FFI-RAPPORT

17/00735

SMART: Situational awareness experiments with the Norwegian home guard using Android

–

Frank T. Johnsen
Marianne R. Brannsten
Ann-Kristin Elstad
Trude H. Bloebaum
Federico Mancini

SMART: Situational awareness experiments with the Norwegian home guard using Android

Frank T. Johnsen
Marianne R. Brannsten
Ann-Kristin Elstad
Trude H. Bloebaum
Federico Mancini

Norwegian Defence Research Establishment (FFI)

28 April 2017

Keywords

Heimevernet
Eksperimentering
Android
Linux
Situasjonsforståelse
Tjenesteorientert arkitektur

FFI-rapport

FFI-RAPPORT 17/00735

Prosjektnummer

5176

ISBN

P: 978-82-464-2924-3
E: 978-82-464-2925-0

Approved by

Bjørn Jervell Hansen, *Research Manager*
Anders Eggen, *Director*

Summary

SMART – pervasive situational awareness at the individual soldier level – was a Concept Development and Experimentation (CD&E) project carried out during 2016. The concept being tested was the use of smart technology as a cheap and low-complexity platform for collaboration and situational awareness for the Norwegian home guard (HV). In conjunction with HV, we decided to focus on the HV area forces. Due to the large number of area forces, and the limited time these forces have available for training, a technical solution that aims to improve the situational awareness of the individual soldier within the HV area forces need to be simple and intuitive in use and have a low cost. This means that smart technology is of particular interest to this group of users.

Furthermore, these forces primarily require exchanging unclassified information, but they need this information exchange to be as secure as possible. This lead to SMART targeting “trusted unclassified” communications, which meant that unclassified information should be exchanged with sufficient security for the users to trust using the platform to share their information. SMART includes initial discussions on the security aspects of utilizing smart technology as a platform. As there are no clear security guidelines for “trusted unclassified” communications, what we did was to define some reasonable requirements and discuss whether they could be met by the current solution in different contexts. Furthermore, we explored the idea of using external secure elements, also known as smart cards, to store securely sensitive information independently from the device status.

SMART included building a demonstrator based on the Android platform. This demonstrator was tested iteratively by HV, first through several technical trials, and finally during an operational exercise. Before and after the exercise we used questionnaires to map the users’ expectations and experiences regarding the demonstrator, respectively. Summarized, the respondents both expected and experienced a more rapid and efficient execution of their missions using the SMART demonstrator. This mapping of expectations and experiences also revealed that the soldiers brought their own phones to the exercise and used them if there were issues with their primary communications channel. This shows that a better coordinated and controlled use of such resources in accordance with the “trusted unclassified” concept in SMART was both timely and relevant.

The final experiment report from SMART was delivered to the HV at the end of 2016. In general, the results from the activity indicate that using civilian smart technology yields an operational value. The SMART demonstrator and concept can provide cheap and low-complexity “trusted unclassified” communications to the HV’s area forces and others who may need this capability.

Sammendrag

SMART - gjennomgående situasjonsoversikt på enkeltmannsnivå - var et eksperimentprosjekt (Concept Development and Experimentation (CD&E)) som ble gjennomført i 2016. Konseptet som ble testet var det å benytte enkel og billig smartteknologi som en plattform for situasjonsoversikt og samhandling for Heimevernet (HV). I samråd med HV bestemte vi at det var HVs områdestyrker som var hovedmålgruppen for aktiviteten. Disse styrkene omfatter et høyt antall personer, og disse har begrenset tid tilgjengelig til trening. En teknisk løsning som har som målsetting å bedre situasjonsforståelsen til enkeltmann i disse styrkene må derfor være enkel og intuitiv i bruk, og ha lav kostnad. Dette betyr at smartteknologi er av spesiell interesse for disse styrkene.

Videre trenger områdestyrkene primært å utveksle ugradert informasjon, men det er behov for at denne informasjon deles på en måte som er så sikker som mulig. På grunn av dette hadde SMART en målsetning om å støtte det vi kalte “sikrere ugradert” kommunikasjon, noe som betyr at håndteringen av denne ugraderte informasjonen skal gjøre sikker nok til at brukerne får nok tillit til løsningen slik at de er villige til å ta den i bruk. SMART inkluderer en innledende diskusjon om sikkerhetsaspektene ved det å bruke smartteknologi på denne måten. Sikkerhetsloven ikke gir noen retningslinjer for “sikrere ugradert” kommunikasjon. Vi har derfor selv lagt til grunn de kriteriene vi støtter i SMART-konseptet og diskuterer disse i rapporten. Videre har vi også sett på muligheten til å benytte eksterne sikre elementer, i form av smartkort, til sikker lagring av sensitiv informasjon uavhengig av smartenhetene.

SMART inkluderte det å bygge en demonstrator basert på Android-plattformen. Denne demonstratoren ble testet av HV i flere runder, først gjennom tre tekniske tester, og deretter som en del av en øvelse. Både før og etter øvelsen brukte vi spørreundersøkelser for å kartlegge brukernes forventinger til og erfaringer med demonstratoren. Kort oppsummert kan vi si at brukerne både forventet og erfarte en raskere og mer effektiv gjennomføring av oppdragene sine når de benyttet SMART-demonstratoren. Kartleggingen av forventinger og erfaringer viste også at brukerne allerede tok med seg sine egen smartenheter på øvelsen, og benyttet disse til kommunikasjon når det var problemer med primærsambandet deres. Dette viser at en bedre koordinert og kontrollert bruk av smarttelefoner i henhold til “sikrere ugradert”-konseptet i SMART er både tidsriktig og relevant.

Den avsluttende eksperimentrapporten fra SMART ble levert til HV i slutten av 2016. Oppsummerende kan vi si at bruken av sivil smart-teknologi synes å gi en operativ nytteverdi. Den gjør det mulig med en enkel og billig teknisk instrumentering for HVs områdestyrker og andre som kan ha behov for "sikrere ugradert" kommunikasjon.

Content

1 Introduction

This report gives an overview of a concept development and experimentation activity (CD&E) called "EP 1667 SMART - Pervasive common situational awareness at the individual soldier level", hereafter called SMART. The purpose of this CD&E was to investigate whether advanced smart technology (e.g., Android smartphones) can be used as a platform to provide increased situational awareness for forces that currently have a low degree of technological instrumentation. SMART was performed by the Norwegian Defence Research Establishment (FFI), Cyber Systems and Electronic Warfare Division in 2016, with the goal of delivering research-based advice on the feasibility of using smart technology for the Norwegian Home Guard (HV).

The target demographic for the concept experimentation was HV, which is one of the branches of the Norwegian Armed Forces. HV is the, when measured in number of soldiers, largest branch of the Norwegian Armed Forces, and serves as a quick mobilization force. Their main tasks are to safeguard territorial integrity, protect critical infrastructure, support national crisis management, and provide support to civil society.

HV consists of more than 45 000 soldiers distributed in four regions, 11 districts and 241 areas covering all of Norway (Forsvaret, 2017). As HV is a mobilization force, the majority of soldiers are not employed by the military on a daily basis, but train on a regular basis. There exist 15 rapid reaction intervention forces, which consist of highly trained and equipped personnel. The remaining forces, which make up the 241 areas, have longer reaction times, are less equipped and have less training, but have higher endurance than the intervention forces.

Due to the large number of area forces, and the limited time these forces have available for training, a technical solution that aims to improve the situational awareness of the individual soldier within the HV area forces need to be simple and intuitive in use and have a low cost. This means that civilian smart devices, which are seeing an increased use for defence purposes worldwide (Boddhu et al., 2012), is a platform of interest for these forces: mobile devices provide a small, light form factor while at the same time providing a powerful sensor platform. Furthermore, civilian technology like mobile phones comes with a much lower cost than special purpose military hardware such as tactical radios. An additional benefit is that end users are already familiar with such devices, which enable them to be put to use with little additional training. On the downside, using these devices raise questions related to trust and security.

The main goal of SMART was to determine whether leveraging cheap, low-complexity consumer electronics is a feasible approach to enable pervasive situational awareness all the way down to the individual soldier level. In addition to improving the situational understanding of the individual, equipping soldiers with smart devices also enable these individuals to contribute information, such as their own geographical position, to the common operational picture. This information can, if managed correctly, also contribute to improving the situational awareness of decision makers elsewhere in the command structure.

The Norwegian Armed Forces has a number of current Command and Control (C2) systems, which are used by all branches of the Norwegian Armed Forces, including HV. These systems are primarily focused on sharing classified information, and thus run on accredited and trusted platforms. Within HV, these systems are available to prioritized users, but due to the cost and training required to deploy these systems, they are not available at the individual soldier level. This lack of technological instrumentation means that the individual soldiers have limited access to information that is available at higher levels. In addition, their ability to share information with others is limited by their available communications channels.

In SMART, the aim was to determine whether using unmodified commercial smart devices as a platform for collecting and sharing situational information at the individual soldier level will give an operational benefit without compromising the security of the operation. There already exists a number of other initiatives utilizing smart devices for situational awareness (see related work in Chapter 2), but these tend to be targeted more towards the needs of highly trained army forces, and aim to support classified information exchange between such forces. Such specialized systems often require using modified devices, specially developed software and/or connecting the devices to military communications equipment. In SMART, the target demographic primarily requires a cheap communications platform for exchanging unclassified information securely. Hence, we see the need for at least two different system approaches for the entire land forces, illustrated in Figure 1.1. Note that the figure illustrates whether exchange of classified information is supported for the different forces. All land forces require exchanging unclassified information, but some also have the need and the means to exchange classified information in addition.

The goal of SMART was to determine whether smart technology can efficiently, cheaply and securely fill the role as the platform for unclassified information exchange. In order to achieve this, SMART includes both Bring Your Own Device (BYOD) and using dedicated devices in its concept for the area forces.

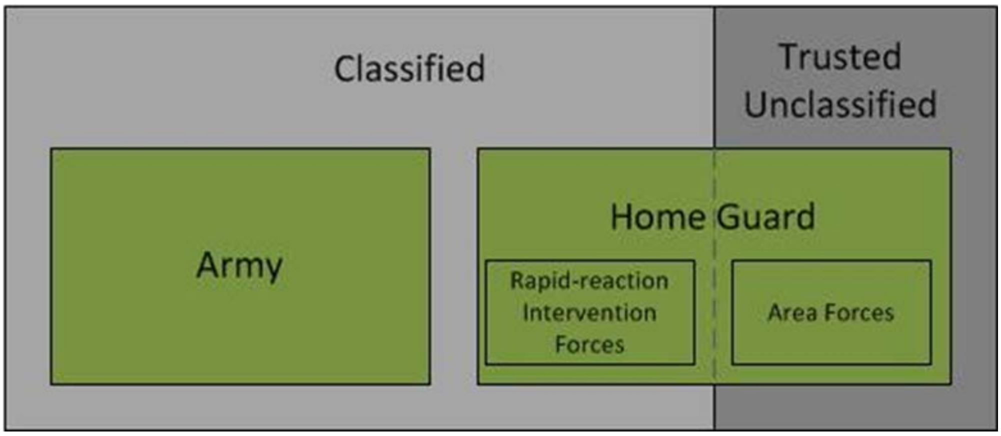


Figure 1.1 Classified vs Trusted unclassified suggested deployment and use

The main goal of SMART was to determine the feasibility of the concept, which required testing the concept in an operational context. In order to support the evaluation of the concept we developed a demonstrator; a technical solution intended to showcase the operational potential of the solution, and enable us to identify the requirements the HV area forces have with respect to this concept. The demonstrator is not intended to be a production system. This means that, if the concept proves to be beneficial, the CD&E activity should be followed by a system procurement phase before the concept is deployed operationally.

1.1 SMART project execution

SMART went through four phases:

The first phase involved finding the focus and scope of the project together with the HV. They wanted to test a concept for the area forces that was both low cost and easy to use without extensive technical training. This means that the time available for training could be spent on military training and not technical issues. Hence, we agreed on building a demonstrator in SMART based on civilian technologies using Android as a platform.

In the second phase we developed the demonstrator according to the basic functional requirements identified in the first phase: support for blue force tracking, observation reports with text, sound and images, instant messaging (chat), and document distribution. During the second phase we also performed technical trials with HV. The results from these trials were used to improve the demonstrator.

In the third phase, the demonstrator was used in an HV exercise in eastern Norway. The demonstrator was used continuously during the entire exercise and proved to be useful as a secondary means of communications. Before and after the exercise we used questionnaires to map expectations and experiences regarding the demonstrator, respectively.

The fourth and final phase involved results analysis and writing of the experiment report, which was delivered to the HV by the end of 2016.

1.2 The SMART technology demonstrator

The SMART technology demonstrator was developed in order to enable us to test the SMART concept in practice, and thus allow us to assess the potential operational value of the concept.

In order to keep costs for platform and software development at a reasonable level, the SMART concept relies on utilizing a combination of both first and third party software running on a commercially available platform; required functionality that can be realized utilizing existing third party applications of sufficient quality is not duplicated in first party software.

Thus, the functionality requested by HV was realized partially through Android application (app) development and partially through third-party apps from Google Play. Two of the key systems requirements for SMART were that the technological solutions had to be cheap and have low complexity, so software was chosen to reflect this, both through our own development and in the selection of free software from Google Play. The app we developed, CAGED, covers the functionality that we could not realize in a sensible way using third party solutions. CAGED is an abbreviation for "Communication Application with Geographical Element Data", a name that reflects that the user can interact with the app, where the map is the main part of the interface.

The demonstrator consists of the following three components (see Figure 1.2):

1. Android applications (CAGED and third-party applications)

2. Back-end server (Athena and third-party software Openfire)

3. Web user interface toward Athena (Metis)

The system was set up as described in (Bekkelund et al., 2016). Here, the back-end server was deployed on a standalone server at FFI. During the technical trials we had used a commercial cloud provider for the backend, due to the ease and flexibility of such an approach. The main reason moving the server in-house was to retain full control of the server and the information that was stored there. Since the demonstrator now should be used during an actual exercise, it was deemed necessary to have physical control of the server. Communication from clients to the server (both from Android and the Web clients in the headquarters (HQ)) was protected with a Virtual Private Network (VPN) solution, OpenVPN. Installation and setup of the OpenVPN software is described in more detail in a separate FFI note, see (Johnsen, 2016).

The technical trials were used to improve the demonstrator in iterations.

