. Hugo Haas and Allen Brown (eds.). `http://www.w3.org/TR/ws-gloss/`.