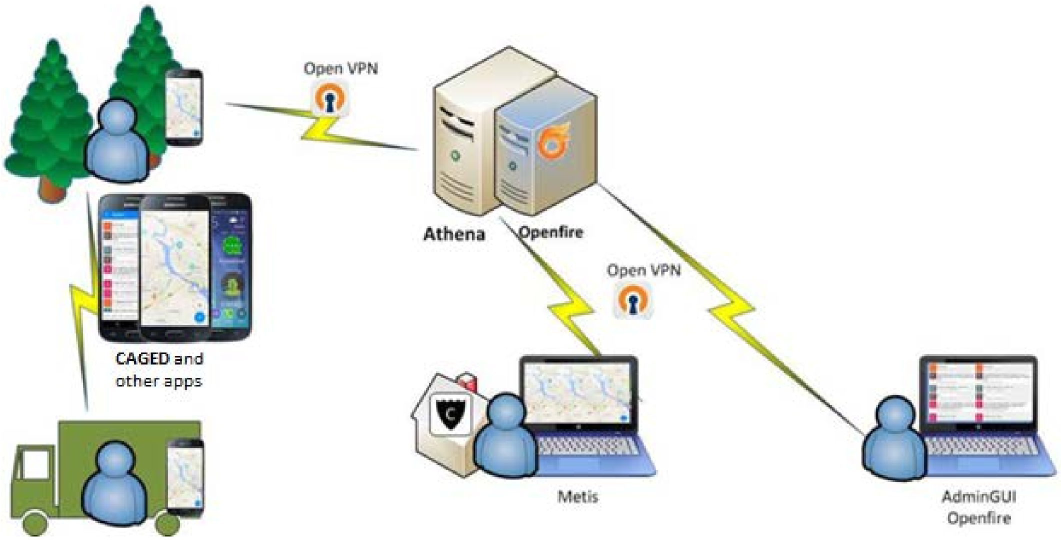


Figure 1.2 SMART demonstrator overview

1.3 Report structure

This report focuses on the SMART concept, and the performed evaluation of the perceived operational value of the concept. Full details of the technical solutions utilized in the demonstrator are not included.

As a part of the initial phase of SMART, we performed a survey of other national and international efforts on using smart technologies for defense purposes. An overview of some significant such efforts are given in Chapter 2, as experiences from these efforts helped influence the development of the SMART technology demonstrator.

Chapter 3 discusses the security implications of using commercial smart technology, and utilizing BYOD as part of the SMART concept.

The execution of the technical trails and the concluding experiment is described further in Chapter 4, while the findings are explained in Chapter 5. Summarized, the respondents both expected and experienced a more rapid and efficient execution of their missions using the SMART demonstrator.

Chapter 6 concludes this report. In general, we can establish that using civilian smart technology seems to yield an operational value. The SMART demonstrator and concept can provide cheap and low-complexity “trusted unclassified” communications to the HV’s area forces and others who may need this capability.

2 Related work

There are several situational awareness systems for collaboration at the individual soldier level, and we look to them for inspiration. The main difference between the SMART concept and related systems is that the related systems are mostly specialist systems with dedicated devices where the users need comprehensive training whilst SMART looks at a scenario using COTS solutions, soldiers possibly using their own devices in a BYOD concept, and minimal training necessary.

2.1 TIGR

The Tactical Ground Reporting (TIGR) system was developed by DARPA in 2005 and has been in use since 2007 by the U.S Army (Evans et al., 2013).

The TIGR system supports storing and information sharing, between Company Commanders and Platoon Leaders and also information sharing with the ground units. The system is meant to fill the void between coordination of operations and surveillance. Soldiers on patrol in operational areas can report events and observations using the system and these reports can in turn be used for planning future patrols in the area. It is not meant as a typical soldier system, but a system for reporting, planning and situational awareness on the tactical level.

The system is inspired by social media and is based on concepts like peer-to-peer, but still there is a client-server architecture and one logical common database for all reports. To make this possible in a tactical setting there are several servers sharing information to enable horizontal information sharing.

2.1.1 TIGR information model

The TIGR information model tries to be as simple and general as possible, with the avoidance of compulsory fields to make it as intuitive as possible for the users.

The most important information objects are events, places, reports, tasks, and collections. These are for describing events, such as hostile activity, the places of events, reports of a mission and how it was executed, tasks for planning future missions, and collections of events, places, tasks and reports.

The TIGR system supports a number of data formats using manual import/export. It also allows external services to manipulate data in the system through a SOAP-based service.

2.1.2 TIGR servers, networks and clients

TIGR is a distributed cloud-based system designed to work in Disconnected, Intermittent and Limited (DIL) environments where DIL reflects the properties of tactical communication environments, with the potential of connection loss(short or long), low data rate, low battery capacity, and other limitations. TIGR consists of a distributed server architecture consisting of mobile-, edge-, and core servers. With a relative large number of servers available, the thought is that there should always be an available server close to the user in the user's LAN. The system is self-contained if no reach back links to central servers are available. The servers are not replicated throughout the system, but all servers save all metadata in search indexes. If a server is disconnected, it will trigger synchronization mechanisms when the WAN connection is reestablished.

System policy is for data produced by the clients to flow all the way back to the core servers. The core servers distribute metadata, thumbnails, and compressed versions of media to the mobile and edge servers. The data is prioritized, and this helps TIGR work even in networks with limited capacity. Metadata is prioritized over all other data and pictures are first distributed as thumbnails.

The TIGR users access the system using a web browser, and in principle the client can be run on all devices running a relatively new web browser. The client needs to be on the same LAN as one of the servers. The client design is inspired by well-known social media sites in order to make TIGR as intuitive as possible for the users.

2.1.3 Thoughts about TIGR

TIGR inhabits several of the properties of a silo system, but still its data centric approach with one logical centralized database and simple information objects can give a flexible system.

The TIGR system is of great interest because it inhabits properties still new in military systems, such as horizontal information flow, web technology, simple data models, and inspiration from social media, and has been in operational use for some time

2.2 Nett Warrior

Nett Warrior is a tactical level situational awareness and C2 system, developed by the US Army for tactical leaders, on foot in real operations. The system was developed with an additional motivation to make it cheap and light-weight (Gourley, 2013).

2.2.1 Nett Warrior functionality

Nett Warrior is a system consisting of both software and hardware, covering everything from the communications layer to the user application. The Nett Warrior system support sharing of tactical data and communications through functionality such as friendly force tracking, virtual chemlights, medical evacuation, navigation, image sharing, and short messages.

Galaxy Note II was introduced in 2013 as the end user device for the Nett Warior system (Dixon and Henning, 2013). The devices are stripped of communication possibilities, including the antennas for communication. To use it for communication, and position information, the devices are connected to a Rifleman tactical radio using a USB connection. The devices are also stripped of all preloaded content and applications and instead loaded with a FSA-security cleared version of Android and the Nett Warrior application. The system is said to be able to exchange messages with TIGR.

2.2.2 Thoughts about Nett Warrior

Even though there are possibilities for interoperability with other systems, Nett Warrior is for the most part a closed silo system meant only for a small group of operatives. The system is not that different from other soldier systems, e.g., NORMANS (see Section 2.5).

The system is of special interest as it is in active use. Another interesting property of the system is the use of commercial devices and Android applications.

2.3 Android Tactical Assault Kit (ATAK)

Android Tactical Assault Kit (ATAK) was developed as part of the Marti project, an information management platform project for information exchange beyond line-of-sight between sensors and soldiers in tactical networks, see (Usbeck et al., 2015) and (Website, 2017). ATAK is an Android library for smartphones and tablets, providing a map application/engine with user interface for situational awareness.

Some of the ATAK library functionality can be used for civil purposes, such as online/offline maps, interactions in maps, position sharing, navigation, and controlling the phone, WiFi and civilian radios. Strictly available for military users, there are functions such as controllers for military radios, standards for messages and MIL-STD-2525B-symbols. ATAK is licensed as "Government Open Source", which means that it can be used only by American projects if they have a government sponsor. It is recommended, by the American Army Geospatial Center, that ATAK is used in Nett Warrior.

ATAK supports a number of communication carriers, including libraries for commercial and tactical radios, WiFi, and mobile networks. It is designed for environments without servers, but can use such infrastructure when available.

2.3.1 Thoughts about ATAK

The license policy for the ATAK library makes the library unavailable for the Norwegian Armed Forces, but there is still inspiration to be had from the initiative. ATAK is a comprehensive project with lots of interesting functionality and technical solutions.

2.4 CEI – Collective Environment Interpretation

CEI is a data centric social tactical reporting system inspired by TIGR. The users are able to report observations and share their positions, adding to the information using text and pictures. It is developed at FFI, not in operational use, but has been tested in field experiments. The aim of CEI is to give a better situational awareness to the individual user by allowing information exchange of non-sensitive data. In addition to situational awareness the system introduces simple social aspects to help the individual users interpret the situation through a collaborative interpretation assuring a common view of the situation between all users in an area.

The system is to be used over the internet or other networks with similar infrastructure. It has a web browser client and an Android client (the CEI-app) (Karlsen and Reitan, 2014). If there is no back link to the system, the Android-client encompasses functionality for functioning off-line and synchronizing when a new connection is established. Through CEI in experiments, FFI found it critical to have intuitive user interfaces, appropriate security, and robust communication in such systems.

2.4.1 Thoughts about CEI

Even though CEI is not in operational use, and is intended to only demonstrate the technology, it is a system that is inspirational for similar systems. Making the socio-tactical property important, helping the users improve communication and potentially eliminate misunderstandings, could possibly facilitate a more collective understanding of the situation in situational awareness systems.

2.5 NORMANS Command and Control System

With the initial prototype developed at FFI, NORMANS was described as a total system for the individual soldier, with both physical equipment carried by the soldier, and also a situational awareness system available through a network based computer system. The situational awareness part of the system is described in this section.

The communication architecture in NORMANS divides the communication between a soldier level and a higher tactical level. Communication protocols chosen for the system are directed towards handling problems one often comes across in tactical networks, such as packet loss and low data rate. Industrialization started in 2007 together with Thales. For further details about NORMANS, see the product sheet (Thales, 2017).

2.5.1 Thoughts about NORMANS

A very important result from the testing of NORMANS Command and Control System is that the system provides the individual soldier with a clear operative improvement. NORMANS is meant for professional soldiers and a lot of training is required to fully achieve the value of the system. As training is an expensive task, this is not viable route for the HV area forces.

2.6 DINA

A competitor to NORMANS is named DINA (Teleplan, 2016) and it is being developed by Teleplan GLOBE. DINA is described as a handheld device, integrated in the soldier’s uniform/equipment, offering the individual soldier a better situational awareness, navigation and other C2-functionality between the individual soldier and command central.

There are several methods of communication available for DINA: GPRS/3G, VHF/UHF/HF-radios and Satcom. It is possible to integrate DINA with other national BMS-solutions and through a diode solution for operations on different restricted levels. All mobile device networks in DINA are connected to a HQ, and several HQs can also be connected.

Teleplan has evaluated available devices of military grade to be mostly Windows devices, and there the development so far has been on the Windows platform. A multiplatform solution is under development and this includes a solution for iOS and Android.

2.6.1 Thoughts about DINA

DINA aims to support specialist soldiers, using dedicated equipment. Comprehensive training of soldiers using the system is necessary. In the DINA system, the devices are required to be military grade water resistant and shock proof. The aim is to have this system at the national restricted level, hence it can be seen as a Norwegian national counterpart to the PROMISE project described below.

As SMART aims towards a simple, cheap and "trusted unclassified" system for the HV's area forces, the cost of equipping all soldiers with specialist devices and giving them extensive training is too high. DINA would be a good tool for the Army.

2.7 PROject Multi-touch Information System Experiment (PROMISE)

PROject Multi-touch Information System Experiment (PROMISE) 1.0 (Defence Material Organisation, Ministry of Defence, 2015) is an experimental C2 solution based on the use of smart devices and applications. The system aims to give increased situational awareness through Friendly Force Tracking, chat, pictures, and video. Notice that speech is not considered, in PROMISE 1.0 only data traffic is considered. The idea is that a military appstore facilitates fast access to and installation of important C2 functionality through applications. One of the goals of PROMISE is to achieve a Dutch national "restricted" security grade through commercial mobile solutions and security solutions. To achieve this, BYOD is not part of the concept, as the devices need to be fully under control.

For hardening purposes the devices operating systems was switched to CyanogenMod 10.2. Security aspects implemented in PROMISE are VPN for network security, application locker to only allow PROMISE-applications to be installed on the devices, hardening by removing Google APIs and Internet access, strict policies for lock screens, encrypted storage and private appstore.

2.7.1 Thoughts about PROMISE

PROMISE has an interesting approach to the use of smart technology, as they use commercial solutions and build upon them. E.g., the security mechanisms of the OS are extended to accommodate PROMISE's security properties.

Also, developing their own functionalities only if it is not available from third party applications is a very interesting and cost-effective approach. PROMISE, just like DINA, aims at instrumenting specialist soldiers and obtaining a high security grade on their data. This is why BYOD is not part of the system setup. However, the work has been highly influential to that of SMART, as reading the experiment report provided us with guidance on approaches that work and do not work when leveraging Android phones for situational awareness.

3 Security considerations

In this chapter we discuss SMART CD&E activity from a security perspective. The aim of the activity is to demonstrate how it is possible to realize a user-friendly Android app to gather and share information among the troops in order to provide increased situational awareness. The key assumption being that it is possible to use commercial off-the-shelf Android devices also in actual deployment. Since the information that is being collected and shared can be critical for the mission, its confidentiality, integrity, and availability should also be protected accordingly. In order to establish whether the proposed solution provides adequate protection, we need to formulate clear security requirements and establish whether they are met or not. If not, additional security measures should be proposed and evaluated before moving to actual production and deployment. However, it is difficult to formulate these requirements at this point, as the app has been tested only in the context of military exercises where security was not a concern and the focus was mainly on functionality. Real deployment scenarios and discussions with end-users and domain experts are needed to conduct meaningful risk-assessment.

Additionally, it has been made clear that it is not classified information that will have to be handled by the app, but “trusted unclassified”. While this means that there is no obligation to be compliant with the Norwegian Security Act (“Sikkerhetsloven”)[1], it also means that we do not have clear security guidelines to follow. What we can do is to define some reasonable requirements and discuss whether they can be met by the current solution in different contexts. Where we find that they are not met, we propose some additional security solutions that may be adopted to increase the protection of critical information. Whether such solutions are appropriate, both security- and functionality-wise, will need to be evaluated by further experimentation.

3.1 Security requirements

Based on the desired operative capabilities, we can roughly define some security requirements that are technology independent and can be used to evaluate a proposed solution. These can be extended as needed when more information become available from further discussions, tests or activities:

- Mutual authentication between users and server is necessary to guarantee that observations are reported to the correct server and information is accessed only by authorized users

- Access control should be differentiated based on users roles and trust in the equipment used to connect to the server

[1] LOV-1998-03-20-10

- Availability of information should be guaranteed also off-line. In this case authentication should be performed also locally on the device so that only authorized users can access information off-line

- Information's confidentiality and integrity should be protected when in storage and in transit

- If this is done by means of encryption, cryptographic keys should also be protected against unauthorized access under all conditions

- Provisioning and updating of security policies, identities, software, cryptographic keys and other security critical management should be administrated centrally and remotely through a secure channel

- Data may be labeled with origin, reliability, sensitivity, freshness and other attributes to simplify targeted sharing, aggregation, and security management

Just as important is that the security design is based upon usability principles so that users are not forced to adopt unpractical solutions that could significantly diminish their operative capability. Negative examples can be: frequent authentication to perform basic tasks; password that are difficult to remember and enter in the device; additional equipment; or non-standard interfaces.

With these requirements in hand, summarized in Figure 3.1, we can assess whether the current security mechanisms offered by android devices offer adequate security or can be used to develop solutions that do that.

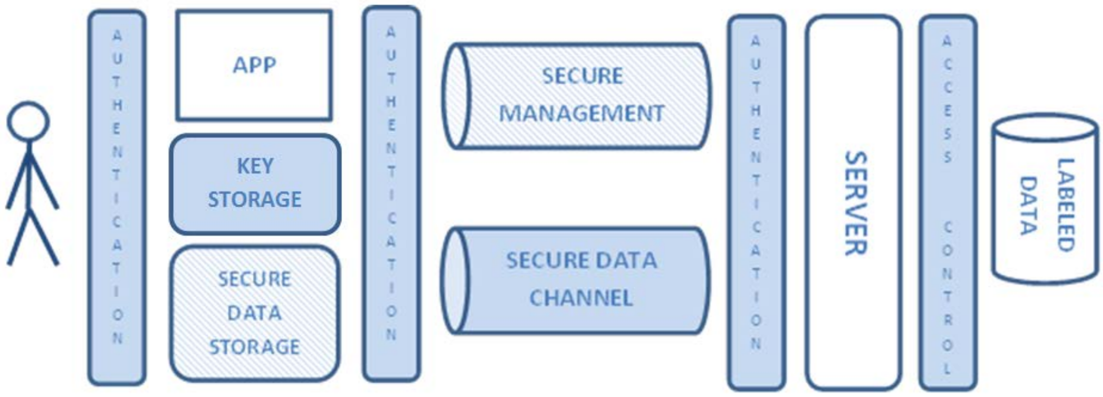


Figure 3.1 An overview of the secure capabilities needed to use mobile devices to increase situational awareness. Those with a pattern fill like secure data storage and secure management have not been implemented in this CD&E activity. Others have been implemented, but not in a consistent and integrated manner.

3.2 Android security

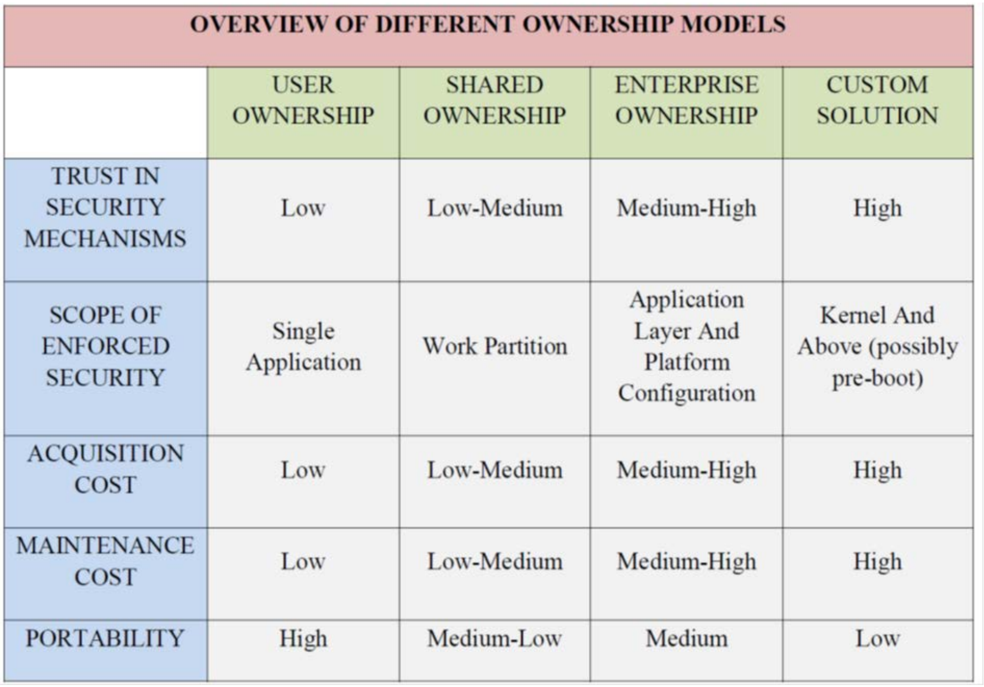
Modern mobile devices implement a wide range of security mechanisms that apps can use to secure their data. The problem is that mobile devices are by nature platforms that need to support conflicting interests and the resulting overall security is a compromise among such interests. On one hand we have users who want to have full control on the device they own and the data on it, while on the other hand we have app developers or network operators who need to generate revenue and wish to prevent users from accessing content they are supposed to pay for or that is copyrighted. Additionally, all the devices should be protected from external attackers. A consequence is that security is quite good if the device is used properly, but a motivated user can usually circumvent security mechanisms, and therefore open the way also for external attackers. The problem is exactly that in general we do not know how careful users are with their devices, and if we need a particular high degree of trust in the security mechanisms and their integrity (assurance), the only solution is to enforce stricter security policy that go to the detriment of users' control over the device, and possibly implement additional security measures.

A more extensive discussion and an overview of existing security mechanisms can be found in a dedicated report (Mancini, 2016), but we repeat the main findings here: Android provides some good security mechanisms, but they are not very flexible; the risk of finding new vulnerabilities in commercial mobile devices is relatively high, but good security practices can avert most common attacks; users are often responsible for security breaches by not following security recommendations; and increased security requires increased device control and costs.

Among existing security mechanisms that can be used to satisfy our security requirements, we find: trusted boot; disk encryption; support for various authentication protocols; support to establish secure connections like TSL and VPN; local authentication in form of screen lock; support for third party device management tools; hardware-based keystore; app store and secure verification of installed apps and updates; and the possibility to create a secure work partition. The problem with most of these mechanisms is that they are non-customizable and can be applied only at platform level. For instance, there is no API an app can use to encrypt its own files, so the user must activate a full-disk encryption feature if we want to enforce encryption. Secure boot verifies that the device is started with an approved configuration, but this information is used only by the device itself and the app can only use this information indirectly through Google proprietary APIs. Although encryption protocols like TLS are available it is not clear how to use them in conjunction with client authentication in order to achieve mutual authentication with the server. The Google Play Store is after all public, and anyone could be able to download our app and reverse engineer it. Finally, local authentication is only available at device level through screen lock, and not at application level. If we wanted to develop a custom local authentication, there is very little support and we would have to do it for each new app that uses our services. Similarly, if we wanted to use third-party applications, we would have challenges in implementing a unified security solution for all of them. We have not extensively studied the possibility of creating a dedicated work partition, but it could be a viable solution that may solve some of this inflexibility. At the end, it boils down to how much control we can exert on the device, and therefore what kind of ownership model we are willing to adopt. This is going to greatly influence also the cost of the solution.

In order to keep cost low, we would like users to be able to just download the app on their devices and use it right away. Unfortunately, we have no way to establish how secure their devices are since we have no control over them. Therefore, it is a matter of either accepting a higher risk by using standard security mechanisms in an untrusted environment (User Ownership) or adopting more expensive solutions. One might be able to buy a license for a Mobile Device Management software (MDM) and force the users to create dedicated working partition on their device we can manage (Shared Ownership). The second is to buy and configure the devices ourselves (Enterprise Ownership). The third, and more extreme, is to create our own secure system on top of commercial hardware and software (Customized Solution). The table reported in Figure 3.2 summarizes these alternatives.

While in an Enterprise Ownership Model or Customized Solution we might actually be able to satisfy all security requirements through a combination of native security mechanisms and more advanced ones provided by the additional software installed, the cost is not acceptable for the scenario we consider here. In any model there would also be some threats that are difficult to protect against because of the underlying nature of the hardware and software mobile devices are based on: they are not designed for high assurance and are not tamper-resistant. We explored therefore additional security solutions that could help satisfying as many requirements as possible also in the two other ownership models, as well as further increasing security in the remaining models.



OVERVIEW OF DIFFERENT OWNERSHIP MODELS

	USER OWNERSHIP	SHARED OWNERSHIP	ENTERPRISE OWNERSHIP	CUSTOM SOLUTION
TRUST IN SECURITY MECHANISMS	Low	Low-Medium	Medium-High	High
SCOPE OF ENFORCED SECURITY	Single Application	Work Partition	Application Layer And Platform Configuration	Kernel And Above (possibly pre-boot)
ACQUISITION COST	Low	Low-Medium	Medium-High	High
MAINTENANCE COST	Low	Low-Medium	Medium-High	High
PORTABILITY	High	Medium-Low	Medium	Low

Figure 3.2 Ownership alternatives (Mancini, 2016).

3.3 Additional security with smart cards

The tests run in this CD&E activity used off-the-shelf Android devices that were configured manually with no security policy installed. This simulates a User Ownership model scenario, but in the future it seems plausible that a Shared Ownership model will be used. In either case, even though most of Android security mechanisms can be used to provide some of the needed protection, there are some threats that are particularly difficult to defend against for mobile devices that are not completely under the enterprise control:

1. Compromise of sensitive data confidentiality if the adversary has prolonged physical access to the device

2. Lack of a secure channel to provision: the app; the user credentials; and other sensitive information like server URL and certificates

3. Impossibility to verify if a device has been compromised

It has been shown that a resourceful attacker can manage to extract information from a device to which they have physical access, as they are not tamper-resistant or certified to have a high level of assurance. The reason being that the access control mechanisms can by bypassed if the data is stored in clear text or that the encryption key is also stored on the device or it is easy to generate. Secure provisioning is also a challenge. If we do not want to use Google Play Store, the app must be installed from an untrusted source and could be spoofed. User credentials are always difficult to deliver in absence of a secure channel, since mail or SMS can be compromised if the device itself gets compromised. Similarly we need to obtain a server certificate we trust to correctly authenticate it the first time we connect to it. This is known as the problem of bootstrapping trust. The first information that is used to establish trust must be communicated over a secure channel, but a secure channel cannot be established without that information. Lastly, the server has very little chance to know whether the device it communicates with is trusted at any point, since it could be sending false status information if compromised.

In order to mitigate these risks and fully satisfy our security requirements we explored the idea of using external secure elements, also known as smart cards, to store securely sensitive information independently from the device status.

3.3.1 Smart cards

Smart cards are hardware portable devices consisting of an integrated circuit usually embedded in a plastic support of the size of a credit card, but possibly also in other formats, which is used to store and process information in a highly secure manner (Chirico, 2014). Smart cards can be classified based on the type of functionalities and communication interfaces they offer. The simplest type of cards are “memory-only smart cards”, which only offer secure data storage using strong access control that enforces read/write permissions and they communicate usually through an NFC (Near Field Communication) interface. “Microprocessor smart cards” offer a wider range of functionalities and have an on-board operating system and a dedicated cryptographic coprocessor. This allows them to perform various cryptographic algorithms and to support customized applications, which results in “multi-application smart cards”. Additionally they can enforce strong access control through the use of a simple PIN code or even biometric data like fingerprints, which are verified directly on the card and can resist brute-force attacks. They offer both a contact and a NFC interface.

For this CD&E activity we considered both types of cards. In particular we used MIFARE DESFireEV1[2] NFC cards, which are memory-only cards, and Gemalto Core Java Card in microSD[3] and Dual-interface[4] format (meaning they have both contact and NFC interface), which are multi-applications cards. The main idea has been to use the cards to store all sensitive information needed to bootstrap trust in the user, the app and the server. This would include: a user certificate to be used as credentials; a server certificate to establish a secure connection; a card certificate to establish trust between the device and the card; other cryptographic keys to encrypt data on the device; and possibly some kind of policy the server could manage on the card and which could be enforced regardless the device status. The user would then just need to remember a simple PIN code, which in some cases could be personalized and most of the security configuration would happen automatically at registration time. Multi-applications cards could also be used as a trusted execution environment the server can securely communicate with, regardless the status of the device, thus providing a secure management channel. Cryptographic keys could also be generated, destroyed or changed on the fly.

Unfortunately, in both cases we used most of the time trying to get the cards to work as we were dependent on getting both documentation and proprietary software and drivers from the manufacturers. In particular, we were never able to test Gemalto cards in the CD&E activity because they were defect and some of the key functionalities did not work correctly. A master student managed to test some features and implement algorithms to bind card and device (Sivertsgård, 2016), but eventually we focused on the MIFARE cards and sketched a concept of how they could be integrated with an Android app to enhance security.

3.3.2 Conceptual solution with MIFARE cards

As these cards are memory-only, we can expect only a fraction of the features we were planning to implement. On the other hand they are very cheap and easy to initialize. The main challenge is that once they are initialized, they cannot be modified while in use with the device as GEMALTO cards could. In addition, they are not designed to authenticate against the user, but rather against a card reader. Therefore, instead of a PIN code authentication system, they rely on symmetric keys which the device needs to know. As functionality goes, they can mainly store secret keys and not much else.

What we tried to do is to design a protocol that can simulate a PIN code authentication, and a system that requires the use of the card in order to access the app data locally by decrypting

[2] http://www.nxp.com/products/identification-and-security/mifare-ics/mifare-desfire:MC_53450
[3] http://www.gemalto.com/products/top_javacard/8030_MicroSD.html
[4] http://www.gemalto.com/dwnld/6589_IDCore3010_Product_Datasheet_Jan14.pdf

some secret on the device with a key on the card. The security requirements we can satisfy in this way are:

- An adversary cannot access the app data locally without the card and the PIN code
- An adversary cannot extract the keys from the card without the device and the PIN code
- The provisioning of credentials takes place through an interactive session with the server where the user must prove to know the PIN code
- The server certificate and secret key to access user credentials are provisioned securely through the card
- The user does not need to know more than a PIN code to configure the app and start using it

If the device is compromised, the PIN code can be stolen and the symmetric key to communicate with the card can be generated by brute force, but the card would still be necessary to extract the key to the credentials. The security of the first communication with the server is based solely on the PIN code and therefore there must be mitigations in place on server side to prevent abuse. Alternatively a one-time password (OTP) can be used, but the genuineness of the card cannot be verified as no interactive authentication can be performed by the server as it would be possible with a Gemalto card.

Most of the security of this solution is based on the new Android keystore that provides hardware-based protection of the secret material used to generate the keys to communicate with the card, since the user cannot authenticate directly to the card. However, the access control to the keys in the Android keystore cannot be linked to a customized authentication process. Keys can be used only by the app that generated them and the only other condition we can add is that the user has authenticated to the device through a secure screen lock. Therefore, in order to make the card an essential part of the local authentication process, we were forced to store encrypted user credentials outside the keystore so that they could only be decrypted by using the keys stored in the card. A schematic of the solution is given in Figure 3.3.

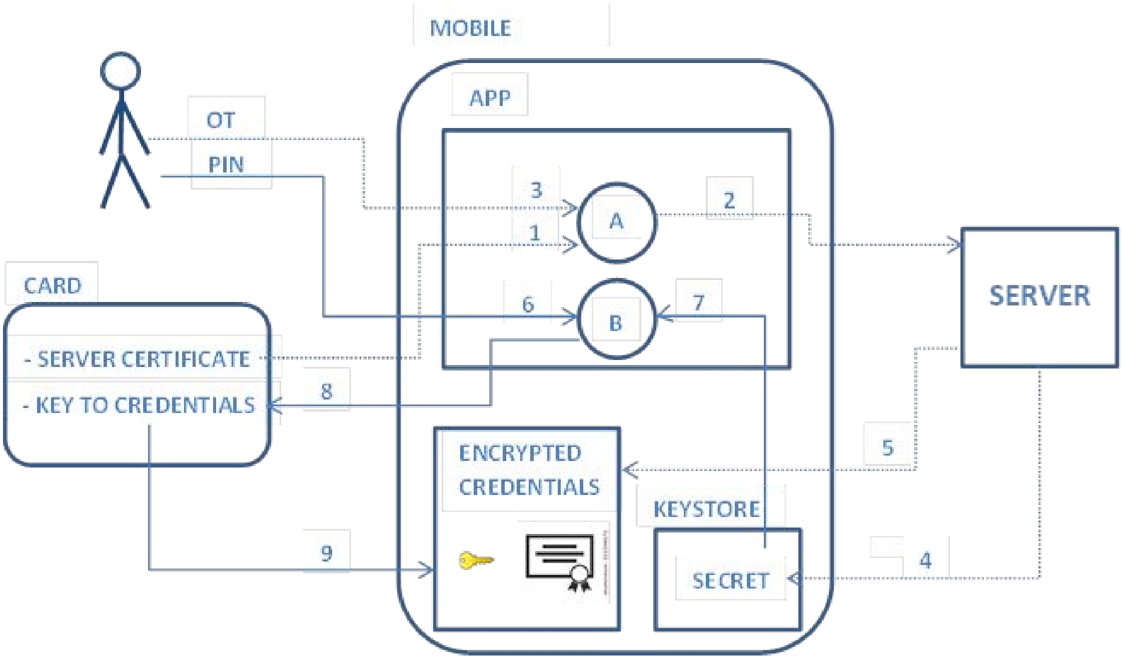


Figure 3.3 The conceptual solution consists mainly of two processes: registration (A) and authentication (B). The registration is performed only once per device, while authentication is performed every time a session expires and the user needs to access the app again by decrypting his or her credentials.

The solution consists of two phases: registration (A) and authentication (B). The registration phase uses the server certificate in the card (1) to establish a secure communication to the server (2). Then the user authenticates through an OTP (One Time Password) (2). The server responds by sending: a secret value to be stored in the device keystore (4) so that it is bound to the device; and the user's encrypted credentials (5). Now the app is ready and the user can authenticate off-line by entering the PIN (6), which is combined with the secret in the keystore through some cryptographic hashing (7) to generate the symmetric key used to authenticate to the card (8) and obtain the key to the encrypted credentials (9). The next step would be to decrypt the app data with the credentials or authenticate to the server to download data, but we have not designed that part yet.

This conceptual solution is currently being implemented and tested by three bachelor students at FFI, so it was not tested during the exercise described in the following chapter. It should be considered only a prototype as there are many logical and implementation details that have not been carefully analyzed from a security perspective and that can represent serious vulnerability of the solution. It is used mainly to test how additional security controls may affect performance and usability, and to offer an additional authentication method that the server can use to differentiate among user groups when information needs to be shared. So, further experimentation is necessary, but we think that smart card could greatly improve security and facilitate provisioning also for any ownership models that will be chosen.

4 Exercise execution

During the three technical trials preceding the main exercise, we equipped every soldier with an Android phone with our selection of apps pre-installed, except for the few that participated according to the BYOD concept. This means that we had full system coverage during the trials, all the way completely down to the individual soldier level. Such a rollout was selected under these trials for several reasons:

- Participants on these courses change roles from mission to mission, so that it would have been difficult to choose a partial rollout.
- The number of participants on the courses was low enough so that it was economically possible to provide enough units to all.
- Since the main purpose of the user tests was to get the most feedback that could be used to improve the quality of the technical solution, it was desirable that as many people as possible tested system.

We also included the course supervisors in rollout. Their experience was that the system was a valuable support tool in education and training.

After the technical trials were concluded, we tested the SMART technology demonstrator in an operational context during an exercise. This exercise encompassed a full HV district, and was thus far larger in scope than the preceding technical tests. Considering the size of the exercise, it was natural to deploy the phones somewhat differently than before. For this exercise, none of the soldiers wanted to use their own devices. Hence, we decided that we should do a partial rollout, where the platoon leaders, assistant platoon leaders, squad leaders and assistant squad leaders got issued a finished assembled unit. Such a rollout will, if the concept is taken further to an operating solution, be a realistic alternative to a full rollout because the costs of such a partial rollout will be lower but at the same time ensures that all the teams have access to the system.

In connection with the rollout of the system, we created user accounts for all participants both for use in CAGED and the chat app. The user accounts for CAGED were set up through the control panel Metis, and all the users were set up to be common end users without specific rights. In addition, the users' affiliation and roles were entered. The user accounts for chat were set up through the chat server administration panel. Each user had a separate account with the same login information as we had set up in CAGED. The users automatically got their contact lists updated in the chat app so that they were able to find the other users easily. The experience gained with the use of chat during technical trials, showed that users mainly preferred to make use of the group chat. Because of this we had created a common chat room for all users, one chat room per squad and a dedicated chat room for support. We pre-configured the group memberships so that all users were members of the common room, the dedicated support room, and the room for the squad that the user was affiliated with.

The last user configuration that was made was that all the users were entered in the phone's contact list. This was done to make it easier to use your phone's own contact opportunities (dialing and sms) for those users who wanted this.

The users were given a short review of the system (20 minutes PowerPoint brief) before they were issued equipment together with a “cheat sheet” with the most important functions in CAGED listed, before it was up to the individual to use the system. In the presentation it was made clear that only the data traffic would be encrypted with VPN, while if they used voice it would go open with the usual commercial carrier. In relation to the support it was limited to a support channel over the chat that was manned during the day by scientists from FFI.

On the phones we had installed the following software:

- CAGED for blue force tracking, observations and more.
- FrozenChat for instant messaging.
- OpenVPN for the encrypted channel between the phone and the backend.
- Twilight for preserving night vision.
- DrawOnPhoto for drawing on the images.

Prior to issuing the devices to the users, we had created a map file covering the exercise area. The map image can be downloaded from Athena if it is absent on the phone, but as this requires a lot of time and data capacity, we chose to pre-install the map on the phones in the same way as in the technical trials. The map engine in CAGED is built up around the use of OpenStreetMap (OSM). It is worth to note that after the SMART project started, OSM changed its terms of use. From the summer of 2016, they no longer allow downloading large amounts of tiles for offline use. This means that if HV wants to pursue the SMART concept in the future, they will need a different approach to maps than is currently implemented in the technology demonstrator.

During the technical trials, we followed the users through the test days, collected the phones for maintenance and observed users in the field. This allowed us to both provide tech-support to users as well as to observe the system while it was being used. Such an audit was neither possible nor desirable in this exercise since the objective was to evaluate the operative usability of the system and its impact on operation execution. In addition, it was not desirable to interfere with the forces in what was their main task that was to practice their operational tasks.

The control panel Metis was introduced during the third technical trial. There, Metis was used with assistance from FFI at all times. During the exercise, the aim was to observe the operational use of the entire system, and Metis was therefore set up in the HQ. The users could call us or send us chat messages for tech-support if needed.

5 Experiences

5.1 User experiences

The results presented in this report were gathered from a cross-sectional study employing multiple data collection methods, including questionnaires, unstructured group interviews and observations. Johnson (1997) and Eisenhardt (1989) recommend multiple data collection methods to strengthen the theory's grounding by triangulating evidence.

This study used questionnaires as its primary data collection method. The participants had to answer two questionnaires, one of which was related to expectations and answered before the experiment started. This questionnaire sought to identify the user's expectations toward the system, as well as their attitude towards, and use of, smart technology in the HV. After the experiment, the participants answered questions about their user experiences. Both of the surveys are based on established theories and variables, such as those established by Davis (1989), Venkatesh, Morris, Davis, Davis (2003), and Wixom and Todd (2005).

All questions were measured using a seven-point semantic differential scale, or a seven-point Likert scale, with anchors of "1" as strongly disagree and "7" as strongly agree. In order to fit within a military domain, the questions were reworded and modified appropriately. The measurements scales have been found to be reliable and acceptably valid in previous research, including in military settings (Elstad & Reitan, 2015; Elstad, Reitan, & Gran Jackbo, 2015; Reitan, Elstad, & Gran Jackbo, 2016). The reliability of the scales was further assessed through the Cronbach α coefficient, and overall, the analysis showed acceptable values, suggesting that the scales were reliable (Venkatesh, Thong, James, & Xu, 2012). We also did not need to exclude any questionnaires due to missing data.

Unfortunately, this study does have some weaknesses. First, the study is cross-sectional, which means that the data is only collected once. The results presented in this report are the respondents' perceptions at one point in time, and is not a longitudinal study. Perceptions could change over time or the answers at the time of the study possibly not representing the respondent's typical view. Furthermore, this study had only a few respondents, making the results indications rather than more broadly generalizable conclusions.

The analysis showed that the majority of the respondents were male, and the average service time in HV was seven years. The rest of this chapter will present the initial results from our study.

5.2 Expectations

We wanted to measure the respondents' attitude and potential performance expectancy. This chapter presents the initial descriptive analyses of such.

5.2.1 Attitude

One of the examined variables was the respondents' attitude towards smart technology. Attitude is defined as "an individual's overall affective reaction to using the system" (Venkatesh et al., 2003, p. 455). The questions used to measure this are taken from established measuring scales (for details, see Appendix A).

The results (Figure 5.1) showed that the respondents had a positive attitude towards smart technology. For example, the respondents perceived smart technology to be useful and a development in the right direction.

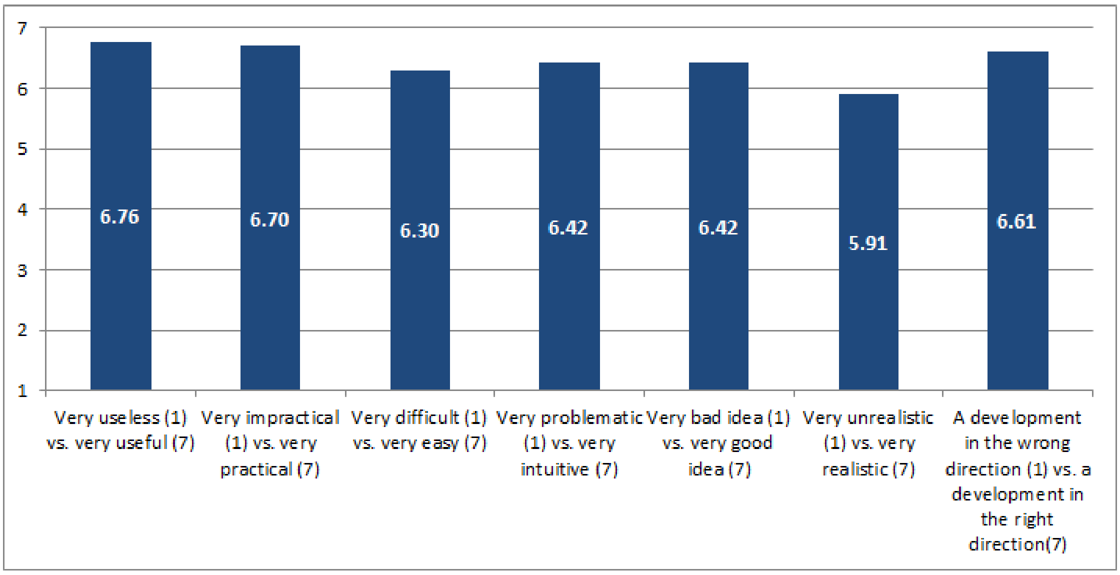


Figure 5.1 Attitude towards smart technology

Figure 5.1 shows that the respondents tended to perceive smart technology as very useful (mean 6.76), and that they perceived smart technology to be between a good idea and a very good idea (mean 6.42). Furthermore, the respondents perceived smart technology as very practical (mean 6.70) and easy to use (mean 6.30), as well as a development in the right direction (mean 6.61). The lowest average was for the degree of realism, as the respondents tended to agree that smart technology was very realistic (mean 5.91).

5.2.2 Perceived usefulness

The reason for including perceived usefulness (also called performance expectations) is that this variable is described in the literature as one of the main determinants of new technology's acceptance (see, for example, Bhattacherjee, 2001; Bhattacherjee & Premkumar, 2004; Bhattacherjee & Sanford, 2006; Venkatesh et al., 2003; Venkatesh et al., 2012). Perceived usefulness is defined in this report as "the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis, 1989, p. 320).

We sought to investigate the extent of the respondents' expectations concerning outcomes from using CAGED. Therefore, we asked whether they perceive CAGED to be useful in their job at HV, whether it saves them time and whether it potentially increases their productivity (Figure 5.2). The questions were collected primarily from Venkatesh et al. (2003), and they were somewhat reworded so as to fit the military context.

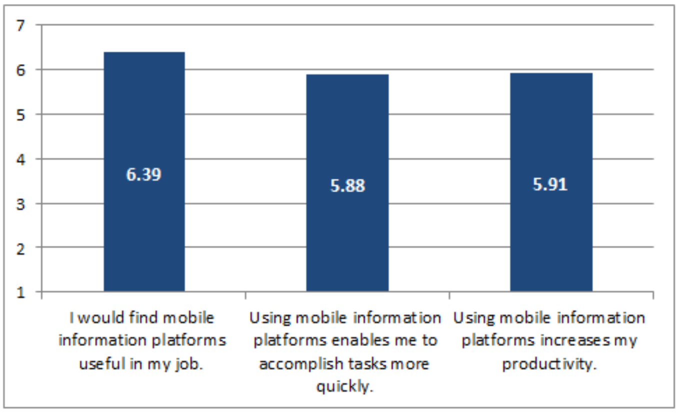


Figure 5.2 Perceived usefulness 1

The respondents perceived that CAGED could be useful in their work in HV (mean 6.39). Furthermore, they perceived that CAGED could enable one to accomplish tasks more quickly (mean 5.88) and that using CAGED could increase productivity (mean 5.91).

The next questions concerns perceptions about the future and the respondents' usefulness expectations (Figure 5.3).

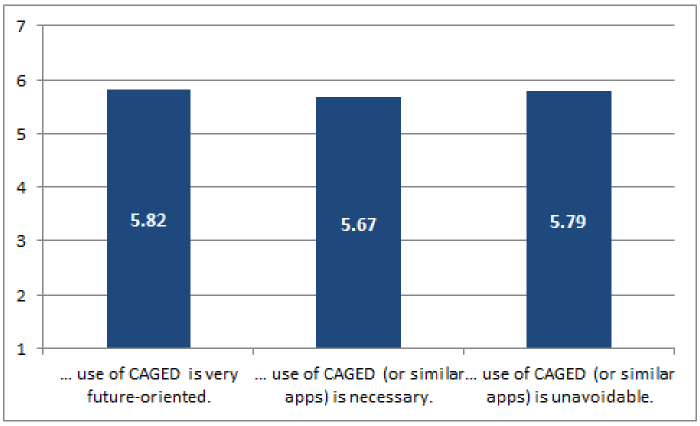


Figure 5.3 Perceived usefulness 2

The respondents agreed that use of the CAGED app is very future-oriented (mean 5.82) and that CAGED (or similar apps) was needed (mean 5.67). Furthermore, the respondents perceived that use of CAGED (or similar apps) are unavoidable (mean 5.79).

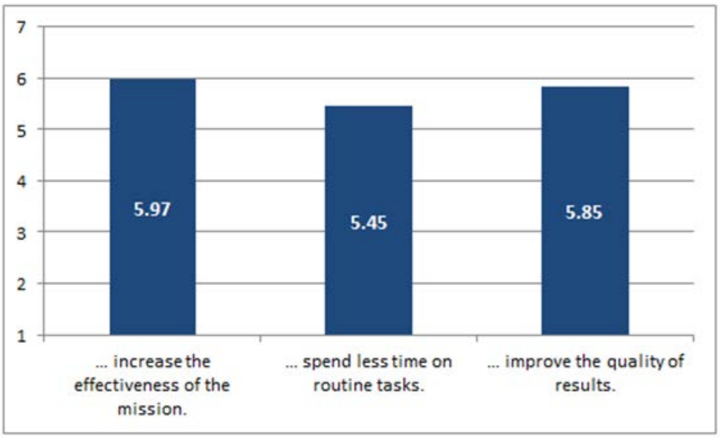


Figure 5.4 Perceived usefulness 3

As Figure 5.4 shows, the respondents also agreed that a permanent use of CAGED would increase a mission's effectiveness (mean 5.97). The respondents also varied between slightly agreeing and agreeing that the use of CAGED could allow them to spend less time on routine tasks (mean 5.45). The respondents also agreed that the permanent use of CAGED would enable them to improve the quality of the results (mean 5.85).

5.3 Experiences

We wanted to measure the respondents' perception after they tested the smart technology, including CAGED and the chat app. This chapter presents the resulting initial descriptive analyses.

We also tested for significant differences (ANOVA) between experience in HV and the type of smart phone used by the respondents during the experiments. We comment when significant differences between these groups occur.

5.3.1 Attitude and user satisfaction

In this section, we present results from the respondents' experience after testing the smart technology. The focus here is on attitude and the degree of user satisfaction with (1) the smart phone, (2) the applications (in general) and (3) CAGED.

Smart phone

Figure 5.5 presents the mean values from the questions measuring attitude and degree of user satisfaction with the smart phone tested during the experiment.

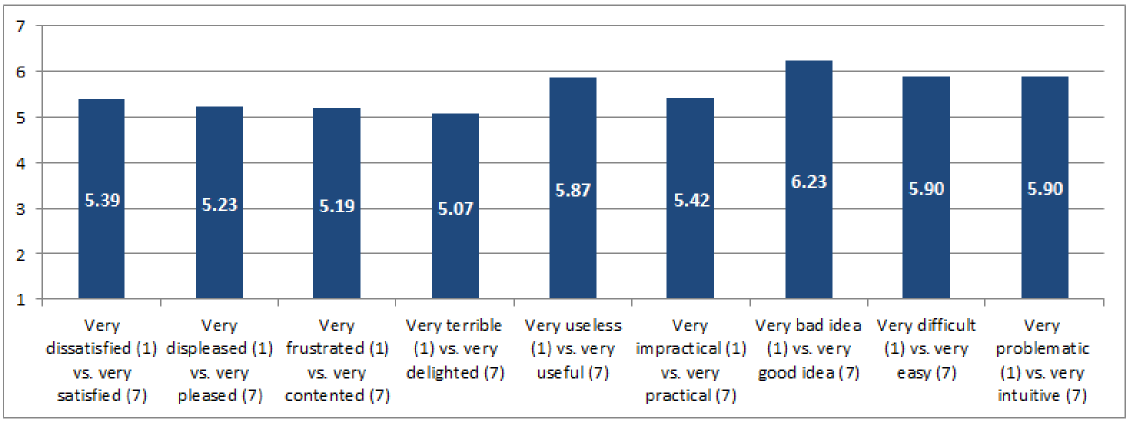


Figure 5.5 Attitude and user satisfaction: Experience with the smart phone used in the experiment

The results showed that the users were satisfied with the smart phone. As shown in Figure 5.5, all of the means were greater than 5 (very dissatisfied vs. very satisfied mean 5.39; very displeased vs. very pleased mean 5.23; very frustrated vs. very contented mean 5.19; very terrible vs. very delighted mean 5.07).

The rest of the questions measure the respondents’ attitude regarding the smart phone used during the experiment. Overall, the results showed that the respondents had a positive attitude towards the smart phone.

The respondents agreed that the use of smart phones is useful (mean 5.87), easy (mean 5.87) and a good idea (mean 6.23). Furthermore, the respondents’ perception of the smart phone varied between more or less practical and practical (mean 5.42), as well as between more or less intuitive and intuitive (mean 5.42).

Marginal differences between the groups were noted in two questions: very good idea vs. very bad idea and very difficult vs. very easy. The participants that used Motorola, Samsung, Nexus and CAT perceived smart phones to be a very good to good idea. However, those that used Sony had a neutral attitude towards smart phones.

Applications

Figure 5.6 presents the mean values from the questions measuring attitude and degree of user satisfaction with the applications tested during the experiment.

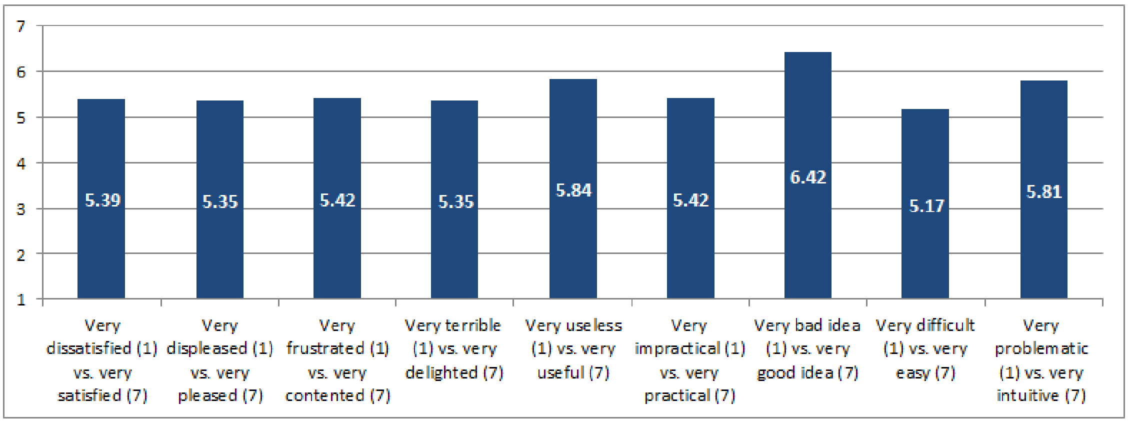


Figure 5.6 Attitude and user satisfaction: Experience with the applications used in the experiment

The questions examining user satisfaction with the applications showed that the users were satisfied. As shown in Figure 5.6, all of the means were greater than 5 (very dissatisfied vs. very satisfied mean 5.39; very displeased vs. very pleased mean 5.35; very frustrated vs. very contented mean 5.42; very terrible vs. very delighted mean 5.35). For the question “very terrible vs. very delighted,” a significant difference between the groups was noted. The lowest average belonged to the CAT users (mean 4.50), followed by users of Samsung (mean 4.92) and HTC (mean 5.00). The highest mean belonged to users of Sony (mean 6.00) and Motorola (mean 6.60).

The results show that the respondents tended to have positive attitudes towards the applications they used during the experiment. The respondents agreed that using the applications is a (very) good idea (mean 6.42). Furthermore, it is useful (mean 5.84), intuitive (mean 5.81) and easy to use (mean 5.71). The respondents’ perception of the applications varied between more or less practical to practical (mean 5.42), and between more or less intuitive.

CAGED

Figure 5.7 presents the mean values from the questions measuring attitude and degree of user satisfaction with CAGED during the experiment.

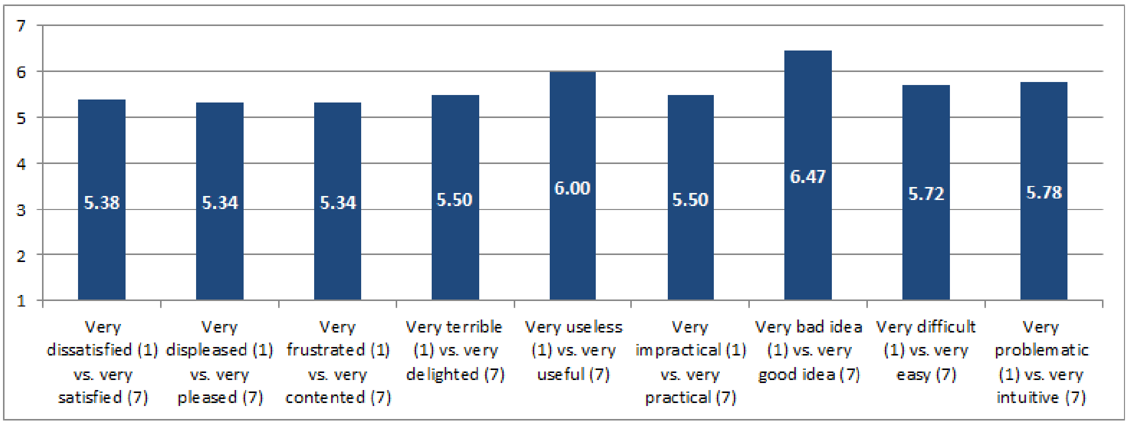


Figure 5.7 Attitude and user satisfaction: Experience with the applications used in the experiment

The questions examining user satisfaction with CAGED showed the same pattern as with the smart phone and the applications, meaning that the users were satisfied with CAGED. As we can see from Figure 5.7, all of the means were greater than 5 (very dissatisfied vs. very satisfied mean 5.38; very displeased vs. very pleased mean 5.34; very frustrated vs. very contented mean 5.34; very terrible vs. very delighted mean 5.50).

The result show that the respondents held positive attitudes towards CAGED. The respondents agreed that using CAGED is a (very) good idea (mean 6.47). Furthermore, CAGED is useful (mean 6.00), intuitive (mean 5.78) and easy to use (mean 5.72). The respondents’ perception of CAGED varied between more or less practical to practical (mean 5.50), and between more or less intuitive.

5.3.2 Information quality

This survey measured information quality through the dimensions of the information’s completeness, accuracy and usefulness. Information quality can be understood as: “The user’s perception of the quality of the information included in the system […] completeness represents the degree to which the system provides all the necessary information; accuracy represents the user’s perception that the information is correct […]” (Wixom & Todd, 2005 p. 91). The questions were taken primarily from Wixom and Todd (2005) and were reworded appropriately so as to fit the context.

CAGED

Figure 5.8 presents the mean values from the questions measuring perceived information quality from CAGED.

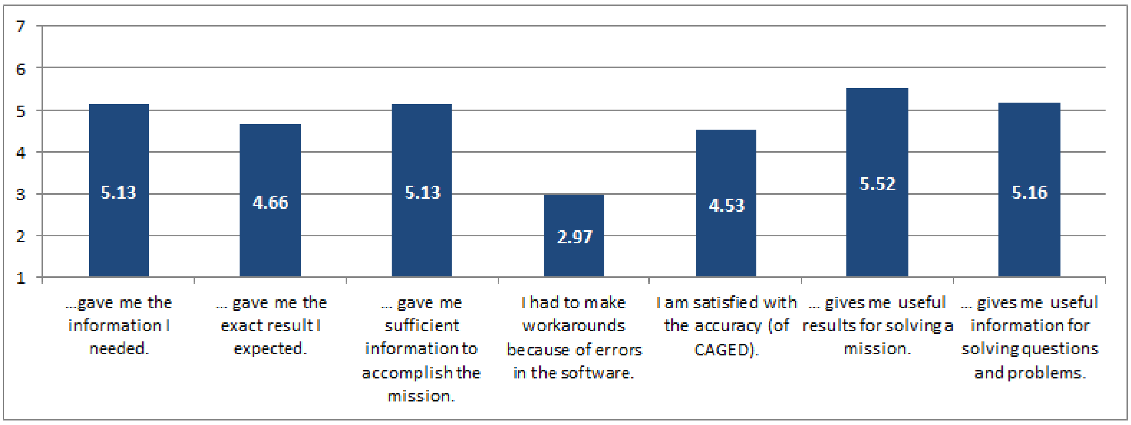


Figure 5.8 Information quality: CAGED

Overall, the respondents slightly agreed that CAGED gave the necessary information (mean 5.13). There was a marginally significant difference between the groups regarding experience in HV when it came to this question, though (Mean < 4 years = 5.56; mean 5–9 years = 4.57; mean > 10 years = 4.78). The group with less experience produced the highest average, while the groups with more experience produced lower averages.

The respondents slightly agreed that CAGED gave sufficient information to accomplish the mission (mean = 5.13). There was a marginally significant difference between the groups concerning experience in HV (Mean < 4 years = 5.50; mean 5–9 years = 4.14; mean > 10 years = 5.22).

The respondents also slightly agreed that CAGED gave them useful information for solving questions and problems (mean = 5.16). For this question, a marginally significant difference between groups existed depending on the type of smart phone used during the experiment. The Motorola users (mean 6.40) had the highest mean, followed by Nexus (mean 5.75), Sony (mean 5.00) and HTC users (mean 5.00). The lowest mean belonged to the users of Samsung (mean 4.64) and CAT (mean 3.67).

The respondents were a bit more negative with the question of whether CAGED gave exactly the expected results (mean 4.66). The same tendency was seen in the question concerning accuracy (mean 4.53). Likewise, the respondents slightly disagreed that CAGED had errors that they had to work around (mean 2.97).

Overall, the respondents' answers varied between slightly agree and agree when it came to whether CAGED produced results that were useful for solving a mission (mean 5.52). There were marginally significant differences between the groups concerning experience in HV and the type of mobile phone used during the experiment. The means for the different groups of experience break down as follows: < 4 years mean 5.93; 5–9 years mean 4.71; > 10 years mean 5.44. Regarding the type of smart phone, the Sony users (mean 6.33) had the highest mean, followed by Nexus (mean 6.00), Motorola (mean 5.80) and Samsung (mean 5.27). The two lowest means belonged to the users of HTC (mean 5.00) and CAT (mean 4.00).

CHAT

Some of the same questions about information quality (Figure 5.9) were asked about chat use (with some rewording so as to fit the context).

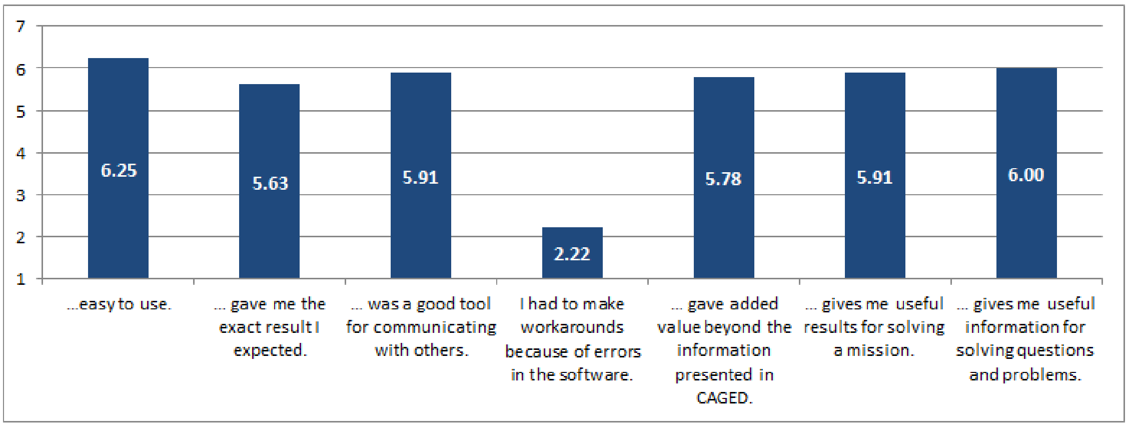


Figure 5.9 Information quality: Chat app

The respondents perceived the chat application as easy to use (mean 6.25). Furthermore, they tended to agree that the chat application gave exactly the expected results (mean 5.62).

The results showed that the respondents agreed that chat was a good tool for communicating with others (mean 5.91). There were marginal differences between the groups when it came to the type of smart phone used during the experiment. The highest average belonged to the users of HTC (mean 7) and Motorola (mean 6.80), followed by Nexus (mean 6.13) and Sony (mean 6.00). The lowest average belonged to the Samsung (mean 5.55) and CAT users (mean 5.00).

The respondents tended to agree that chat gave more value than just the information provided by CAGED (mean 5.78). The respondents agreed that the chat-application gave results that were useful for solving missions (mean 5.91), and that the app was useful for solving questions and problems (mean 6.00). The respondents did not find any application errors that they had to work around (mean 2.22).

5.3.3 System quality

We wanted to measure different aspects about system quality, as seen in Figure 5.10.

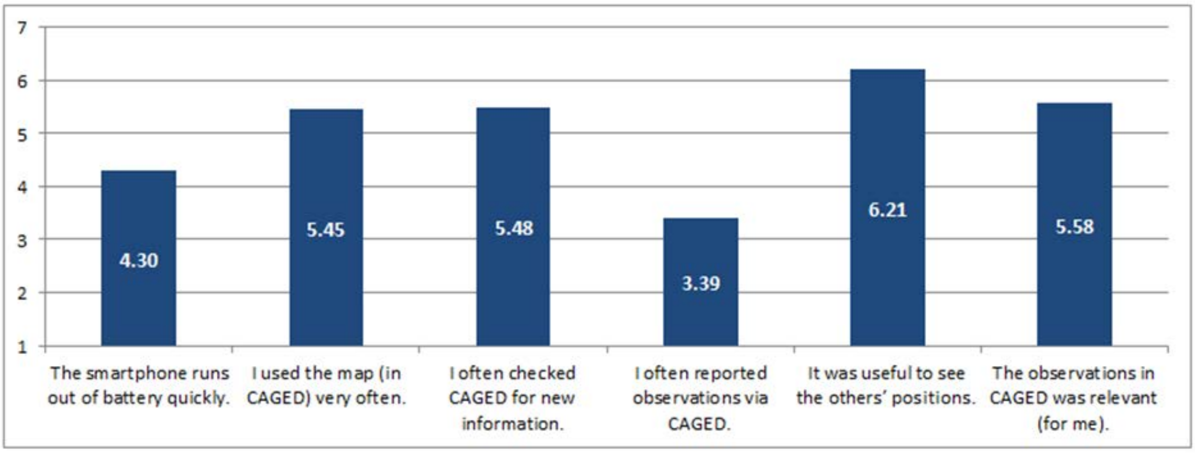


Figure 5.10 System quality

The respondents varied to be between neutral and some agree that the smartphone runs out of battery quickly (mean 4.3).

The results showed that the respondents were between somewhat agree and agree that they checked CAGED often for new information (mean 5.48). On the other hand, the respondents tended to slightly disagree that they often used CAGED to report observations (mean 3.39). Likewise, the respondents were between slightly agree and agree that they used the map in CAGED (mean 5.45), and that the reported observations in CAGED were relevant (mean 5.58).

The respondents, overall, agreed that it was useful to see other people's position, with a total mean of 6.21. However, there was significant difference between the groups (mean < 4 years = 6.25; mean 5–9 years = 5.38; mean > 10 years = 6.89).

5.4 Other user experiences

We had a lot of great feedback from users on both the positive and negative aspects of the demonstrator and the concept during the technical trials and the final exercise.

Some of the things that were outlined as particularly good were that they received a good overview of your squad and that it was useful to be able to enter observations.

Short battery life and lack of recharge capability were perceived as the biggest challenges with smart phones. We had supplied one power bank for every team (so two people had to share one powerbank), but in principle we should have had a power bank per phone. We had also supplied the users with regular phone chargers, something they could not easily use during the exercise. Rather, we should have offered car chargers, since several users had access to a vehicle.

As for CAGED, several issues were reported. The most frequently occurring comments here included poor map basis, imprecise GPS positioning, and that it was cumbersome to work with observations. Regarding observations, users wanted to have updated observations highlighted (Android notifications could be used to implement this). Furthermore, users wished more control over the information, such as the possibility to filter on the time observations were created. There were also proposals that CAGED could be improved by allowing history of mobility (a “tail” behind the blue dot), and that there was a desire to automatically report when crossing certain points or lines in the map. It was also mentioned by several users that they would prefer to have had chat inside the CAGED app instead of as an extra app, to get closer integration and prevent different information flow in CAGED and over the chat.

Regarding the Twilight app, some users reported problems with, including that it covered the screen for different apps (Twilight adds a red filter over the screen to reduce the blue light and thus preserve night vision) in such a way that they did not work properly. It is worth to remember here that we used Android 5.0 and 6.0 phones in the SMART. Starting with Android 7.0, there should be functionality along the lines of Twilight built into the operating system, which should operate independently and not negatively influence running apps. It can therefore be a good idea to test this at a later occasion if the concept is to be taken further.

Another aspect that users requested was encrypted voice communications. SMART only focused on data communications, and did not address voice at all. For future tests one could consider including this aspect as well. There are already apps one could consider to support such a concept, e.g. Teamspeak was mentioned by one of the users. Another much used solution among online gamers is Murmur/Mumble that could also be considered – there it would be possible to get both the app and the server side for free. By adding this on a server with VPN as we have done for the other apps in SMART, we could then provide users with encrypted voice as well.

In general we noticed a positive attitude among our respondents, something the following quote illustrates: "This is a step in the right direction! Simple, user-friendly and helpful."

5.5 Experiences with Metis

Metis is the user interface toward Athena, and in the HQ it gives situational awareness in the browser just like CAGED provides on Android phones. During the HV exercise Metis was set up in the HQ and users started using the system after a short introduction. Experiences from this usage are described after an interview with one of the users:

The user thought Metis was easy to use and very clear, but he also had ideas for some adjustments he would like to see made. For example, being able to add specific positions and lines to the map, as well as the possibility to better handle and process observations (for example, mark events as "finished").

Metis also holds a report function where you can export the information to an Excel spreadsheet. This functionality was used with success. The main input here from the user was that ideally pictures from observations should be included, as well as a general improvement of the formatting (larger column widths) would make the spreadsheet even more useful.

When asked if Metis provided an operational value, the user stated "absolutely". He appreciated being able to see where the troops were in relation to each other, and being able to use chat to get in contact with them.

Finally, the user pointed out that it would have been good to have the opportunity to try the system with several different HV areas together. All in all the user found Metis a valuable tool during the exercise.

6 Conclusion

In SMART, the main goal was to determine whether commercial smart technology is a viable concept for providing pervasive situational awareness support to the HV area forces. Due to the large number of area forces, and the limited time these forces have available for training, a technical solution that aims to improve the situational awareness of the individual soldier within the HV area forces need to be simple and intuitive in use and have a low cost.

During the experiments performed with the SMART technological demonstrator, we gathered information from the users about their experiences using a set of two questionnaires. Summarized, the respondents both expected and experienced a more rapid and efficient execution of their missions using the SMART demonstrator. We also found that the soldiers brought their own phones to the exercise and used them if there were issues with their primary communications channel. This shows that a better coordinated and controlled use of such resources in accordance with the “trusted unclassified” concept in SMART was both timely and relevant.

In general, we can establish that using civilian smart technology seems to yield an operational value. The SMART demonstrator and concept can provide cheap and low-complexity “trusted unclassified” communications to the HV’s area forces and others who may need this capability.

The series of technical tests and the exercise which concluded the SMART CD&E activity have shown us that users in general are happy with the concept and would want to use it for a later occasion. They pointed out, as expected, that improvements can be made, but in general they have a positive attitude towards the demonstrator system we developed and the SMART concept in general. This feedback comes from both the users in the field and the users in the HQ.

Appendix

A Tables

A.1 Expectations

Attitude N = 33; α = .777	**Mean**	**SD**	**Skew**	**Kurt**	**αilD**
Very useless (1) vs. very useful (7)[5]	6.76	.502	-2.018	3.594	.760
Very impractical (1) vs. very practical (7)[6]	6.70	5.29	-1.553	1.679	.753
Very difficult (1) vs. very easy (7)[7]	6.30	.810	-.626	-1.173	.782
Very problematic (1) vs. very intuitive (7)[8]	6.42	.751	-.903	-.587	.721
Very bad idea (1) vs. very good idea (7)[9]	6.42	.830	-.965	-.822	.727
Very unrealistic (1) vs. very realistic [10]	5.91	1.100	-.560	-1.014	.748
A development in the wrong direction (1) vs. a development in the right direction[11]	6.61	.704	-1.543	.964	.748

Perceived usefulness 1 N = 33; α = .885	**Mean**	**SD**	**Skew**	**Kurt**	**αilD**
I would find mobile information platforms useful in my job.	6.39	.0899	-1.171	.066	.951
Using mobile information platforms enables me to accomplish tasks more quickly.	5.88	1.219	-.748	-.634	.747
Using mobile information platforms increases my productivity.	5.91	1.118	-.840	.004	.758

Perceived usefulness 2 N = 33 (Single items)	**Mean**	**SD**	**Skew**	**Kurt**	**αilD**
… use of CAGED is very future-oriented.	5.82	1.380	-1.629	3.486	-
… use of CAGED (or similar apps) is necessary.	5.67	1.242	-.251	-1.202	-
… use of CAGED (or similar apps) is unavoidable.	5.79	1.409	-1.383	2.526	-

[5] Based on the measuring scale: perceived usefulness is measured here via a semantic differential scale
[6] Additional item related to ease of use
[7] Bhattacherjee and Sanford (2006)
[8] Additional item related to ease of use
[9] Davis (1989), Bhattacherjee and Sanford (2006)
[10] Bhattacherjee and Sanford (2006)
[11] Bhattacherjee and Premkumar (2004)

Perceived usefulness 3 N = 33; α = 767	**Mean**	**SD**	**Skew**	**Kurt**	**αiID**
… increase the effectiveness of the mission.	5.97	1.045	-.461	-1.128	.640
… spend less time on routine tasks.	5.45	1.348	-.752	.212	.668
… improve the quality of results.	5.85	1.004	-.468	-.781	.742

A.2 Experience

A.2.1 Difference between groups: Experience HV

Table A.1 Attitude and user satisfaction: Smartphone

α = .924	**Group**	**N**	**M**	**SD**	**Skew**	**Kurt**	**αiID**	**F**	**Sig (p)**
Very dissatisfied (1) vs. very satisfied (7)	< 4 years	16	5.38	1.088	.154	-1.388	.916	.791	.463
	5–9 years	7	5.00	1.155					
	> 10 years	8	5.75	1.282					
	Total	31	5.39	1.145					
Very displeased (1) vs. very pleased (7)	< 4 years	16	5.19	1.515	-.924	2.078	.906	.273	.763
	5–9 years	7	5.00	1.155					
	> 10 years	8	5.50	1.069					
	Total	31	5.23	1.309					
Very frustrated (1) vs. very contented (7)	< 4 years	16	5.06	1.879	-.859	.506	.904	.379	.688
	5–9 years	7	5.00	1.414					
	> 10 years	8	5.63	1.188					
	Total	31	5.19	1.600					
Very terrible (1) vs. very delighted (7)	< 4 years	15	4.87	1.727	-.692	.949	.907	.785	.466
	5–9 years	7	8.86	1.069					
	> 10 years	8	8.63	1.188					
	Total	30	5.07	1.461					
Very useless (1) vs. very useful (7)	< 4 years	16	6.00	.894	-.215	-1.068	.921	.963	.394
	5–9 years	7	5.43	1.134					
	> 10 years	8	6.00	.926					
	Total	31	5.87	.957					
Very impractical (1) vs. very practical (7)	< 4 years	16	5.44	1.569	-.837	.721	.910	.005	.995
	5–9 years	7	5.43	1.272					
	> 10 years	8	5.38	1.061					
	Total	31	5.42	1.361					
Very bad idea (1) vs. very good idea (7)	< 4 years	16	6.06	1.569	-2.576	8.468	.922	.899	.418
	5–9 years	7	6.00	1.155					
	> 10 years	8	6.75	.463					
	Total	31	6.23	1.283					
Very difficult (1) vs. very easy (7)	< 4 years	16	6.00	1.033	-.344	-1.250	.921	.514	.604
	5–9 years	6	5.50	1.378					
	> 10 years	8	6.00	.926					
	Total	30	5.90	1.062					
Very problematic (1) vs. very intuitive (7)	< 4 years	16	5.81	1.223	-.800	-.209	.924	.092	.912
	5–9 years	6	6.00	1.095					
	> 10 years	8	6.00	1.195					
	Total	30	5.90	1.155					

Table A.2 Attitude and user satisfaction: Applications

α = .955	Group	N	M	SD	Skew	Kurt	αilD	F	Sig (p)
Very dissatisfied (1) vs. very satisfied (7)	< 4 years	16	5.50	1.155	-.235	-.858	.947	.527	.596
	5–9 years	7	5.00	1.155					
	> 10 years	8	5.50	1.069					
	Total	31	5.39	1.116					
Very displeased (1) vs. very pleased (7)	< 4 years	16	5.50	1.115	-.152	-.853	.946	.900	.418
	5–9 years	7	4.86	1.069					
	> 10 years	8	5.50	1.069					
	Total	31	5.35	1.112					
Very frustrated (1) vs. very contented (7)	< 4 years	16	5.31	1.195	-.287	-.741	.950	.809	.455
	5–9 years	7	5.14	1.345					
	> 10 years	8	5.88	1.126					
	Total	31	5.42	1.205					
Very terrible (1) vs. very delighted (7)	< 4 years	16	5.38	1.310	-.292	-.562	.948	.169	.846
	5–9 years	7	5.14	1.069					
	> 10 years	8	5.50	1.069					
	Total	31	5.35	1.170					
Very useless (1) vs. very useful (7)	< 4 years	16	5.94	.998	-.234	-1.230	.949	.704	.503
	5–9 years	7	5.43	1.272					
	> 10 years	8	6.00	.926					
	Total	31	5.84	1.036					
Very impractical (1) vs. very practical (7)	< 4 years	16	5.56	1.153	-.495	-.476	.950	.318	.730
	5–9 years	7	5.14	.900					
	> 10 years	8	5.38	1.408					
	Total	31	5.42	1.148					
Very bad idea (1) vs. very good idea (7)	< 4 years	16	6.44	.727	-1.311	.848	.959	.595	.558
	5–9 years	7	6.14	.1.215					
	> 10 years	8	6.63	.744					
	Total	31	6.42	1.006					
Very difficult (1) vs. very easy (7)	< 4 years	16	6.00	.894	-.202	-.995	.949	1.914	.166
	5–9 years	6	5.14	1.345					
	> 10 years	8	5.63	.744					
	Total	30	5.17	1.006					
Very problematic (1) vs. very intuitive (7)	< 4 years	16	5.81	1.109	-.603	-.081	.951	.282	.757
	5–9 years	6	5.57	1.272					
	> 10 years	8	6.00	.926					
	Total	30	5.81	1.078					

Table A.3 Attitude and user satisfaction: CAGED

α = .959	Group	N	M	SD	Skew	Kurt	αilD	F	Sig (p)
Very dissatisfied (1) vs. very satisfied (7)	< 4 years	16	5.69	1.078	-.551	.556	.953	1.147	.332
	5–9 years	8	5.00	1.069					
	> 10 years	8	5.13	1.458					
	Total	32	5.38	1.185					
Very displeased (1) vs. very pleased (7)	< 4 years	16	5.50	1.211	-.604	.643	.951	.276	.761
	5–9 years	8	5.13	0.991					
	> 10 years	8	5.25	1.488					
	Total	32	5.34	1.208					
Very frustrated (1) vs. very contented (7)	< 4 years	16	5.56	1.315	-.759	.410	.953	.671	.519
	5–9 years	8	4.88	1.356					
	> 10 years	8	5.38	1.506					
	Total	32	5.34	1.359					
Very terrible (1) vs. very delighted (7)	< 4 years	16	5.63	1.025	-.628	.545	.951	.159	.853
	5–9 years	8	5.38	1.302					
	> 10 years	8	5.38	1.598					
	Total	32	5.50	1.218					
Very useless (1) vs. very useful (7)	< 4 years	16	6.19	0.911	-1.065	.491	.953	.468	.631
	5–9 years	8	5.75	1.282					
	> 10 years	8	5.88	1.356					
	Total	32	6.00	1.107					
Very impractical (1) vs. very practical (7)	< 4 years	16	5.81	1.276	-1.150	2.079	.952	.814	.453
	5–9 years	8	5.25	1.165					
	> 10 years	8	5.13	1.808					
	Total	32	5.50	1.391					
Very bad idea (1) vs. very good idea (7)	< 4 years	16	6.44	0.892	-1.721	2.293	.966	.652	.529
	5–9 years	8	6.25	1.165					
	> 10 years	8	6.75	0.463					
	Total	32	6.47	0.879					
Very difficult (1) vs. very easy (7)	< 4 years	16	5.88	1.088	-.658	-.399	.955	.432	.653
	5–9 years	8	5.38	1.408					
	> 10 years	8	5.75	1.389					
	Total	32	5.72	1.224					
Very problematic (1) vs. very intuitive (7)	< 4 years	16	5.81	1.047	-.611	-.535	.958	.370	.694
	5–9 years	8	5.50	1.195					
	> 10 years	8	6.00	1.414					
	Total	32	5.78	1.157					

Table A.4 Information quality: CAGED

α = .825	Group	N	M	SD	Skew	Kurt	αilD	F	Sig (p)
…gave me the information I needed.	< 4 years	16	5.56	.964	.027	-.716	.792	2.748	**.081**
	5–9 years	7	4.57	.976					
	> 10 years	9	4.78	1.302					
	Total	32	5.13	1.129					
… gave me the exact result I expected.	< 4 years	16	4.94	1.181	-.494	1.411	.768	.988	.385
	5–9 years	7	4.57	.787					
	> 10 years	9	4.22	1.563					
	Total	32	4.66	1.234					
… gave me sufficient information to accomplish the mission.	< 4 years	16	5.50	1.033	.058	-.985	.777	3.261	**.053**
	5–9 years	7	4.14	.900					
	> 10 years	9	5.22	1.563					
	Total	32	5.13	1.264					
I had to make workarounds because of errors in the software.	< 4 years	16	3.44	2.190	.871	-.088	.869	.990	.384
	5–9 years	7	2.43	1.397					
	> 10 years	9	2.56	1.590					
	Total	32	2.97	1.892					
I am satisfied with the accuracy (of CAGED).	< 4 years	16	5.00	1.155	-.399.	-.781	.828	1.641	.211
	5–9 years	7	4.14	1.345					
	> 10 years	9	4.00	2.000					
	Total	32	4.53	1.502					
… gives me useful results for solving a mission.	< 4 years	16	5.93	.961	-.603	-.273	.778	3.075	**.062**
	5–9 years	7	4.71	1.113					
	> 10 years	9	5.44	1.236					
	Total	32	5.52	1.151					
… gives me useful information for solving questions and problems.	< 4 years	16	5.20	1.699	-.659	.815	.794	.214	.809
	5–9 years	7	4.86	1.345					
	> 10 years	9	5.33	1.118					
	Total	32	5.16	1.440					

Table A.5 Information quality: Chat app

α = .832	Group	N	M	SD	Skew	Kurt	αilD	F	Sig (p)
…easy to use.	< 4 years	16	6.31	0.946	-1.132	.081	.797	.705	.503
	5–9 years	7	5.86	1.215					
	> 10 years	9	6.44	1.014					
	Total	32	6.25	1.016					
… gave me the exact result I expected.	< 4 years	16	5.81	1.047	-.417	-.490	.819	.906	.415
	5–9 years	7	5.14	1.345					
	> 10 years	9	5.67	1.000					
	Total	32	5.63	1.100					
… was a good tool for communicating with others.	< 4 years	16	5.81	1.047	-1.196	1.734	.821	.227	.798
	5–9 years	7	5.86	1.464					
	> 10 years	9	6.11	0.782					
	Total	32	5.91	1.058					
I had to make workarounds because of errors in the software.	< 4 years	16	2.44	2.032	1.720	2.085	.881	.883	.424
	5–9 years	7	1.43	0.535					
	> 10 years	9	2.44	1.878					
	Total	32	2.22	1.773					
… gave added value beyond the information presented in CAGED.	< 4 years	16	5.69	1.621	-1.532	-.524	.780	.969	.391
	5–9 years	7	5.29	1.799					
	> 10 years	9	6.33	1.118					
	Total	32	5.78	1.539					
… gives me useful results for solving a mission.	< 4 years	16	6.06	1.063	-.763	.178	.769	1.217	.311
	5–9 years	7	5.29	1.380					
	> 10 years	9	6.11	1.269					
	Total	32	5.91	1.201					
… gives me useful information for solving questions and problems.	< 4 years	16	6.06	0.998	-.913	6.528	.789	.079	.924
	5–9 years	7	5.86	1.069					
	> 10 years	9	6.00	1.414					
	Total	32	6.00	1.107					

Table A.6 System quality: Smartphone and CAGED

α = .666	Group	N	M	SD	Skew	Kurt	αilD	F	Sig (p)
The smartphone runs out of battery quickly.	< 4 years	16	4.38	2.156	.-465	-1.115	.742	.395	.677
	5–9 years	8	3.75	2.550					
	> 10 years	9	4.67	1.803					
	Total	33	4.30	2.128					
I used the map (in CAGED) very often.	< 4 years	16	5.81	1.328	-1.139	.994	.611	.996	381
	5–9 years	8	4.88	1.553					
	> 10 years	9	5.33	1.936					
	Total	33	5.45	1.563					
I often checked CAGED for new information.	< 4 years	16	5.50	1.713	-.884	.044	.540	1.105	.344
	5–9 years	8	4.88	1.642					
	> 10 years	9	6.00	1.118					
	Total	33	5.48	1.564					
I often reported observations via CAGED.	< 4 years	16	3.69	1.778	.414	-.633	.647	.405	.671
	5–9 years	8	3.00	2.070					
	> 10 years	9	3.22	1.922					
	Total	33	3.39	1.853					
It was useful to see the others' positions.	< 4 years	16	6.25	0.856	-1.977	4.210	.550	3.873	.**032**
	5–9 years	8	5.38	1.923					
	> 10 years	9	6.89	0.333					
	Total	33	6.21	1.219					
The observations in CAGED were relevant (for me).	< 4 years	16	5.56	1.263	-.336	-1.218	.639	.538	.589
	5–9 years	8	5.25	1.282					
	> 10 years	9	5.89	1.269					
	Total	33	5.58	1.251					

A.2.2 Difference between groups: type of smart phone

Table A.7 Attitude and user satisfaction: Smartphone

	Group	N	M	SD	F	Sig (p)
	Samsung	12	5.08	1.165		
	Sony	2	6.50	.707		
	Nexus	7	5.43	.976		
Very dissatisfied (1) vs. very satisfied (7)	Motorola	5	6.20	1.304	1.414	.254
	CAT	4	4.75	.957		
	HTC	1	5.00	.		
	Total	31	5.39	1.145		
	Samsung	12	5.17	1.115		
	Sony	2	4.00	4.243		
	Nexus	7	5.43	.787		
Very displeased (1) vs. very pleased (7)	Motorola	5	6.00	1.225	.826	.543
	CAT	4	4.75	.957		
	HTC	1	5.00	.		
	Total	31	5.23	1.309		
	Samsung	12	5.00	1.758		
	Sony	2	4.00	4.243		
	Nexus	7	6.00	.816		
Very frustrated (1) vs. very contented (7)	Motorola	5	5.80	1.304	1.046	.413
	CAT	4	4.25	.500		
	HTC	1	5.00	.		
	Total	31	5.19	1.600		
	Samsung	11	4.73	1.272		
	Sony	2	4.00	4.243		
	Nexus	7	5.43	1.134		
Very terrible (1) vs. very delighted (7)	Motorola	5	6.20	1.304	1.176	.350
	CAT	4	4.50	.577		
	HTC	1	5.00	.		
	Total	30	5.07	1.461		
	Samsung	12	5.67	.985		
	Sony	2	6.50	.707		
	Nexus	7	6.14	.690		
Very useless (1) vs. very useful (7)	Motorola	5	6.20	1.095	.829	.541
	CAT	4	5.25	1.258		
	HTC	1	6.00	.		
	Total	31	5.87	.957		
	Samsung	12	5.42	1.443		
	Sony	2	4.50	3.536		
	Nexus	7	5.57	.976		
Very impractical (1) vs. very practical (7)	Motorola	5	6.00	1.000	.432	.822
	CAT	4	5.00	1.414		
	HTC	1	5.00	.		
	Total	31	5.42	1.361		
	Samsung	12	6.08	.900	2.135	**.094**

	Group	N	M	SD	F	Sig (p)
Very bad idea (1) vs. very good idea (7)	Sony	2	4.00	4.243		
	Nexus	7	6.57	.535		
	Motorola	5	7.00	.000		
	CAT	4	6.00	1.414		
	HTC	1	7.00	.		
	Total	31	6.23	1.283		
Very difficult (1) vs. very easy (7)	Samsung	11	5.82	1.079	4.202	**.007**
	Sony	2	7.00	.000		
	Nexus	7	6.00	.816		
	Motorola	5	6.80	.447		
	CAT	4	4.50	.577		
	HTC	1	5.00	.		
	Total	30	5.90	1.062		
Very problematic (1) vs. very intuitive (7)	Samsung	11	5.73	1.421	1.522	.220
	Sony	2	7.00	.000		
	Nexus	7	6.00	.816		
	Motorola	5	6.60	.548		
	CAT	4	5.00	1.155		
	HTC	1	5.00	.		
	Total	30	5.90	1.155		

Table A.8 Attitude and user satisfaction: Applications

	Group	N	M	SD	F	Sig (p)
Very dissatisfied (1) vs. very satisfied (7)	Samsung	12	5.08	1.240	1.000	.438
	Sony	2	6.50	.707		
	Nexus	7	5.43	.787		
	Motorola	5	6.00	1.225		
	CAT	4	5.00	1.155		
	HTC	1	5.00	.		
	Total	31	5.39	1.116		
Very displeased (1) vs. very pleased (7)	Samsung	12	5.08	1.240	1.207	.335
	Sony	2	6.50	.707		
	Nexus	7	5.43	.787		
	Motorola	5	6.00	1.225		
	CAT	4	4.75	.957		
	HTC	1	5.00	.		
	Total	31	5.35	1.112		
Very frustrated (1) vs. very contented *(7)*	Samsung	12	5.08	1.311	1.612	.193
	Sony	2	6.50	.707		
	Nexus	7	5.57	.976		
	Motorola	5	6.20	1.304		
	CAT	4	4.50	.577		
	HTC	1	6.00	.		
	Total	31	5.42	1.205		
Very terrible (1) vs. very delighted (7)	Samsung	12	4.92	1.165	2.658	**.046**
	Sony	2	6.00	1.414		
	Nexus	7	5.57	.976		
	Motorola	5	6.60	.894		
	CAT	4	4.50	.577		
	HTC	1	5.00	.		
	Total	31	5.35	1.170		
Very useless (1) vs. very useful (7)	Samsung	12	5.58	.996	2.007	.112
	Sony	2	7.00	.000		
	Nexus	7	5.86	.900		
	Motorola	5	6.60	.548		
	CAT	4	5.00	1.414		
	HTC	1	6.00	.		
	Total	31	5.84	1.036		
Very impractical (1) vs. very practical (7)	Samsung	12	4.92	1.240	1.980	.117
	Sony	2	6.50	.707		
	Nexus	7	5.43	.976		
	Motorola	5	6.40	.548		
	CAT	4	5.00	1.155		
	HTC	1	6.00	.		
	Total	31	5.42	1.148		
Very bad idea (1) vs. very good idea (7)	Samsung	12	6.25	.866	.835	.537
	Sony	2	6.50	.707		
	Nexus	7	6.43	.787		

	Group	N	M	SD	F	Sig (p)
	Motorola	5	7.00	.000		
	CAT	4	6.00	1.414		
	HTC	1	7.00	.		
	Total	31	6.42	.848		

Very difficult (1) vs. very easy (7)	Samsung	12	5.58	.996	1.746	.161
	Sony	2	7.00	.000		
	Nexus	7	5.86	.690		
	Motorola	5	6.00	1.225		
	CAT	4	4.75	.957		
	HTC	1	6.00	.		
	Total	31	5.71	1.006		
Very problematic (1) vs. very intuitive (7)	Samsung	12	5.67	1.231	1.838	.142
	Sony	2	7.00	.000		
	Nexus	7	5.86	.690		
	Motorola	5	6.40	.894		
	CAT	4	4.75	.957		
	HTC	1	6.00	.		
	Total	31	5.81	1.078		

Table A.9 Attitude and user satisfaction: CAGED

	Group	N	M	SD	F	Sig (p)
Very dissatisfied (1) vs. very satisfied (7)	Samsung	12	5.33	1.371	.961	.459
	Sony	3	6.67	.577		
	Nexus	7	5.29	1.113		
	Motorola	5	5.40	1.140		
	CAT	4	4.75	.957		
	HTC	1	5.00	.		
	Total	32	5.38	1.185		
Very displeased (1) vs. very pleased (7)	Samsung	12	5.00	1.414	1.344	.277
	Sony	3	6.67	.577		
	Nexus	7	5.43	1.134		
	Motorola	5	5.80	.837		
	CAT	4	4.75	.957		
	HTC	1	5.00	.		
	Total	32	5.34	1.208		
Very frustrated (1) vs. very contented (7)	Samsung	12	4.83	1.642	1.442	.243
	Sony	3	6.67	.577		
	Nexus	7	5.57	.976		
	Motorola	5	6.00	1.225		
	CAT	4	4.75	.957		
	HTC	1	5.00	.		
	Total	32	5.34	1.359		
Very terrible (1) vs. very delighted (7)	Samsung	12	5.17	1.337	1.292	.298
	Sony	3	6.67	.577		
	Nexus	7	5.43	.976		
	Motorola	5	6.20	1.304		
	CAT	4	5.00	1.155		
	HTC	1	5.00	.		
	Total	32	5.50	1.218		
Very useless (1) vs. very useful (7)	Samsung	12	5.75	1.138	1.343	.278
	Sony	3	7.00	.000		
	Nexus	7	6.00	1.155		
	Motorola	5	6.60	.548		
	CAT	4	5.25	1.500		
	HTC	1	6.00	.		
	Total	32	6.00	1.107		
Very impractical (1) vs. very practical (7)	Samsung	12	5.17	1.801	.971	.454
	Sony	3	6.67	.577		
	Nexus	7	5.29	.951		
	Motorola	5	6.20	.837		
	CAT	4	5.00	1.414		
	HTC	1	6.00	.		
	Total	32	5.50	1.391		
Very bad idea (1) vs. very good idea (7)	Samsung	12	6.42	.669	1.103	.383
	Sony	3	7.00	.000		
	Nexus	7	6.14	1.215		

	Group	N	M	SD	F	Sig (p)
	Motorola	5	7.00	.000		
	CAT	4	6.00	1.414		
	HTC	1	7.00	.		
	Total	32	6.47	.879		

Very difficult (1) vs. very easy (7)	Samsung	12	5.42	1.443	1.912	.127
	Sony	3	6.00	1.000		
	Nexus	7	6.14	.690		
	Motorola	5	6.60	.894		
	CAT	4	4.50	1.000		
	HTC	1	6.00	.		
	Total	32	5.72	1.224		
Very problematic (1) vs. very intuitive (7)	Samsung	12	5.67	1.371	2.649	.046
	Sony	3	6.00	1.000		
	Nexus	7	6.14	.690		
	Motorola	5	6.60	.548		
	CAT	4	4.25	.500		
	HTC	1	6.00	.		
	Total	32	5.78	1.157		

Table A.10 Information quality: CAGED

	Group	N	M	SD	F	Sig (p)
…gave me the information I needed.	Samsung	11	5.00	1.265	1.057	.406
	Sony	3	6.00	1.000		
	Nexus	8	5.13	1.126		
	Motorola	5	5.60	.548		
	CAT	4	4.25	1.258		
	HTC	1	5.00	.		
	Total	32	5.13	1.129		
… gave me the exact result I expected.	Samsung	11	4.18	1.722	.740	.600
	Sony	3	5.00	.000		
	Nexus	8	4.75	1.035		
	Motorola	5	5.40	.894		
	CAT	4	4.50	.577		
	HTC	1	5.00	.		
	Total	32	4.66	1.234		
… gave me sufficient information to accomplish the mission.	Samsung	11	4.91	1.375	.806	.556
	Sony	3	5.00	2.000		
	Nexus	8	5.50	1.195		
	Motorola	5	5.60	1.140		
	CAT	4	4.25	.500		
	HTC	1	6.00	.		
	Total	32	5.13	1.264		
I had to make workarounds because of errors in the software.	Samsung	11	3.64	2.420	1.336	.280
	Sony	3	1.33	.577		
	Nexus	8	2.38	1.061		
	Motorola	5	2.40	1.949		
	CAT	4	4.00	1.414		
	HTC	1	4.00	.		
	Total	32	2.97	1.892		
I am satisfied with the accuracy (of CAGED).	Samsung	11	4.55	1.864	.267	.927
	Sony	3	5.00	1.000		
	Nexus	8	4.63	1.506		
	Motorola	5	4.60	1.140		
	CAT	4	3.75	1.708		
	HTC	1	5.00	.		
	Total	32	4.53	1.502		
… gives me useful results for solving a mission.	Samsung	11	5.27	1.272	2.187	**.088**
	Sony	3	6.33	.577		
	Nexus	8	6.00	1.069		
	Motorola	5	5.80	.447		
	CAT	3	4.00	1.000		
	HTC	1	5.00	.		
	Total	31	5.52	1.151		
… gives me useful information for solving questions and problems.	Samsung	11	4.64	1.748	2.420	**.064**
	Sony	3	5.00	.000		
	Nexus	8	5.75	1.165		

	Motorola	5	6.40	.548
	CAT	3	3.67	.577
	HTC	1	5.00	.
	Total	31	5.16	1.440

Table A.11 Information quality: Chat app

	Group	N	M	SD	F	Sig (p)
…easy to use.	Samsung	11	6.36	.674	1.295	.296
	Sony	3	7.00	.000		
	Nexus	8	5.88	1.356		
	Motorola	5	6.60	.894		
	CAT	4	5.50	1.291		
	HTC	1	7.00	.		
	Total	32	6.25	1.016		
… gave me the exact result I expected.	Samsung	11	5.64	.809	.648	.666
	Sony	3	6.00	1.000		
	Nexus	8	5.50	1.414		
	Motorola	5	5.80	1.095		
	CAT	4	5.00	1.414		
	HTC	1	7.00	.		
	Total	32	5.63	1.100		
… was a good tool for communicating with others.	Samsung	11	5.55	1.128	2.198	**.085**
	Sony	3	6.00	1.000		
	Nexus	8	6.13	.641		
	Motorola	5	6.80	.447		
	CAT	4	5.00	1.414		
	HTC	1	7.00	.		
	Total	32	5.91	1.058		
I had to make workarounds because of errors in the software.	Samsung	11	2.91	2.468	.988	.444
	Sony	3	1.00	.000		
	Nexus	8	2.00	1.069		
	Motorola	5	2.00	1.732		
	CAT	4	1.50	.577		
	HTC	1	4.00	.		
	Total	32	2.22	1.773		
… gave added value beyond the information presented in CAGED.	Samsung	11	5.45	1.916	1.211	.332
	Sony	3	6.67	.577		
	Nexus	8	6.00	1.069		
	Motorola	5	6.60	.894		
	CAT	4	4.50	1.915		
	HTC	1	6.00	.		
	Total	32	5.78	1.539		
… gives me useful results for solving a mission.	Samsung	11	5.91	1.221	.963	.459
	Sony	3	6.00	1.000		
	Nexus	8	6.13	1.356		
	Motorola	5	6.40	.894		
	CAT	4	4.75	1.258		
	HTC	1	6.00	.		
	Total	32	5.91	1.201		
… gives me useful information for solving questions and problems.	Samsung	11	5.82	1.401	.654	.661
	Sony	3	6.33	1.155		
	Nexus	8	6.25	1.035		

	Motorola	5	6.40	.548
	CAT	4	5.25	.957
	HTC	1	6.00	.
	Total	32	6.00	1.107

Table A.12 System quality: Smartphone and CAGED

	Group	N	M	SD	F	Sig (p)
The smartphone runs out of battery quickly.	Samsung	12	4.92	1.832	.754	.591
	Sony	3	2.33	1.528		
	Nexus	8	4.13	2.167		
	Motorola	5	4.00	2.828		
	CAT	4	4.75	2.630		
	HTC	1	4.00	.		
	Total	33	4.30	2.128		
I used the map (in CAGED) very often.	Samsung	12	5.67	1.371	.882	.507
	Sony	3	6.33	1.155		
	Nexus	8	5.63	1.506		
	Motorola	5	5.00	2.345		
	CAT	4	5.00	1.414		
	HTC	1	3.00	.		
	Total	33	5.45	1.563		
I often checked CAGED for new information.	Samsung	12	4.92	1.832	.618	.687
	Sony	3	6.33	1.155		
	Nexus	8	5.63	1.685		
	Motorola	5	6.00	1.000		
	CAT	4	5.75	1.500		
	HTC	1	5.00	.		
	Total	33	5.48	1.564		
I often reported observations via CAGED.	Samsung	12	3.00	1.758	.301	.908
	Sony	3	4.00	2.646		
	Nexus	8	3.88	2.167		
	Motorola	5	3.60	1.342		
	CAT	4	3.00	2.309		
	HTC	1	3.00	.		
	Total	33	3.39	1.853		
It was useful to see the others' positions.	Samsung	12	6.42	1.240	1.216	.329
	Sony	3	6.33	.577		
	Nexus	8	6.50	.756		
	Motorola	5	6.40	.894		
	CAT	4	5.00	2.160		
	HTC	1	5.00	.		
	Total	33	6.21	1.219		
The observations in CAGED were relevant (for me).	Samsung	12	5.33	1.231	.265	.928
	Sony	3	6.00	1.000		
	Nexus	8	5.75	1.488		
	Motorola	5	5.80	1.643		
	CAT	4	5.25	.957		
	HTC	1	6.00	.		
	Total	33	5.58	1.251		

References

Bekkelund, K.H., Frøseth, I.M., Bloebaum, T.H., Johnsen, F.T., and Brannsten, M.R. (2016) EP1667 «SMART» installasjon og oppsett av demonstratorprogramvaren. (FFI- Eksternnotat 16/02009). Kjeller: Forsvarets forskningsinstitutt, 2016 (in Norwegian)

Bhattacherjee, A. (2001). Understanding information systems continuance: An Ecpectation-Conformation Model. MIS Quarterly, 25(3), 351-370.

Bhattacherjee, A., and Premkumar, G. (2004). Understanding changes in belief and attitude toward information technology usage: a theoretical model and longitudional test. MIS Quarterly, 28(2), 229-254.

Bhattacherjee, A., and Sanford, C. (2006). Influence processes for information technology acceptance: an elaboration likelihood model. MIS Quarterly, 30(4), 805-825.

Boddhu, S.K., Williams, R.L., Wasser E., and Kode, N. (2012). Increasing situational awareness using smartphones. Proc. SPIE 8389, Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR III, 83891J (May 1, 2012); doi:10.1117/12.920035; http://dx.doi.org/10.1117/12.920035

Chirico, U. (2014) Smart Card Programming - A comprehensive guide to smart card programming in C/C++, Java, C#, VB.NET, Lulu, Second Edition 2014.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), 318-340.

Defence Material Organisation, [Dutch] Ministry of Defence (2015). Promise 1.0 final report. Final version 1.3, 30 April 2015.

Dixon, A. and Henning, J. (2013). Nett Warrior gets new end-user device. http://www.army.mil/article/107811/ 2013.

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. Academy of Management Review, 14(4), 532-550.

Elstad, A. K., and Reitan, B. K. (2015). Mobile information platforms in the military domain. In J. Fog, A. Karlsen, J. Kaasbøll, B. E. Munkvold, G. Netteland, A. Opdahl, and G. Sindre (Eds.), Norsk Konferanse for Organisasjoners Bruk av Informasjonsteknologi (NOKOBIT) (Vol. 23). Ålesund.

Elstad, A. K., Reitan, B. K., and Gran Jackbo, C. (2015). Baselineundersøkelse fra eksperimentserie på sammensatte læringssystemer (MCLS). (FFI-notat 2015/00618). Kjeller: Forsvarets forskningsinstitutt. (in Norwegian)

Evans, J.B., Ewy, B. J., Swink, M. T., Pennington, S. G., Siquieros, D. J., and Earp, S. L. (2013). TIGR: the tactical ground reporting system. IEEE Communications Magazine, vol. 51, pp. 42-49, 2013.

Forsvaret (2017). The Home Guard. https://forsvaret.no/en/organisation/home-guard 20 January 2017.

Gourley, S.R. (2013). Nett Warrior: Mission - Command at the Tactical Edge. ARMY Magazine 24-27, https://www.ausa.org/publications/armymagazine/archive/2013/06/Documents/Gourley1_June2013.pdf 2013

Johnsen, F.T. (2016). Oppsett av OpenVPN på Ubuntu 14.04 LTS. (FFI- Eksternnotat 16/01791). Kjeller: Forsvarets forskningsinstitutt, 2016 (in Norwegian)

Johnson, R. B. (1997). Examining the Validity Structure of Qualitative Research. Education, 118(2), 282-292.

Karlsen, L. H. and Reitan, B. K (2014). CEI — et sosialt taktisk rapporteringssystem — teknisk beskrivelse av Android klient for smarttelefon og nettbrettstøtte til CEI-systemet. FFI-notat 2014/00526, 2014. (in Norwegian)

Mancini, F. (2016), «Modern mobile platforms from a security perspective,» FFI report 16/00319, Kjeller, NO, 2016.

Reitan, B. K., Elstad, A. K., and Gran Jackbo, C. (2016). En ny klasse kommando og kontroll informasjonssystemer(K2IS) – eksperimenter med smarttelefoner og samhandling. (2015/02298). Kjeller: Forsvarets forskningsinstitutt (FFI).

Sivertsgård, H. M. (2016) Using Smart Cards to Mitigate Security Threats on Mobile Devices. Master Thesis, University of Bergen, Norway 2016.

Teleplan (2017). DINA — soldier system. DINA produktark, http://www.teleplanglobe.no/hubfs/DEF/DINA/DINA_productsheet.pdf 2016

Thales (2017). NORMANS Soldier System. https://www.thalesgroup.com/sites/default/files/asset/document/thales-normans.pdf Accessed 28 April 2017

Usbeck, K., Gillen, M., Loyall, J.P., Gronosky, A., Sterling, J., and Kohler Jr, R. L. (2015) Improving Situation Awareness with the Android Team Awareness Kit (ATAK). SPIE Conference on Defense and Security (SPIE.DSS), Baltimore, MD, 2015.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2003). User acceptance of information technology: toward a unified view. MIS Quarterly, 27(3), 425-478.

Venkatesh, V., Thong, L., James, Y., and Xu, X. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. MIS Quarterly, 36(1), 157-178.

Website (2016). Android Tactical Assault Kit. https://atakmap.com/p_about.aspx 2016

Wixom, B. H., and Todd, P. A. (2005). A Theoretical Integration of User Satisfaction and Technology Acceptance. Information Systems Research, 16(1), 85-102.

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

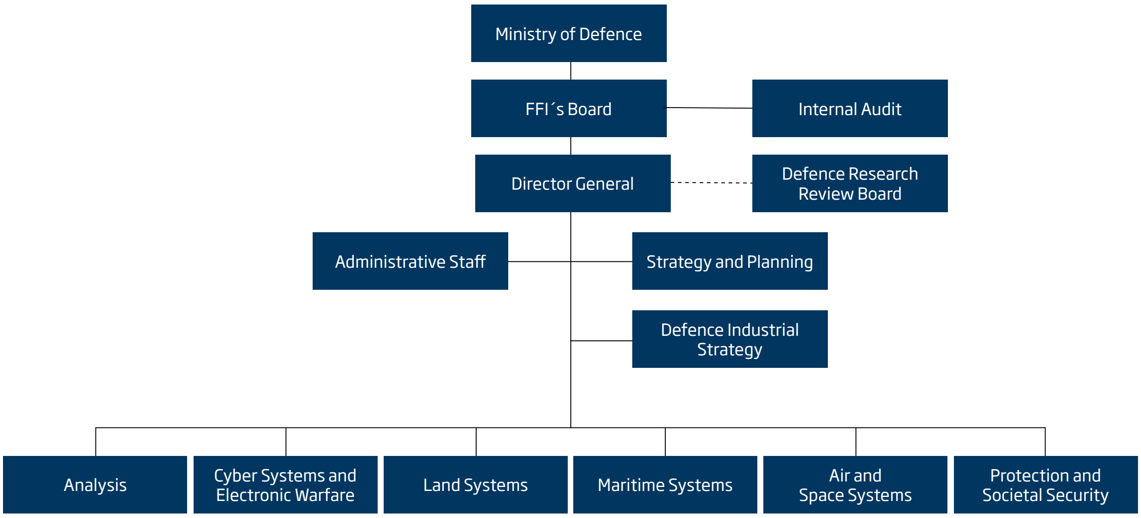
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment