NTNU
Norwegian University of
Science and Technology

The role of trust when implementing Network Based Defence in the Norwegian Armed Forces

Tonje Andreassen

Master in Information Security

Submission date:	May 2017
Supervisor:	Jose J Cabeza Gonzalez, IIK
Co-supervisor:	Ivar Kjærem, Norwegian Defence Roger Johnsen, Norwegian Defence

Norwegian University of Science and Technology
Department of Information Security and Communication

Preface

This thesis is the final part of my Master's education in the subject of Information Security. The education was carried out at the Norwegian University of Science and Technology in the Faculty of Information Technology and Electrical Engineering. The department responsible for the education was Department of Information Security and Communication Technology at Gjøvik. The project described in this report, was carried out during the spring semester of 2017.

The practical research was conducted in three different military units in the Norwegian Armed Forces, including field research, questionnaires and interviews. Preliminary research was conducted at the Norwegian Defence University College of Engineering - Telematics. The results from this preliminary research served as a basis to adjust the developed questionnaire and interview guide for further use in two additional army units (not denoted with names during this report). It also served as a basis to understand how technology was considered in relation to knowledge and in a military context.

The problem described in this project, is of great interest for the researcher. The problem challenges military operations and introduces obstacles for the operators residing in the tactical level of the Norwegian Armed Forces. It was important for me to make decision-makers aware of some of the problems related to Network Based Defence. More specifically, I wanted to enlighten how perceived trust affected the operators ability to employ the tactical technical platform. Fortunately, this was also of interest for my military supervisors.

This report is written for readers holding some academic competence both related to information security and organisational processes. It can be assumed that senior students attending the Master's program for Information Security have sufficient knowledge to understand the contents of the report. However, the report is written in such a manner, that personnel with some knowledge related to military operations and human interaction will understand the described main issues.

31-05-2017

Acknowledgment

First of all, I would like to thank my academic supervisor, Josè Gonzalez, for supervising my work with this Master Thesis. Despite a tight schedule, he has contributed with valuable inputs and advice in addition to concrete and insightful feedback. His knowledge and experience related to science and system dynamic processes have made this a very inspiring and motivating process. In addition, his network of academic professionals made it possible to adapt already existing models, also contributing to proposed future work in this project.

I would also like to thank Ying Qian for permitting reuse and adaption of developed system dynamic models from her PhD "Mitigating Information security risks during the Transition to Integrated Operations". The adapted models support results obtained during the practical research in this project. In addition, the adapted models enable simulations of possible outcomes, supporting future implementations of technical platforms.

It would not have been possible to carry out the practical research without help from the Norwegian Defence University College of Engineering - Telematics and two army units. I would like to thank all the participants contributing with their inputs during field research, questionnaires and interviews. Their feedback enabled relevant analyses, resulting in reasonable findings and conclusions.

I would like to thank my military supervisors, Ivar Kjærem and Roger Johnsen contributing with guidelines and support related to the military context. Their support made it possible to investigate problem issues important to me, and highly relevant to the Norwegian Armed Forces.

Last, but not least, I would like to thank my two sons and my boyfriend for their patience and support during this Master's programme.

T.A.

Abstract

The Norwegian Armed Forces are supposed to implement Network Based Defence within the next couple of decades to achieve information superiority and to enable speed of command during operations. The process of implementing Network Based Defence is however suffering from different obstacles, challenging and slowing down the process. The delayed implementation affects the entire Norwegian Armed Forces, and puts soldier lives and operations at stake. Studied literature emphasizes that technology, procedures and intellectual capital are not aligned to each other, introducing gaps between technology implemented and knowledge needed to utilize it. Similar obstacles have been identified during practical research in this project. Inappropriate technological solutions, education of operators at random, complex information collection together with inadequate level of trust among the operators, suggest that technology, procedures and intellectual capital are not aligned to each other. Comparable challenges can be found in Integrated Operations in the oil sector. In this project, adapted system dynamic models primarily developed for Integrated Operations, were employed as preliminary hypothesis. The adapted models also supported results obtained during interviews and questionnaires conducted in two different army units. The purpose of the research was to identify factors delaying the implementation process of Network Based Defence, and to investigate if the models would support future implementations. The results in total suggest that knowledge is not very well adjusted to the operation transition of Network Based Defence. A knowledge gap might be introduced, affecting the operators' perceived trust level. Inadequate level of trust might result in inappropriate use of the technological platform, which again increase the probability of incidents during military operations. If the knowledge development and operation transition is not aligned to each other, the implementation process will most likely be delayed and suffer from increased cost. Empirical studies have shown significant cost benefit utilization when employing system dynamic models in parallel with new technology adoption. The project therefore suggests employing a full-fledged system dynamic model in parallel with the implementation process of Network Based Defence. Technological implementations can then be simulated in advance to identify possible difficulties. Hence, system dynamic models of sufficient detail can support the implementation of Network Based Defence to ensure implementation in time, within the estimated cost and with reduced risk.

Contents

List of Figures

1 Introduction

Technology has changed the way military operations are conducted throughout the twentieth century, and most of the communication is today conducted via technological networks. It has been a shift from personal interaction to dependence on technology, to achieve the stated objectives. Due to insufficient budgets, the number of soldiers and officers are reduced simultaneously as the objectives are maintained. Operations depend on information delivered via the networks, whether it is position data resulting in a blue or red spot on an interactive map, or information delivered as intelligence directly from the soldiers via the networks.

1.1 Topic covered by the project

The Norwegian Armed Forces are supposed to implement Network Based Defence within the next couple of decades [8] in order to modernize the entire Norwegian Armed Forces. Even if the political and strategic management have the same visions and objectives in relation to Network Based Defence, the process is delayed. Several obstacles are slowing down the process. Some operative units are impatiently expediting adjusted solutions for testing of Network Based Defence, but the defence in total has lacking will and ability for implementation [9]. The gap between actual and proposed cooperation might lead to reduced operative effect and increased risk in some scenarios. Unaligned processes related to operation transition and knowledge improvement will also introduce gaps, leading to possible vulnerabilities [10]. Increased number of vulnerabilities can increase the number of incidents, ranging from small accidents to collateral damage on the battlefield . Often, technology is implemented before the operators get proper education and training, resulting in a knowledge gap. This knowledge gap might lead to vulnerabilities as inadequate level of trust and reduced situational awareness (SA).

Preliminary studies suggest that there are differences between various military units. Some of the units have been able to implement the technological platform in a better manner than others. Based on this assumption, research will be conducted within various military units to investigate and identify factors affecting the employment of the technological platform during military operations. The identified factors will be supported by system dynamic models adapted from Integrated Operations in the oil sector. The models are denoted "preliminary NbF SD models" and will be employed to identify intentional and unintentional effects related to the implementation of Network Based Defence. By identifying such factors, it

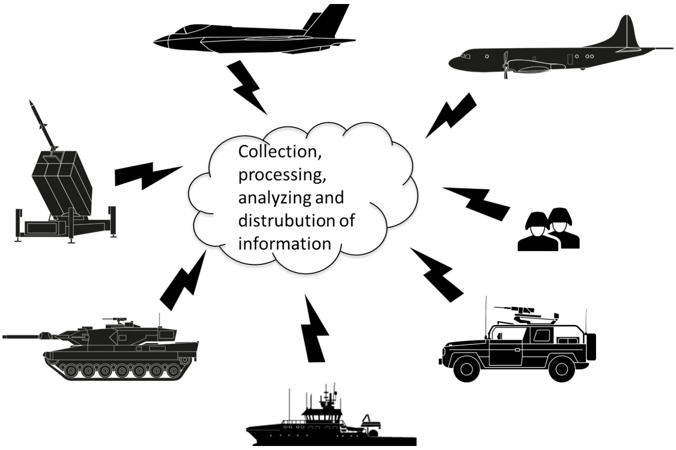


Figure 1: Conceptual model of Network Based Defence

might be possible to suggest recommendations to simplify and reduce risks related to the implementation of Network Based Defence.

1.1.1 Network Based Defence

Network Based Defence is comparable to the concept Network Centric Warfare (NCW). Both concepts seek to utilize network connected information systems in order to achieve information superiority [11]. The main idea is to connect intelligent sensors, command and control systems together with precision weapons, to enable enhanced situational awareness, rapid target assessment and distributed weapon assignment [12]. The concept of NCW also has the ability to enable development of speed of command, leading to more effective operations and disruption of the enemy's strategy [11]. The strategic objective of Network Based Defence is to efficiently utilize technological infrastructure to support network based national operations and network based operations abroad [8]. A successful implementation relies on compatible systems, an excellent information infrastructure and intellectual capital [11]. In addition, technology, organization and doctrines must be aligned to each other. Hence, Network Based Defence is to perceive technology, organization, competence and processes in a common context [13].

The concept of Network Based Defence is illustrated in figure 1, where various network components are connected together in networks. The idea is that data and information continuously are collected by different sensors, and transmitted into the system for processing and analysing. Processed and analysed information is then distributed to appropriate levels of the command hierarchy to support current and future operations. The increased amount of processed and analysed informa-

Source: Store Norske Leksikon

Figure 2: NATO defined

tion has the possibility to increase the situational awareness (SA) for commanders in all levels of the organization. Better SA supports faster and more correct decisions, enhances the cooperation and coordination between different entities.

Implementation of Network Based Defence

The Norwegian Defence department’s policy for Network Based Defence [14] was published in 2008, and is by Forsvarsdepartementet defined as interaction in network [14]. The policy is a foundation for the development of Network Based Defence in Norway. Cyberforsvaret in the Norwegian Armed Forces is responsible for the use and implementation of Network Based Defence [8]. The strategic objective of Network Based Defence is to efficiently utilize technological infrastructure in order to support network based operations home and abroad. Capabilities are to be developed in accordance with NATO’s objectives for "Network Enabling Capabilities (NEC)", where the main goal is to change a culture, starting with the people. Hence, the actual networks consist of humans conducting the interaction, and technology supporting human processes as situational awareness, leadership, planning and implementation.

From the outside, it seems that the political and strategical management are consistent and coherent in their visions and objectives related to Network Based Defence. The implementation of Network Based Defence is, however, delayed and suffering from different obstacles slowing down the process. The human factor is central when implementing new technology. Individuals must be able to integrate information, anticipate what’s going to happen and plan the next move [15]. This depends heavily on cognitive ability. But the human factor is in many cases neglected or underestimated [16], changing the focus from person to tool, placing the responsibility on the systems instead of the commanders [17]. Making information available in all levels might also result in micro-management and collapsing lines of communication due to the human factor [18].

> "Warfare is not ’network centric’. It is either ’people centric’, or it has no center at all". Lieutenant General William S. Wallace, U.S. Army [17]

A study conducted by FFI [19] concludes with three main reasons for the delayed implementation of Network Based Defence. Interaction between different levels of the organization is complicated because of the traditional structure of the Norwegian Armed Forces. Even today, the hierarchical organization has a strong position in the military, complicating the transformation into network based forces. Another issue is the lack of understanding for the Network Based Defence process. The third problem is related to a gap between the processes going top-down and bottom-up. In addition, lack of ownership and implementation capacity is emphasized as two transverse problem issues in "Støtte til Forsvarets NbF-utvikling – sluttrapport" [9].

The concept of Network Based Defence is neither further operationalized in the Norwegian military doctrine [20]. Network Based Defence seems to be viewed in isolation without relation to cyber operations, command and control. The main direction for Network Based Defence is stated, but none of the studied documents elaborate further how to accomplish Network Based Defence, how to do the practical implementation, the operationalization. The deficient documentation related to practical implementation suggests that there is no formal way of educating personnel within the subject of Network Based Defence. The lack of a common educational plan and static operation procedures can help explain why the defence in total has lacking will and ability for implementing Network Based Defence [9].

Cebrowski and Garstka [11] stated that Network Centric Warfare and all other changes associated with military affairs, were related to changes in the American society. In 1998 the underlying information technology changed from platform based to network centric based, starting the explosive growth of the Internet. The technological change happened much faster than the development within culture and organizations. The same can be said about Network Based Defence, where the cost driver mainly is technology based [21]. An introduction of more technological platforms and an increased amount of information, put higher demands on the analytical capacity. This can only be achieved by increasing the number of staff officers, hence reducing the number of soldiers in the other end.

> " We now know more, but this makes one more, not less, uncertain."
> (Karl von Clausewitz, Vom Krieg (1832))

1.1.2 Unadjusted processes

A successful implementation of Network Centric Warfare will rely on a holistic approach, also including the human factors [22]. In addition, technology, organization and doctrine must be viewed as a whole. Human and organizational issues must be part of the transformation to Network Based Defence, in line with technology, to achieve satisfactory situational awareness [23]. As technology is often implemented much faster than knowledge, organization and doctrines are developed, it can be assumed that the described processes are not aligned to each other, complicating and challenging the implementation of Network Based Defence. Comparable processes and consequences can be found in the paper "Emergent vulnerabilities in Integrated Operations: A proactive simulation study of economic risks" by Rich et al [10]. System dynamics (SD) is employed to simulate and study two processes in parallel, to investigate how these processes are affecting each other when new technology is implemented. One of the processes is related to work processes; the other process is the development of new knowledge and skills needed to operate the platform safely. When these two processes are not adjusted to each other, vulnerability is affected. If the work processes are implemented faster than the knowledge needed to use them, simulations show that the number of vulnerabilities will increase. With fast work process implementation, the vulnerability rate will increase significantly, increasing the number of incidents. The incidents can range from accidents within different units to collateral damage on the battlefield.

System dynamics include a modelling and simulation technique, first developed by Jay Forrester and described in his article "Industrial Dynamics—A Major Breakthrough for Decision Makers" from 1958 [24]. The technique was originally developed for industrial systems, but can be applied to all complex systems to predict behaviour over time. The technique includes both qualitative and quantitative models. Even if the qualitative models cannot be simulated, they can be employed to understand causes and relations in a complex system. It also serves as a good communication tool. System dynamics helps identifying unintentional effects acting against the stated objectives. In this project, the objective is find obstacles slowing down the implementation of Network Based Defence. One assumption is that the lack of knowledge and skills act as counter forces to Network Based Defence achievement, creating unintentional effects in the total system. Unintentional effects in this context will be related to possible vulnerabilities increasing the probability of risk. Unadjusted processes related to Network Based Defence are described in detail in chapter 3.

1.1.3 Possible vulnerabilities

The neglect of the human factor might be crucial to understand why there are problems related to the implementation of Network Centric Warfare, and hence also Network Based Defence. Focusing on knowledge and skills as the main reasons for unadjusted processes, possible vulnerabilities introduced into a human-technical system might be inadequate level of trust and inappropriate situational awareness [25].

> “Trust is defined "to believe that someone is good and honest and will not harm you, or that something is safe and reliable" [26] “
> “Situational awareness (SA) is how individuals collect and utilize information;

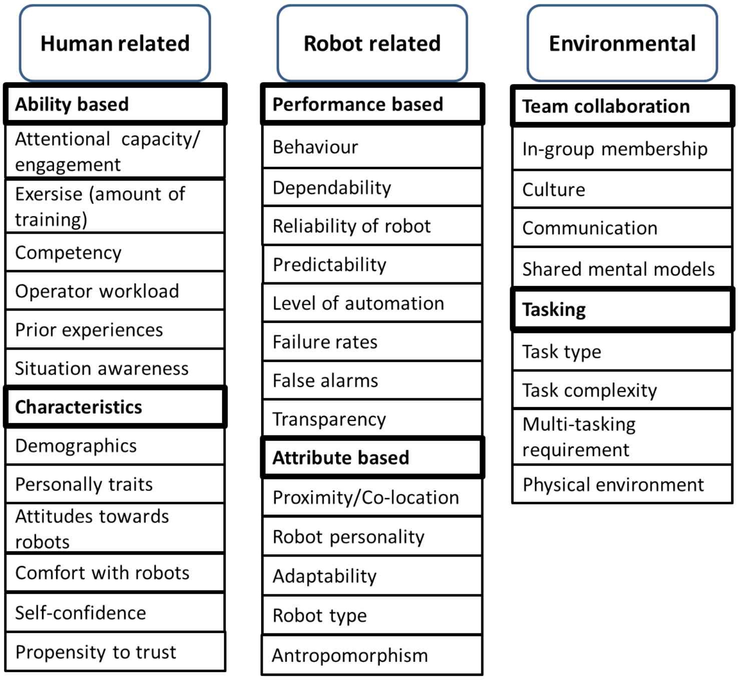


Figure 3: The triadic model. Adapted from Hancock et al [1]

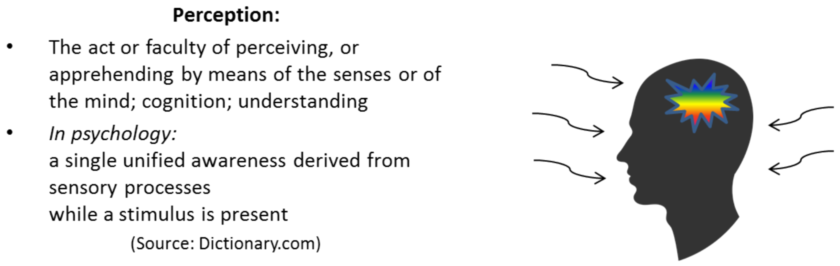
.

and is based on attention, recognition and communication [27]".

Trust

Jian et al [28] found that people do not perceive trust differently whether the relationship was general trust, human-human trust or human-machine trust. This indicates that results from studies related to human-human relations, also can be employed to understand the trust between humans and networked systems.

During the PhD study "The perception and measurement of human-robot trust" done by Schaefer [25], trust between humans and robots are thoroughly described. A trust scale is developed to measure an individual's trust to a robot, and also what inflicts the individual's change in trust. Attributes related to humans, robots and the environment are identified based on the work "A Meta-Analysis of Factors Influencing the Development of Human-Robot Trust" by Hancock [1], representing potential antecedents of trust. The identified antecedents are organized into 3 different areas; human related, robot related and environmental. The antecedents have the potential to affect the development of trust within human-robot interaction. Figure 3 illustrates the organization of the antecedents, and is referred as the triadic model of trust.



Perception:

- The act or faculty of perceiving, or apprehending by means of the senses or of the mind; cognition; understanding
- *In psychology:*
  a single unified awareness derived from sensory processes
  while a stimulus is present

(Source: Dictionary.com)

Figure 4: Perception

The triadic model of trust includes several factors, also relevant to military technological command and control systems. Competency, training and situation awareness are parts of the human related antecedents of trust, and are central aspects for knowledge based processes in relation to Network Based Defence. In addition, trust is tightly connected to the user's perception, because the definition of trust is to believe that something is reliable or good. In "Trust in Automation: Designing for Appropriate Reliance" [29], Lee emphasized that appropriate trust is necessary to achieve superior performance in a human–automation system. It is therefore important that the operators get proper training in order to understand the intended use of the system, and expected reliability. Inappropriate trust levels can affect the operator's willingness to employ the system [16]. On the flip side, too high reliance on the system can result in the operator not noticing system fails. Inappropriate trust levels can be caused by unreliable systems, but also that the user is not familiar with the systems, or do not have the correct competence and experience.

Situational awareness

Correct situational awareness (SA) is a prerequisite for information superiority [11], and is also said to be an antecedent of trust. In addition, SA is about predicting and planning future actions based on present information [30]. If the operators are not able to collect the correct data, and if the data is analysed based on wrong assumptions, the result will be faulty plans and increased number of incidents. Reduced or wrong SA will therefore represent vulnerability in military operations in addition to be an antecedent of trust.

In a military context, situational awareness (SA) is the ability to identify, process, and comprehend important information affecting the mission; understanding the situational picture. In the simplest form, SA is about perceiving relevant information from the environment, meaning that relevant data has to be identified and collected in its raw form [2]. The more complex part of SA, is to comprehend

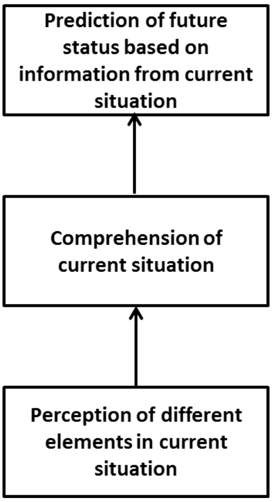

Prediction of future status based on information from current situation
Comprehension of current situation
Perception of different elements in current situation

Figure 5: Three-level model of situational awareness. Adapted from Endsley [2]

the current situation based on perceived information, and to predict future actions. The three levels illustrated in figure 5 represent an increasing degree of awareness, as the information is processed at the higher levels. By achieving appropriate situational awareness, the commanders are able to know their risks, vulnerabilities and current capabilities to make informed tactical and strategic decisions.

SA is said to be enhanced by Network Enabled Operations [11], enabling more information sharing in a shorter time, and also improving the collaboration between different units. By faster information exchange, the speed of commands increases significantly, enhancing the effectiveness of the missions. It is assumed that the more information shared, the better situational awareness due to information superiority [11]. But the quality of the situational picture depends on the information quality. Bolia et al [16] argue that a higher quantity of information can lead to the cost of quality within the information, resulting in wrong information. Wrong information can be a result of wrong analyses of the data, but also due to compromised or missing data, faulty sensors or inaccurate software. In addition, the enemy can fill the system with wrong sensor data or other misleading intelligence. The illusion of a complete war picture might also lead to wrong information, not knowing or not being aware that some information is missing. Incomplete, wrong, compromised and unavailable data or information is part of the CIA triad [31]. CIA is an abbreviation for confidentiality, integrity and availability and has for several decades been the main components of information security.

When the operator is presented a vast amount of information, it exceeds his ability to analyse it in a proper way, and the information lost might be the most critical. When it comes to interpretation of the situation, it can be assumed that knowledge and previous experience will affect how well this is done. Situational awareness (SA) is described by Schaefer [25] as an antecedent of trust, but is also about predicting and planning future actions based on present information [30]. If the operators are not able to collect the correct data, and if the data is analysed based on wrong assumptions, the result will be faulty plans and increased number of incidents. Wrong interpretation of the situation together with varying quality of the information, will affect the SA. Reduced SA will therefore represent vulnerability in military operations in addition to be an antecedent of trust. It can be assumed that an experienced commander is able to analyse a situation correctly even with reduced information quality. SA is therefore tightly connected to knowledge, including both competence and experience. In addition, knowledge will highly affect how the users employ the system. In order to accomplish the objectives of Network Based Defence, the people employing the information systems needs to know what to report, understand the importance of what they are reporting and also trust the system so they do not avoid to report.

1.1.4 Contents of the project

This project seeks to identify obstacles slowing down and challenging the implementation of Network Based Defence. Preliminary studies suggest that there are differences between various army units. Some of the units have been able to implement the technological platform in a better manner than others. Based on this assumption, research will be conducted within various military units to investigate and identify factors affecting the employment of the technological platform. The research will be conducted using tools as field research, questionnaires and interviews. The focus will be to identify and elaborate factors affecting trust and situational awareness based on the identified antecedents of trust; competency, training and situational awareness. The identified factors will be supported by system dynamic models adapted from Integrated Operations in the oil sector, preliminary NbF SD models. The models will seek to identify intentional and unintentional effects related to the implementation of Network Based Defence. By identifying such factors, it might be possible to suggest recommendations to simplify and reduce risks related to the implementation of Network Based Defence.

The remainder of this project report is structured as follows. In chapter 2, previous related work is briefly described, included Network Centric Warfare and Network Based Defence, unadjusted processes in Integrated Operations and research focusing on human related antecedents of trust. In chapter 3, a methodology used as hypothesis is introduced and described. The methodology is based on system dynamic models first described in general terms, before specifically looking into how preliminary NbF SD models adapted from Integrated Operations will support this project. Chapter 4 includes the results from the preliminary research conducted at The Norwegian Defence University College of Engineering - Telematics. In chapter 5, results from research conducted in two various army units are presented. The results from the practical research, supported by the preliminary NbF SD models, are discussed in chapter 6. The conclusion and recommendations of this project can be found in chapter 7. The closing chapter of the project includes proposals for future work.

1.2 Keywords

Network Centric Warfare (NCW), Network Centric Operations (NCO), military operations, situational awareness (SA), human factor(s), Network Based Defence (NbF), trust, NATO Network Enabled Capabilities (NEC, NNEC)

1.3 Problem description

Command and control within military operations are today relying on technological networks, and the Norwegian Armed Forces are supposed to implement Network Based Defence within the next couple of decades. The political and strategic management seem coherent in their visions and objectives, but the implementation process is suffering from different obstacles, challenging and slowing down the process. Interaction between different levels is complicated due to the hierarchical structure of the military [19]. There is a lack of understanding for Network Based Defence, and there is a gap between the processes going top-down and bottom-up. It also seems that Network Based Defence is viewed isolated from other operative processes, and the concept is not further operationalized [20]. Some operative units use adjusted solutions for testing, but in total, the defence has lacking will and ability for implementation.

It seems that technological solutions are implemented before military doctrines are adjusted, and before the educational system is prepared to take advantage of the new functionality. This might introduce a gap between operations conducted on the technological platform and the knowledge needed to utilize it. This gap can lead to an unbalance between the two processes, introducing vulnerabilities, which again can increase the probability of incidents. Inadequate trust level and wrong perception of the situation might be the most significant vulnerabilities introduced, if the processes are not aligned to each other. As there are differences between various military units, it might be possible to identify factors affecting these vulnerabilities. Identification of such factors has the possibility to align the processes to each other, and reduce the number of vulnerabilities introduced. It would possibly also enhance and speed the implementation of Network Based Defence in the Norwegian Armed Forced. In this project, the focus will be to identify and elaborate factors affecting trust and situational awareness (SA) through practical research. The practical research will consist of interviews, questionnaires and field research. The factors will mainly be based on and limited to competency; training and SA, as SA both appear as an antecedent of trust and a possible vulnerability if perceived wrongly. Even if the implementation of Network Based Defence includes both technology and humans, the main objective is to identify issues related to the human factor.

The identified factors will be supported by system dynamic models adapted from Integrated Operations in the oil sector, to identify intentional and unintentional effects related to the implementation of Network Based Defence. The adapted models are denoted "preliminary NbF SD models". By analysing the identified factors and identifying possible effects, it should be possible to make recommendations for how to ensure implementation in time, within the estimated cost and with reduced risk.

1.4 Justification, motivation and benefits

Network Based Defence is necessary both in current and future military operations. Obstacles described by Rutledal [9] and Fridheim [19] are, however, slowing down the process of implementing Network Based Defence into the Norwegian Armed Forces. The gap between operations residing on the technological platform and the knowledge and skills needed to utilize it, introduces several vulnerabilities, putting soldier lives and operations at stake. It is therefore important to identify factors delaying the implementation of Network Based Defence. Taking a broad approach, countries could benefit from such identification, as the problem is prevalent in other countries than Norway as well. For the Norwegian Armed Forces, a solution could improve military operations significantly, achieving the goals stated in relation to Network Based Defence. It could also save lives, as the commanders, officers and soldiers could become more aware of the actual situation, and take more informed decisions. In addition, identification of described factors could significantly enhance and increase the speed of the implementation of Network Based Defence with reduced risk.

1.5 Research questions

- **RQ1: How are the two processes of operation transition and knowledge development in Network Based Defence adjusted to each other?**
  A literature study together with adapted system dynamic models will serve as preliminary methodologies to investigate issues related to RQ1. Referred

literature focusing on unadjusted processes can be found in page 4 and 15. Adapted system dynamic models, denoted preliminary NbF SD models, are thoroughly described in section 3.1. Findings from the methodology chapter will support results obtained during the practical research. A summary of the practical research can be found in section 5.5. The answers to RQ 1 are discussed in section 6.5.1 and the conclusion can be found in section 7.1.

- **RQ2: Which factors related to knowledge affect the implementation of Network Based Defence?**
  Information collection related to RQ2 is mainly based on practical research. The practical research is described in chapter 5, and a summary of the findings can be found in page 101. The results are discussed in section 6.5.2 and the conclusion can be found in section 7.1.
- **RQ3: How are the identified factors related to knowledge and situational awareness affecting the operators' perceived trust level?** Information collection related to RQ3 is based on practical research. RQ3 is also supported by a preliminary NbF SD model explained in section 3.1.7 and studied literature in page 6. The practical research is described in chapter 5, and a summary of the practical research can be found in page 101. All the results are discussed in section 6.5.3 and the conclusion can be found in section 7.1.
- **RQ4: How will the perceived trust level affect the implementation of Network Based Defence?**
  Described preliminary NbF SD models in page 35, together with studied literature in section 1.1.3 and chapter 2 serve as a basis to elaborate RQ4. RQ4 is further discussed in section 6.5.4. The conclusion focusing on RQ4 can be found in section 7.1.
- **RQ5: How will a system dynamic model simplify and reduce risk related to the integration of Network Based Defence?**
  Answers and results obtained when investigating RQ1 to RQ4 will serve as a basis to discuss and analyse RQ5. The discussion related to RQ5 can be found in section 6.5.5 and the conclusion focusing on RQ5 in section 7.1

1.6 Limitations

The main focus in this project is to identify obstacles slowing down and challenging the process of implementing Network Based Defence focusing on the human factor. The implementation process can be viewed as several individual processes. The scope of this work is to look into processes related to technology implementation and knowledge improvement to identify possible unbalances between these two processes. One assumption is that unbalances might introduce vulnerabilities, increasing the probability of incidents. To identify and analyse intentional

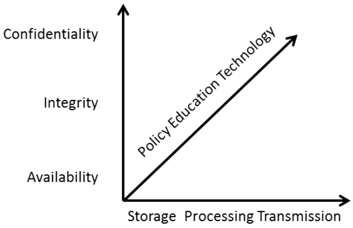


Figure 6: Information security as defined by CNSS [3]

and unintentional effects of the two processes, a system dynamic approach will be employed. Identified unintentional effects will only be analysed in relation to operation transition and knowledge improvement. The implementation of Network Based Defence includes both technology and humans. The technological solutions will not be elaborated and analysed during this project. The purpose is to find out how the human factor is considered in relation to the concept of Network Based Defence.

The implementation of Network Based Defence and technological platforms increases the amount of available information. The information serves as the basis for both tactical and strategical planning in addition to decision-making. Hence, the information must be secured in such a way that it is available, correct and not compromised. This is the traditional way of defining information security; assure the confidentiality, integrity and availability of the information. As vulnerabilities introduced in this project mainly affect the quality and the availability of the information, only integrity and availability will be an issue during this project in an information security perspective.

The practical research will include field research, questionnaires and interviews conducted at The Norwegian Defence University College of Engineering - Telematics and within various army units. The military units are very busy during the winter; the research must therefore be conducted in a limited time frame, between the first of February to the first of April, at times the units are available.

The Master's project is limited in time, from the 1st of January to the 1st of June.

1.7 Definitions

- **Risk** is the probability of an unwanted event occurring, resulting in a potential loss [32].
- **Risk in a military context** can be seen both as a possibility of winning or losing something, and is further explained related to operational risk [33].

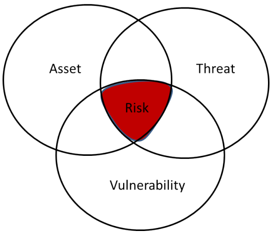


Figure 7: Risk as a combination of threat, vulnerability and asset

- **Operational risk** is associated with the characteristics gearing between strategic objectives and tactical activity [33]. Risk occurring at the tactical level might lead to potential impacts, affecting the force's ability to accomplish their strategic objective. The core of operational risk is the balance between security concerns and operational effectiveness.
- **Information security** is by the Committee on National Security Systems (CNSS) defined as the protection of information and its critical elements including systems and hardware that use, store, and transmit the information [3]. Information security is about keeping the information free from threat in all its locations, during creation, processing, storing and transmition. This is obtained during application of policies, education and training, together with appropriate technology. The CNSS model is illustrated in figure 6.
- **Risk, threat, asset**: Threat together with vulnerability create risks for assets in an information system, as stated by Sengupta et al [34] and illustrated in figure 7.

2 Related work

Both Network Centric Warfare (NCW) and Network Based Defence (NbF in Norwegian) have been described in a variety of documents. The origin of NCW can be found in the paper “System of systems” by Admiral William Owens from 1996 [12]. At the same time, Joint Vision 2010 was released from Joint Chiefs of Staff [35], introducing the military concept of full-spectrum dominance. The first publication of the concept NCW was presented in 1998 by vice admiral Arthur K. Cebrowski and John Garstka, in the proceedings article “Network-Centric Warfare: Its Origin and Future” [11]. NCW implemented in military forces was said to enable development of speed of command, and organizing from bottom-up or self-synchronized forces. The idea of NCW was further elaborated by Alberts, Garstka and Stein [36]. New theory of warfare was based on case studies from commercial business, using information and communication technology to improve their competition advantages.

Network Based Defence has the purpose of increasing the mission effectiveness, enhancing the information sharing and the situational awareness (SA) [11]. The term and approach for Network Based Defence differ slightly from the original NCW, but the main ideas are comparable. Network Based Defence was first referred in Forsvarssjefens Militærfaglige Utredning 2003 [37] and described as a concept for connecting together military capabilities by the use of information technology. The concept of Network Based Defence is further elaborated in a variety of documents ([23], [20] , [8]).

Several studies have been conducted in relation to Network Centric Warfare and Network Based Defence, the majority looking into different technical aspects challenging or enhancing the implementation process ([38], [39], [40], [41]). There are, however, several studies focusing on how the human factor can affect the implementation of Network Centric Warfare (NCW) and Network Based Defence. Bolia et al [16] address several aspects in relation to trust and the lack of attention to human factors in accordance with NCW. Human factors are also addressed in Baker’s study "Human factors in network centric warfare" [18]. Making information available in all levels might result in micro-management and collapsing lines of communication. Baker [18] identified several incompatibilities between humans and the machines of NCW, introducing a gap between human and network capabilities. Baker stated that the military must study the incompatibilities, develop and implement solutions quickly. Cognitive readiness in Network Centric Operations (NCO) is addressed by Wesensten et al [15]. Individuals must be able to integrate information, anticipate what is going to happen and plan the next move. This depends heavily on cognitive ability. Wallace [17] elaborates Network Centric Operations (NCO) and emphasizes that warfare is people centric or not centric at all. Wallace is concerned about the change of focus from person to tool placing the responsibility on the systems instead of the commanders. Control can become more important than command. Wallace emphasizes that the network still is a tool while the art and science of Battle command is the centrepiece.

Hafnor et al [23] conducted an exploratory experiment focusing on how new technology and new ways of collaboration affected situational awareness among decision makers at different levels. Hafnor et al concluded that both human and organizational issues must be part of the transformation into Network Based Defence, and in line with technology, to achieve satisfactory situational awareness. This conclusion is supported by Bjornstad [22], stating that a successful implementation of Network Centric Warfare will rely on a holistic approach also including the human factors.

Obstacles challenging a successful implementation of Network Based Defence are elaborated in a series of research conducted by Forsvarets Forskningsinstitutt (FFI) from 2011 to 2015. In the report "NbF – nå! – hvordan får vi et nettverksbasert forsvar raskere?" [19], the most prevalent reasons for the delayed implementation are discussed. Inconsistent use of terms related to Network Based Defence might lead to more confusion than necessary. Interaction between different levels of the organization is complicated because of the traditional structure of the Norwegian Armed Forces. Another issue is the lack of understanding for the process of Network Based Defence. The third problem is related to a gap between the processes going top-down and bottom-up. In addition, lack of ownership and implementation capacity are emphasized as two transverse problem issues in "Støtte til Forsvarets NbF-utvikling – sluttrapport" [9].

Daltveit et al [21] stated that up to this point, technology has been the main cost driver for the implementation of Network Based Defence . Their work "Trender i militære operasjoner" emphasizes that an introduction of more technological platforms and an increased amount of information, put higher demands on the analytical capacity. This can only be achieved by increasing the number of staff officers, hence reducing the number of soldiers in the other end. To achieve the necessary effect, technology, organization and doctrine must be viewed as a whole, and changed coordinated.

When technology is implemented and viewed in isolation, vulnerabilities will most certainly be introduced [10]. In the paper "Emergent vulnerabilities in integrated operations: a proactive simulation study of economic risk" [10], unadjusted processes related to technology implementation are described. The processes in this context, are related to work processes and processes including development of new knowledge and skills. When the two processes are not aligned to each other, a gap might arise. When the gap increases, the number of vulnerabilities increases with the possibility to introduce more incidents.

Possible vulnerabilities introduced into a human-technical system as a result of lacking knowledge and skills, can be found in a PhD study conducted by Schaefer [25]. Trust between humans and robots are thoroughly described, and a trust scale is developed to measure an individual's trust to a robot, and also what inflicts the individual's change in trust. Competency, training and situation awareness (SA) are described as important human related antecedents of trust. Lee [29] stated that appropriate trust is necessary to achieve superior performance in a human–automation system. Lee also emphasized the importance of giving the operators proper training in order to understand the intended use of the system, and expected reliability. Inadequate trust can therefore be assumed to be a possible vulnerability in a human-technical system.

Different studies related to human trust have been conducted throughout the years, focusing on interpersonal relationships, organizational aspects and through the last three decades also trust in automation. Jian et al [28] found that people do not perceive trust differently, whether the relationship is general trust, human-human trust or human-machine trust. This indicates that results from studies related to human-human relations also can be employed to understand the trust between humans and networked systems.

Situational awareness (SA) is said to be an antecedent of trust, but as described by O'Brien [30], SA is also about predicting and planning future actions based on present information. If the operators are not able to collect the correct data, and if the data is analyzed based on wrong assumptions, the result will be faulty plans and increased number of incidents. Inadequate SA will therefore represent vulnerability in military operations in addition to be an antecedent of trust. The same is supported by Bolia et al [16], arguing that a higher quantity of information can lead to the cost of quality within the information, resulting in wrong information. Wrong interpretation of the situation, together with varying quality of the information, will affect the situational awareness.

Incomplete, wrong, compromised and unavailable data or information are described throughout numerous of books and papers as part of the CIA triad [42], [43], [31]. CIA is an abbreviation for Confidentiality, Integrity and Availability. The three factors have for several decades been the main components of information security. Information security is about keeping the information in all its locations, during creation, processing, storing and transmition, free from threats, see figure 6. Threat together with vulnerability creates risks for assets in an information system, as stated by Sengupta et al [34]. Risk is illustrated in figure 7. The focus of this project is to look into Network Based Defence, and why the concept is not up to speed. In order to find necessary information, tools as questionnaires and interviews will be employed. A questionnaire developed by Bjornstad et al [44], "Utvikling og evaluering av spørreskjema med fokus på organisasjon og bruk av samhandlingsteknologi", includes factors relevant to this project. Even if the questionnaire can be used for different purposes, the main objective of the questionnaire still is to evaluate the organization in relation to Network Based Defence. The areas trust, information sharing, situational awareness and the use of collaboration technologies focusing on perceived usefulness and user satisfaction from the questionnaire, are in line with this project. These areas include most of the factors already pointed out in relation to trust. The questionnaire is therefore highly relevant.

Other related work will be directly cited when used during the project.

3 Methodology

Methodologies employed in the research are elaborated in this chapter. Studied literature indicates that technology often is implemented much faster than knowledge, organization and doctrines are developed. It can therefore be assumed that technology, procedures and intellectual capital are not aligned to each other, complicating and challenging the implementation of Network Based Defence. Comparable processes can be found in Integrated Operations for the oil sector. This is in line with the first research question: How are the two processes of operation transition and knowledge development in Network Based Defence adjusted to each other? In order to investigate the first research question and hence also find indications to answer the remaining research questions, System Dynamic (SD) models developed for Integrated Operations, will be employed as analytic methodology. First in this chapter, system dynamics are explained in general, before preliminary NbF SD models are employed as preliminary hypothesis for the research questions. Living SD models of NbF will be suggested as a tool to simulate possible technical solutions in advance of the practical implementation of Network Based Defence. The system dynamic models will support findings obtained during practical research. The basis of the practical research is explained in the last part of this chapter. In addition, tools for information collection and discussion are elaborated. More specifically, interviews, questionnaires and field research will be employed for information collection. The development of these tools is therefore included in this chapter.

3.1 Analytical methodology

As already described during chapter 1 and 2, the process of implementing Network Based Defence is delayed, and suffers from different obstacles slowing down the process. In this project, it is assumed that the implementation of Network Based Defence can be compared to the process of implementing Integrated Operations in the oil industry. Unadjusted processes related to the implementation of Integrated Operations were identified by Rich et al [10] and further developed by Qian in her PhD work "Mitigating Information security risks during the Transition to Integrated Operations" [6]. Similar to Integrated Operations, the transformation to Network Based Defence introduces new vulnerabilities as new processes are introduced simultaneously as old ones are phased out. New processes will require new knowledge. The implementation is endeavoring, lasting for several decades, making the processes and knowledge related to Network Based Defence interact in unexpected ways. The traditional way of doing risk and security analysis is based on analysis of previous events and historical data, in addition to vulnerability identification [45]. The transformation to Network Based Defence will include implementation of new technological equipment and information technology. Because the equipment and technology are new, there are no existing records of previous events [10]. System dynamics will therefore be a helpful tool to simulate possible pitfalls and drawbacks before implementation. Another consideration is that possible events related to military operations might have low probability, but high impact, making an ordinary risk analysis inadequate. In addition, the project of implementing Network Based Defence into the Norwegian Armed Forces is rather complex. Using a system dynamic model to understand how the transition speed, process change, knowledge and vulnerability are connected, might therefore be a viable option. In addition, empirical studies related to system dynamic models employed in parallel with project management, have shown significant utilization related to cost benefit (Source: Josè Gonzalez, expert in System Dynamics, 4th of May 2017). To reduce giant overruns and avoid delays in the implementation process, using system dynamic models seems relevant. By connecting cause and effect, it is possible to estimate risk related to the operation transition.

There are two possible approaches for building a system dynamic model.

1. One way is to identify and analyse all factors included in the process, and use these factors to model a causal loop diagram (CLD). Interviews have to be done iterative in order to build the model gradually. This approach gives a higher level of freedom in the process, and a higher probability of detecting different challenges. But there is also a higher risk associated with this approach. The method is more demanding, and it increases the probability of not succeeding with the model within the time frame.
2. The other approach is to build a model based on assumptions, and use this model as a hypothesis. Feedback and limitations related to the base model, serve as corrections to the model accordingly. The models developed for Integrated Operations can be employed for this purpose, acting as preliminary hypothesis to check if the assumptions are true or not. The models have the ability to enlighten certain problem issues. The chosen models can then be employed to conduct simulations and help identifying possible outcomes.

The implementation of Network Based Defence shares several similarities with the Integrated Operation transition in the oil industry. Due to time limitations, it will only be possible to conduct one interview per participants. The increased risk related to approach number one must also be considered. Even if the first approach allows a higher degree of freedom during the process, the advantages related to the second approach is superior to the first approach in this context. The models from Integrated Operations will with permission from Ying Qian, therefore be used as a basis to model the implementation process of Network Based Defence. The system dynamic models will be adapted in such a manner, that they fit to the transformation process related to Network Based Defence. The simplicity of the adapted models support understanding of cause and effect relationships in the transformation process. The purpose of the models is to raise awareness around central aspects significant to Network Based Defence. In addition, their simplicity and scope are well adjusted to the the ambition and limitations related to a Master's project. The adapted models serving as hypothesis in this project will be referred as "preliminary NbF SD models".

One parent model with few feedback loops will be employed to describe the core problem issues. More detailed models will be used to identify and illustrate additional factors. The models will then be further developed based on feedback and limitations from colleagues and co-workers, acting as experts in their respective domains. The proposed models will support results found during the practical research presented in chapter 5. Development of system dynamic models is described in general terms during the next section, while the specific models for this project will be elaborated during consecutive sections.

3.1.1 Causal loop diagrams

As a system dynamic model is a representation of the reality, it is less complex and easier for humans to understand than the real world [4]. Simplicity assists thinking and decision making. System dynamic models also help improving already existing mental models, which is important to improve organizational security and development. Archetypes are short-hand versions of system dynamic models and are usually drawn as causal feedback loops, modelling a problem over time and conceptualizing real world systems. A causal feedback loop consists of arrows connecting cause and effect. When cause and effect change in the same direction, the arrow is marked with a plus sign. If the cause and effect change in opposite directions, the arrow is marked with a minus sign. Cause and effect relationships are illustrated in figure 8 and explained as follows. When the number of customers increases, a company's profit will also increase. This relationship is illustrated with a positive marked arrow. The right hand side of the figure illustrates a negative cause and effect relationship. By increasing the physical security in a building, it can be assumed that the number of burglaries will decrease.

System dynamic models can include both quantitative and qualitative models [4]. System archetypes are mostly qualitative and very effective to communicate

customers
profit
+
physical security
burglary
-

Cause and effect change in same direction

Cause and effect change in opposite direction

Figure 8: Cause and affect relationships

problems in an organization. System archetypes cannot be simulated, but represent intended and unintended actions or behavior in different settings. A lot of system archetypes were proposed by Senge in his book, “The fifth discipline” [46], looking into system thinking in organizational development. The archetypes suggested by Senge are reduced to four generic archetypes by Wolstenholm [4] in his article "Towards the definition and use of a core set of archetypal structures in system dynamics". The generic archetypes consist of reinforcing (R) and balancing (B) feedback loops, resulting in intended and unintended results and outcomes. The four archetypes suggested by Wolstenholme, illustrated in figure 9, are:

- *Underachievement*, including a reinforcing feedback loop for the intended outcome, and a balancing feedback loop resulting in an unintended outcome.
- *Out of control* including a balancing feedback loop for the intended outcome, and a reinforcing feedback loop for the unintended result.
- *Relative achievement* including reinforcing feedback loops both for the intended and unintended outcome.
- *Relative control* including balancing feedback loops both for intended and unintended outcome or results.

The four generic problem archetypes also include a solution feedback loop. The intention of the solution feedback loop, is to reduce the unintended consequences. Unintended consequences are often and wrongly ignored, because they tend to happen delayed in time, and possibly also in other places compared to the intended outcome. This is illustrated by the line labelled "system boundary". The system boundary can be the boundary for the actual organization, but also the boundary between different departments in an organization. In order to employ system dynamics in a proper manner, it is important to acknowledge that the system boundaries exist, and take them into account.

The archetypes need some further explanation. For the *underachievement archetype*, investments are spent to increase the intended outcome. The intended outcome might for instance be to increase the number of sold tickets or items. The more

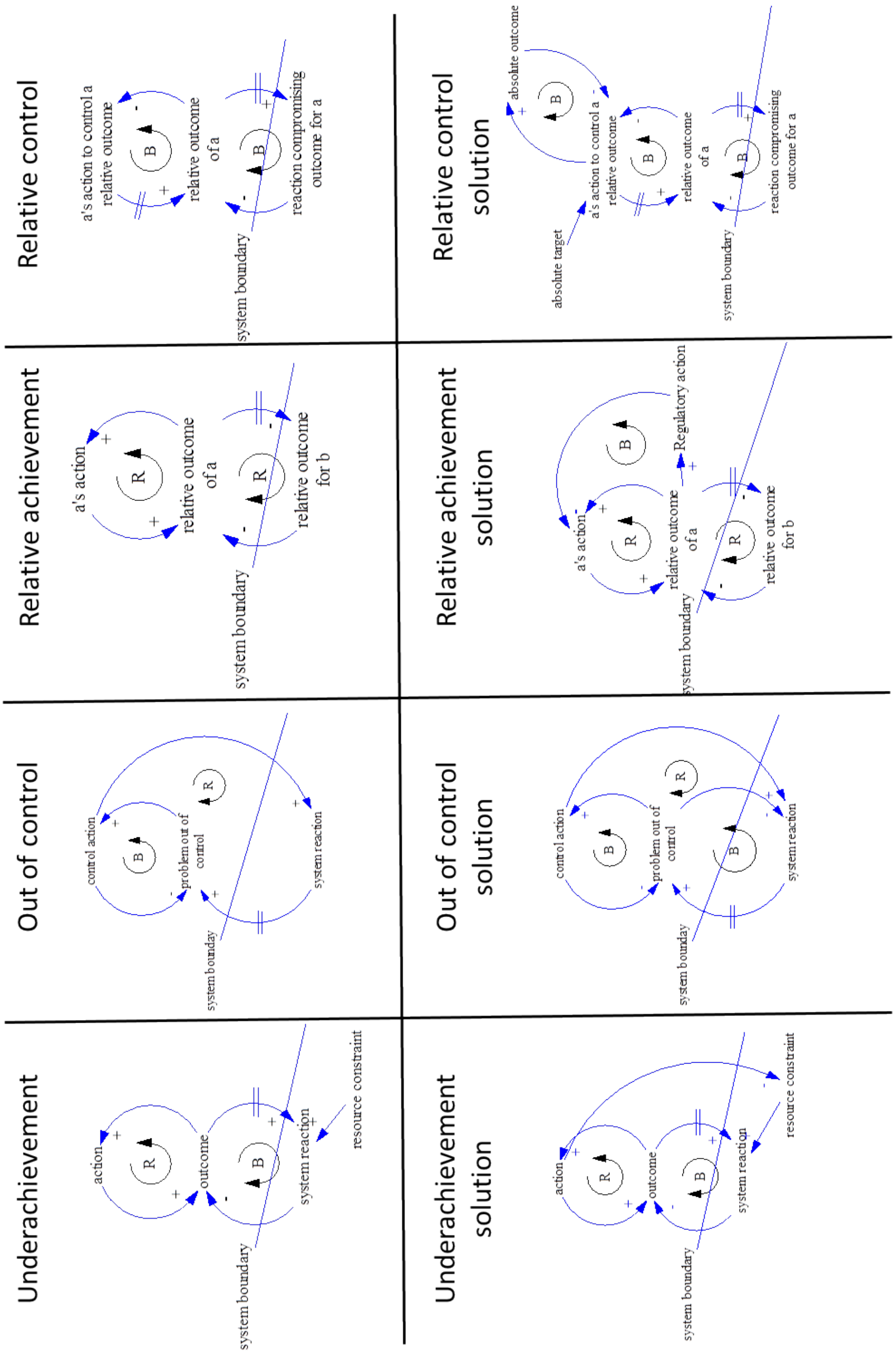


Figure 9: Generic system archetypes. Adapted from Eric Wolstenholme [4]

items sold, the higher profit, and the feedback loop is reinforcing itself. After a while (delayed), the production line is not able to deliver the demanded number of items within the requested time frame. The intended achievement fails to be realized. A new feedback loop will appear, giving unintended consequences and opposing the intended outcome. The unintended consequence loop is balancing, acting against the intended outcome. The balancing loop is a result of resource constraints, for instance limited number of employees and equipment. The solution is to use some of the resources obtained in the reinforcing loop, to minimize the resource constraints creating the balancing loop. For this example, hiring new employees and improving the equipment, could be a possible solution.

The intended purpose of an *out of control* archetype is to introduce a control action in order to control or reduce a problem. One example related to information security, might be the introduction of new and more detailed laws for security the organization has to adhere to. The intention of the new laws might for instance be to reduce the number of vulnerabilities in the information system, improving the security. In the beginning, the employees are following the new laws, and the number of vulnerabilities is reduced. As long as the control action is reducing the number of vulnerabilities, the feedback loop is balancing. But often the control action introduces a system reaction, giving unintentional consequences acting against the intended outcome. For this example, following the new laws require more effort by each employee, exhausting the workers over time, introducing a reinforcing loop acting against the intended outcome. The unintended outcome is often much delayed in time, making the problem even worse. When the workload increases, the implementation becomes less effective, introducing more vulnerability. The solution is to introduce a direct link between the problem that needs to be controlled and the system reaction. In order to comply with the new laws, the organization has to invest in higher capacity. The solution archetype acts as a balancing loop reducing the unintended consequences.

The reinforcing, intended loop in the *relative achievement* archetype increases one organization's success on the expense of another organization. In order to reduce the unintended consequences, regulatory actions are necessary. In the *relative control* archetype, the intended consequence feedback loop results in a relative outcome for one department in an organization. But this relative outcome induces a reaction in another department of the same organization, acting against the intended outcome. An absolute target therefore has to be defined in a solution feedback loop in order to stabilize the outcome.

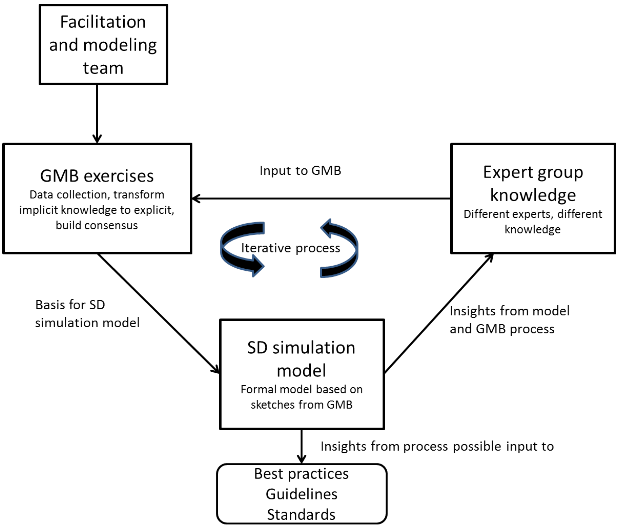

Facilitation and modeling team
GMB exercises
Data collection, transform implicit knowledge to explicit, build consensus
Input to GMB
Expert group knowledge
Different experts, different knowledge
Iterative process
Basis for SD simulation model
Insights from model and GMB process
SD simulation model
Formal model based on sketches from GMB
Insights from process possible input to
Best practices
Guidelines
Standards

Figure 10: Group Model Building. Adapted from Gonzalez [5]

3.1.2 The system dynamic process

A system dynamic process often includes developing models in several levels. The first step is to comprehend the client's understanding and mental model of the system. The information collected and analysed during this phase serve as a basis for a qualitative model, referred to as a Causal Loop Diagram model (CLD) in system dynamics. The CLD model serves as a basis for a quantitative model, if this is required. Often Group Model Building (GMB) is employed in order to transform a real life problem into a model of the problem. Knowledge and lacking information must be identified in order to make the model as complete as possible, to support deeper understanding. In order to increase the relevance and importance of the model, many participants must be involved in the modelling process, and the problem owners must play an active role. A complete Group Model Building process is illustrated in figure 10.

Group Model Building is an interaction between the modelling team and domain experts. Participants from the client or problem owner contribute with expert knowledge in their respective domains. In addition to be sources of information, they also support the model development. By contributing in the process, the mental models of the participants are improved, and their active role facilitates ownership into company processes. The modelling team develops the model based on the problem owner's descriptions, and improves the model along the process. The process is iterative and normally consists of 5 different roles [5]. A *facilitator* ensures a good group process, a *recorder* documents the process, a *modeller* develops the actual model of the problem, a *process coach* ensures process progress and a *gatekeeper* makes sure that the output actually deals with the problem in question. Information is collected from different sources; written documents, numerical and historical data and tacit knowledge, with the latter probably as the most important.

> "Tacit knowledge: Unwritten, unspoken, and hidden vast storehouse of knowledge held by practically every normal human being, based on his or her emotions, experiences, insights, intuition, observations and internalized information [47]".

For this project, only domain experts, the researcher and the supervisors will contribute to the model development. Colleagues and co-workers act as domain experts, contributing during field research, questionnaires and interviews, ensuring that different knowledge is brought to the table. All gathered knowledge is input to the Group Model Building process. Gathered knowledge together with knowledge from the military supervisors, will be gathered through the practical research and dialogue, to make the knowledge explicit and build consensus. The process will be facilitated and modelled by the researcher, with supervision from the academic supervisor. The process will start out with system dynamic models based on preliminary research. Gathered data will be employed in order to verify or falsify the modelled hypothesis and to possibly correct the preliminary NbF SD model. This will serve as a basis to develop guidelines for the Network Based Defence implementation process. The researcher also needs to document the process and ensure progress. Due to time limitations, iterative interviews are not a viable option. Interviews in several units will still make the process somewhat iterative.

With permission from Ying Qian, models from her PhD study "Mitigating Information security risks during the Transition to Integrated Operations" are adapted and will serve as hypothesis to check if the assumptions are true or not. The models are based on reviewed literature and previous related work. Feedback and limitations related to the base model will serve as corrections to the model accordingly. The model has the ability to enlighten certain problem issues, and can be employed to conduct simulations and help identifying possible outcomes in advance of implementation.

3.1.3 System dynamic models related to Network Based Defence

The causal loop diagram illustrated in figure 11 is used as a parent model, and as a basis to model the implementation of Network Based Defence. NbF is used as an abbreviation for Network Based Defence (Nettverksbasert Forsvar in Norwegian spelling). R1 acts as a reinforcing feedback loop with the objective to transform more and more of the traditional operations to Network Based Defence. When more technology is implemented and connected together in network, the knowl-

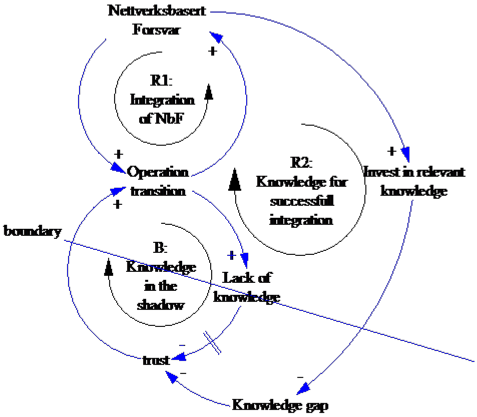


Figure 11: Parent model Network Based Defence implementation

edge related to current operations decreases, and results in a knowledge gap. One assumption is that the trust related to Network Based Defence decreases when the knowledge gap increases. The decrease of trust acts as a balancing feedback loop counteracting the effect of R1, introducing obstacles for the implementation of Network Based Defence. This counteracting effect is most likely delayed in time, making it difficult to understand why the Network Based Defence process is not proceeding as expected. To reduce the effect of the balancing loop, investments in relevant knowledge must be done simultaneously as Network Based Defence is implemented. By investing in relevant knowledge, it can be assumed that the Network Based Defence process is advancing in an appropriate manner.

> "Knowledge: Facts, information, and skills acquired through experience or education; the theoretical or practical understanding of a subject [48]".

Similarities can be found in the PhD work "Mitigating Information security risks during the Transition to Integrated Operations" by Qian [6]. With permission from Ying Qian, models from her PhD will be employed and adapted. The models will be employed to analyse and explain possible vulnerabilities introduced, as a result of unadjusted processes related to operation transition and knowledge improvement, in the Network Based Defence process.

3.1.4 General preliminary NbF SD model

The model employed in this section, is based on a general model structure derived during the PhD work "Mitigating Information security risks during the Transition to Integrated Operations" by Qian [6]. The model is showed in figure 12. The general model simplifies the relationships and dependencies between various variables and parameters. It is therefore easier to understand the complete picture of feedback processes affecting the transition from traditional operations to mature NbF (Network Based Defence). Key issues in the transition are organizational change, incidents, and learning from incidents, all marked with circles. The main idea behind the model is that new type of operations require new knowledge. As the implementation of NbF is a prerequisite to use new technology, new technology is assumed to be a part of the NbF and knowledge transition. A knowledge gap will be introduced, because knowledge is matured later than the actual NbF operations, resulting in a higher vulnerability and increased number of incidents. In addition, immature NbF and immature new knowledge will also increase the vulnerability level. When the NbF and knowledge grow mature, the vulnerability level will decrease accordingly. The severity of the incidents is reduced when the organization is able to learn from incidents.

Organizational change can be compared to burden of new initiatives. Implementing NbF (Network Based Defence) will affect the organizational structure and change the social structure. Other communication patterns will appear, challenging the communication, and increase the workload for the operators. Challenges related to communication will reduce productivity of learning NbF and acquiring of new knowledge. In addition, organizational change will in most cases meet some resistance. For the NbF transformation, some issues have been identified. The hierarchical structure of the military seems to introduce some obstacles. Lack of ownership and responsibility is a huge challenge. In addition, there is no common understanding for the NbF process. For simplicity, all the factors addressed in this paragraph are gathered in the variable "new initiatives burden" in the further models.

The circle "incidents" includes the frequency and severity of incidents, affected by threats and vulnerabilities introduced as a result of the operation transition. For this project, threats are mainly related to users not employing or comprehending the technical platform correctly, resulting in increased vulnerability. The severity of incidents is mostly influenced by the users not detecting the presence of possible threats, and also by the operation transition. Assuming that the incidents are detected, it is possible to learn from incidents, and hence reduce the vulnerability. This is captured by the circle "Learning from incidents" which affects the maturation of NbF and knowledge. Learning from incidents might be minimal if the organization does not have proper routines for detection and registration of incidents. If there are few severe incidents, this might be the case. Information about incidents must also be shared among the operators to have any importance.

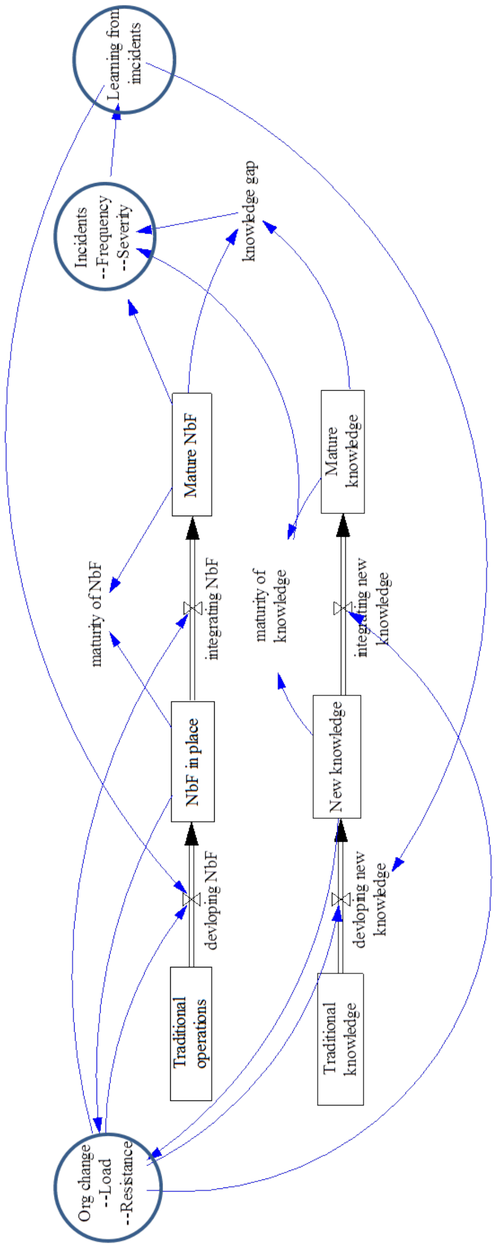


Figure 12: General model structure adapted from Qian [6]

3.1.5 The concept of Network Based Defence and knowledge development

The conceptual model of the transition from traditional operations to Network Based Defence is adapted from the article "Managing information security risks during new technology adoption" by Qian [7] and presented in figure 13.

The transition to Network Based Defence is illustrated by two chains. One chain includes the transformation of "traditional operations" via "NbF in place" to "mature NbF". The other chain includes development of "traditional knowledge" into "new knowledge" and "mature knowledge". The two chains must follow each other to achieve the desired improvements. The operators therefore have to learn what to do (the new type of operations) and how to do it (new knowledge) in order to adopt new technology. Then they can use the new technology effectively and achieve the desired improvements.

To understand how the model translates to reality, the various variables and parameters can be described as follows:

- *Developing NbF* is a rate describing how fast Network Based Defence is developed. To start the development, traditional operations must first be reviewed. Desired changes must be identified and new type of operations must be documented and transformed into user's guides. Developing NbF is the process owner's responsibility.
- *Integrating NbF*. In order to integrate NbF, the operators need to be familiar with what to do and remember the tasks. The operators are relying on the user's guide developed previously. The actual rate describes how fast the operators are able to familiarize with the new type of operations.
- *NbF in place*. Even if NbF is in place, the operators are not familiar with the new type of operations, and old routines might appear unintentionally. Continuous follow ups are therefore necessary, typically by colleagues or user manuals. "NbF in place" is a stock accumulating as more and more NbF is implemented. The stock is decreased when "NbF in place" matures.
  NbF in place=(developing NbF - integrating NbF)
- *Mature NbF*. The NbF process is mature when the operators are familiar with new type of operations and can work independently. "Mature NbF" is a stock increasing when more NbF is integrated. The productivity is higher with mature NbF than with NbF in place.
- *Developing new knowledge* is a rate describing how fast new knowledge is developed. The rate includes development of information material and education related to Network Based Defence (NbF). This process is a typical management responsibility.
- *Integrating new knowledge* is a rate describing how fast the operators learn

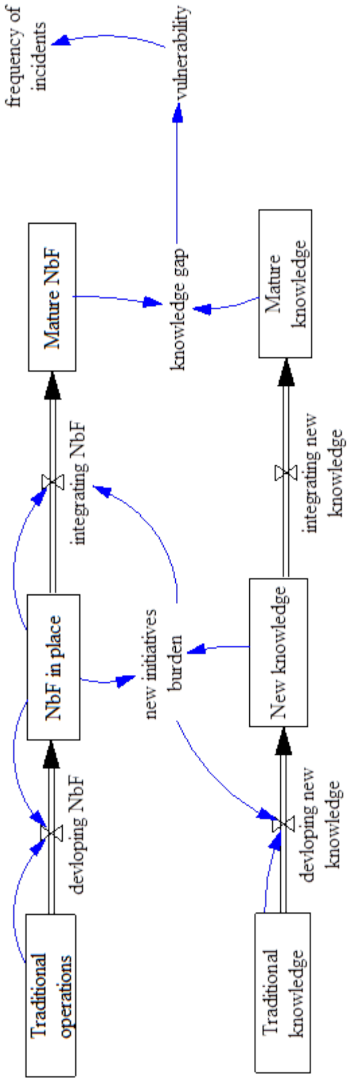


Figure 13: Conceptual model for the transition of Network Based Defence. Adapted from Qian [7]

how to use Network Based Defence. The rate includes how and why they should use the new type of operations. The operators are responsible for this rate.

- *New knowledge* is a stock representing new knowledge when it is introduced together with Network Based Defence processes and technology. The operators' knowledge is not quit up to speed yet, and they are not able to utilize the new type of operations optimal due to misinterpreting or misunderstanding of information. Their productivity is therefore lower than wanted. The stock "New knowledge" increases when new knowledge is developed and decreases when knowledge matures.
  New knowledge = (developing new knowledge - integrating new knowledge)
- *Mature knowledge* is a stock describing knowledge when details related to NbF operations have become routine, and the desired productivity is achieved. Mature knowledge increases when new knowledge is integrated.
- *New initiatives burden* traps transition to NbF. Because change is difficult, NbF in place and new knowledge are burden to people, slowing down the integration of NbF and development of new knowledge.
- *A knowledge gap* is generated, because knowledge maturation takes time. It is easier to understand what to do than how to do it. Acquiring new knowledge is necessary to understand how to accomplish a task effectively in accordance with Network Based Defence. When new type of operations is introduced, corresponding knowledge is desired, but the knowledge maturation takes time. A knowledge gap is introduced between desired mature knowledge and the actual mature knowledge. The knowledge gap drives vulnerability, and hence also frequency of incidents.
- *Time to mature new type of operations*. In ordinary workplaces, where the platform is continuously in use, several weeks are necessary to memorize what to do if new type of operations are in place. Operative military units work in a different manner, and employ the technical tactical platform only some weeks during a year, when the units are doing operative exercises. Without proper routines for repetition, the operators might need heavy guidance and follow ups to employ the platform properly next time. Time to mature might therefore take several months if not followed up properly. For simplicity, an estimate equal to 3 months is used, suggesting that exercises conducted during three months are sufficient.
- *Time to mature new knowledge* is more time demanding than implementing new technology, and productivity improvements can be measured for several years as the operators continuously are "learning by doing". In this project, practice through the exercises during three months are estimated to

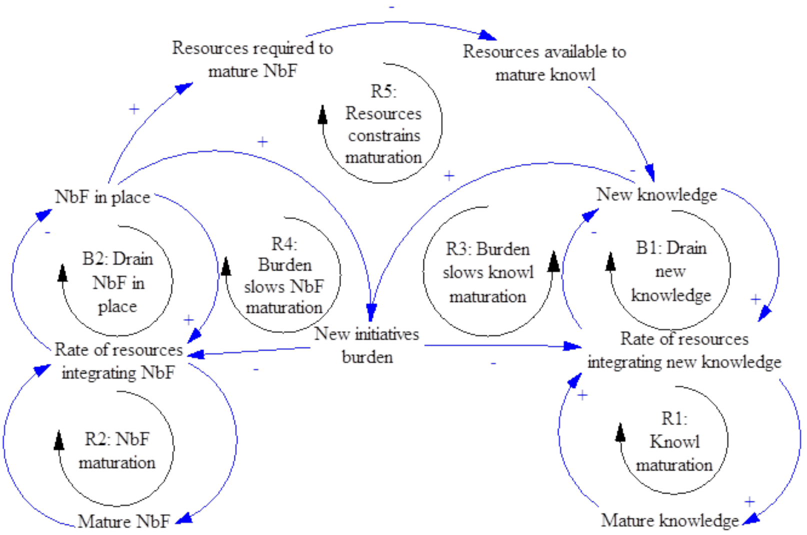

Resources required to mature NbF
Resources available to mature knowl
R5: Resources constrains maturation
NbF in place
New knowledge
B2: Drain NbF in place
R4: Burden slows NbF maturation
R3: Burden slows knowl maturation
B1: Drain new knowledge
New initiatives burden
Rate of resources integrating NbF
Rate of resources integrating new knowledge
R2: NbF maturation
R1: Knowl maturation
Mature NbF
Mature knowledge
+
-

Figure 14: Major causal loop diagram for transition of Network Based Defence adapted from Qian [6]

be enough time, to employ the platform sufficiently.

3.1.6 Preliminary NbF SD models serving as hypothesis

The conceptual model is further developed, and first illustrated by causal loop diagrams to visualize the major feedbacks in the system. The causal loop diagrams and system dynamic models from Qian's PhD work [6] are adapted with some adjustments, and will serve as hypothesis in this project. The models are denoted preliminary NbF SD models. The causal loop diagram for the transition of Network Based Defence (NbF) is shown in figure 14 and described as follows.

The introduction of Network Based Defence results in new processes related to operation- and knowledge-integration. The causal loop diagram comprises 7 feedback loops:

- *B1 and B2, drain NbF in place and new knowledge.*
  The balancing loops, B1 and B2, drain new knowledge and NbF in place. B1 and B2 are also the starting points for integration and maturation of NbF and new knowledge. New knowledge and NbF are assumed to be in place, but still not integrated. Resources must be added to the processes to ensure

integration and maturation. The balancing loops, B1 and B2, contain the integration processes that drain NbF in place and new knowledge, and make the processes mature. When more NbF in place is introduced together with appropriate new knowledge, there is a higher potential to incorporate NbF and learn about NbF processes. When more NbF is incorporated and learned, the processes grow mature and drain the potential of NbF in place and new knowledge. As the potential of NbF in place and new knowledge decreases, more mature NbF and knowledge are produced. Less immature NbF and immature new knowledge will then be left to be integrated and matured in the next iteration, resulting in a lower rate of integration. Hence, the balancing loops, B1 and B2, try to match the need for integration. The processes will slow down as the demands decrease and erode.

- *R1 and R2, NbF and knowledge maturation*.
  The reinforcing loops, R1 and R2, visualize that experience assists the integration and maturation processes of producing mature NbF and mature knowledge. The maturation process is based on experience, where NbF becomes incorporated and the knowledge matures. When more NbF and knowledge become mature, the operators are experienced in working with NbF and the technology embedded in it. More experience results in the process of integrating additional NbF and knowledge, accumulating additional experience. The reinforcing loops are hence speeding up the process of integration in accordance with experience.
- *R3 and R4, burden slows NbF and knowledge maturation*.
  The reinforcing loops, R3 and R4, illustrate that the burden of new initiatives slows down the integration and maturation of NbF in place and new knowledge. The maturation process is highly affected by organizational change. New type of operations require a new organizational structure, which tends to be difficult to accomplish. People like to interact with persons they know well. Unfamiliarity might lead to communication difficulties, resulting in extra work. In addition, some transformation issues have been identified for the process of implementing Network Based Defence. The hierarchical structure of the military seems to introduce some obstacles. Lack of ownership and responsibility is a huge challenge. In addition, there is no common understanding for the Network Based Defence process. All the mentioned factors in this paragraph are represented by the variable "new initiatives burden". As a result, the speed of learning new type of operations is reduced, and new knowledge must be obtained. When the operators learn to conduct the operations in a new manner, NbF and knowledge are matured gradually, reducing the new initiatives burden. When the new initiatives burden is decreased,

maturation of NbF and knowledge can be accomplished even faster.

- *R5, resources constrain maturation*.
  R5 contains the resource allocation that constrains the maturation of NbF and new knowledge. When more NbF is implemented, more resources are required to mature the new type of operations. Spending more resources on maturing new type of operations, reduce available resources to mature new knowledge. The result is slower maturation of new knowledge, and an increase in new knowledge, which in turn will increase the new initiatives burden. The rate of maturing NbF will be reduced, and more of the NbF will be immature. This visualizes what will happen if Network Based Defence is introduced too fast. Too fast implementation causes slow maturation both due to new initiatives burden and the resource constraints.

The knowledge gap introduced as a result of unadjusted processes related to development of Network Based Defence (NbF) and development of new knowledge, will most likely increase the frequency of incidents. The frequency of incidents will affect the transition speed of Network Based Defence as illustrated in figure 15. The balancing loops B3 and B4 both affect the transformation speed from traditional operations to Network Based Defence. The change of speed is directly affected by the incident cost. Cost might be related to damage happening during military operations, but also cost related to delayed implementation and increased cost during the implementation.

If the transformation speed is increased, the vulnerability also will increase. A higher vulnerability will result in an increased frequency of incidents and a higher incident cost. With a high incident cost, the management will probably reduce the transformation speed, resulting in slower introduction of Network Based Defence and new knowledge. With a reduced transformation speed, the operations and knowledge will grow mature over time, the vulnerability will be reduced and the frequency of incidents will decrease. With fewer incidents, each incident can be detected and handled in a more appropriate way, reducing the severity of the incidents. Vulnerability, frequency of incidents, cost of incidents and severity of incidents are all factors affecting and adjusting the operator's perceived trust level. The mentioned factors are driven by the knowledge gap resulting from unadjusted processes and partly explain research question 4. How will the perceived trust level affect the implementation of Network Based Defence? Inadequate level of trust might result in the operators employing the platform in an inappropriate manner or analysing information based on wrong assumptions. In addition, inadequate trust levels can affect the operator's willingness to employ the system, and too high reliance on the system can result in the operators not noticing system fails [16]. The frequency and severity of incidents might help adjusting the perceived trust to

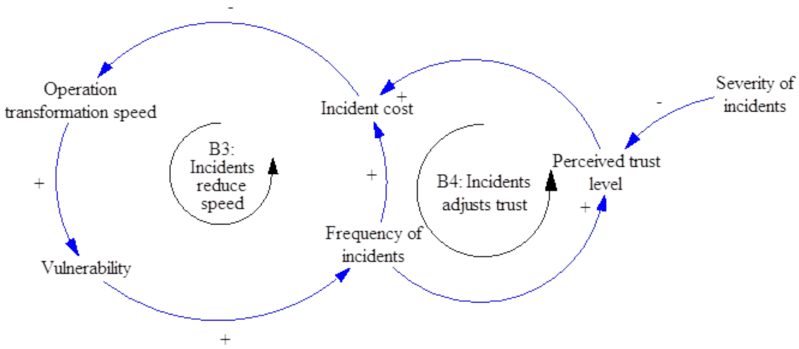


Figure 15: Causal loop diagram for incidents, affecting transition speed. Adapted from Qian [6]

correct level, if appropriate routines for registering incidents are in place. Adequate level of perceived trust will most likely help reducing the incident cost.

3.1.7 Comprehensive description of preliminary NbF SD model

Military operations can be divided into multiple smaller processes, consisting of analysis, planning, orders and actions, denoted traditional operations. One assumption is that the majority of these processes require modification, in order to enable Network Based Defence. Knowledge development must follow the process in parallel. To ensure proper security and safety for the personnel, the transition from traditional operations to Network Based Defence must be conducted in a proper manner. To describe the process further, this section includes three system dynamic models adapted from "Mitigating Information security risks during the Transition to Integrated Operations" by Qian [6]. Only models and variables relevant to this project will be elaborated in this section, included processes related to operation transition, knowledge development and adjustment of perceived trust level.

Development of new type of operations

In figure 16, the operation transition is considered in three stages.

Traditional operations are the way operations have been conducted before Network Based Defence is considered. The stock *NbF in place* illustrates that Network Based Defence is implemented, but not tested and adjusted in accordance with field demands. *Mature NbF* is considered to be stable Network Based Defence processes, working and supporting the desired level of operations. The transition depends on several parameters and variables affecting the rates *developing and integrating*

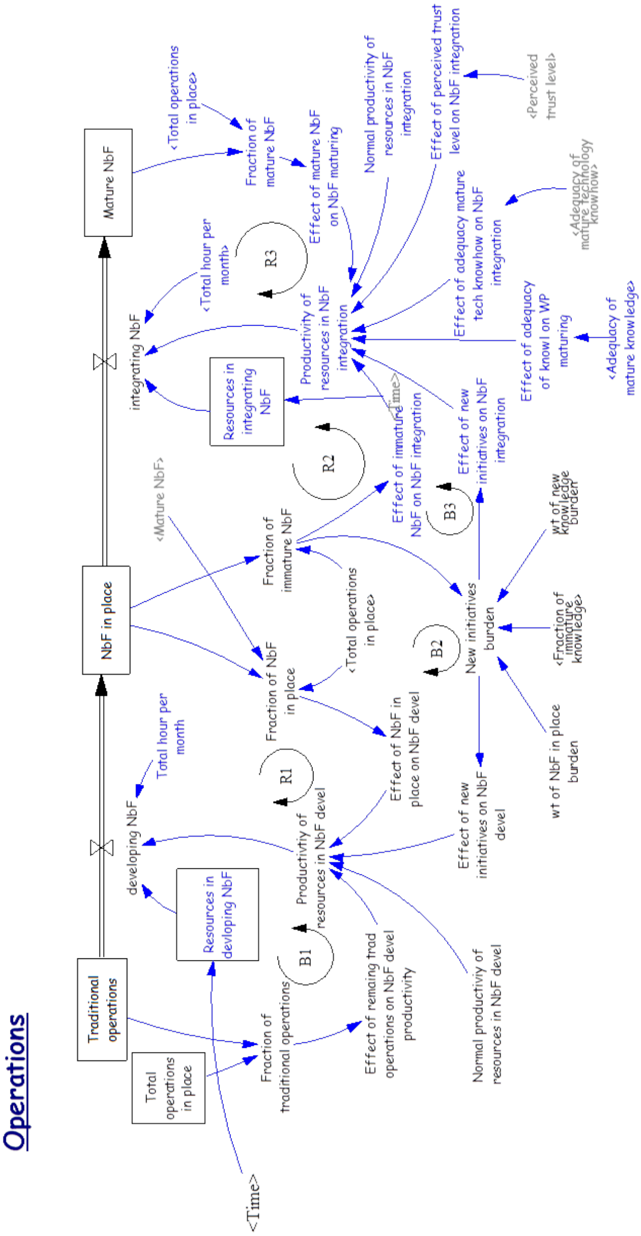

Operations
Traditional operations
Total operations in place
NbF in place
Mature NbF
developing NbF
integrating NbF
Resources in devloping NbF
Resources in integrating NbF
<Time>
Fraction of traditional operations
Total hour per month
<Total hour per month>
Productivtiy of resources in NbF devel
Productivity of resources in NbF integration
Effect of remaing trad operations on NbF devel productivity
Normal productiviy of resources in NbF devel
Fraction of NbF in place
Fraction of immature NbF
Fraction of mature NbF
<Mature NbF>
<Total operations in place>
Effect of NbF in place on NbF devel
Effect of new initiatives on NbF devel
New initiatives burden
wt of NbF in place burden
<Fraction of immature knowledge>
wt of new knowledge burden
Effect of immature NbF on NbF integration
Effect of new initiatives on NbF integration
<Time>
Effect of adequacy of knowl on WP maturing
<Adequacy of mature knowledge>
Effect of adequacy mature tech knowhow on NbF integration
<Adequacy of mature technology knowhow>
Effect of mature NbF on NbF maturing
Normal productivity of resources in NbF integration
Effect of perceived trust level on NbF integration
<Perceived trust level>
B1
R1
B2
R2
B3
R3

Figure 16: Development of new type of operations. Adapted from "Mitigating Information security risks during the Transition to Integrated Operations" by Qian [6]

NbF. First of all, available resources will affect how fast the development and integration of NbF happen. The resources in this case are working hours, and are implemented as stocks denoted *resources in developing NbF* and *resources in integrating NbF*. They affect the rates *developing NbF* and *integrating NbF* accordingly, which in turn decide how fast the stocks *NbF in place* and *mature NbF* change over time. It is assumed that more resources will increase the development and integration rate of NbF (+). In addition, feedback loops will affect the development and integration of Network Based Defence. Feedback loops are either Balancing (B) or Reinforcing (R). The figure includes 3 balancing and 3 reinforcing loops. The loops are not named in the figure to save space and reduce the complexity of the figure. The names are, however, included in the further explanation:

- *R1 - NbF development learning curve*.
  A reinforcing loop captures how effective the transition to Network Based Defence is related to fractional NbF in place. One assumption is that the personnel is least effective when the transition starts, meaning when all operations still are traditional. The efficiency increases when the number of traditional operations decreases, and NbF in place increases due to an increasing learning curve. The development experience increases in accordance with the learning curve, which again is assumed to improve the development productivity.
- *R2 and R3 – NbF integration learning curve from immature and mature NbF*.
  The loops illustrate the integration productivity of NbF, based on immature and mature NbF. The loops act in a similar manner as the reinforcing loop R1, and the productivity increases according to fractional immature and mature NbF.
- *B1 - Later NbF changes harder*.
  B1 illustrates that the development of Network Based Defence will be more difficult as the process moves along. This is based on the assumption that the easiest changes will be developed first, and the most difficult will remain to the end of the development process. Hence, the process will slow down gradually due to reduced productivity.
- *B2 – Transition slows NbF implementation*.
  B2 will in addition increase the challenges related to the change. When traditional operations and knowledge are in transition at the same time, productivity related to development is reduced as the burden increases due to extra work load.
- *B3 – Transition slows NbF integration*.
  B3 will similar to B2 increase the challenges related to the change. When operations and knowledge are in transition at the same time, productivity

related to integration of Network Based Defence is reduced as the burden increases.

In addition, the variable "Effect of perceived trust level on NbF integration", affects the operation transition speed. If the perceived trust level among the operators is inadequate, vulnerability, frequency of incidents, severity of incidents and cost of incidents are highly affected. It will also affect the productivity of resources in NbF integration. It might therefore be too dangerous to continue the operation transformation, resulting in delayed transition.

As a transition from traditional operations to Network Based Defence is very comprehensive and complex, it is important to do it well in the first place. All transitions create knowledge and process gaps, possibly resulting in increased risk. By letting the dynamics of the transition facilitate the development, later transitions are easier to implement.

Knowledge development

An equivalent model is adapted for the knowledge development, shown in figure 17. Knowledge is developed in parallel with the implementation of Network Based Defence (NbF), included knowledge and skills needed to employ the NbF platform in a proper manner. The knowledge transition is conducted during three stages, *Traditional knowledge, New knowledge and Mature knowledge*. Similar to the NbF implementation and integration, the knowledge development and integration depend on available resources and consist of six feedback loops. The three reinforcing feedback loops are:

- *R4 - knowledge development learning curve*
- *R5 - knowledge integration learning curve from immature knowledge*
- *R6 - knowledge integration learning curve from mature knowledge*

The three reinforcing feedback loops capture the knowledge development and integration learning curves. When the learning curves increase, the development and integration experience are improved. This again is assumed to improve the development and integration productivity.

The balancing feedback loops B4, B5 and B6 work in a similar manner as the balancing feedback loops B1, B2 and B3 for the NbF process:

- *B4 - later knowledge change harder*
- *B5 - transition slows knowledge development*
- *B6 - transition slows knowledge integration*

It is assumed that the more knowledge changed, the more challenging knowledge remains, slowing down the process (B4). B5 and B6 take into consideration the increased burden when the NbF implementation, integration and knowledge change

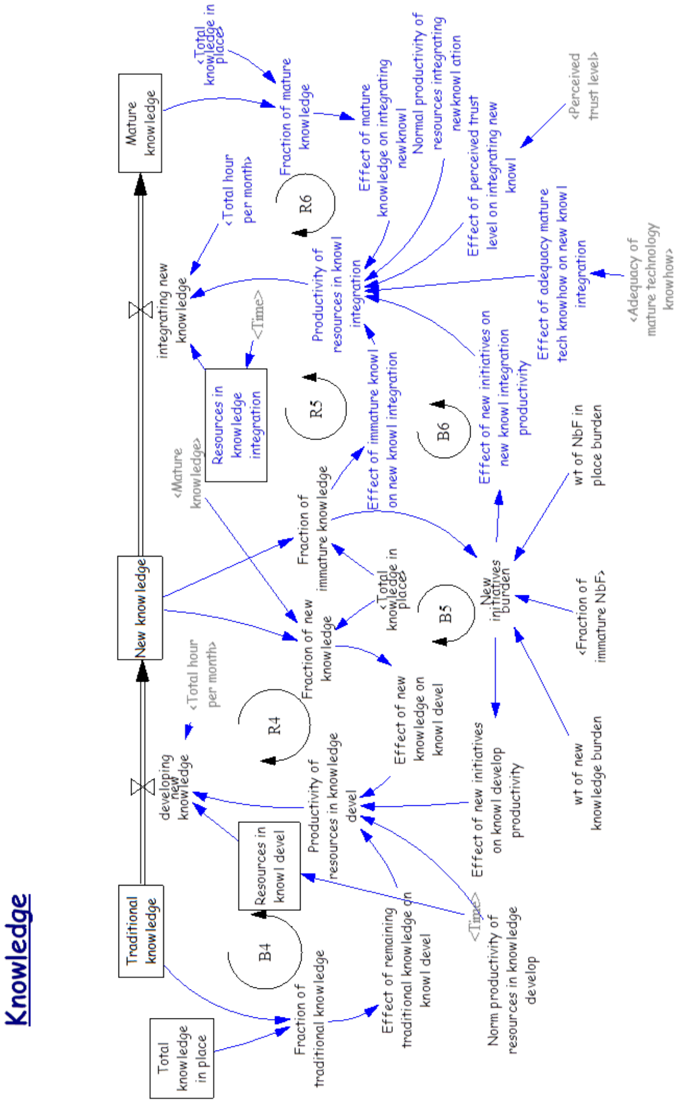

Knowledge
Mature knowledge
<Total knowledge in place>
Fraction of mature knowledge
R6
Effect of mature knowledge on integrating newknowl
Normal productivity of resources integrating newknowl ation
Effect of perceived trust level on integrating new knowl
<Perceived trust level>
<Total hour per month>
integrating new knowledge
Productivity of resources in knowl integration
<Time>
Effect of adequacy mature tech knowhow on new knowl integration
<Adequacy of mature technology knowhow>
Resources in knowledge integration
R5
<Mature knowledge>
Effect of immature knowl on new knowl integration
Effect of new initiatives on new knowl integration productivity
B6
Fraction of immature knowledge
New knowledge
<Total knowledge in place>
B5
New initiatives burden
wt of NbF in place burden
<Fraction of immature NbF>
Fraction of new knowledge
<Total hour per month>
R4
Effect of new knowledge on knowl devel
developing new knowledge
Productivity of resources in knowledge devel
Effect of new initiatives on knowl develop productivity
wt of new knowledge burden
Resources in knowl devel
Traditional knowledge
B4
Effect of remaining traditional knowledge on knowl devel
<Time>
Norm productivity of resources in knowledge develop
Total knowledge in place
Fraction of traditional knowledge

Figure 17: Development of new knowledge. Adapted from "Mitigating Information security risks during the Transition to Integrated Operations" by Qian [6]

happen simultaneously.

In addition, the variable "Effect of perceived trust level on integrating knowledge ", affects the knowledge integration speed. If the perceived trust level among the operators is inadequate, vulnerability, frequency of incidents, severity of incidents and cost of incidents are highly affected. It will also affect the productivity of resources in knowledge integration. It might therefore be too dangerous to continue the operation transformation, resulting in delayed transition and hence also delaying the knowledge integration.

Perceived trust level

The NbF transformation and knowledge development can be assumed to have an impact on the operator's and leader's perceived trust to available information and the information system. Introduction of new NbF processes and new knowledge reduce the personnel's competency for using the technological platform to support military operations. Inadequate competency will most likely result in less correct perceived trust level. When the perceived trust level is too high or too low, information and systems are not handled as expected to support NbF and military operations, delaying the transformation process. The introduction of new type of operations and new knowledge often results in a knowledge gap due to unaligned processes. A knowledge gap together with increased transition speed, will introduce new vulnerabilities, which again will increase the frequency of incidents. In order to adjust the perceived trust to adequate level, the operators and organization need to learn from the various incidents. This is illustrated in the system dynamic model adapted from the PhD work "Mitigating Information security risks during the Transition to Integrated Operations" by Qian [6] in figure 18. The model also gives indications to partly answer research question 3, how are the identified factors related to knowledge affecting the operators' perceived trust level?

"Perceived trust level" is a stock accumulated by the rate "adjusting perceived trust level" and drained by the rate "obsolete of perceived trust level". Perceived trust level is assumed to become obsolete over time, if the organization does not learn from incidents or register that incidents happen. Learning from incidents will adjust the perceived trust level, and more severe incidents will have more significant effect on the adjustment. The security culture will also affect the organization's learning ability, but this variable will not be further elaborated in this project.

When the perceived trust level is inadequate, the frequency of possible events will most likely increase. An increased level of events can result in a higher frequency of incidents, having impact on both personnel and military equipment, described by the variable "Incident cost per month". A possible lack of trust in relation to the NbF process or to the technical systems implemented, might result in inadequate level or lack of trust to available information as well.

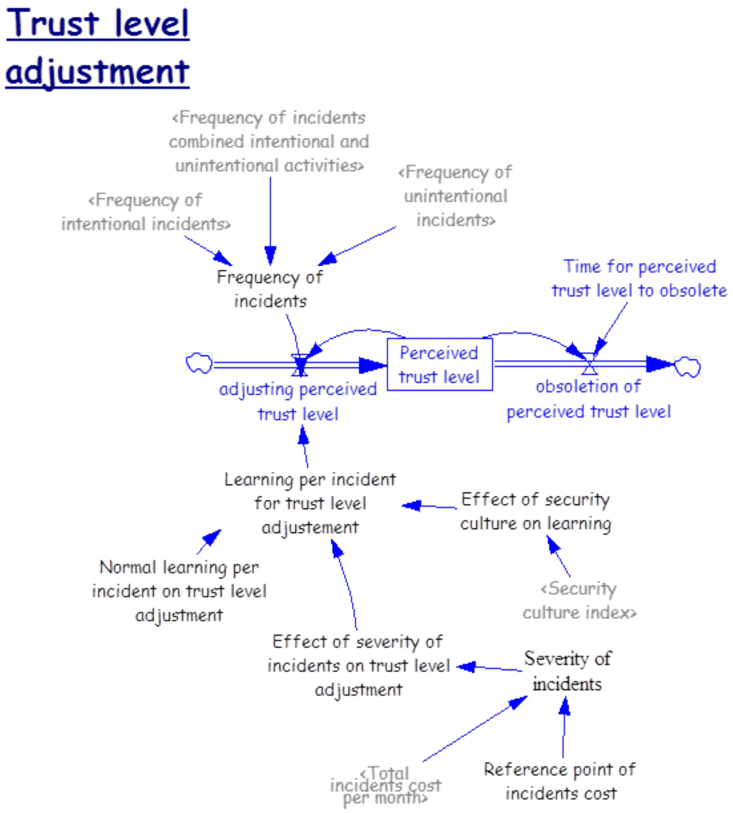

Trust level adjustment
<Frequency of incidents combined intentional and unintentional activities>
<Frequency of intentional incidents>
<Frequency of unintentional incidents>
Frequency of incidents
Time for perceived trust level to obsolete
Perceived trust level
adjusting perceived trust level
obsoletion of perceived trust level
Learning per incident for trust level adjustement
Effect of security culture on learning
Normal learning per incident on trust level adjustment
<Security culture index>
Effect of severity of incidents on trust level adjustment
Severity of incidents
<Total incidents cost per month>
Reference point of incidents cost

Figure 18: Perceived trust related to incidents and their severity. Adapted from "Mitigating Information security risks during the Transition to Integrated Operations" by Qian [6]

To visualize how the preliminary NbF SD dynamic models can support the implementation of Network Based Defence, hypothetical simulations of the adapted models are shown in figure 19. Values for the various variables and parameters are based on educational guesses, and a time frame equal to 10 years (120 months). Adding sufficient resources is crucial to achieve the simulated results. The only resources considered in these models, are working hours per month.

The operation transition is visualized with the graph denoted "Operations". By time zero, it is assumed that all operations are traditional. As time goes by, more of the traditional operations are transformed to NbF in place (red line) before integrated to mature NbF (green line). After ten years, it is assumed that all type of operations are transformed to mature NbF.

Maturation of knowledge is more time demanding than maturation of operations, as already described in page 27. This is clearly illustrated by the graph denoted "Knowledge", and more specifically by the green curve denoted "Mature knowledge". The green curve increases more slowly than mature operations and will not achieve the maximum level within ten years of development. Traditional knowledge (blue line) decreases much slower than traditional operations. Some of the traditional knowledge also remains after ten years with development, suggesting that continuously follow ups are necessary even after this long period of time.

Similarities can be found in the graph "Technology knowhow". The curves representing "Immature new technology knowhow" and "Mature technology knowhow" will behave in the same manner as the curves "New knowledge" and "Mature knowledge" in the graph "Knowledge". The blue line describing "Immature new technology knowhow" illustrates the limited understanding of newly adopted technology. In the beginning, the operators only know enough about the technology to perform their daily duties. When "technology knowhow" matures, the operators have a comprehensive understanding of the technology, included benefits and problems related to it. When the "technology knowhow" is mature, the operators are able to utilize the technology effectively.

The last graph visualizes simulations related to incidents. Frequency and severity of incidents will both reach a top after approximately five years. This coincidences with maximum NbF in place and maximum new knowledge, meaning that neither of the two processes are mature yet and new initiative burden is very high. The operators are not very familiar with the new type of operations, and they lack knowledge for how to employ the new type of operations. As the operations grow mature, the knowledge also will grow mature (but delayed), reducing the number of incidents and the severity of the incidents.

The models described in this chapter, will be employed to support results from

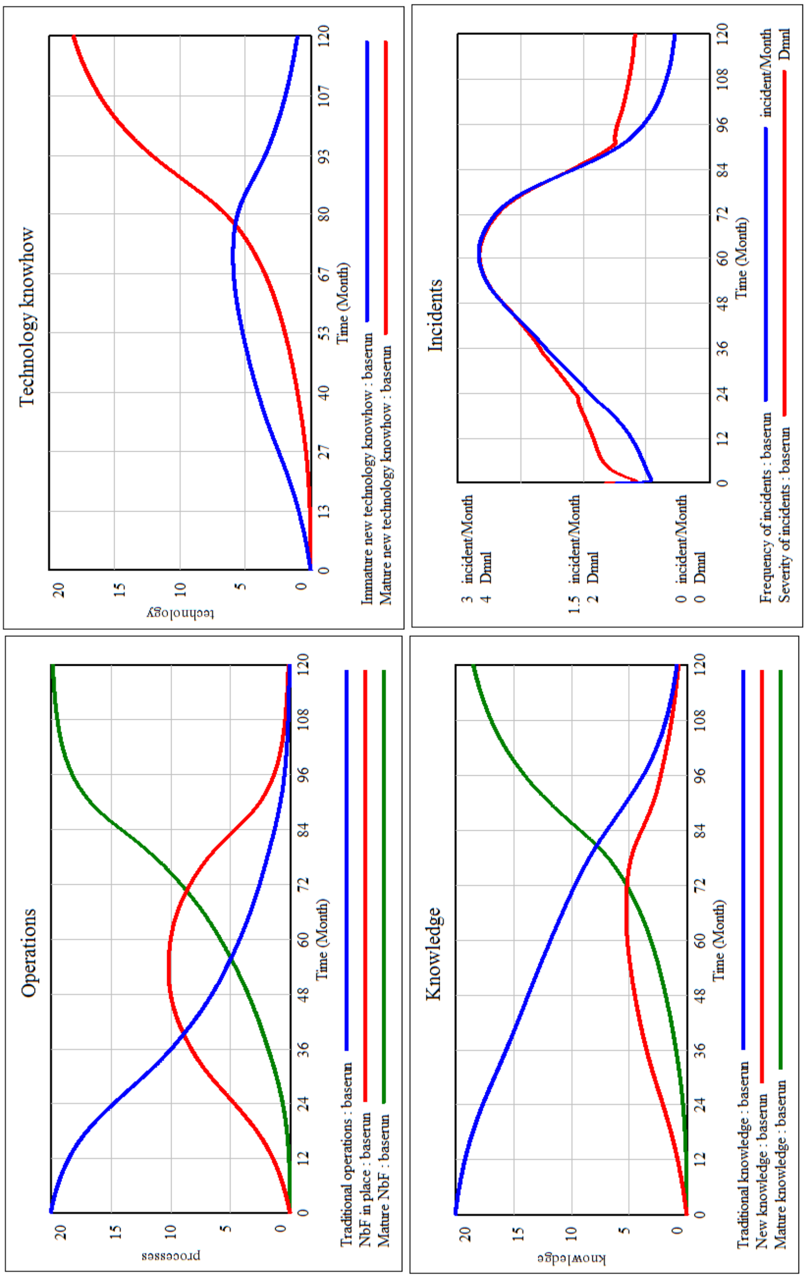


Figure 19: Hypothetical simulations showing possible outcomes when adjusting the processes of operation transition and knowledge development to each other. Adapted from "Mitigating Information security risks during the Transition to Integrated Operations" by Qian [6]

the practical research described in chapter 5.

3.2 The practical research

A possible lack of trust in relation to the process of implementing Network Based Defence or to the technical systems implemented, might result in inadequate level or lack of trust to available information. A possible lack of trust will also challenge the stated objectives of Network Based Defence. The strategic objective of Network Based Defence is to efficiently utilize technological infrastructure to support network based national operations and network based operations abroad [8] to achieve information superiority [11]. Connection of sensors, effectors and decision-makers has the ability to enable development of speed of command and decision-making, leading to more effective operations and disruption of the enemy's strategy by enhanced situational awareness [11]. A successful implementation relies on compatible systems, an excellent information infrastructure and intellectual capital aligned to each other. Described theory in chapter 1, studied literature in chapter 2 together with the preliminary NbF SD models presented earlier in this chapter, suggest that there are several obstacles slowing down the implementation process. The obstacles also partly answer some of the research questions:

1. **RQ1: How are the two processes of operation transition and knowledge development in Network Based Defence adjusted to each other?**. Technology, procedures and intellectual capital are not aligned to each other. Technology has been the main cost driver for the implementation of Network Based Defence [21]. There exist gaps and incompatibilities between the technology implemented, and procedures and knowledge needed to utilize it [18]. Vulnerabilities will most certainly be introduced, when technology is implemented and viewed in isolation [10]. When human and organizational issues are not aligned to technology, it is difficult to achieve satisfactory situational awareness [23]. The traditional structure of the military hierarchy challenges interaction between the different levels of the organization [19]. There exist gaps between the processes going top-down and bottom-up, challenging the implementation[19] of Network Based Defence. Lack of ownership and implementation capacity are transverse problem issues [9], because the implementation responsibility is placed in an inappropriate level of the command hierarchy. In addition, the change of focus from person to tool, might place responsibility on the systems instead of the commanders, making control more important than command [17].
2. **Q3. How are the identified factors related to knowledge and situational awareness affecting the operators' perceived trust level?** Competency, training and experience are important contents of intellectual

capital. The operators need proper training to understand the intended use of the system and expected reliability [29]. Competence, training and experience in addition to cognitive ability, are prerequisites to achieve situational awareness. Human ability to integrate information, anticipate what is going to happen and plan the next move, is part of situational awareness [15]. Wrong interpretation of the situation together with varying quality of the information, will affect the situational awareness in a bad manner ([30] and [16]). Competency, training and situation awareness are important human related antecedents of trust [25], and appropriate trust is necessary to achieve superior performance in a human–automation system [29]. Results from studies related to human-human relations can be employed to understand the trust between humans and networked systems [28]. There is no comprehensive understanding for the process of implementing Network Based Defence among military employees. Inconsistent use of terms related to Network Based Defence might lead to more confusion than necessary, and lack of understanding for the Network Based Defence process introduce additional obstacles [19].

Knowledge employed as a basis for the practical research

Based on the described system dynamic models and previous literature, it seems obvious that several obstacles are slowing down the implementation process. The focus in this project is to investigate how knowledge is considered in relation to the implementation process of Network Based Defence. More specifically, gaps between processes related to operation transition and knowledge development will be investigated in order to identify possible vulnerabilities. As described above; competence, training and experience are important prerequisites to situational awareness, and all of them are antecedents of trust. Knowledge will therefore be investigated from different angles, assuming to be of relevance for situational awareness and perceived trust. Investigating knowledge will also serve as a basis to answer research question 2: Which factors related to knowledge affect the implementation of Network Based Defence?:

1. **Knowledge of how to develop a technological platform supporting military operations, putting high demands on the developer**. To investigate this issue, the following key points are of interest:
    - Is the functionality well adjusted to the unit's demand?
    - Is the technological platform supporting information collection and information sharing?
    - Possible obstacles to information sharing, if technical or human obstacles are most prevalent.

   - Is the technological platform reliable, and enabling faster and easier task performance?

2. **The user's knowledge of how to utilize the technological platform in an appropriate manner either based on education, course, experience or training**:
   - Are the users able to employ the different systems, and to understand how they are connected?
   - Do the users know how to understand and analyse information presented by the systems?
   - Do the users know how the systems can support their need of information?
   - Do the users recognize important information, and do they know how to register it into the systems?

3. **Knowledge about the operational objectives and the situational picture during military operations among all participants, investigating**:
   - The user's ability to perceive own and enemy situation correctly.
   - The user's ability to predict enemy actions based on available information, and to plan future actions.

4. **Know to what extent it is possible to trust information presented by the technological platform, that the information is**:
   - Correct
   - Complete
   - Not manipulated

In order to collect relevant information, an interview guide and a questionnaire are developed in addition to an agreement. The developed interview guide, questionnaire and agreement are included in appendix B, and are based on the described focus areas, an earlier developed questionnaire by Bjørnstad [44] and also this thesis' problem description. In order to make the interview guide and the questionnaire more user friendly, the listed factors are divided into the following main areas:

- **Technical information systems** to see if the functionality is well-adjusted to the different unit's demand, and if the operators understand how the systems function and are connected.
- **Competence and training** including how the operators are educated and trained, so they can employ the systems in an appropriate manner. Internal education will also be part of this issue.

- **Information collection and sharing** to find out if the operators are able to detect, register and verify important and necessary information related to current operations. It is also interesting to find out if the operators are satisfied with the information they send and receive, and if the received information is updated and accurate.
- **Obstacles to information sharing**. Find out if there are obstacles to information sharing, and what the probable obstacles are.
- **Situational awareness** looking into the operator's ability to perceive, comprehend and predict their own and the enemy's situation, also with lacking information.
- **Trust** in order to investigate to what extent the operators trust information presented by the information systems, and if they are aware that the information might be wrong, manipulated or incomplete.
- **Trustworthiness** investigating if the operators mean that the systems are reliable and functional, and if the systems enable faster and easier task performance.

This project is focusing on knowledge and how this factor is considered into a Network Based Defence context. Examination of the context and other conditions related to the case is necessary to understand the problem in question [49], but also to produce a deeper understanding resulting in new learning [50]. In addition, the subject of the research is related to human and social science. A qualitative case study is therefore a suitable option and will be employed in this project.

Preliminary studies suggest that different military units employ the technological platform differently, and that the knowledge and expertise differ greatly between the units. Interviews and questionnaires will therefore be conducted within various military units to find out how they are employing the technological platform. In addition, a field research will be conducted at The Norwegian Defence University College of Engineering - Telematics. As the results from the three different units probably will differ greatly, this represents multiple cases with maximum variation as described by Flyvbjerg [50]. Cases with maximum variation have the objective to achieve maximum variations in a specific dimension. Cases with maximum variations are information based selection, and the purpose is to maximize the usefulness of the information extracted from a few cases. Even if the results might be different, more cases will probably ensure greater confidence or certainty in the findings.

The field research will be based on direct observations focusing on, but not limited to, key points decided in advance. The key points will focus on how information is collected and verified, and how this will affect the team members' situational awareness. In addition, the field research will look into how the teams employ the technological platform and how dependent they are of the platform. Hence, the field observations have the objective of looking into human actions in a real-world context. The advantage in such a setting, is the possibility to use the five human senses in addition to make field notes and make a summary of the observations [49]. The field observations will be used as a basis to get some insight into how the technological platform is employed, and how well the operators are trained.

The interviews will be open-ended, but based on an interview guide developed in advance. Interviews have the ability to offer richer and more extensive material than results from questionnaires [49]. In this project, the interviews will be supported by results from a questionnaire to get deeper insight into the subjects in focus. Interviews also have the ability to get insight into how participants construct reality and perceive different situations, providing important insight into the case.

Questionnaires are not originally assumed to be included in a case study, because the results from a questionnaire are assumed to be "derived" data, collected outside natural settings. In this project, the results will support information collected during field research and interviews, and all the collected data will be used to triangulate the findings. Doing a triangulation is about checking and rechecking the consistency of the findings from different and the same sources, making the results as robust as possible [49].

Case studies are tightly connected to reality, and attributes related to case studies complicate the possibility to summarize the process. In order to understand the findings, issues need to be described related to context and the surrounding landscape [50]. Then the results are easier to understand, and misunderstandings can be avoided. Often case studies must be read as complete stories, not as single results taken out of context. The conclusions in this project will therefore seek to explain results related to context, in addition to make concrete suggestions for improvement.

4 Results from preliminary research

In order to collect information to investigate the research questions, practical research was conducted in three different military units in the Norwegian Armed Forces. Field research, questionnaires and interviews were first carried out at The Norwegian Defence University College of Engineering - Telematics during their winter exercise "Cold fusion". The results from this preliminary research served as a basis to adjust the developed questionnaire and interview guide for further use in two army units. It also served as a basis to understand how knowledge was considered in relation to technology in a military context. The preliminary research conducted at the Norwegian Defence University College of Engineering - Telematics is described in detail in this chapter. The chapter includes results from the field research, the questionnaire and the interviews. Some closing remarks are added at the end of the chapter together with the main findings. The practical research conducted in two different army units is described in the next chapter.

4.1 Research conducted at The Norwegian Defence University College of Engineering - Telematics

This section includes the practical research conducted at The Norwegian Defence University College of Engineering - Telematics, included results from the field research, interviews and the questionnaire. The main findings are summed up in the closing section of this chapter. The complete results can be found in appendix D.

The university college educates officers with engineering competence during 3,5 years of schooling. The university college combines technical and military skills, and supplies various units in the Norwegian Armed Forces with necessary technical competence. During the 3,5 years of schooling, the university college conducts several exercises to teach the students various practical skills related to military and technical subjects. The students cover different roles in the various exercises, ranging from ordinary infantry soldiers to staff members in the top level. The roles and complexity increase according to the student's competence. Different from other officer's schools, they will not be educated to perform excellent in one specific role, but achieve experience from different roles. Results from this unit might therefore not be directly comparable to the other two units, which employ specialists in their respective fields. The results from The Norwegian Defence University College of Engineering - Telematics will therefore be used to get an indication of how the human factor is considered when employing a technical platform during military operations. In addition, the results will help adjusting the questionnaire and interview guide for the further research.

Preliminary appointments and arrangements with The Norwegian Defence University College of Engineering - Telematics were done during the Research Project Planning phase (November 2017) in order to be in advance of the exercise planning. The following main focus areas were decided for the field research:

- Investigate how various amount of technical equipment affect team performance in military operations.
- Investigate how the operators react to radio jamming of the communication system.
- Investigate how the operators react to different incidents in the computer network.

> "In military terms, jamming is the offensive use of electromagnetic spectrum or directed energy to directly attack enemy combat capability, blocking or interfering with the authorized wireless communications [51]"

4.1.1 Field research

The objective of the field research was to find out if the support of technical tools improved the planning and implementation of operations, and how technical tools affected the team's and unit's interaction. In addition, it was assumed that the leader's personality would highly affect to what extent the team trusted the given information. The field research was conducted from Monday the 13th to Wednesday the 15th of February 2017 at Kittilbu, and was divided into four main areas:

- Investigate the company staff's ability to achieve situational awareness and lead military operations based on personality and available technical tools.
- Investigate the technical support element's ability to employ a technical network sensor to detect suspicious activity in the company network, and to put possible incidents into an operative context.
- Investigate if the presence or absence of technical tools affect team performance in military operations.
- Investigate how radio jamming of the military communication system is detected and handled.

Ability for situational awareness and management of operations in the company staff

The company staff was responsible for planning and leading different operations during the entire exercise. The company in total, included a communication platoon, an infantry platoon and a company staff with a technical support element. The company had radio communications, networks and computer systems to support their operations. The computer systems included software for graphical maps, systems for order development and tools for management of the operations. All technical equipment was present during the entire exercise in the company staff. The senior students were followed by supervisors. Based on own observations together with observations from one supervisor, the following issues were identified.

The operational officer (responsible for planning and leading the operations)
The students holding the role of the operational officers searched for relevant, updated and correct information collected from other members of the staff and the technical support systems. The information was quality assured to some extent, but only at random and with different sources. The operation officer's situational awareness (SA) seemed to be increased as a result of the technical support systems, but suffered from coincidental quality assurance. The technical systems reduced the interaction between the individuals in the staff. On the flip side, one of the operational officer's personality supported interaction within the staff in a constructive manner.

The intelligence officers (responsible to keep track of enemy actions and movements).
The students holding the role of the intelligence officers had some difficulties due to lack of necessary prerequisite and competence related to intelligence. The searched information was not entirely relevant, updated or correct, and correct situational awareness was not possible due to incomplete information. A defensive approach to handle different situations due to lack of competence, resulted in reduced trust to their analyses of the enemy's situation. Interaction within and across own responsibility was not optimal.

Common to all functions in the company staff.
The operations relied heavily on the technical support systems. Errors in the technical platform resulted in focusing on technical challenges, forgetting about the military operations. Even when mentored and guided, some of the students were still paralysed without support from the technical systems. Some individuals were, however, able to see alternative solutions and actions without support from the technical platform.

Detection of suspicious activity by network sensor in the technical support element

As part of the exercise, senior students were to employ a network sensor to detect suspicious network traffic in the company network. The suspicious activity included a hostile port scanning attack to simulate suspicious activity, and an attack of a military installation to get physical access to the company network. In order to find out how the senior students handled the different incidents, all situations were observed by supervisors and the researcher. The following observations were made:

Port scanning.

The incident was detected immediately, and the students searched for information to solve the case. On the flip side, they did not have enough knowledge for how to use the tool effectively. Too much information challenged the incident handling, and the information was not quality assured. In addition, the incident was viewed total isolated from the company operations, and was not put into an operative context. Overall, the incident was handled in an inappropriate manner, and was reported to the company staff significantly delayed and only by chance. The port scanning incident was presented at the daily brief in the company staff, but the presentation was not coordinated between the technical element and the company staff, resulting in duplicated presentations. Interaction within the technical element happened more or less at random and the overall situational awareness was weak.

Attack on a military installation to get physical network access.

The physical attack continued for several hours before detected. But when first detected, the attack was handled better than the port scanning incident. Because the attack happened out in a peripheral installation, the technical personnel had to relate to the operative setting to some extent. The technical personnel and the company staff also had to interact to locate and solve the situation. On the flip side, the interaction still suffered from weak management, and the senior students in the technical element still had weak situational awareness.

Is presence or absence of technical tools affecting team performance in military operations?

The infantry platoon consisted of three different teams executing similar operations during three phases. One of the missions was to perform reconnaissance against a target. This was conducted by three different teams in three consecutive phases. During the field research, the three teams were somewhat different equipped. In the first phase, the team was equipped with map in paper, compass, pencil and paper notebook, in addition to radio communications. In phase two and three, the teams were equipped with computer based maps for the planning process, and a GPS for the executing team out in the field. The computer based map gave access to more details in the terrain, included 3D photos. The GPS gave automatically location updates when the settings were correct. The reason for equipping two groups with the same type of tools, was to get some insight into how the leader's personality affected the mission. Based on observations from the researcher and two supervisors, the following observations were made:

Phase 1, no technical tools.

Information was collected mainly on the given map. The information lacked some details in addition to be outdated. Information was not quality assured even if the supervisors were available for questioning, and the team seemed to have poor skills related to navigation with map and compass. The orders were supported by a

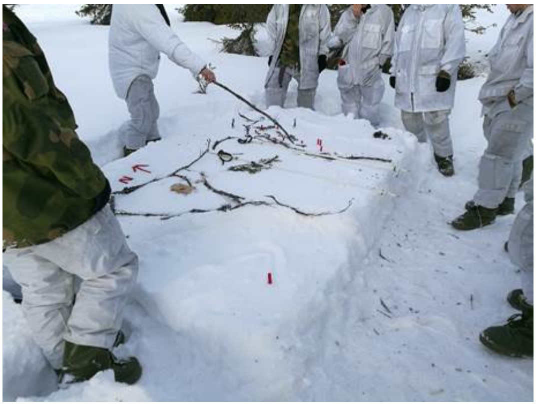


Figure 20: Illustration of a model board

model board which highlighted important key points in the terrain. A model board is illustrated in figure 20, and is a visualization of the terrain in the operation area. The model board supported a common situational understanding, but the leader's reduced commitment reduced the involvement from the rest of the group. Incorrect and not quality assured information affected the interaction within the team in a negative manner. The result was inadequate situational awareness and delayed execution of the mission.

Phase 2, computer based maps for the planning phase and a GPS for the executing team in the field.
Information was collected from the map in the graphical interface of the computer, with a high degree of details in the terrain. The team sought information within the group, in the staff and by the supervisor. The collected information was to some extent relevant to the mission, correct and updated, with some small errors. The orders were supported by a model board, which highlighted important key points in the terrain, and was adjusted to the actual landscape only with minor errors. In addition, the model board acted as a good source for creating a common situational understanding. The team leader was a bit tied up in the computer during the orders meeting, as the orders were stored there. The team leader recovered overview when he asked the team members questions about the given orders. The leader's commitment probably increased the situational awareness (SA) and motivation among the group members. Increased SA together with the use of a GPS during the mission, increased the effectiveness and reduced the uncertainty. On the flip side, introduction of technical tools reduced the interaction between the team members during the planning phase.

Phase 3, computer based maps for the planning phase and a GPS for the executing *team in the field.*

Information was collected from maps in the graphical interface of the computer, showing a high degree of details in the terrain. The unit sought information within the group, in the staff and from the supervisors. The collected information was to some extent relevant to the mission, correct and updated, with some small errors. The orders were supported by a sketch on a whiteboard. The sketch lacked the details and granularity used by the leaders in phase 1 and 2. In addition, the team tended to bury itself deep into the technical tools. A reduced situational awareness due to lack of details in the sketch and a focus mainly into the technical tools affected the mission in a negative manner.

Radio jamming of communication system in company staff

The company staff was exposed to radio jamming several times during the exercise. The radio jamming was detected immediately and handled in a proper manner, by implementing the emergency communication plan.

Possible error sources

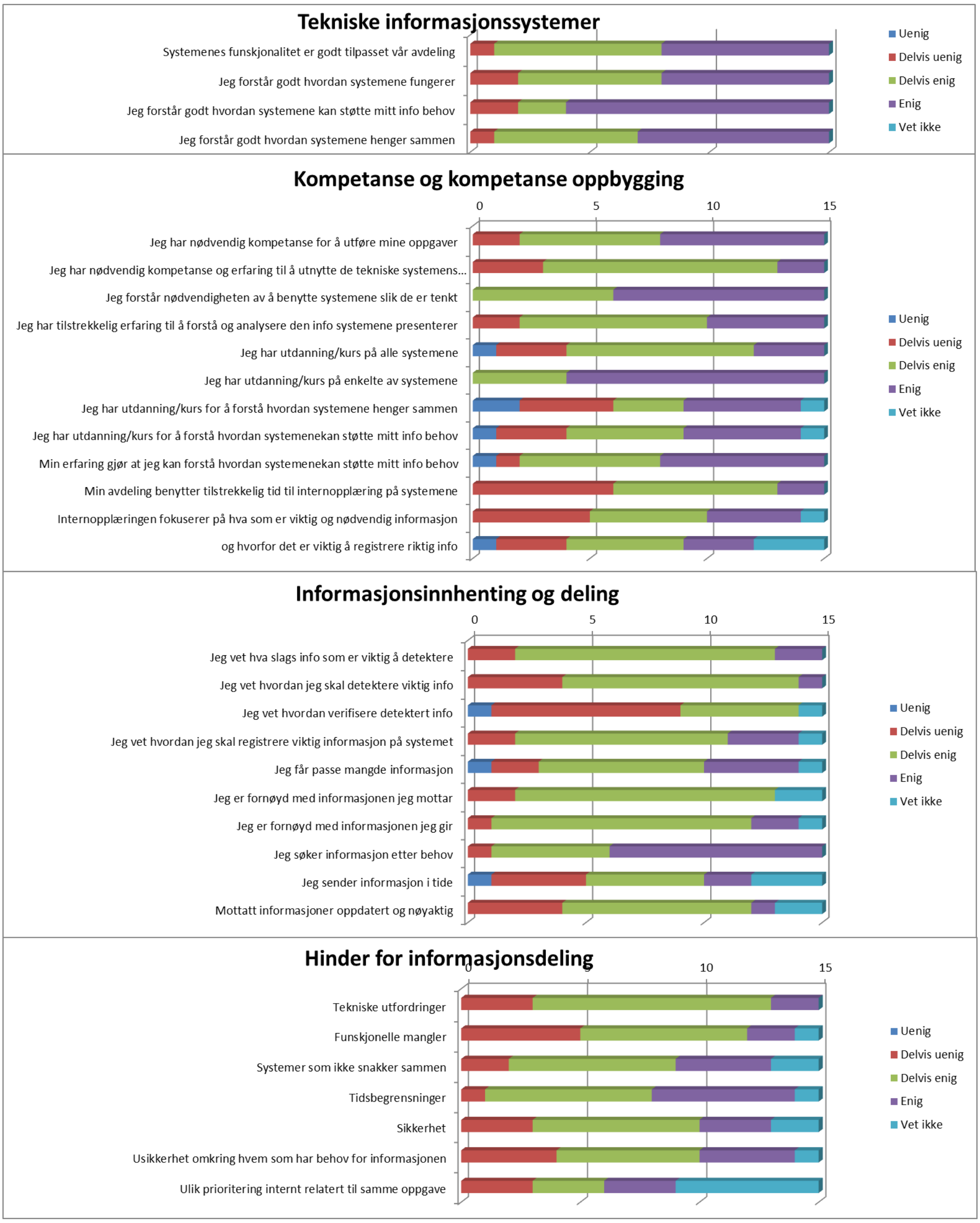
The results from the field research are based on perceptions and observations done by different people. Different persons might have different perception of the same situation. Different leaders have different personality and leader characteristics. In addition, the operations had to be adjusted to available time, resulting in different time limitations for the various missions. These are all factors possibly introducing uncertainties into the findings of the field research.

4.1.2 Questionnaires

15 senior students from the company staff and the technical support element participated in the questionnaire after signing the needed agreement. The developed questionnaire and agreement are shown in appendix B and include seven main areas; technical information systems, competence and training, information collection and sharing, obstacles to information sharing, situational awareness, trust and trustworthiness. The questionnaire was conducted immediately after completed exercise to make sure the students had the exercise clear in mind. The detailed results are included in appendix D and illustrated in the graphs in figure 21 and 22. FIH is an abbreviation in Norwegian for The Norwegian Defence University College of Engineering - Telematics. The results are discussed as follows.

Technical information systems

Most of the students agreed to some extent that the system's functionality is well adjusted to their unit, that they understand how the systems work and how they are connected. In addition they agree that the systems support their information need.


Tekniske informasjonssystemer

Kompetanse og kompetanse oppbygging

Informasjonsinnhenting og deling

Hinder for informasjonsdeling

Figure 21: Results from the questionnaire conducted at FIH illustrated by graphs - part 1

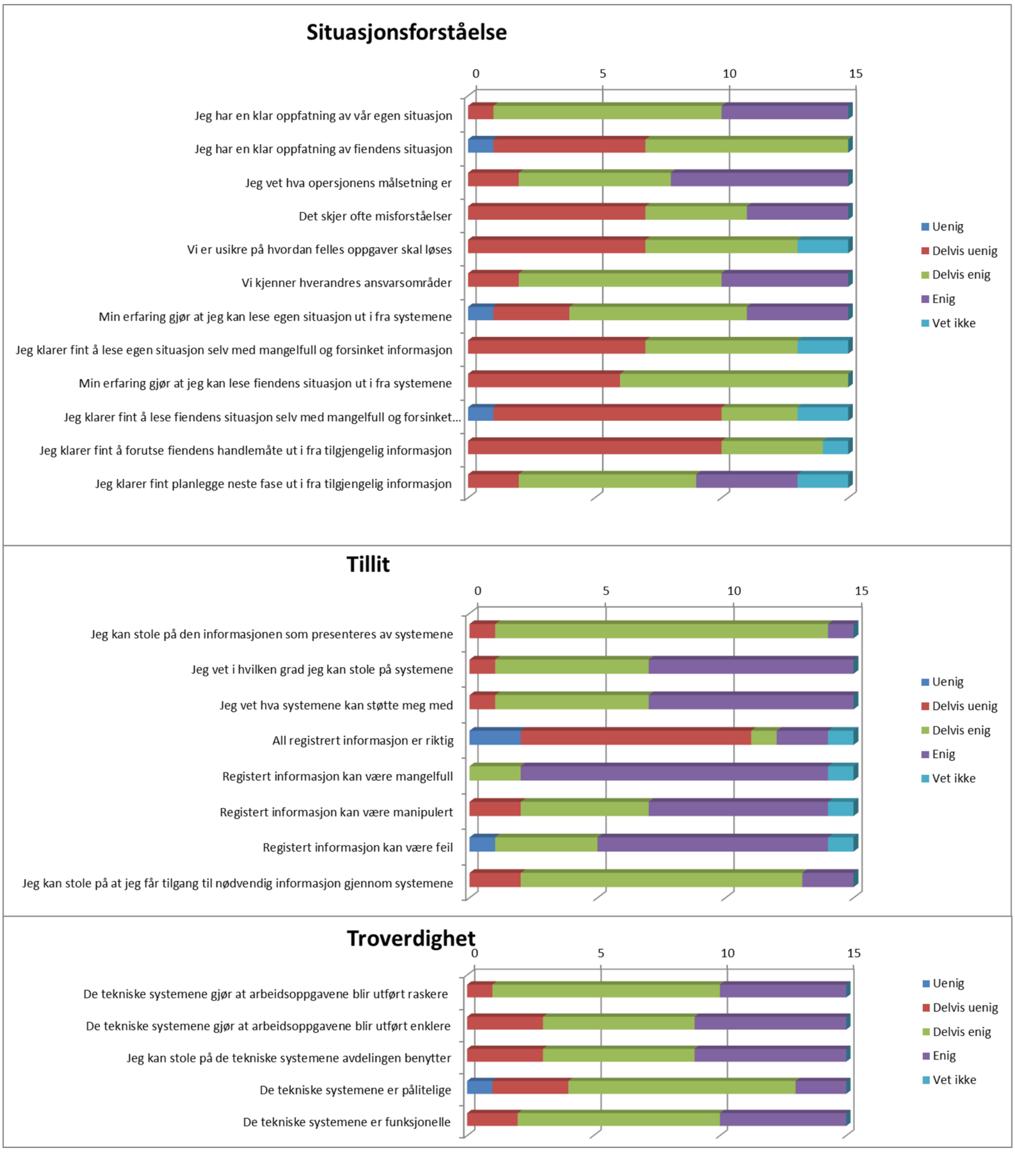


Figure 22: Results from the questionnaire conducted at FIH illustrated by graphs - part 2

Competence and training

The majority of the students agreed to some extent to hold necessary competence to perform their duties and to hold necessary experience to understand and analyse the information presented by the systems. Most of the students also agreed to some extent to hold necessary competence and experience to utilize the technical platform. All the students understood to some extent why it is necessary to employ the systems the way they are supposed to. All the students had course or education for some of the systems. The majority of the students agreed that education and experience were necessary prerequisites to understand how the systems could support their need of information. Fewer agreed to have course or education to understand how the systems were connected. Internal learning was partly covered for, but not focusing on what type of information to search for during operations.

Information collection and sharing

The majority of the respondents agreed to some extent to know what type of information to search for and register into the systems. Only a minority knew how to verify the information. Most of the students agreed to some extent to receive enough information and to be satisfied with the information they sent and received. They were only partly satisfied with the timeliness and quality of the information. The majority of the students agreed to seek information on demand.

Obstacles to information sharing

Obstacles to information sharing seem to be divided between technical challenges, systems not talking together, functional errors, time limitations and security. Only a minority of the students answered that different internal prioritizing was an obstacle to information sharing.

Situational awareness

The majority of the students agreed to some extent to be aware of their own situation, but a minority agreed to be aware of the enemy situation. Most of the student's knew to some degree the operation's objectives and half of the students partly agreed that misunderstandings happened a lot. Experience seems essential to understand own situation, but only a minority of the students agreed to understand own situation with lacking information. Even more of the respondents struggle to understand the enemy's situation and predict the enemy's next move based on available information. Most of the respondents are to some extent able to plan the next phase of the operation based on available information.

Trust

The results indicate some contradiction between the various answers. The majority of the students answered that they trust the information presented by the systems to some extent. However, they seem to be aware that information presented by the systems might be incorrect either due to lacking details, that they are manipulated or wrong. Most of the students know how the systems can support the operations.

Trustworthiness

Most of the students agreed to some extent that the technical systems enable faster task performance, and that task performance is easier due to the technical support systems. The majority of the students agreed to some extent that the systems are functional and reliable.

4.1.3 Interviews

Interviews at The Norwegian Defence University College of Engineering - Telematics were conducted among senior students holding roles in the company staff and the technical support element. Three students were interviewed. The complete interviews are only available in paper format, stored by the researcher. The interview guide contained 6 main areas, and the results from the interviews are referred accordingly. The interviews were also conducted immediately after the exercise was finished.

Technical information systems

The company staff employed military radio communications for speech, systems for support of situational updates and graphical interfaces with maps. The listed systems worked most of the time, and supported the company staff during their missions. Some of the data transmissions did not work properly, speech was therefore used as substitution to keep track of the current situational picture. Power Point was employed in order to keep track of personnel status and maintenance, and to support orders during the orders meeting. In addition, civilian communication systems were employed on top of the military communication system, but the civilian systems worked properly only one day. Two cameras were employed out in the field to transfer live stream data into the company staff. Relying on military communication lines, this turned out to be a challenge. The live stream only worked some hours of the exercise. In addition, light sensitivity reduced the cameras' ability to work in the darkness. The network sensor employed into the company network functioned well during the exercise, and was well suited both to the mission and to train the students for their future work.

Even if the company staff and the technical support element were collocated, the two elements had very different focus, resulting in highly different information need. The technical element only seemed concerned about their own technical systems. Their responsibility was to ensure that all the technical systems functioned well, and to support teams out in the field with technical issues. The technical support element seemed to view the technical information in isolation, and only employed to solve technical issues. They seemed to lack some knowledge related to how the technical systems supported military operations, and information was put in an operative setting only at random. On the flip side, personnel working in the company staff had a better overview of the situational picture, and knew what the different systems were supposed to deliver. They employed the systems for situational updates, enabling easier follow ups of the mission and further planning of the operations. The automatically situational updates on the systems seemed to be correct most of the time, but slightly delayed.

Competence and training

During the exercise, the students had to employ a variety of technical systems. They only knew how to operate some of them in advance. The systems' functionality was only partly known to the students before the exercise. Their previous knowledge was based partly on course and education on single systems, and experience from previous exercises. Based on internal guidance and supervision in addition to self-studying, the students learned how to employ the systems during the set-up phase and the exercise. Again, the technical support element was mainly concerned about information related to technical issues. They were, however, able to deal with later attacks in a better manner than the first incident, based on experience achieved during the first incident.

Information collection and sharing

For the company staff, there were some uncertainties related to what information to search for, and what information they needed to support own operations. Most of the personnel verified received information, often via voice communication. Intelligence about the enemy often had to be checked twice. The company staff could not be 100 percent certain that all received information was correct, but in most cases they believed it was. Radio keying, bad radio routines and lack of procedures for internal information flow, reduced the information exchange in the company. The reduced information exchange highly affected the situational awareness in a negative manner. It also reduced the amount of enemy information sent from the company staff to the rest of the company.

The personnel in the technical support element found it challenging to find necessary information in the technical systems without sufficient experience and training. Incidents and exact times had to be viewed in the correct context, and configuration control became an important issue. Supervision was necessary during the first phase of the exercise to find and understand necessary information. The quality of the collected information from the network sensor was good, and enabled understanding of various events. Understanding served as a basis for recommendations related to the technical platform, communicated to the company staff. On the flip side, the technical support element lacked knowledge about the operational situation until the company network was attacked. Then they were forced to comprehend the operational picture in a better manner. But in general, the lack of operational focus in the technical support element affected the information exchange with the company staff, suffering from bad routines. In addition, personnel in the technical support element struggled to explain for personnel in the company staff how technical issues actually affected the ongoing operations.

Situational awareness

The interview objects were mainly concerned about their own tasks, but the company staff was able to see the operational and situational picture to some extent. Enemy information was not analysed in a proper manner, resulting in reduced quality of the enemy picture. Due to reduced situational awareness related to the enemy, it was difficult to predict what the enemy would do next and to plan accordingly. The personnel in the technical support element were not particular aware of the situational picture. Again there was an artificial separation between the company staff and the technical support element, where the company staff had the operational focus (partly) and the technical support element mainly were concerned about technical issues. The technical support element was however forced to consider the operational importance of the network, when an installation was attacked and employed to infect the rest of the company network. The company staff seemed more aware of the operational settings and the ongoing operations.

Trust and trustworthiness

All the interview objects trusted the information presented by the different systems, because they did not have any reason not to. They also meant that the different systems supported them with all necessary information. The interview objects all depended on the technical information systems to do their job in a proper manner, and within reasonable time. In general, the technical information systems were functional and reliable, but relied on proper competence to utilize presented and available information. Some of the additional technical systems challenged the communication system's bandwidth and capacity, making the network act as a bottleneck.

General/other issues

To improve the current technical platforms, the interview objects recommended development of one common platform for support of military operations. The developed platform should then include all necessary functionality in order to improve the technical solution significantly, and also reduce the number of introduced errors. A better adjusted software solution would also be beneficial. In addition, development of routines for handling incidents, especially related to the company network was recommended, as such routines were lacking.

4.1.4 Summary and closing remarks for the preliminary research

This section includes a summary of the findings and some suggestions for improvement for the further research.

Field research

The objective of the field research was to find out how support of technical tools affected the planning and conduct of operations, and interaction between various team members. The main findings can be summed up as follows:

- **Situational awareness and management in the company staff**
    1. **The operational officers** had pretty good situational awareness (SA), which was supported by the technical systems. The SA suffered from coincidental quality assurance.
    2. **The intelligence officers** were not able to achieve correct situational awareness due to lack of prerequisite and competence, resulting in reduced trust to their analyses of the enemy's situation.
    3. **Common to all functions in the company staff**. The technical systems affected interaction in the company in a negative manner. Errors in the technical platform resulted in focus on technical challenges, forgetting about the military operations.
- **Detection of suspicious activity by network sensor.** The port scanning incident was detected immediately, the physical attack with the purpose of getting network access much later. The second incident was however handled in a better manner than the first incident. In addition, the technical personnel had to relate to the operative setting during the attack, because the attack happened in a peripheral military installation. Even if the technical personnel and the company staff had to interact to solve the situation, the interaction still suffered from weak management and weak situational awareness.
- **Is presence or absence of technical tools affecting team performance?**. Teams were equipped with various amounts of technical equipment. The support of analogue and manual tools resulted in collection of outdated information with low granularity during the planning phase. This was significantly improved when using technical support tools. Quality assurance was highly personnel dependent. The same can be said about motivation, interaction and commitment within the team. The use of appropriate tools during the orders meeting, as for instance a model board together with commitment from the leader, highly affected the situational awareness (SA) and motivation among the group members. Appropriate situational awareness and com-

mitment from the team resulted in effective and successful operations. On the flip side, too high focus on the technical tools was contra productive, and reduced the situational awareness.

- **Radio jamming of communication system**. The radio jamming was detected immediately and handled in a proper manner by implementing the emergency communication plan.

Questionnaires

The questionnaire includes seven main areas; technical information systems, competence and training, information collection and sharing, obstacles to information sharing, situational awareness, trust and trustworthiness. A summary of the main findings will follow.

- **The technical information systems** seemed to some extent to be adjusted to the unit's need, and to support the respondents' need of information.
- **Competence and training**. The majority of the students seemed to some extent to hold necessary competence and experience to utilize the technical platform and to perform their duties. All agreed that education, internal learning and experience were necessary prerequisites to understand how the systems could support their need of information.
- **Information collection and sharing**. Most of the respondents knew to some extent what information to search for, but only a minority knew how to verify the information. They agreed to receive enough information, but were only partly satisfied with the timeliness and quality of the information.
- **Obstacles to information sharing** seem to be divided between technical challenges, systems not talking together, functional errors, time limitations and security. Only a minority meant that different internal prioritizing was an obstacle to information sharing.
- **Situational awareness**. Most of the students seemed to some extent to be aware of their own situation, but emphasized experience as essential to understand the situation. Only a minority were aware of the enemy's situation and able to predict he enemy's next move based on available information. Most of the respondents were aware of the operation's objectives.
- **Trust**. The results indicate some contradictions. Most of the students trusted information presented by the systems to some extent, even if they were aware that some information could be incorrect either due to lacking details, that the information was manipulated or wrong.
- **Trustworthiness**. Most of the respondents meant that the technical systems enabled faster and easier task performance. In addition, the systems in general were functional and reliable.

Interviews

The interview guide contained 6 main areas, and main findings from the interviews are referred accordingly.

- **The technical information systems** worked most of the time and supported company operations. To keep track of the current situational picture, voice was used in addition to the graphical interface. Power Point was employed in order to get a better overview. Civilian communication systems were tested during the exercise with limited results. Due to limitations in the military communication system, transmission of live stream data was difficult, and light sensitivity in the sensors reduced their usability. The information need in the company staff differed between the various tasks. The personnel in the technical element seemed to view the technical information in isolation, and only employed the technical systems to solve technical issues. Personnel working in the company staff, employed the systems for situational updates enabling easier follow ups of the mission and further planning of operations. The automatically situational updates on the systems were correct most of the time, but slightly delayed.
- **Competence and training**. Even if the students had to employ a variety of technical systems during the exercise, they only knew how to operate some of them in advance. Their previous knowledge was based partly on course and education on single systems, and experience from previous exercises. Internal guidance and supervision increased their competence during the exercise.
- **Information collection and sharing**. The students found it a bit difficult to find necessary information to support ongoing operations. Information about the enemy was even more difficult. Information was in general verified by voice communication, but in most cases they believed that the information was correct. Lack of information exchange due to bad radio routines and lacking procedures for internal information flow, highly affected the situational awareness in a negative manner. In addition, the technical support element's lack of knowledge related to the operational situation also affected the information exchange with the company staff, suffering from bad routines.
- **Situational awareness**. Even if the interview objects mainly were concerned about their own tasks, the company staff was able to see the operational and situational picture to some extent, but with reduced quality of the enemy picture. The personnel in the technical support element were not particular aware of the situational picture, but mainly concerned about technical issues.
- **Trust and trustworthiness**. The respondents trusted information presented by the different systems, and meant that the different systems were essential to do their job in a proper manner and within reasonable time. In general,

they found the technical information systems functional and reliable, but that they relayed on proper competence to utilize presented and available information.

- **General/other issues**. One improvement would be to develop one common technological platform for support of all military operations, included all necessary functionality. Better adjusted software solutions would also be beneficial.

Main finding

- **Factors related to knowledge affecting the use of the technological platform**
  - The majority of the students seem to some extent to hold necessary competence to use the technological platform. Experience was emphasised as necessary to understand the intended use of the systems.
  - The communication system supporting the technical platform, introduced obstacles to information sharing due to limitations in the bandwidth.
  - Internal guidance and supervision increased the students' competence during the exercise, enhancing their ability to employ the technical platform in an appropriate manner.
  - Lack of prerequisites and competence reduced the situational awareness.
  - Technical errors resulted in lost operative focus.
  - Technical staff was mainly concerned about technical issues, suffering from weak situational awareness.
- **Factors related to knowledge affecting situational awareness (SA) and trust**
  - Varying situational awareness and coincidental quality assurance of the information resulted in reduced trust to some of the products from the staff.
  - Team using analogue and manual tools collected outdated information with low granularity. The collected information was employed without quality assurance, resulting in an inaccurate situational picture.
  - The use of technical support tools together with commitment from the leader, increased the information quality, and hence also the situational awareness.
  - Most of the students knew what information to search for, but not how to verify it, suggesting that information was trusted without quality as-

surance.

- The majority of the respondents were only partly satisfied with the quality and timeliness of the information, suggesting that information were outdated or wrong.
- Most of the respondents seemed to be aware of their own situation, but few were able to understand the enemy situation and predict the enemy's next move. This indicates inaccurate situational awareness possibly resulting in inadequate level of trust to presented information.
- Even if most of the students were aware that some information could be incorrect or outdated, they tended to trust information presented by the systems.
- Voice communication was essential to keep track of the current situation. This indicates that verification by voice was necessary to achieve correct situational awareness.
- Lack of information exchange due to bad radio routines and lacking procedures for internal information flow, highly affected the situational awareness in a negative manner.

In addition, some remarks were done by the respondents both related to the questionnaire and to the interview guide. They pointed out that some of the questions were too general, and made exact answers difficult. Based on the feedback, the results and experience obtained during this preliminary research, the interview guide and questionnaire were slightly adjusted. The adjusted versions are shown in appendix C. The adjusted questionnaire and interview guide are assumed to be better suited to the problem description, and help avoiding confusion among the participants.

5 Results from the practical research

In order to investigate the research questions in depth, practical research was conducted in two different army units in the Norwegian Armed Forces. In this chapter, results from interviews and questionnaires conducted in these army units will be analysed and presented. The transcribed interviews are appended outside the project report to ensure confidentiality for the participants. The detailed results from the questionnaire can be found in appendix E. The contents of the transcribed interviews vary a lot due to different backgrounds and skill levels among the participants. Not all the questions are relevant to all the respondents. Only the answered questions are referred in the appendix. Due to military classification, some of the answers are not included in the transcription and the various systems are not named.

The interviews and questionnaires were conducted in two different army units to investigate factors related to knowledge in the implementation of Network Based Defence. It was important to choose these two army units due to their differences related to personnel categories and how they conduct their operations. In both units, personnel from three different levels were interviewed and participated in the questionnaire, representing top level, intermediate level and lower level carrying out the actual operations.

The results from interviews conducted in the two army units are presented in section 1 and 2 of this chapter. A summary of the findings from the interviews can be found in section 3. The 4th section of this chapter looks into results from the questionnaire. The findings from the interviews and questionnaire are discussed in the last part of the chapter together with result supporting research question 1 and 2.

5.1 Results from interviews conducted in army unit 1

The transcribed interviews appended to the project for unit 1 are the basis for the analyses conducted in this section. The results will be presented looking into knowledge from different angles affecting military operations and the successfulness of implementing Network Based Defence. The results are referred in the same manner as described in chapter 3:

- Knowledge for how to develop a technological platform supporting military operations, putting high demands on the developer.

- The user's knowledge of how to utilize the technological platform in an appropriate manner either based on education, course, experience or training.
- Knowledge about the operational objectives and the situational picture during military operations among all participants.
- Know to what extent it is possible to trust information presented by the technological platform.

Suggestions for improvement are also included. The analysed interviews describe common issues pointed out by the majority of the respondents, but also significant challenges or benefits pointed out by single individuals.

5.1.1 Knowledge for developing the technological platform

This section looks into knowledge for how to develop a technological platform to support military operations. To achieve sufficient development knowledge, high demands are put on the developer and other resources supporting the development. The analyses are based on answers related to the following questions:

- How well are the technical solutions adjusted to the unit's operative needs?
- How well do the technical solutions support information collection and sharing?
- What are the obstacles to information sharing?
- How reliable and functional are the technical systems? (Enable faster and easier task performance?)

Technical solution adjusted to the unit's operative need?)

The battalion employs military radio systems, technical command and control systems for support of the situational picture and updates including a graphical interface with maps connected to military GPSs. All the systems are extremely important for support of the operations and are continually in use. The technique behind the systems is fairly well suited to the unit, but the technical systems are very difficult to employ for the user. Several technical obstacles challenge the usefulness of the technical systems. The systems are too complex, including several layers of menus where all the settings must be correct and set in the correct order. Additional hardware also needs careful consideration when included into the network. In order to make the hardware work, it must be added to the network before start up and configured correctly.

The knowledge related to the technological platform is deficient, and small tasks are difficult to accomplish. Even connecting small devices into the network is challenging due to complex user interfaces deviating a lot from comparable, civilian devices. In addition, set-up and troubleshooting of the information systems are difficult and time demanding. Putting high demands on the user, more time needs to

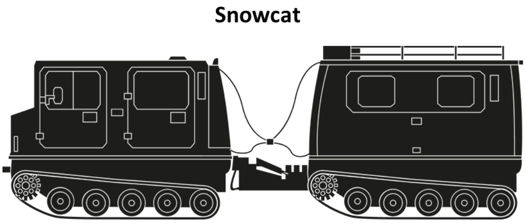


Figure 23: Snowcat

be spent on technical issues and less on operative tasks. This really is a huge problem as personnel reductions already challenge the manoeuvre warfare, creating holes in the operative structure.

The battalion focuses mainly on soldier skills, and with a high throughput and turnover it is difficult to build necessary skills in the lower levels of the unit. Small errors and user failures create a lot of frustration. The largest challenge is connected to the hardware, which is large and heavy with low battery capacity. It seems that the technical solutions are more adjusted to newer and larger vehicles, not to the traditional snowcat, introducing challenges related to integration of all the system parts. The battalion is supposed to be platform independent, but all the technical units expand the weight beyond what is possible to carry or move with alternative transportation.

Lack of interoperability with other systems and interoperability within the system are other challenges. The system consists of several different subsystems. Plans and orders therefore need to be transformed when exchanged from one system to another moving down the command hierarchy. Planning systems are employed as combat management systems, and the top level commanders require detailed and updated information about current operations on available systems at all times. In addition, the plans tend to be too comprehensive including too much information. As time passes by, more and more technical systems, not supporting battle force, are put on the lower levels of the command hierarchy. In addition, the technical systems are more vulnerable than earlier due to how information is distributed. Situational updates related to own units are done automatically all the time, giving all levels of the battalion the same information at the same time. The question arises then if this information is appropriately secured from a possible enemy? Otherwise the operative consequences will be enormous.

In addition, the majority of the technological systems employed by the unit seem to be under continuous development with new patches all the time, confusing the operators. This might be due to the fact that the developer and the project in total do not know exactly what the actual operative need is. The unit is not especially involved and represented in various projects for development of new technological systems. Power Point (PPT) is employed in addition to the military apps to support a better situational overview, and military apps are employed outside their expected use. The system also lacks apps to follow up supplies and maintenance, and additional spreadsheets are therefore in use.

Breakdowns of vehicles introduce additional obstacles, forcing the battalion to employ inappropriate, temporary underlying platforms. Computer breakage in command vehicles is also a challenge due to the computer configurations. It is not possible to just change the computer without reconfiguration. Another challenge related to solutions based on temporary platforms are that the technical systems are not adjusted to smaller, more mobile platforms. This is because of the system's number of computers, cables, screens and radios.

Obstacles to information collection and sharing

Limitations and challenges related to the technical platforms and lack of appropriate technical expertise introduce obstacles to information collection and sharing. Most of the problems are common to all army units, but no common decisions or solutions are present. All units need to find their own way due to lack of ownership and responsibility. The technical challenges include several issues. The user interface is difficult for the ordinary user, and not especially intuitive. The physical bandwidth limits the amount of information possible to send and receive across the communication network, especially related to large appendixes and pictures/live streams. Not all operators understand the necessity to reduce the amount of information sent within the network. Technical competence will also limit the ability to send and receive live stream, which might be a future requirement. Coverage and range limit the operational area and atmospheric conditions introduce additional challenges. The routines related to radio communication are adjusted to southern conditions, not taking into account differences between night and day in the various parts of the country.

Due to limitations in radio coverage, supplies are sometimes difficult to deliver outside the ordinary operational area. Due to random or lacking competence and experience, some of the communication systems are seldom in use, reducing the coverage area significantly. There are also limitations related to how information is distributed throughout the network. Information is distributed from the top node and down along the hierarchy, putting high demands on the receiver's ability to filter out unnecessary information as excessive appendixes and duplicated interpretations before distributing further down the hierarchy. In addition, the proper level of technical competence takes time to build, and turnover among technical personnel makes the skills a rare commodity - especially when they quit before new personnel are in place. Proprietary, military cables also hamper information

Figure 24: Atmospheric conditions introduce obstacles. (Photo used with permission from the Norwegian Defence).

sharing.

Many of the operations and exercises conducted by the Norwegian army units are based on collaboration with other nations or other Norwegian units. Proprietary systems and Norwegian cryptology restrict and prohibit information exchange with other units and foreign countries, introducing huge obstacles to information collection and sharing.

Another challenge related to information collection and sharing is duplication of messages, which can result in an unwanted overlap in information handling by one or more people. One person alone is not able to process all incoming information due to the amount of messages. The processing is more time consuming than earlier, putting high demands on the operator. In addition, the cognitive ability among the operators varies a lot. Not all operators are therefore suited to receive and handle all kinds of messages, and the roster has to take this into consideration. All the information also needs proper filtering before sent further down the line. The quality of the filtering depends on the operator's cognitive and processing abilities. Plans, orders and administration are mostly sent as messages, leaving the communication network more silent. On the flip side, messages require a higher level of management from the operators, as the mail system might present a wrong status for received and sent mails. Duplicate logs and time consuming follow ups are therefore required to ensure control and that the message is received in the other end. Also, the receiver is not notified that a message has been sent to be aware of available information. All these factors steal time from the actual operations, which is most critical in the lowest levels of the command hierarchy.

Information received from a unit above the battalion is often lacking crucial details related to communications and signals. The battalion then has to deduce the lacking information themselves, case in point: planning of radio coverage for the battalion during the brigade's movements. This is only possible due to heavy experience and coordination with neighbouring units. Misunderstandings might happen due to different dialects and language. By using English as a common language, some of the misunderstandings can be avoided.

Are the systems reliable and functional, enabling faster and easier task performance?

The technical information systems simplify many of the tasks related to operational planning and control and they are reliable most of the time. Situational drawings in the digital interface are also more precise than drawings on paper maps. The technical systems are formidable capacities, making it easier to find and read available information in low intensity periods. The technical systems support speed of command and are essential to achieve the necessary speed during operations. But the system's capacity is not utilized fully and the unit does not depend 100 percent on the technical information system. The technical systems are, however, a success factor for progress and precision. On the flip side, becoming too dependent of the systems might introduce additional vulnerabilities if the manual skills are reduced accordingly. A possible attack might disable the technological platform, challenging the unit's ability to continue the battle without technical support tools. Manual skills like navigation with a map and compass must therefore be maintained. This is to some extent a challenge already today, even if some of the participants rely on both manual and technical methods. In addition, the number of technical systems is increasing all the time and no standard operational procedures define what type of communication system to use for different kinds of messages. Therefore several systems must be monitored continuously. Introduction of new and more systems puts higher demands on the operators' competence. It also challenges the interoperability between the different systems.

If the set-up phase is done properly, the technical systems tend to function well during an exercise, but due to lacking competence this is not always the case. During high intensity periods, the operators fear that the systems will shut down resulting in lost information. The systems are functional when implemented in vehicles, but too heavy to carry when deployed by foot. The lacking options for recharging them further reduces their usefulness when deployed for more than several days at a time.

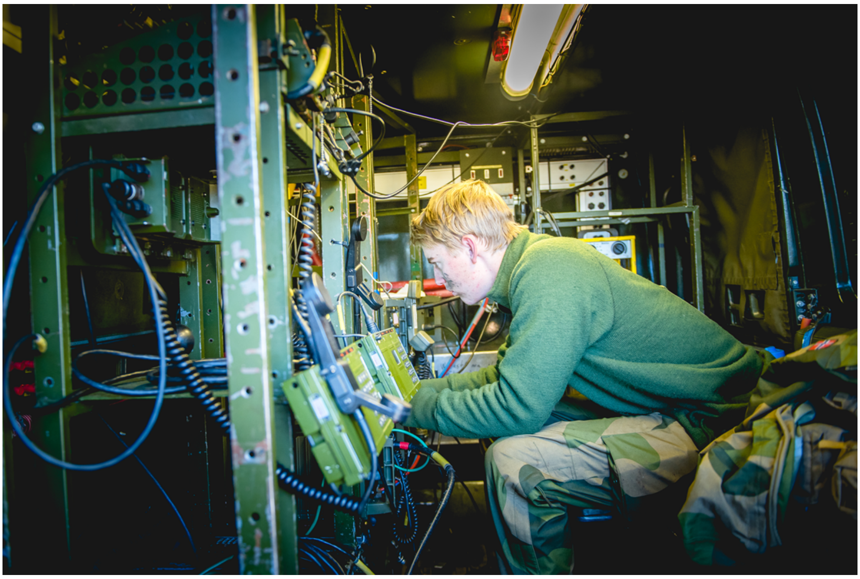


Figure 25: Hardware configuration inside vehicle. (Photo used with permission from the Norwegian Defence.)

Some of the lacking reliability is related to inappropriate hardware configuration, especially due to a huge amount of cables used to connect the various items inside the vehicle platform. New hardware is added to old hardware, introducing possible interference between different equipment. In addition, many antennas create additional challenges. There are no routines to handle breakages in the communication system inside a vehicle resulting in temporary solutions vulnerable to additional errors. Complete overhauls are never done; experience is therefore transferred from one driver to the next to account for inherent errors.

5.1.2 The users' knowledge for employing the technological platform

This section looks into the user's knowledge for how to utilize the technological platform in an appropriate manner either based on education, experience or training. This part of the analysis is mainly based on the questions belonging to competence and training.

Basic knowledge is achieved during education and courses related to the different subsystems, but the further down in the hierarchy one looks, the less education the operators get. And the technical competence in general is too low, also among young operators. Regardless of that, competency, training and experience are essential to achieve the necessary level of knowledge, depending on each individual's initiative for competency development. Practice is achieved during exercises in the

Figure 26: Practice during exercises. (Photo used with permission from the Norwegian Defence).

battalion and during deployment to international operations, where the tactical solutions are in use all the time. In addition, discussions and conversations with other persons with relevant knowledge serve to increase the personnel's competence. Different personnel in the unit hold expert competency on different systems, but all persons employing the technological platform need to be able to perform some level of troubleshooting, software set-up and cable checking.

Internal training related to the technological platform is to some extent implemented and adjusted to the different users and levels. Due to personnel reductions it is however more difficult to conduct internal training and courses. Internal learning and training also happen during exercises, ensuring a transfer of skills from experienced to less experienced personnel. In the company level, key personnel attend official courses related to technical information systems, and are given the responsibility to share their knowledge after the course is completed. The number and type of key personnel variates between the different companies, ranging from administration officers to platoon assistants, acting as signals officers in addition to their ordinary roles. Their knowledge and competency deviate; in addition they all have duplicate roles, complicating and challenging their ability to fulfil their responsibilities related to the technological platform.

The battalion is able to set-up the technological system to some extent, but a lot of hard work is required from some of the staff members. The technical expertise is mainly gathered in the top level of the battalion, educated at The Norwegian Defence University College of Engineering - Telematics. There are some random personnel with radio and technical competence out in the lower levels of the unit. Their competency is essential to make the systems work in the entire battalion, and is based on vested interest and voluntary training during several field exercises and deployments. Platoons and companies lacking this kind of competence struggle during the set-up phase and exercises especially when technical issues occur. They then have to rely on expertise from other companies and platoons. Their lack of technical competence also makes it difficult to explain problem issues and what kind of help they need. The respondents request a comprehensive approach for education and also a plan for regular repetition to maintain the necessary level of user competence related to radio and communication systems. They also emphasize that competence has to be duplicated in the future to make the systems function properly. In addition, there are challenges related to turnover with lacking routines for knowledge transfer from experienced to new personnel.

5.1.3 Knowledge about operational objectives and the situation

In this section, knowledge about the operational objectives and the situational picture among all participants are analysed based on answers from situational awareness.

The top level in the battalion updates the situational picture continually, and transmit the updates down in the command hierarchy. These routines ensure a more correct and updated situational picture throughout the entire battalion. The same picture can be sent both to the company staff and the battalion, but depends heavily on network capacity and radio coverage. In order to achieve situational awareness, the participants need to collect and seek information from several systems. The situational picture is updated continually in the graphical map interface during the operation, supporting command and control. In addition, radio communication is essential to understand the complete picture. Information achieved by dialogue and speech during meetings is also required.

By listening to relevant communication and coordinating with other units, it is possible to understand the situation and to plan the next phase. By coordinating directly with neighbour units, misunderstandings can be avoided. In addition, the commander can ensure that the unit is relevant to the mission and not misplaced, creating obstacles to the manoeuvre operation. It is necessary to think a ahead a bit in order to support the commander in an appropriate manner. But listening to the radio communication has become more difficult as more of the communication is done via messages as opposed to voice. More information distribution must therefore be done, leaving the company staff more as information managers than

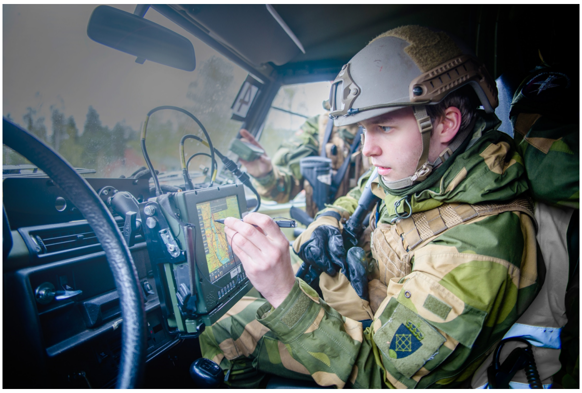


Figure 27: Technical platforms available in vehicle. (Photo used with permission from the Norwegian Defence).

company commanders supporting their units.

The participants agree that they often have enough information to understand the situation; but relying on several sources is complicated. And critical data has to be verified by speech introducing more time obstacles. The ability to understand and analyse available information depends to some extent on the individual's background, and experience is essential to comprehend the actual situational picture. Experience is also essential to understand how effective one's own operations are. In addition, personnel responsible for reporting must report correctly, evenly and timely putting high demands on the operator's cognitive ability.

Personnel with technical background tend to focus on technical issues, while operative personnel are able to understand and analyse the operative setting. Technical personnel are, however, able to realize more of the operative setting with sufficient operative experience. In order to comprehend more of the situational picture at an earlier stage, more operative competence would have been beneficial during The Norwegian Defence University College of Engineering - Telematics. Especially because many of the engineers educated at this college are employed at the higher levels in the battalion.

Information is available in different platforms when deployed by vehicle; everything becomes more difficult when units are deployed by foot. All technical equipment is large and heavy with insufficient battery capacity. It is therefore not practical or possible to carry all the platforms in such circumstances. Some new solutions show promising results, but their usefulness and stability are limited. The implementation is also delayed because the industry holds all the competence and decides new, expensive and unnecessary connections and cables.

It seems that the personnel are aware that registered information might be wrong or manipulated some times, but based on experience, the information seems to be correct most of the time. The quality of the information delivered will vary to some extent, depending on available time and ability to filter out essential information. Even with messages instead of voice, it is still important to think before sending information to not overload the receivers with large amounts of unnecessary information. Today, more messages are sent than earlier, and they tend to be more elaborating. This might result in more misunderstandings because different persons perceive words differently.

Some meta data is probably lost due to extensive use of messages instead of voice. Data messages hide the commander's emotions and feelings, which are important factors to understand the seriousness in different situations. Listening to higher commander's voice communication is therefore necessary to comprehend the complete situational picture. To complicate the situation further, the technical systems limit the possibility to update previous plans both due to the actual application and how the plan is distributed. Once the plan is distributed, it is difficult or even impossible to make updates to this plan.

5.1.4 Can information presented by the systems be trusted?

To analyse this issue, answers related to the operator's trust within the information are of interest. To what extent do the operators trust the information presented by the information systems and are they are aware that the information might be wrong, manipulated or incomplete?

The participants are aware that some of the information presented by the technological platform might be incomplete or outdated. Some participants are also sceptical to the information presented by the systems due to user errors resulting from lacking knowledge and competence. In addition, some of the position plots are done manually and also need to be removed manually. If the unit does not have proper routines to verify targets, the screen will be polluted with erroneous targets. But at the end of the day, the operational success will rely on humans. Today, old manual routines from the 80's are employed to avoid firing on friendly units due to incorrect graphical situational picture. To deal with the challenges related to the technical platform, the battalion demands centralized development of procedures with dedicated roles. With a comprehensive approach, it is possible to ensure uniform and timely reporting, ownership, distribution and to avoid double reporting of the same target. Today, there are lacking routines resulting in misplaced, duplicated and incorrectly plotted targets.

5.1.5 Suggestions for improvement

- Today, the technical solutions are tightly connected to systems developed about two decades ago, resulting in heavy and old fashioned equipment. By using the main ideas from the old systems, but base the new solutions on new technology, the equipment could have been lighter, more user friendly and more interoperable.

- Simplify the user interface making it more intuitive, because the technical platform will be employed when the user is tired and exhausted. The platform must be adjusted to the humans employing them and not the other way around.
- Make the solutions available also in garrison for regular practice and advocate a "work as you fight" mentality. With little practice inside the garrison, the user has to spend 1-2 days of practice before reaching the necessary level of skill again.
- Test and verify new technical solutions properly before released to the user to ensure correct functionality and minimal errors. Hence also reducing the number of patches afterwards.
- Using common materials and systems in all platforms to reduce some of the complexity.
- Implement improved and adjusted hardware. For instance lighter, thinner and more intuitive computers with lighter and smaller batteries reducing the weight.
- New solutions must be adjusted to the platforms the army employs, including both old and new vehicles in addition to possible deployments by foot covering the entire army's relevant need.
- Several levels of the users must be included in new projects in order to make the systems as relevant and user friendly as possible, in addition to make the solutions more plug-and-play.
- Develop improved and practical solutions during workshops with the supply chain.
- Make the systems more stable so they function all the time. The communication systems and the digital platform, hardware and software are perceived unstable by the users. This might be because new functionality continuously is added to an old platform.
- To reduce the uncertainty related to the communication systems, it is necessary with a comprehensive approach where implementation is followed by proper regulations, decisions and course plans. Today it seems that the competence decreases continuously. The systems arrive fast and are employed accordingly without any predetermined procedures or educational plans. This situation will get even worse if not followed up properly.
- Implement education focusing on tactical technical solutions during the officer's school in order to increase the various commanders' technical and user

competence related to the technical platform. Today a digital learning platform is totally absent during the education, not employed during exercises nor practical training at all.
- Implement a lighter plan process reducing the amount of information sent down along the hierarchy.
- Implement civilian protected solutions with encrypted cards similar to other NATO countries, and employ COTS where possible.
- The army needs digital guidelines, standard operational procedures and centralized user forums for technical communication platforms. Today most of the competence is in the user domain.

5.2 Results from interviews conducted in army unit 2.

The transcribed interviews appended to this project report for unit 2 are the basis for the analyses conducted in this section. The results will be presented looking into knowledge from different angles affecting military operations and the successfulness of implementing Network Based Defence. The results are referred in the same manner as described in chapter 3:

- Knowledge for how to develop a technological platform supporting military operations, putting high demands on the developer.
- The user's knowledge of how to utilize the technological platform in an appropriate manner either based on education, course, experience or training.
- Knowledge about the operational objectives and the situational picture during military operations among all participants.
- Know to what extent it is possible to trust information presented by the technological platform.

Suggestions for improvement are also included. The analysed interviews describe common issues pointed out by the majority of the respondents, but also significant challenges or benefits pointed out by single individuals.

5.2.1 Knowledge for developing the technological platform

This section looks into knowledge for how to develop a technological platform to support military operations. To achieve sufficient development knowledge, high demands are put on the developer and other resources supporting the development. The analyses are based on the answers related to the following questions:

- How well are the technical solutions adjusted to the unit's operative needs?
- How well do the technical solutions support information collection and sharing?
- What are the obstacles to information sharing?

- How reliable and functional are the technical systems? (Enable faster and easier task performance?)

Technical solution adjusted to the unit's operative need?

In general, the technical systems employed by the battalion seem to work, and most of the operators are aware of how to use the most basic functions. The unit uses several radio systems ensuring redundancy and different frequencies supporting various ranges. The radios support both speech and data communication, which are the planning and command and control systems for the battalion. The design of the technical systems seems to only partly support the operational requirements, and the systems function only to some extent. Lack of interoperability with other systems and interoperability within the system are other challenges. Plans and orders need to be transformed when exchanged from one system to another. In addition, the majority of the technological systems employed by the unit seem to be under continuous development with new patches all the time, confusing the operators. This might be due to the fact that the developer and the project in total do not know exactly what the actual operative need is. The unit, represented by the top level technicians, therefore needs to spend a lot of time with the project and industry informally to suggest improvements and to report errors.

The more advanced part of the tactical platforms is employed by the top level in the battalion, but the advanced current modules are not very well suited to the lower levels need. Either they are cumbersome or they do not cover the full spectrum of functions the battalion need. Power Point is employed in addition to military apps to support a better situational overview, and military apps are employed outside their expected use. The system also lacks apps to follow up supplies and maintenance, and additional spreadsheets are therefore in use.

Proprietary systems employed by some of the units in the battalion are not adjusted to the rest of the platform. The user interface of these respective systems might be even more difficult than the user interface for the ordinary systems. Strict regulations related to safety (for the personnel) introduce challenges due to lack of interoperability with the common systems. The systems are not connected, and hardware limitations make duplication impossible. One system must be monitored at the time, leaving potentially new information from the other systems unchecked. On the flip side, strict regulations related to safety ensure that messages are correct when they are sent, because they need to include some predefined fields. In addition, the messages must be controlled by all levels when sent along the command hierarchy, which is an absolute success factor.

The technical platforms are becoming increasingly complex and advanced, putting high demands on the operators and the technical support personnel. More time has to be spent both to understand and use the technological platform at the cost of manual and vital skills in all levels of the battalion. In addition, the tactical systems are tightly connected to the physical platform they belong to. Breakdowns of vehicles introduce additional obstacles, forcing the battalion to employ inappropriate temporary underlying platforms. Personnel with the right technical and operative competence are therefore essential but scarce today. The operative need is only covered randomly by competence available in the unit harbouring the actual need. The objective is to increase the number of officers with technical expertise in all levels to ensure redundancy and reduce problems related to turnover. Today technical civilian suppliers often are involved to help solve problems outside the reach of the unit's own competence.

Information collection and sharing also including obstacles.

Limitations and challenges related to the technical platforms and lack of appropriate technical expertise introduce obstacles to information collection and sharing. Most of the problems are common to all army units, but no common decisions or solutions are present. All units need to find their own way due to lack of ownership and responsibility. The technical challenges include several issues. The user interface is difficult for the ordinary user and not especially intuitive. The physical bandwidth limits the amount of information possible to send and receive across the communication network, especially related to large appendixes and pictures/live streams. The communication network is the underlying transmission system and physical connection for the command and control system. Coverage and range limit the operational area and there are limitations related to how information is distributed throughout the network. Information is distributed from the top node and down along the hierarchy, putting high demands on the receiver's ability to filter out unnecessary information. Excessive appendixes and duplicated interpretations must be filtered out before being distributed further down the hierarchy. Proprietary ports and military cables also hamper information sharing.

Most of the plans and orders are sent as messages, leaving the communication network more silent. On the flip side, messages require a higher level of management from the operators, as the mail system might present a wrong status for received and sent mails. Duplicate logs and time consuming follow ups are therefore required to ensure control. This steals time from the actual operations which is most critical in the lowest levels of the command hierarchy. Too much focus on the technical systems and a hectic environment might result in information not reaching the intended destination.

When the information is received, misunderstandings and misinterpretations may still occur. The messages need to be concise, precise and structured in a good manner in order to be understood and utilized. Standard formats that denote whether or not the information is factual, speculative or conclusive is there-

Figure 28: Communication network supporting command and control system. (Photo used with permission from the Norwegian Defence).

fore essential. The receiver also needs to be notified that a message is sent to be aware of available information. But sometimes the routines fail, resulting in lost and misinterpreted information.

Many of the operations and exercises conducted by the Norwegian army are based on collaboration with other nations. The Norwegian systems use cryptology with strict regulations, prohibiting information exchange with foreign countries, which introduces huge obstacles to information collection and sharing.

Are the systems reliable and functional, enabling faster and easier task performance?

The technical information systems simplify many of the tasks related to operational planning and control and they are functional and reliable most of the time. In addition, the technical systems support speed of command and are paramount to achieving the necessary speed during operations. The unit does not depend 100 percent on the technical information system, but it is a success factor for progress and precision – making the same task faster and ensuring information sharing with others. On the flip side, becoming too dependent of the systems might introduce additional vulnerabilities if the manual skills are reduced accordingly. A possible attack might disable the technological platform, challenging the unit's ability to continue the battle only with manual procedures. Manual skills like navigation with a map and compass, and old routines as manually distribution of information and orders by foot or car, must therefore be maintained.

The technical systems prevent distinctiveness, resulting in both positive and negative effects. In addition, too much information becomes available, exhausting the operators which in turn results in low utilization of the systems. The number of technical systems is increasing all the time. Standard operational procedures are therefore necessary to define what type of communication to use for different kinds of messages. There are internal procedures already in place in the battalion, but such procedures are only loosely implemented at higher levels in the hierarchy. Thus, monitoring several systems simultaneously is a necessity.

5.2.2 The user's knowledge for employing the technological platform

This section looks into the user's knowledge for how to utilize the technological platform in an appropriate manner either based on education, experience or training. This part of the analysis is mainly based on the questions pertaining to competence and training. The analysis will mainly be based on answers related to how the operators are educated and trained. Internal education is also part of this issue.

Some of the respondents have formal education related to some or all of the technical systems. The respondents request a comprehensive approach related to education and also a plan for regular repetition to maintain the necessary level of user competence. Personnel participate at random based on initiative and available time. User manuals are not developed when new patches are released, even if the user interface is changed. Technical solutions outside the ordinary technical platform are totally left alone and competence building among technical personnel are based on close interaction with the industry. The industry offers courses at random limited to few participants.

Education is to some extent necessary, but regular practice based on vested interest and curiosity is essential to employ the solutions properly and get insight into advanced functionality. This applies both to the underlying radio systems and the technical platform supporting command and control. Practice is achieved during exercises in the battalion and during deployments to international operations, where the tactical solutions are in use all the time. On the flip side, stationary service inside a garrison in Norway gives little practice. The user then has to spend 1-2 days of practice before reaching the necessary level of competence again. In addition to technical skills, the soldiers and officers need to master their weapons, sanitary skills and other military skills.

The unit also conducts courses for new personnel; level 1 and 2 courses to increase the common knowledge for everybody, and level 3 courses to motivate and teach the cleverest. Level 3 courses are held by external instructors with advanced knowledge about a subject related to the technical platform. In addition, they have regular meetings for exchange of experiences related to the technical platform. Interaction with other relevant technical environments and developers is also necessary to achieve the required competence, because the battalion employs many, complex systems. In some circumstances, engineering competence alone is sufficient to understand the complex and large computer networks the command and control system relies on. Technical personnel need a comprehensive overview to understand how everything is connected in addition to operative signals education. One big challenge is related to turnover. There is no good plan for the transferral of knowledge to new personnel when experienced and competent personnel are leaving.

5.2.3 Knowledge about operational objectives and the situation

In this section, knowledge about the operational objectives and the situational picture among all participants is investigated. To analyse this issue, answers from situational awareness are investigated. More specifically, answers related to the operator's ability to perceive, comprehend and predict their own and the enemy's situation is investigated.

The participants more or less command a situational overview depending on their role. Education together with experience and practice is necessary to achieve an appropriate level of situational awareness related to the operators' current level in the command hierarchy. With appropriate experience, it is possible to foresee what the enemy is able to do, and consider the possible courses of actions. Some of the roles are more dedicated to the actual and current situation than others, especially the operational officer. Technical personnel might for instance need to focus on technical challenges and challenges related to the communication at the cost of the operational picture. They therefore need regular updates from the operational officer to keep track of the ongoing operations. If the situational overview is lacking, the technical support will not be adjusted to the recognized picture and thus be inept to properly support troop movement.

In order to achieve situational awareness, the participants need to collect and seek information from several systems. The operational orders ensure basic understanding for the operation by emphasizing intentions, objectives and directions. The situational picture is updated continually in the graphical map interface during the operation, supporting command and control. In addition, radio communication is essential in order to understand the complete picture. Information achieved by dialogue and speech during meetings is also crucial. To ensure hereditary succession it is important that also the lower levels have enough information, depending on information distributed down along the hierarchy. To avoid misunderstandings, all levels of the hierarchy coordinate directly with other units at the same or different levels to verify that their perceived situational awareness is correct. Misunderstandings still happen and sometimes result in events with the possibility of escalating to incidents. There are no formal routines for registering events or incidents in the unit, but are discussed during back brief sessions at random. By listening to relevant communication and coordinate with other units, the commander can ensure that the unit is relevant for the mission and not misplaced creating obstacles to the manoeuvre operation.

Correct situational awareness is critical, especially with regard to avoiding friendly fire when utilizing heavy ordinance such as missiles and artillery. Verification by speech is therefore necessary, but time consuming and tiring for the personnel. In addition, most of the information is collected and refined by the lower levels before being exchanged with the higher levels, complicating the situation further. A high level of cognitive ability is therefore required among operators at the lower levels, responsible both for the operative progress and the timely reporting of verified information up in the command hierarchy.. Time critical information is sent as speech in a standard format to avoid misunderstandings. To make the messages as precise as possible, the operators need to analyse all their observations based on earlier experience and presumed patterns of the enemy's behaviour. Because the analyses are conducted by human operators, the respondents point out the importance of knowing the skills and trustworthiness of their team mates in order to trust the information.

Most of the participants agree that they have enough information to make the right decisions and judgements. However, an increased use of sensors increases the amount of information available, challenging the ability to process and comprehend all the information. In the future, human operators will probably not be able to analyse all the information without automated systems. To complicate the situation further, the technical systems limit the possibility to update previous plans both due to the actual app and how the plan is distributed. Once the plan is distributed, it is difficult or even impossible to make updates to this plan. Units without radio coverage will not receive the distributed plan, or even know that a plan has been distributed at all. The sender will not be aware of units lacking the newest information, resulting in units with different situational pictures. In addition, it is difficult to update units far away from the information source in a timely manner.

The users are to some extent able to predict the enemy's next step, but this depends on access to information from different sources. The operational orders contain intention and possible enemy actions. By correlating this information with the graphical picture that includes position updates and historical data, some predictions can be done. In addition, a close and regular dialogue with the human

Figure 29: Peripheral units also need timely updates. (Photo used with permission from the Norwegian Defence).

sensors out in the field is necessary to get a comprehensive understanding. Speech is equally important as watching maps; and the speed of using speech is superior to digital data plots. The respondents agree that available information is enough to plan the next phase, but it is necessary to remove noise and old information from the digital systems.

5.2.4 Can information presented by the systems be trusted?

To analyse this issue, answers pertaining to the operators trust to the information are of interest. To what extent do the operators trust the information presented by the information systems and are they are aware that the information might be wrong, manipulated or incomplete?

The participants are aware that some of the information presented by the technological platform might be incomplete or outdated, but point out that the ordinary user tends to trust and depend on the graphical interface completely. Some technical sensors give inaccurate information leaving the interpretation to the receiver. Other technical platforms are so complex that the users are not employing all the systems properly. Sometimes operations are conducted faster than the system is able to update the situation virtually. If the operators are not aware of this fact, misunderstandings and incidents can happen. Common sense is therefore very important. In addition, some of the targets are plotted manually and also need to be removed manually. If the unit does not have proper routines to follow up this issue, the screen will be polluted with erroneous or non-existing targets. In the battalion, procedures based on dedicated roles are developed in order to ensure uniform and timely reporting, ownership, distribution and to avoid double reporting of the same target. The practical implementation is albeit not quit up to speed yet.

In addition, new parts and versions of the technological platform are not tested properly before being released to the user, and contain a lot of errors. If the errors have large impacts, the user's trust in the platform itself might be reduced, resulting in users returning to old solutions. The user also becomes a major part of the test and verification environment. In some circumstances, it is not possible to improve the solutions after implementation due to lack of resources, leaving the user with an incomplete and faulty solution.

5.2.5 Suggestions for improvement:

- Using common materials and systems in all platforms would reduce some of the complexity, enabling use of technical and communication experts interchangeable and independently of the platform type. By using a comprehensive approach, systems could interact with each other, enhancing the information sharing due to fewer communication channels. To achieve such an objective, standardizing would be necessary. Easy in theory, but difficult in practice, especially because demands related to security act against operational needs introducing vulnerabilities due to small, simple errors.
- Simplify the user interface, making it more intuitive.
- Make the systems more stable so they function all the time. The communication systems and the digital platform, hardware and software, are perceived unstable by the users. Today, systems will stop functioning during operations, introducing an unnecessary layer of issues into the ongoing mission. This might be because new functionality is continuously added to an old platform. The users also question why the systems are not stable after this long period of development.
- New technical solutions should have been tested and verified properly before released to the user to ensure correct functionality and minimal errors. By implementing proper test and verification procedures before release, the systems would be more mature. The user would then have more confidence in and trust in the solution, even more willing to use it.
- In order to increase the platoon commander's technical and user competence related to the technical platform, it is necessary to implement education, focusing on tactical technical solutions during the officer's school. Today this is totally absent during the education, not clinically employed during exercises

nor practical training at all.

- To reduce the uncertainty related to the communication systems, it is necessary with a comprehensive approach where implementation is followed by proper regulations, decisions and course plans. Today, the systems arrive fast and are employed accordingly without any predetermined procedures. This situation will get even worse if not followed up properly.
- Today the technical solutions are tightly connected to systems developed about two decades ago, resulting in heavy and old fashioned equipment. By using the main ideas from the old systems, but base the new solutions on new technology, the equipment could have been lighter and more user friendly. Weight is especially limiting to troop mobility in the context of today's solutions.
- Exercises at the top level are conducted very seldom, leaving the operators at this level with minimal practice. The respondents worry if the competence at this level is up to speed.
- Several levels of the users must be included in new projects in order to make the systems as relevant and user friendly as possible. The best would be if the solutions were more plug-and-play.

5.3 Summary of findings from the interviews

This section includes a summery of the findings from interviews conducted in army unit 1 and 2.

Knowledge for developing a military technological platform

In general, the technical systems seem to work most of the time and support the military units during their operations. The technique behind the systems is fairly well suited to the units, but the technical systems are too difficult to employ for the user both due to the system's complexity and the little intuitive user interface. The operators are therefore forced to spend more time on the technological platform than on manual and vital skills. Most of the systems seem to be under continuous development, resulting in new patches all the time. The tactical technical platform is not very well adjusted to all levels in the battalions, and the need for using different underlying vehicle platforms seems not to be accounted for. Employing the technical platforms by foot is even more challenging due to large and heavy equipment. Different systems are not connected and cannot communicate with each other, challenging interoperability also with other nations. In addition, interoperability is a huge challenge related to Norwegian security regulations. Personnel with correct, technical and operative competence are scarce and only covered at random. Technical civilian suppliers are therefore sometimes involved to solve technical issues.

Figure 30: Military forces employ technical systems also by foot. (Photo used with permission from the Norwegian Defence).

In addition, both technical and human limitations introduce challenges for information collection and sharing. Most of the problems are common to all army units, but no common decisions or solutions are present. All units need to find their own way due to lack of ownership and responsibility. Physical bandwidth, coverage and range limit the operational area and the amount of information possible to distribute across the communication network. The routines related to radio communication are adjusted to southern conditions. The shift from voice to data transmissions has resulted in a more silent network. On the flip side, messages require a higher level of management from the operators, as the mail system might present a wrong status for received and sent mails. Duplicate logs and time consuming follow ups are therefore required to ensure control and that the message is received in the other end. All this steal time from the actual operations. Proprietary ports and military cables also hamper the information sharing. In addition, the technical systems limit the possibility to update previous plans both due to the actual app and how the plan is distributed.

The technical information systems simplify many of the tasks related to operational planning and control. The information systems employed by the units support speed of command and are crucial to achieve the necessary speed during operations. The information system is also a success factor for progress and precision. But becoming too dependent of the systems might introduce additional vulnerabilities if the manual skills are reduced accordingly. A possible attack might disable the technological platform, challenging the unit's ability to continue the battle with manual procedures.

The increased number of technical systems and sensors implemented also result in an increasing amount of information the operators have to monitor, process and filter out before distributing the information further. In addition, messages and plans are too comprehensive including too much information, and top level commanders require detailed and updated information all the time. The result might be exhausted operators and low utilization of the systems. As situational updates are distributed continuously, this might introduce additional vulnerabilities if not secured properly.

Inappropriate hardware configurations with a huge amount of cables and antennas inside the vehicle platform challenge the reliability. New hardware is added to old hardware, and maintenance of the underlying technical system inside the vehicle is totally absent; experience is therefore transferred from one driver to the next to account for inherent errors.

The user's knowledge for how to utilize the technological platform

The operator's knowledge for how to utilize the technological platform varies in both the units, but unit 2 seems to be more resourced related to technical competence than unit 1. Unit 2 conducts regular courses for new personnel and advanced courses for super users. Unit 2 also has more dedicated personnel for technical tasks. Unit 1 even struggles with small technical tasks and lacks dedicated technical personnel at the lower levels of the command hierarchy due to personnel reductions. Both units have large challenges related to turnover and competence transfer, especially in the lower levels of the battalion. There are also other similarities. Education is to some extent necessary, but regular practice based on vested interest and curiosity is essential to employ the technical solutions properly and get insight into advanced functionality. In some circumstances, engineering competence alone is sufficient to understand the complex and large computer networks employed by the units.

Only some of the respondents have formal education related to the technical systems and participate at random based on initiative and available time. And the time is limited because the operators also need to master skills as weapons and sanitary in addition to technical skills. There is no comprehensive approach related to education, and user manuals are not developed when new patches are released.

Knowledge about operational objectives and the situation

Education together with experience and practice are necessary to achieve the required level of situational awareness related to the operator's current level in the command hierarchy. Most of the participants agree that they have enough information to make the right decisions and judgements related to the operation, but there are some challenges. Several assumptions must be present in order to achieve necessary situational awareness. Information must be collected from several systems, including both manual and technical systems. Noise and old information must be removed manually from the graphical interface. To verify that perceived situational awareness is correct and to avoid misunderstandings all levels of the hierarchy coordinate directly with other units at the same or different levels. Misunderstandings still happen and sometimes result in events with the possibility of escalating to incidents. None of the units seem to have proper routines for registering events or incidents. Time consuming voice verification happens all the time. Information is collected and refined at the lower levels, requiring a high level of cognitive ability and proper experience among the operators.

Can information presented by the systems be trusted?

The participants are aware that some of the information presented by the technological platform might be incomplete or outdated, but point out that the ordinary user tends to trust and depend on the graphical interface completely. There are several sources suggesting that information might be incorrect our outdated. Technical sensors giving location plots can give inaccurate information, leaving the interpretation to the receiver. Operations are conducted faster than the system is able to update the situation virtually. Some of the targets are plotted manually and can be misplaced, duplicated or incorrect. The manually plotted targets also need to be removed manually. The technical platforms are so complex that the users are not employing all the systems properly. New parts and versions of the technological platform are not tested properly before released and contain a lot of errors. This might reduce the user's trust to the platform itself. Some meta data might be lost due to extensive use of messages instead of voice. Data messages hide the commander's emotions and feelings, which are important factors to understand the seriousness in different situations.

Suggestions from the respondents for improvement of the current situation

Several suggestions from the respondents were made for how to improve the current situation. Common materials and systems in all platforms would reduce some of the complexity. By simplifying the interface, the solution would become more intuitive and user friendly. Making the systems more stable would improve the reliability. Proper test and verification before released to the user could ensure more correct functionality and minimal errors. Implementation of technological platforms should have a comprehensive approach including proper regulations, decisions, procedures and education plans. Education focusing on tactical technical solutions during the officer's school should for instance be implemented. By making the solutions available also in garrison, regular practice is possible and advocate a "work as you fight" mentality. Digital guidelines, standard operational procedures (SOP) and centralized user forums for technical communication platforms should be implemented on a parent level ensuring uniformity. Several levels of the operators ought to be involved in new projects to make the systems as relevant, user friendly and plug-and-play as possible. New solutions and technology should be lighter, more relevant and adjusted for all parts of the army, including both old and new vehicles in addition to possible deployments by foot. Implementing civilian protected solutions with encrypted cards as other NATO countries should be viable options.

5.4 Results from questionnaires

Questionnaires were conducted in army unit 1 and 2. Only 2 respondents participated in army unit 1, 15 in army unit 2. All the results will still be analysed and compared to results found during the interviews. To ensure confidentiality for the respondents, the two answers from army unit 1 will be included in the answers from army unit 2.

The results from the questionnaires represent answers from 17 participants from the top level, intermediate level and lowest level of the battalion. The questionnaire included 7 subsections and they will be referred accordingly. The respondents had 5 choices for all the questions; disagree, partly disagree, partly agree, agree or I don't know. The exact results can be found in appendix E. The same results are illustrated in figure 31 and 32.

5.4.1 Technical information systems

Most of the respondents are to some extent satisfied with the technical information systems employed by the unit. Half of the respondents only partly agree that the technical support tools are well adjusted to their unit suggestion that the solutions are not optimal.

5.4.2 Competence and training

The majority of the participants agreed to hold enough education and experience to perform their duties and to understand and analyse information presented by the systems. Most of the respondents only partly agreed to hold enough competence to utilize the technical platform. The majority of the respondents had education for some of the systems, but experience seems equal important as education to understand how the systems can support the respondents' information need. The respondents partly agreed that their unit spend enough time on internal training, suggesting that the participants miss some internal learning focusing on the tech-

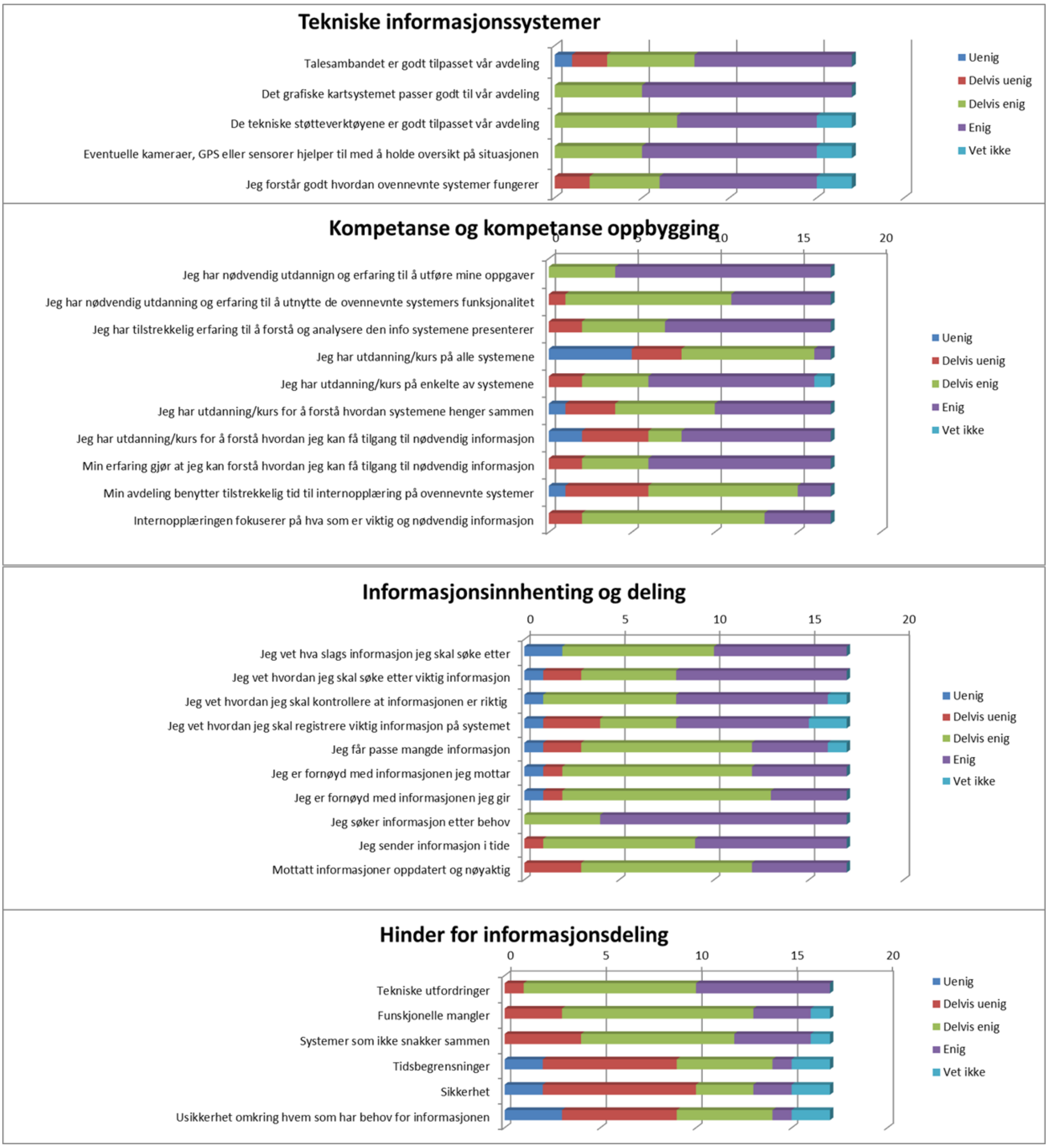


Figure 31: Results from the questionnaire conducted in army unit 1 and 2 illustrated by graphs - part 1

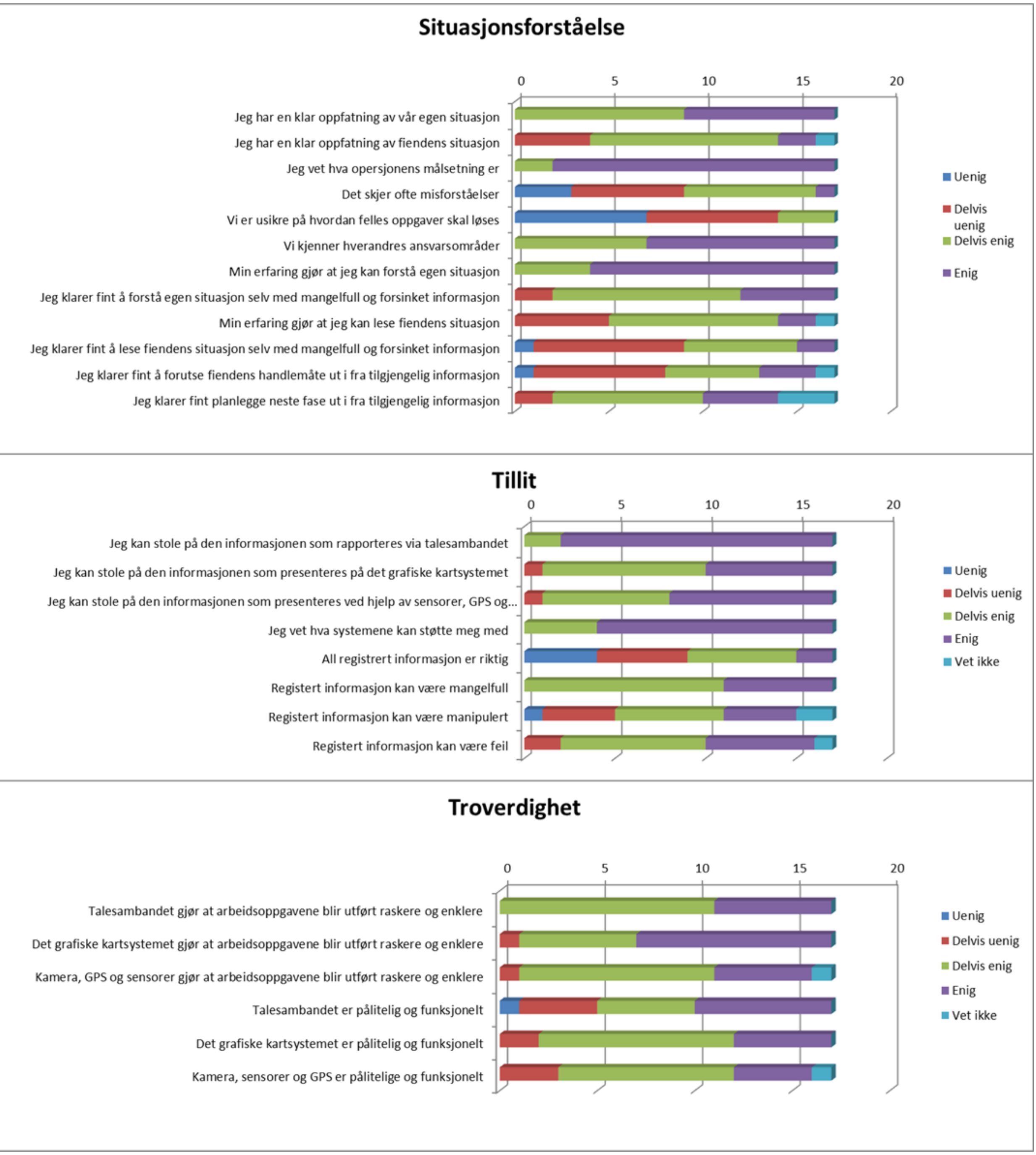


Figure 32: Results from the questionnaire conducted in army unit 1 and 2 illustrated by graphs - part 2

nical platform.

5.4.3 Information collection and sharing

There were separated opinions related to information collection and verification. Half of the respondents only partly agreed to know what kind of information to search for, how to do it and how to verify the information. The majority of the participants only partly agreed to receive enough information and they were only partly satisfied with received and sent information due to lack of timeliness and quality. They agreed to seek information on demand.

5.4.4 Obstacles to information sharing

Technical challenges, functional errors and systems not talking together seem to be the main obstacles to information sharing. Only a minority of the participants point out time limitations and security as obstacles to information sharing. There are some uncertainties related to who will need the information.

5.4.5 Situational awareness

The mission's objective is obvious for all the respondents, and most of the respondents are aware of each others responsibilities. All the participants are more or less aware of their own situation, but less updated on the enemy situation. Misunderstandings happen sometimes. Experience seems to be essential to understand own situation also with lacking and delayed information. More of the respondents struggle to understand the enemy situation and predict the enemy's next move based on experience and available information. Some of the respondents are able to plan the next phase of the operation based on available information.

5.4.6 Trust

All the participants agree that they can trust the information obtained by the communication system. There is more uncertainty related to how much information from other technical systems can be trusted. The majority knows how the technical systems can support the operations. Most of the participants seem to some extent to be aware that information presented by the systems might be incorrect, either due to lacking details, that the information can be manipulated or wrong.

5.4.7 Trustworthiness

All the participants more or less agree that all the technical information systems enable faster task performance. Most of the participants also agree that the systems are functional and reliable to some extent, but there are some deviations related to this issue.

5.5 Summary of findings from interviews and questionnaire

This section includes a summery and a correlation of the findings from the interviews and the questionnaire. The section also seeks to elaborate answers related to research question 2: Which factors related to knowledge affect the implementation of Network Based Defence?

Knowledge for developing a military technological platform

Based on the results from the questionnaire, most of the respondents seem pretty satisfied with the technical information systems, but indications show that the technical support tools are not very well adjusted to their unit. These indications are supported by the findings from the interviews, emphasizing that complexity, difficult user interfaces and continuous development challenge the use of the technological platform. It also requires good, technical expertise which is a scarce resource. Lack of ownership and responsibility seem to result in lack of common solutions. Different vehicle platforms and deployment by foot is not accounted for due to large and heavy equipment. The lack of interoperability within the system and with other nations also support the assumption of unadjusted solutions.

Information collection and sharing also including obstacles to information sharing. Results from the questionnaire indicate that half of the respondents only partly know what kind of information to search for, how to do it and how to verify the information. They were only partly satisfied with received information both due to timeliness and quality. All agreed to seek information on demand. Technical challenges, functional errors and systems not talking together seem to be the main obstacles to information sharing. Only a minority of the participants point out time limitations and security as obstacles to information sharing.

The results from the questionnaire are supported by several findings from the interviews. Even if the technical information systems simplify many of the tasks related to operational planning and control, physical bandwidth, coverage and range limit the operational area and the amount of information possible to send and receive. Hence, more time has to be spent to follow up that messages are received and understood, stealing time from the actual operations. Proprietary ports and military cables hamper the information sharing. Being too dependent of the systems might introduce additional vulnerabilities if the manual skills are reduced accordingly, especially if the technological platform is disabled.

The operators have to monitor, process and filter out an increasing amount of information before being distributed further. Messages and plans are comprehensive including too much information, and commanders require detailed and updated information all the time. The huge amount of information also introduces additional vulnerabilities if not secured properly.

Trustworthiness All the participants in the questionnaire more or less agreed that all the technical information systems enable faster task performance and that the systems are functional and reliable to some extent. Based on the answers from the interviews, the reliability seems challenged by inappropriate hardware configurations, and that new hardware is added to old hardware continuously without maintenance.

The user's knowledge of how to utilize the technological platform

Results from the questionnaire indicate that the participants hold enough education and experience to perform their duties and to understand and analyse information presented by the systems. Experience was emphasized as an important factor for information comprehension. The participants seemed to lack some competence to fully utilize the technological platform. Arguments to explain the findings in the questionnaire can be found in the interviews. There are variations between the two army units suggesting that army unit 2 is more resourced related to technical competence. They also conduct more regular courses. Unit 1 struggles with small technical tasks and lacks dedicated technical personnel at the lower levels due to personnel reductions. Both units have large challenges related to turnover and competence transfer. Knowledge for how to utilize the technological platform varies in both the units. Regular practice based on vested interest and curiosity is essential to employ the solutions properly and get insight into advanced functionality. In general, there is no comprehensive approach related to education, and user manuals are not developed when new patches are released. This is a problem issue the respondents address to a higher level of the military.

Knowledge about operational objectives and the situation

According to the answers from the questionnaire, the mission's objective seems obvious for all the respondents and all of the participants seem more or less aware of their own situation. There are more uncertainties related to the enemy's situation and misunderstandings happen sometimes. Experience seems crucial to achieve situational awareness and to plan the next phase based on available information. Correlations can be found in the answers from the interviews. Education together with experience is necessary to achieve the required level of situational awareness. Most of the participants agree to hold enough information to make the right decisions and judgements related to the operation, but there are some challenges. Information must be collected from several systems, including both manual and technical systems. Noise and old information must be removed manually. To verify that perceived situational awareness is correct and to avoid misunderstandings, coordination is done by voice all the time. Misunderstandings still happen and sometimes result in events with the possibility to escalate to incidents. None of the units seem to have proper routines for registering events or incidents. Information collection and refinement at the lower levels require a high level of cognitive ability among the operators.

Can information presented by the systems be trusted?

Results from the questionnaire indicate that the participants trust the information presented by the communication system, but there is more uncertainty related to information presented by other technical systems. The participants seem to some extent to be aware that information presented by the systems might be incorrect due to lacking details, that they are manipulated or wrong. Correlations can be found in the answers from the interviews.

Even if the participants are aware that some of the information presented by the technological platform might be incomplete or outdated, the ordinary user tends to trust and depend on the graphical interface completely. However, the graphical interface might be incorrect or include outdated information as a result of technical sensors giving inaccurate location plots, or that operations are conducted faster than the system is able to update the situation virtually. Some of the targets are plotted manually and can be misplaced, duplicated or wrong. The targets also need to be removed manually. Due to complexity, the technical platforms are not employed properly. Test and verification are not done before released, possibly resulting in reduced trust to the platform. And at the end of the day, the operational success will rely on humans. Appropriate trust is therefore necessary to achieve the stated objectives of Network Based Defence.

Suggestions from the respondents for improvement of the current situation

During the interviews, the participants presented several suggestions for improvement:

- Implement common materials and systems in all platforms to reduce the complexity.
- Simplify the user interface making it more intuitive and user friendly.
- Make the systems more stable to improve the reliability.
- Implement proper test and verification procedures to ensure more correct functionality and reduce the number of errors.
- Develop a comprehensive approach for the implementation of technological platforms including proper regulations, decisions, procedures and education plans.
- Implement education focusing on tactical technical solutions during the officer's school.
- Making the solutions available also in garrison to enable a "work as you fight" mentality.

- Implement digital guidelines, standard operational procedures (SOP) and centralized user forums on a parent level.
- Involve several levels of the operators in new projects to ensure relevant, user friendly and plug-and-play systems.
- Develop lighter, more relevant and adjusted technology relevant to all parts of the army.
- Implement civilian protected solutions with encrypted cards.

How this Master thesis answers research questions 1 and 2

- **Q2: Which factors related to knowledge affect the implementation of Network Based Defence?**
    - **Knowledge for developing a military technological platform**
        1. The technical support tools are not very well adjusted to the units' operative need. Complexity, difficult user interfaces and continuous development challenge the use of the technological platform.
        2. Good, technical expertise is necessary but a scarce resource.
        3. Lack of common solutions due to lack of ownership and responsibility.
        4. The systems are not adjusted to different platforms.
        5. The systems are not interoperable with other nations.
        6. The technical information systems simplify tasks.
        7. Physical bandwidth, coverage and range limit the operational area and the amount of information possible to send and receive.
        8. Time consuming follow ups steal time from the actual operations.
        9. Proprietary ports and military cables hamper the information sharing.
        10. Additional vulnerabilities are introduced if the manual skills are reduced and the technological platform disabled during operations.
        11. The increasing amount of information introduces additional vulnerabilities if not secured properly. It also requires a high level of cognitive ability among the operators.
        12. The technical information systems enable faster task performance.
        13. Reliability are challenged by inappropriate hardware configurations with new hardware added to old hardware.
    - **The user's knowledge of how to utilize the technological platform**
        1. The operators seem to hold enough education and experience to perform their duties and to analyse information presented by the systems.

2. They lack some competence to fully utilize the technological platform, but unit 2 seems to be more resourced than unit 1 related to technical competence.
3. Both units have large challenges related to turnover.
4. Vested interest and curiosity are crucial to employ the solutions properly and get insight into advanced functionality.
5. The lack of a comprehensive approach related to education and development of user manuals introduce additional challenges.

- **Knowledge about operational objectives and the situation**

  1. The mission's objective are obvious for the respondents.
  2. They are more or less aware of their own situation, but more uncertain of the enemy situation.
  3. Education together with experience are necessary to achieve the necessary level of situational awareness.

- **Q3: How are the identified factors related to knowledge and situational awareness affecting the operators' perceived trust level?**

  - **Knowledge about operational objectives and the situation**

    1. Information must be collected from several systems to achieve appropriate level of situational awareness.
    2. Noise and old information must be removed manually.
    3. Coordination is done by voice all the time to verify information and to avoid misunderstandings.
    4. Misunderstandings still happen with the possibility of escalating to incidents.
    5. None of the units seem to have proper routines for registering events or incidents.

  - **Can information presented by the systems be trusted?**

    1. Even if the participants are aware that some of the information presented by the technological platform might be incomplete or outdated, the ordinary user tends to trust and depend on the graphical interface (there are some deviations related to this issue).
    2. All the participants seem to trust the information presented by the communication system.
    3. The technical platforms are not employed properly due to complexity and poor test and verification procedures affecting the users' trust to the technological platform.

Even if the practical research is directly related to research question 2 and 3, it also serves as a basis to investigate research question 1; How are the two processes of operation transition and knowledge development in Network Based Defence adjusted to each other? The results from the practical research will be further discussed in the next chapter, "Discussion". In addition, answers related to research question 1 and 2 will be further elaborated together with answers to the remaining research questions.

6 Discussion

Command and control within military operations are today relying on technological networks, and the Norwegian Armed Forces are supposed to implement Network Based Defence within the next couple of decades [8]. The political and strategic management seem coherent in their visions and objectives, but the process of implementing Network Based Defence is delayed. Several issues have been used to explain why. Interaction between different levels is complicated due to the hierarchical structure of the military [19]. There is a lack of understanding for Network Based Defence, and there is a gap between the processes going top-down and bottom-up. In addition, indications suggest that Network Based Defence is viewed isolated from other operative processes. The concept of Network Based Defence is not operationalized [20] and it is neither elaborated how to accomplish Network Based Defence. Some operative units use adjusted solutions for testing, but in total the Norwegian Defence has lacking will and ability for the implementation.

6.1 Network Based Defence

Network Based Defence is necessary both in current and future military operations, because the concept seeks to utilize network connected information systems to achieve information superiority [11] and more effectice operations. The main idea is to connect intelligent sensors, command and control systems together with precision weapons enabling enhanced situational awareness, rapid target assessment and distributed weapon assignment [12]. Network Based Defence also has the ability to enable development of speed of command leading to disruption of the enemy's strategy [11]. The strategic objective of Network Based Defence is to efficiently utilize technological infrastructure to support network based national operations and network based operations abroad [8]. But different obstacles are slowing down the process of implementing Network Based Defence ([9] and [19]). The gap between operations residing on the technological platform and the knowledge needed to utilize it, introduces several vulnerabilities putting soldier lives and operations at stake. By identifying factors delaying the implementation of Network Based Defence, countries could benefit from such an identification. For the Norwegian Armed Forces, identification of factors delaying the process could improve military operations significantly, achieving the goals stated in relation to Network Based Defence. It could also improve operative efficiency, making the commanders, officers and soldiers more aware of the actual situation so they could make more informed decisions. In short term, identification of described factors could significantly enhance and increase the speed of implementing Network Based Defence.

6.2 Unadjusted processes

Studied literature indicated that technology often is implemented much faster than knowledge, organization and doctrines are developed. It can therefore be assumed that technology, procedures and intellectual capital are not aligned to each other complicating and challenging the implementation of Network Based Defence. Comparable processes was found in Integrated Operations for the oil sector partly answering the first research question: How are the two processes of operation transition and knowledge development in Network Based Defence adjusted to each other? In order to investigate the first research question and hence also find indications to answer the remaining research questions, adapted system dynamic models developed for Integrated Operations were employed as analytic methodology. The system dynamic models were adapted in such a manner that they fitted to the transformation process related to Network Based Defence. The purpose of the models was to raise awareness around central aspects significant for Network Based Defence. In addition, their simplicity and scope were well adjusted to the the ambition and limitations related to a masters project. The adapted models serving as hypothesis in this project are referred to as "preliminary NbF system dynamic models". System dynamic models are also suggested as a tool to simulate possible technical solutions in advance of the practical implementation of Network Based Defence, referred to as "Living SD models of NbF".

Key issues in the transition of Network Based Defence are organizational change, incidents, and learning from incidents. The main idea behind the preliminary NbF SD models is that new type of operations require new knowledge. As the implementation of Network Based Defence is a prerequisite to use new technology, new technology is assumed to be a part of the transition to Network Based Defence and knowledge transition. A knowledge gap will be introduced because knowledge is matured later than the actual Network Based Defence operations, resulting in a higher vulnerability and increased number of incidents. When Network Based Defence and knowledge grow mature, the vulnerability level will decrease accordingly. The severity of the incidents is reduced when the organization is able to learn from incidents.

Both the transformation to Network Based Defence and knowledge development can be assumed to have an impact on the operator's and leader's perceived trust to available information and the information system. Introduction of new type of operations and new knowledge reduce the personnel's competency for using the technological platform to support military operations. Inadequate competency will most likely result in inadequate perceived trust level. When the perceived trust level is too high or too low, information and systems are not handled as expected to support Network Based Defence and military operations, delaying the transformation process. The introduction of new type of operations and new knowledge often results in a knowledge gap due to unadjusted processes. The knowledge gap might result in increased vulnerability and an increase in the number of incidents. In order to adjust the perceived trust to correct level, the operators and organization need to learn from the various incidents. This partly answered research question 3, how are the identified factors related to knowledge affecting the operators' perceived trust level? The relationships are illustrated in the system dynamic model adapted from the PhD work "Mitigating Information security risks during the Transition to Integrated Operations" by Qian [6] in figure 18.

Another important aspect related to the transition of Network Based Defence, is the transformation speed. By increasing the transformation speed, the vulnerability also will increase resulting in an increased frequency of incidents and a higher incident cost. Vulnerability, frequency of incidents, cost of incidents and severity of incidents are all factors affecting and adjusting the operator's perceived trust level. The mentioned factors are driven by the knowledge gap resulting from unadjusted processes and partly explain research question 4: How will the perceived trust level affect the implementation of Network Based Defence? Inadequate trust might result in the operators employing the platform in an inappropriate manner or analysing information based on wrong assumptions. In addition, inappropriate trust levels can affect the operator's willingness to employ the system, and too high reliance on the system can result in the operators not noticing system fails [16]. The frequency and severity of incidents might help adjusting the perceived trust to correct level if appropriate routines for registering incidents are in place.

Hence, the introduced knowledge gap seemed essentiel to understand how the operation transition and knowledge development were adjusted to each other. Focusing on knowledge and skills as the main reasons for unadjusted processes, possible vulnerabilities introduced into a human-technical system was assumed to be inappropriate level of trust and inadequate situational awareness as described on page 5 [25]. In order to identify and elaborate factors affecting trust and situational awareness (SA), research was conducted within three different military units. The factors were based on and limited to competency; training and SA as SA both appear as an antecedent of trust and a possible vulnerability if perceived wrongly. Identification of such factors has the possibility to align the processes to each other and reduce the number of vulnerabilities introduced.

The implementation of Network Based Defence shares several similarities with the Integrated Operation transition in the oil industry. One assumption in this project was therefore that the implementation of Network Based Defence was comparable to the process of Integrated Operations described by Rich et al [10] and further developed by Qian in her PhD work "Mitigating Information security risks during the Transition to Integrated Operations" [6]. Similar to Integrated Operations, the transformation to Network Based Defence introduces new vulnerabilities as new processes are introduced simultaneously as old ones are phased out. New processes will require new knowledge resulting in possible knowledge gaps. The implementation is endeavouring lasting for several decades making the processes and knowledge related to Network Based Defence interact in unexpected ways. As system dynamic models are connecting cause and effect, the system dynamic models from Integrated Operations were adapted and employed to understand how the transition speed, process change, knowledge and vulnerability were connected. The models were adapted and employed with permission from Ying Qian and used as basis models serving as preliminary hypothesis' to support the research questions. The proposed models were to support results found during the practical research presented in chapter 5, conduct simulations and help identifying possible outcomes in advance of implementing Network Based Defence.

6.3 The practical research

In order to collect information to investigate the research questions further, practical research was conducted in three different military units in the Norwegian Armed Forces. A successful implementation of network Based Defence would rely on compatible systems, an excellent information infrastructure and intellectual capital aligned to each other [11]. Described theory in chapter 1, studied literature in chapter 2 and adapted system dynamic models in chapter 3 suggested several obstacles slowing down the implementation of Network Based Defence. The obstacles also partly answer some of the research questions:

- **RQ1: How are the two processes of operation transition and knowledge development in Network Based Defence adjusted to each other?**.
  - Technology, procedures and intellectual capital are not aligned to each other. There exist gaps and incompatibilities between the technology implemented and procedures and knowledge needed to utilize it [18].
  - The traditional structure of the military hierarchy challenges interaction between the different levels of the organization [19].
- **RQ3. How are the identified factors related to knowledge and situational awareness affecting the operators' perceived trust level?**
  - Lack of proper competency, training and experience. The operators need proper training in order to understand the intended use of the sys-

tem and expected reliability [29]. Competence, training and experience in addition to cognitive ability are prerequisites to achieve situational awareness. Competency, training and situation awareness are important human related antecedents of trust [25], and appropriate trust is necessary to achieve superior performance in a human–automation system [29]

- ○ There is no comprehensive understanding of the Network Based Defence process among military employees [19]. The lack of understanding for the Network Based Defence process introduce additional obstacles [19].

The focus in this project was to investigate how knowledge was considered in relation to the implementation of Network Based Defence. More specifically, gaps between processes related to operation transition and knowledge development were to be investigated in order to identify possible vulnerabilities. Competence, training and experience are important prerequisites for situational awareness and all of them are antecedents of trust. A possible lack of trust in relation to the process of implementing Network Based Defence or to the technical systems implemented, might result in inadequate level or lack of trust to available information, challenging the stated objectives of Network Based Defence. Knowledge was therefore investigated from different angles assuming to be of relevance for situational awareness and perceived trust. In addition, the results would help answering research question 1,2,3 and 4:

- **Knowledge for how to develop a technological platform supporting military operations, putting high demands on the developer**.
- **The user's knowledge of how to utilize the technological platform in an appropriate manner either based on education, course, experience or training**.
- **Knowledge about the operational objectives and the situational picture during military operations among all participants**.
- **Know to what extent it is possible to trust information presented by the technological platform**.

The described focus areas and research questions together with this thesis' problem description, served as basis for development of an interview guide and a questionnaire in addition to an agreement, included in appendix C. The interview guide and the questionnaire were divided into the following main areas to make them more user friendly:

- **Technical information systems**.
- **Competence and training**.
- **Information collection and sharing**.

- **Obstacles to information sharing**.
- **Situational awareness**.
- **Trust**.
- **Trustworthiness**.

6.4 Results from the research

In order to collect information to support and answer the research questions, practical research was conducted in three different military units in the Norwegian armed forces. Field research, questionnaire and interviews were first carried out at The Norwegian Defence University College of Engineering - Telematics during their winter exercise "Cold fusion". The results from this preliminary research served as a basis to adjust the questionnaire and interview guide for further use in two army units. It also served as a basis to understand how knowledge was considered in relation to technology in a military context.

6.4.1 Results from preliminary research

The main findings from the research conducted at The Norwegian Defence University College of Engineering - Telematics are referred as follows:

- **During the field research**, it was obvious that the degree of situational awareness (SA) varied with different roles and competence. The operational officers seem to hold high situational awareness, the intelligence officers struggled a bit more. The situational awareness suffered from coincidental quality assurance also reducing the trust to the situational picture. The technical systems supported situational awareness, but affected the interaction in the company staff in a negative manner. Errors in the technical platform resulted in personnel focusing on technical challenges, forgetting about the military operations. The technical support element learned to handle incidents in the network during the exercise, but suffered from weak situational awareness related to the operational picture. Their main focus was technical issues. Various teams were equipped with various amount of technical equipment during three phases. The support of analogue and manual tools resulted in low granularity and outdated information. This was significantly improved by using technical support tools. Quality assurance, motivation, interaction and commitment were highly personnel dependent. Appropriate tools for the orders meeting together with commitment from the leader highly affected the situational awareness among the team members and how successful the operation was. Too high focus on technical tools was contra productive. Radio jamming of the communication system was detected immediately and handled in a proper manner.

- **The questionnaire** included seven main areas. **The technical information systems** seemed to some extent to be adjusted to the unit's need and to support the respondents need of information. The majority of the students seemed to hold necessary **competence and training** to utilize the technical platform and to perform their duties. In relation to **information collection and sharing**, most of the respondents knew to some extent what information to search for, but only a minority knew how to verify the information. **Obstacles to information sharing** seemed to be divided between technical challenges, systems not talking together, functional errors, time limitations and security. Most of the students seemed to be aware of their own situation to some extent, but emphasized experience as essential to achieve appropriate **situational awareness**. Only a minority were aware of the enemy situation. Most of the students **trusted** information presented by the systems to some extent, but were aware that some information could be incorrect. Related to **trustworthiness**, most of the respondents meant that the technical systems enabled faster and easier task performance, and that the systems in general were functional and reliable.
- **Results from the interviews** indicate that the technical information systems worked most of the time and supported company operations. Voice was used for verification, and Power Point was employed to get a better situational overview. Due to limitations in the military communication system, transmission of live stream data was difficult. The automatically situational updates on the systems were correct most of the time, but slightly delayed. The technical element mainly employed the technical systems to solve technical issues, personnel working in the company staff employed it for situational updates. The student's previous knowledge was based partly on course and education on single systems and experience from previous exercises. Internal guidance and supervision increased their competence during the exercise. The students found it difficult to find necessary information to support ongoing operations. Information about the enemy was even more difficult. Lack of information exchange due to bad radio routines and lacking procedures for internal information flow highly affected the situational awareness in a negative manner. The company staff was able to see the operational and situational picture to some extent, but with reduced quality of the enemy picture. The personnel in the technical support element were not particular aware of the situational picture, but mainly concerned about technical issues. The respondents trusted and relied on information presented by the different systems. In general, the technical information systems were assumed functional and reliable, but it relied on proper competence among the operators to utilize presented

and available information. To improve the current solutions, the respondents suggested a common platform for support of all military operations.

Based on remarks from the respondents, the results and experience during this preliminary research, the interview guide and questionnaire were slightly adjusted. The adjusted versions are shown in appendix C and are assumed to be better suited to the problem description and to avoid confusion among the participants.

6.4.2 Results from research in two different army units

Interviews and questionnaire were then conducted in two different army units to investigate factors related to knowledge in relation to the implementation of Network Based Defence. It was important to choose these two army units due to their differences related to personnel categories and how they conduct their operations. In both units, personnel from three different levels were interviewed and participated in the questionnaire, representing both top level, intermediate level and lower level carrying out the actual operations. The results from the interviews and questionnaire are discussed focusing on knowledge from four different angles.

- **Knowledge for developing the technological platform**. The results from the questionnaire and interviews indicate that most of the respondents are pretty satisfied with the technical information systems. The technical support tools are, however, not very well adjusted to their unit. Findings from the interviews emphasize that complexity, difficult user interfaces and continuous development challenge the use of the technological platform. The technological platform requires good, technical expertise, which is a scarce resource. Lack of ownership and responsibility were suggested as the reasons for lack of common solutions. Systems that are not adjusted to different vehicle platforms and deployment by foot also introduce challenges.
  The respondents emphasize that the technical systems are essential to achieve necessary speed during operations. But even if the technical information systems simplify many of the tasks related to operational planning and control, the participants pointed out that physical bandwidth, coverage and range challenged the information collection and sharing. The challenges limit the operational area and the amount of information possible to send and receive. Hence, time consuming follow ups are stealing time from the actual operations. The increasing amount of information also challenges the operator's cognitive ability and introduces additional vulnerabilities if not secured properly. Proprietary ports and military cables hamper the information sharing. In addition, vulnerabilities are introduced as the manual skills are reduced if the operators depend too much on the systems. These arguments can help explain why half of the respondents in the questionnaire only partly knew

what kind of information to search for, how to do it and how to verify the information. Even if the technical information systems seem to enable faster task performance and are functional and reliable to some extent, the reliability seems challenged by inappropriate hardware configurations and that new hardware is added to old hardware continuously. Technical challenges, functional errors and systems not talking together were pointed out as the main obstacles to information sharing. In addition, the systems are not interoperable with other nations.

- **The user's knowledge of how to utilize the technological platform**. Based on results obtained during the interviews, there are variations between the two army units, suggesting that army unit 2 is more resourced related to technical competence. Unit 2 also conducts more regular courses. Both units have large challenges related to turnover and competence transfer. Knowledge of how to utilize the technological platform varies in both the units. Regular practice based on vested interest and curiosity is essential to employ the solutions properly and to get insight into advanced functionality. In general, there is no comprehensive approach related to education, and user manuals are not developed when new patches are released. This is a problem issue the respondents address to a higher level of the military. Correlations can be found in results from the questionnaire. The results indicate that the participants hold enough education and experience to perform their duties and to understand and analyse information presented by the systems Experience seems to be the most important factor. The participants seemed to lack some competence to fully utilize the technological platform.
- **Knowledge about operational objectives and the situation**. According to the answers from the questionnaire and the interviews, the mission's objective seems obvious for all the respondents and all of the participants seem more or less aware of their own situation. There are more uncertainties related to the enemy situation. Education together with experience are necessary to achieve the required level of situational awareness, but there are some challenges. Information must be collected from several systems, noise and old information must be removed manually, and coordination and verification are done by voice all the time to avoid misunderstandings. Misunderstandings might still happen, resulting in events with the possibility of escalating to incidents. None of the units seem to have proper routines for registering events or incidents.
- **Can information presented by the systems be trusted?** Results from the questionnaire and interviews indicate that the participants trust the information presented by the communication system. There is more uncertainty

related to information presented by other technical systems, where some location plots also need to be removed manually. That might explain why voice communication is necessary to verify digital presented information. But in general, the ordinary user tends to trust and depend on the graphical interface completely. This seems to be a contradiction, as most of the participants are aware that some of the information presented by the technological platform might be incomplete, wrong or outdated. This contradiction might result in inappropriate trust levels among the operators. Inappropriate trust among the operators might also be a result of poor test and verification procedures, resulting in systems with poor performance.

- **During the interviews, several suggestions for improvement were made**. By using common materials and systems in all platforms, the complexity could be reduced. By simplifying the user interface, the systems would be more intuitive and user friendly. Improve the reliability by making the systems more stable. Ensure proper test and verification procedures. Develop a comprehensive approach for the implementation of technological platforms including regulations, decisions, procedures and education plans. Implement education focusing on tactical technical solutions during the officer's school and make the solutions available in garrison to enable a "work as you fight" mentality. Digital guidelines, standard operational procedures (SOP) and centralized user forums should be implemented on a parent level. In order to ensure relevant systems several levels of the operators should be involved in new projects. Development of lighter and adjusted technology relevant to all parts of the army. Implement civilian protected solutions with encrypted cards.

6.5 Discussion focusing on the research questions

6.5.1 RQ1: How are the two processes of operation transition and knowledge development in Network Based Defence adjusted to each other?

Studied literature suggests several obstacles to the implementation process of Network Based Defence. Because technology has been the main cost driver for the implementation of Network Based Defence [21]; technology, procedures and intellectual capital are not aligned to each other. Technology is often implemented much faster than knowledge, organization and doctrines are developed. There exist gaps and incompatibilities between technology implemented and procedures and knowledge needed to utilize it. In addition, the traditional structure of the military hierarchy challenges interaction between the different levels of the organization [19]. Obstacles from the literature are further elaborated on page 3. Similar obstacles have been identified during practical research in this project. Insufficient technical solutions, education of operators at random, complex information collection and sharing together with inadequate level of trust among the operators suggest that technology, procedures and intellectual capital are not aligned to each other. Comparable challenges can be found in Integrated Operations in the oil sector where the processes related to operation transition and knowledge development are not aligned to each other. In this project, adapted system dynamic models primarily developed for Integrated Operations were employed to support results obtained during interviews and questionnaires conducted in two different army units (chapter 5). More specifically, system dynamic models from Ying Qian's work related to Integrated Operations [6] were adapted in order to study the two processes in parallel. The purpose of the research was to identify factors delaying the implementation process of Network Based Defence and to investigate if the models would support future implementations. Such identifications would have the ability to improve military operations significantly and possibly increase the speed of implementing Network Based Defence. The complete methodology is described in chapter 3.

6.5.2 RQ2: Which factors related to knowledge affect the implementation of Network Based Defence?

Results from the practical research indicate that knowledge is not very well adjusted to the operation transition of Network Based Defence. In relation to knowledge for developing a military technological platform, there are several issues to address. The technical solutions are not very well adjusted to the military units. Complexity, difficult user interfaces and continuous development challenge the use of the technological platform. As a result good, technical expertise is necessary, but a scarce resource. There are no common solutions due to lack of ownership and responsibility, and the systems are not adjusted to different platforms. They are neither interoperable with other nations. Even if the technical information systems simplify many tasks, physical bandwidth, coverage and range limit the operational area and the amount of information possible to send and receive. The result is time consuming follow ups stealing time from the actual operations. Proprietary ports and military cables hamper the information sharing. The technical information systems enable faster task performance, but the reliability is challenged by inappropriate hardware configurations. Additional vulnerabilities are introduced if the manual skills are reduced and the technological platform disabled during operations.

In relation to knowledge of how to utilize the technological platform, the operators seem to hold enough education and experience to perform their duties and analyse information presented by the systems. The operators lack some competence to fully utilize the technological platform. Unit 2 seems to be more resourced than unit 1 related to technical competence, but both units have large challenges related to turnover. Vested interest and curiosity is essential to employ the solutions properly and get insight into advanced functionality. The lack of a comprehensive approach related to education and development of procedures introduce additional challenges.

The operators' knowledge about the operational objectives and their own situation seem covered for. There are more uncertainties related to the enemy situation. Education together with experience is emphasized as crucial to achieve the necessary level of situational awareness. Experience seems more important than education. This is supported by the preliminary NbF SD models described in section 3.1.7, suggesting that experience drives development and integration of Network Based Defence.

6.5.3 RQ3: How are the identified factors related to knowledge and situational awareness affecting the operators' perceived trust level?

Results from the practical research indicate that achieving appropriate situational awareness and adequate trust level are complicated. Information must be collected from several systems, and noise and old information must be removed manually. Coordination is done by voice all the time to verify information and to avoid misunderstandings. Misunderstandings still happen with the possibility of escalating to incidents. None of the units seem to have proper routines for registering events or incidents, reducing their ability to achieve appropriate perceived trust level.

Even if the participants are aware that some of the information presented by the technological platform might be incomplete or outdated, the ordinary user tends to trust and depend on the graphical interface. If the users are not aware that the situational picture might be wrong, it can have major impact on the unit, resulting in incidents and damage. All the participants seem to trust the information presented by the communication system. Due to complexity and poor test and verification procedures, the technical platforms are not employed properly, affecting the users' trust to the technological platform.

Based on adapted system dynamic models from section 3.1.7, a knowledge gap will appear if knowledge is not developed in accordance with the operation transition. As a result of the knowledge gap, additional vulnerabilities and risk are introduced into the implementation process of Network Based Defence, also increasing the number of incidents (page 30). The operators' perceived trust level is also affected, possibly resulting in inappropriate use of the technological platform or wrong interpretation of the information presented by the systems (page 8). In addition, inappropriate trust levels can affect the operator's willingness to employ the system, and too high reliance on the system can result in the operators not noticing system fails [16]. It might therefore be difficult for the operators to comprehend the situational picture correctly, reducing their situational awareness. Due to lacking routines for registering events and incidents, the unit's ability to learn from incidents can be assumed to be minimal (page 41). It is also challenging to adjust the perceived trust to appropriate and correct level without proper registering routines.

6.5.4 RQ4: How will the perceived trust level affect the implementation of Network Based Defence?

Based on described adapted system dynamic models on page 35, an increase of the transformation speed related to Network Based Defence will increase the vulnerability. Increased vulnerability might result in an increased frequency of incidents and a higher incident cost. Incidents in military operations might have major impact, ranging from small accidents in the battalion to collateral damage on the battlefield. By increasing the transformation speed of Network Based Defence, the vulnerability will increase resulting in an increased frequency of incidents and a higher incident cost. Vulnerability, frequency of incidents, cost of incidents and severity of incidents are all factors affecting and adjusting the operator's perceived trust level. This is described and illustrated on page 35. Perceived trust level is also an indirect vulnerability together with inadequate situational awareness (page 5). To adjust the perceived trust level and to learn from incidents, incidents must be registered. Studied literature in chapter 1 and 2 states that an inadequate level of trust might result in the operators employing the platform in an inappropriate manner or analysing information based on wrong assumptions. In addition, inappropriate trust levels can affect the operator's willingness to employ the system, and too high reliance on the system can result in the operators not noticing system fails [16]. Inappropriate use of the technological platform or wrong interpretation of the information presented by the systems will most likely result in various events having the possibility to escalate to incidents. The lack of routines and procedures for registering incidents introduce challenges for the organisation to learn from incidents. If management is aware of the increased frequency of incidents, they will probably reduce the transition speed. Lack of registering routines reduces the management's ability to adjust the processes of operation transition and knowledge development to each other. Registering of incidents and severity of incidents are also variables helping to adjust perceived trust to correct level. Without these two variables, it is difficult to achieve adequate trust level. When the operators and units are not aware that their trust level is inadequate, it is difficult to understand the risks related to the operation transition of Network Based Defence. It is also difficult to identify factors challenging the implementation of Network Based Defence.

6.5.5 RQ5: How will a system dynamic model simplify and reduce risk related to the integration of Network Based Defence?

Based on the answers from research questions 1-4, it seems obvious that knowledge development is not very well adjusted to the operation transition of Network Based Defence. In this project, knowledge was studied from four different angles. The arguments achieved during the interviews and the questionnaire support the assumption that the technical systems are crucial to achieve the necessary level of speed during operations. There is however lacking knowledge related to development of the technological platform. The user's knowledge of how to utilize the technological platform is neither properly considered. The operators are able to achieve situational awareness to some extent, but depending on information from several sources complicate this ability. The users are aware to some extent that information presented by the systems can be incorrect or outdated, but the ordinary user tends to trust most of the information presented.

Inadequate level of perceived trust might result in various incidents ranging from small accidents in the battalion to collateral damage on the battlefield. Without routines for registering incidents, the organisation is not able to learn from incidents or to adjust perceived trust to adequate level. Hence, it is difficult to understand the risks related to the operation transition of Network Based Defence and to identify factors challenging the implementation of Network Based Defence. Empirical studies related to system dynamic models employed in parallel with project management have shown significant utilization related to cost benefit (Source: Josè Gonzalez, expert in system dynamics, May 2017). The project therefore suggests employing a full-fledged system dynamic model in parallel with the implementation process of Network Based Defence to simplify the process and reduce risk. Such an approach has the ability to reduce giant overruns, avoid delays and reduce damage resulting from unadjusted processes. Technological implementations can then be simulated in advance to identify possible difficulties. Hence, living SD models of NbF of sufficient detail can support the implementation of Network Based Defence to ensure implementation in time, within the estimated cost and with reduced risk.

7 Conclusion

The Norwegian Armed Forces are supposed to implement Network Based Defence within the next couple of decades [8] to achieve information superiority and to enable speed of command during operations [11]. The political and strategic management seem coherent in their visions and objectives, but the process is suffering from different obstacles challenging and slowing down the implementation. The delayed implementation of Network Based Defence affects the entire Norwegian Armed Forces and puts military lives and operations at stake. This project tried to identify obstacles challenging the implementation process focusing on five research questions elaborated during the following sections.

7.1 Conclusion focusing on the research questions

RQ1: How are the two processes of operation transition and knowledge development in Network Based Defence adjusted to each other?

Studied literature suggests several obstacles to the implementation process (page 3). Because technology has been the main cost driver for the implementation of Network Based Defence [21]; technology, procedures and intellectual capital are not aligned to each other. There exist gaps and incompatibilities between technology implemented and procedures and knowledge needed to utilize it [18]. Similar obstacles have been identified during practical research in this project (chapter 5). Insufficient technological solutions, education of operators at random, complex information collection and sharing together with inadequate level of trust among the operators suggest that technology, procedures and intellectual capital are not aligned to each other.

Comparable challenges can be found in Integrated Operations in the oil sector where the processes related to operation transition and knowledge development were not aligned to each other. In this project, system dynamic models from Ying Qian's work related to Integrated Operations [6] were adapted in order to study the two processes of operation transition and knowledge development in parallel. The adapted models serve as preliminary hypothesis and are denoted "preliminary NbF system dynamic models". The models support results obtained during interviews and questionnaires conducted in two different army units (chapter 5). The purpose of the models has been to raise awareness around central aspects significant to Network Based Defence. In addition, their simplicity and scope were well adjusted to the the ambition and limitations related to a Master's project.

The purpose of the research was to identify factors delaying the implementation process of Network Based Defence and to investigate if the models would support future implementations. Such an identification would have the ability to improve military operations significantly and possibly increase the speed of implementing Network Based Defence. The complete methodology is described in chapter 3.

RQ2: Which factors related to knowledge affect the implementation of Network Based Defence?

Arguments obtained during practical research in chapter (5) support the assumption that knowledge development is not very well adjusted to the operation transition of Network Based Defence. The technical systems are crucial to achieve the necessary level of speed during operations, but there is obviously a lack of knowledge related to development of military, technological platforms (page 98). The systems are complex, difficult and under continuous development challenging the use of the technological platform. There are no common solutions due to lack of ownership and responsibility, and the systems are not adjusted to different vehicle platforms. The technological platform's potential is only partly utilized. The user's competence varies due to education at random based on vested interest and available time (page 99). Experience seems to be essential to employ the technological platform in an appropriate manner, which is supported by preliminary NbF SD models in section 3.1.7, suggesting that experience drives development. There is no comprehensive approach related to education and development of procedures.

RQ3: How are the identified factors related to knowledge and situational awareness affecting the operators' perceived trust level?

Findings from the practical research suggest that knowledge related to the operational objectives and the situational picture seem to be covered for, but only due to appropriate experience and training (page 99). Information must be collected and verified from multiple sources challenged by various obstacles. Misunderstandings happen with the possibility to escalate to incidents. Even if several sources suggest that presented information might be incorrect or outdated, the ordinary user tends to trust the information presented by the technological platform (page 100).

Based on preliminary NbF SD models explained in section 3.1.7, a knowledge gap will appear if knowledge is not developed in accordance with operation transition. As a result of the knowledge gap, additional vulnerabilities and risk are introduced into the implementation process of Network Based Defence, also increasing the number of incidents (page 30). Incidents in military operations range from accidents in the battalion to collateral damage on the battlefield. The operators' perceived trust level is also affected, possibly resulting in inappropriate use of the technological platform or wrong interpretation of the information presented by the systems (page 8). It might therefore be difficult for the operators to comprehend the situational picture correctly, reducing their situational awareness. Due to lacking routines for registering incidents, the unit's ability to learn from incidents can be assumed to be minimal (page 41). It is also challenging to adjust the perceived trust to adequate level without proper registering routines.

RQ4: How will the perceived trust level affect the implementation of Network Based Defence?

Based on described preliminary NbF SD model in page 35, an increase in the transformation speed related to Network Based Defence will increase the vulnerability, frequency of incidents and the incident cost. All the mentioned factors affect and adjust the operator's perceived trust level. Inappropriate perceived trust level is also an indirect vulnerability together with inadequate situational awareness. Without proper routines for registering incidents, the operators might not be aware that incidents happen. Lack of registering routines reduces the management's ability to adjust the processes of operation transition and knowledge development to each other. The trust level will not be adjusted, and the operators are not aware that their trust level is inadequate. It might therefore be difficult to understand the risks related to the operation transition of Network Based Defence and risk during military operations. It might also be difficult to identify factors challenging the successfulness of the implementation of Network Based Defence.

RQ5: How will a system dynamic model simplify and reduce risk related to the integration of Network Based Defence?

Based on the answers from research questions 1-4, it seems obvious that knowledge development is not very well adjusted to the operation transition of Network Based Defence. In this project, knowledge was studied from four different angles supported by adapted preliminary system dynamic models and practical research in three different military units. Identified factors related to knowledge can be assumed to affect the operators' perceived trust level, which again can increase the frequency of incidents. Without proper routines for registering incidents, it is difficult or even impossible to understand the risks related to the operation transition of Network Based Defence.

Empirical studies have shown significant cost benefit utilization when employing system dynamic models in parallel with new technology adoption. The project therefore suggests employing a full-fledged system dynamic model in parallel with the implementation process of Network Based Defence to simplify the process and reduce risk. Such an approach has the ability to reduce giant overruns, avoid delays and reduce damage resulting from unadjusted processes. Technological implementations can then be simulated in advance to identify possible difficulties. Hence, living SD models of NbF of sufficient detail can support the implementation of Network Based Defence to ensure implementation in time, within the estimated cost and with reduced risk.

8 Future work

The preliminary NbF SD models adapted from Integrated Operations supported findings obtained during the practical research as elaborated in the discussion and conclusion. More specifically, the models supported the assumption that the processes of operation transition and knowledge development of Network Based Defence are not not very well aligned to each other. But there are limitations related to the results achieved during this project. Due to time limitations, a complete Group Model Building process was not a viable option. The models adapted with permission from Ying Qian must therefore be viewed only as preliminary models focusing on central parameters. In this project, the preliminary NbF SD models served as working hypothesis highlighting some of the problem issues. The employment of the models shows some promising results, suggesting that the models can be further developed to follow the implementation process in parallel. By employing customized models in the future implementation of Network Based Defence, some of the challenges related to the implementation process can be avoided. In this closing chapter, suggestions for future work are made.

8.1 Delphi method

To verify the results obtained during the practical research, employing the Delphi method is a viable option. The Delphi method is a structured, systematic and iterative process with the objective of structuring a group communication process to achieve consensus about a complex problem [52]. The Delphi method was designed to reduce challenges related to interacting groups while combining knowledge from experts about a subjects. The method consists of multiple, iterative rounds of questionnaires and feedback among the participants. The first round includes a questionnaire distributed to all participants acting as experts. A new round is distributed when all the answers from the first round are collected. The second round includes the experts' previous answers in addition to the mean of the group's ranking. It is assumed that all the experts reflect on earlier answers resulting in some convergence among the experts over time. The following key characteristics are specific for the Delphi method, helping the participants to focus on chosen problem issues. Anonymity allows free expression of opinions preventing dominance from authorities. Interaction allows the experts to refine their answers based on results from the group during iterative rounds. Controlled feedback informs the participants of other participants' opinion. All the participants then have the ability to revise their answers. Statistical aggregation of group responses allow a quantitative analysis and aggregation of data.

It is assumed that two or three iterations are sufficient in most research to achieve the desired consensus [52]. The Delphi method is assumed superior to other collaborative methodologies due to reduced cost in time and displacement. In addition, the iterative process refines the answers and matches the cyclic nature of model building. One drawback might be that the answers are not discussed with other experts outside the project.

By implementing the Delphi method as an extension of this project, the answers from the practical research could have been refined by two additional iterations. The findings could then have been more coinciding, acting as a solid basis for the further research. The results from the cyclic process of the Delphi method would also support the Group Model Building process in a better manner than one single iteration conducted during this project. The Group Model Building process is part of a system dynamic process with the objective of developing system dynamic models to understand complex problems. In the next section, an approach for developing the employed preliminary NbF SD models further, is suggested.

8.2 Development of customized system dynamic models

In order to develop the preliminary NbF SD models further, close cooperation in a cross sectional group from The Norwegian Armed Forces is necessary. The group will then have the ability to extend the work started in this project and to dig deeper into the various elements affecting the process of implementing Network Based Defence. During this project, preliminary NbF SD adapted from Integrated Operations [6] were employed as working hypothesis and to support findings obtained during the field research. The adapted models can support awareness and consciousness around the process of implementing Network based Defence into the Norwegian Armed Forces. By collecting detailed information in advance, the models can be developed further to visualize various processes.

The Norwegian Armed Forces has two options when it comes to customized Nbf SD models:

1. **Proactive full SD model of NbF.**
   Before further implementation of Network Based Defence, a cross sectional and balanced group from the Norwegian Armed Forces can conduct a Group Model Building process together with modelling experts. During the Group Model Building process, a detailed system dynamic model can be developed with the purpose of investigating possible scenarios in the implementation process and conduct what-if studies. The model may be employed to make decisions related to processes and development of knowledge. The models

will be approximately correct, but only illustrate what happens at that time under the prevailing circumstances. In order to develop such a model, support from two experienced modellers is necessary and the cost is estimated to approximately 4 million Norwegian crowns. To emphasize that the model serves as a basis to investigate possible scenarios in advance and make decisions, the model is denoted "A proactive full SD model of NbF".

2. **Living SD model of NbF.**
   The proactive full SD model of NbF could be extended during the implementation of Network Based Defence by collecting regular relevant information. By continuously updating the system dynamic model, the model would give an accurate picture and status of the implementation process of Network Based Defence. It would then be possible to simulate and test possible outcomes in advance of important milestones. Such a model has the ability to support optimal decisions related to processes and knowledge development in all current scenarios. Because the model is continuously updated and will follow the process in parallel, it is denoted "a living SD model of NbF". In order to develop the described model, support from 1-2 experienced modellers each year of the implementation process is necessary. If the implementation process continuous for ten more years, the estimated cost for development of a living SD model of NbF is 10-20 man-year for the system dynamic modellers.

8.3 Recommendations

In order to enhance the process of implementing Network Based Defence, this project has the following recommendations. By employing the Delphi method, results obtained during the practical research in this project can be verified. Results from the Delphi method will then serve as information inputs from experts to the Group Model Building process of system dynamics. Several iterations during the Delphi method will support the iterative process of the Group Model Building between domain experts and modelling experts. The domain experts must be a cross sectional group from The Norwegian Armed Forces representing units from the Navy, the Air Force and the Army. At a minimum, three levels of each units must participate, representing top level, intermediate and the lower levels. The modelling expertise must be based on external support available at some faculties or in consultant companies. Two or three iterations of the Delphi method are assumed sufficient to achieve necessary coincidence. The information collection obtained during the Delphi method must most likely be supported by one or two workshops conducting the Group Model Building. The complete process of the Group Model Building is assumed finished within one year with sufficient commitment. Based on the Group Model Building process, it is recommended to develop a proactive full SD model of NbF to investigating possible scenarios in the implementation process and conduct what-if studies. The proactive model should be further developed to a customized system dynamic model, denoted a living SD model of NbF. It will then be possible to simulate and test possible outcomes in advance of important milestones. A living model enables optimal decisions related to processes and knowledge development in all current scenarios in the implementation of Network Based Defence. By developing a living model in parallel with the implementation process, it is possible to avoid delays, reduce cost and reduce risk by simulating the implementation in advance. The proactive and living models can both serve as a basis to support consciousness around important elements and reduce risk during the implementation of Network Based Defence.

Bibliography

[1] Hancock, P. A., Billings, D. R., Oleson, K. E., Chen, J. Y., De Visser, E., & Parasuraman, R. A meta-analysis of factors influencing the development of human-robot trust. Technical report, DTIC Document, 2011.

[2] Endsley, M. R. 1995. Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 37(1), 32–64.

[3] Whitman, M. E., Mattord, H. J., & Green, A. 2013. *Principles of incident response and disaster recovery*. Cengage Learning.

[4] Wolstenholme, E. F. 2003. Towards the definition and use of a core set of archetypal structures in system dynamics. *System Dynamics Review*, 19(1), 7–26.

[5] Jose Gozalez. 2016. Group model building. Written appendix from lessons in the subject of System Dynamics at HiG 2016.

[6] Qian, Y. *Mitigating Information security risks during the Transition to Integrated Operations: Models & Data*. PhD thesis, 2010.

[7] Qian, Y., Fang, Y., & Gonzalez, J. J. 2012. Managing information security risks during new technology adoption. *computers & security*, 31(8), 859–869.

[8] Forsvarsdepartementet. 2009. Iverksettingsbrev for forsvaret for gjennomfØringsÅret 2010 (2009). Available at https://www.regjeringen.no/globalassets/upload/fd/budsjettdokumenter/ivb-2010_18-des-2009.pdf (15.11.2016).

[9] Rutledal, F., Fridheim, H., Danielsen, T., & Malerud, S. Støtte til forsvarets nbf-utvikling – sluttrapport. Technical report, Forsvarets forskningsinstitutt FFI, 2015.

[10] Rich, E., Gonzalez, J. J., Qian, Y., Sveen, F. O., Radianti, J., & Hillen, S. 2009. Emergent vulnerabilities in integrated operations: a proactive simulation study of economic risk. *International Journal of Critical Infrastructure Protection*, 2(3), 110–123.

[11] Cebrowski, A. K. & Garstka, J. J. 1998. Network-centric warfare: Its origin and future. In *US Naval Institute Proceedings*, volume 124, 28–35.

[12] Owens, W. A. The emerging us system-of-systems. Technical report, DTIC Document, 1996.

[13] Forsvarets Sikkerhetstjeneste. 2009. Sikkerhetskonsept for et nettverksbasert forsvar.

[14] Forsvarsdepartementet. 2008. *Policy for utviklingen mot nettverksbasert forsvar*.

[15] Wesensten, N. J., Belenky, G., & Balkin, T. J. Cognitive readiness in network-centric operations. Technical report, DTIC Document, 2005.

[16] Bolia, R. S., Vidulich, M. A., & Nelson, W. T. Unintended consequences of the network-centric decision making model: Considering the human operator. Technical report, DTIC Document, 2006.

[17] Wallace, W. S. 2005. Network-enabled battle command. *Military Review*, 85(3), 2.

[18] Baker, M. E. Human factors in network centric warfare. Technical report, DTIC Document, 2002.

[19] Fridheim, H. Nbf – nå! – hvordan får vi et nettverksbasert forsvar raskere? Technical report, Forsvarets forskningsinstitutt (FFI), 2015.

[20] Forsvarsstaben. 2014. *Forsvarets fellesoperative doktrine*. Forsvaret.

[21] Daltveit, E., Geiner, J. F., & Ydstebø, P. Trender i militære operasjoner. Technical report, Forsvarets forskningsinstitutt (FFI), 2010.

[22] Bjørnstad, A. L. Ncw in theory and practice: A human factors perspective on why it might work and why we might not get there. Technical report, Forsvarets forskningsinstitutt (FFI), 2004.

[23] Hafnor, H. & Normark, R. Ad hoc organization of distributed picture compilation and support for situation awareness in network based defence-an exploratory experiment. Technical report, DTIC Document, 2005.

[24] Bérard, C. 2010. Group model building using system dynamics: an analysis of methodological frameworks. *Electronic Journal of Business Research Methods*, 8(1), 35–45.

[25] Schaefer, K. E. *The perception and measurement of human-robot trust*. PhD thesis, University of Central Florida Orlando, Florida, 2013.

[26] Cambridge. 2016. trust. Available at http://dictionary.cambridge.org/dictionary/english/trust (15.11.2016).

[27] Van Bezooijen, B. & Essens, P. 2007. Situation awareness in modern military operations. In *12th International Command and Control Research and Technology Symposium. Retrieved from http://www. dodccrp. org/events/12th_ICCRTS/CD/html/papers/229. pdf*.

[28] Jian, J.-Y., Bisantz, A. M., & Drury, C. G. 2000. Foundations for an empirically determined scale of trust in automated systems. *International Journal of Cognitive Ergonomics*, 4(1), 53–71.

[29] Lee, J. D. & See, K. A. 2004. Trust in automation: Designing for appropriate reliance. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 46(1), 50–80.

[30] O'Brien, K. & O'Hare, D. 2007. Situational awareness ability and cognitive skills training in a complex real-world task. *Ergonomics*, 50(7), 1064–1091.

[31] Merkow, M. S. & Breithaupt, J. 2014. *Information security: Principles and practices*. Pearson Education.

[32] Whitman, M. E. & Mattord, H. J. 2011. *Roadmap to information security. For IT and INFOSEC managers*. Cengage Learning.

[33] NATO Standardization Agency. Ajp-01(e), allied joint doctrine. ratification draft 1. Technical report, NATO Standardization Agency, 2015.

[34] Sengupta, A., Mazumdar, C., & Bagchi, A. 2011. A formal methodology for detecting managerial vulnerabilities and threats in an enterprise information system. *Journal of Network and Systems Management*, 19(3), 319–342.

[35] Joint Cheifs of staff. 1996. Joint vision 2010. Available at http://www.dtic.mil/jv2010/jv2010.pdf (11.01.2017).

[36] Alberts, D. S., Garstka, J. J., & Stein, F. P. Network centric warfare: Developing and leveraging information superiority. Technical report, DTIC Document, 2000.

[37] Forsvaret. 2003. Forsvarssjefens militærfaglige utredning 2003. Available at https://forsvaret.no/ifs/ForsvaretDocuments/Forsvarssjefens%20milit%C3%A6rfaglige%20utredning%202003.pdf (11.01.2017).

[38] Burbank, J. L., Chimento, P. F., Haberman, B. K., & Kasch, W. T. 2006. Key challenges of military tactical networking and the elusive promise of manet technology. *IEEE Communications Magazine*, 44(11), 39–45.

[39] Pang, C. K. & Mathew, J. 2015. Dynamically reconfigurable command and control structure for network-centric warfare. *Simulation*, 0037549715581076.

[40] Arneson, V. & Gjellerud, M. Innledende kartlegging av alternative plattformer for bruk som elevert kommunikasjonsrele i nbf. Technical report, Forsvarets forskningsinstitutt (FFI), 2003.

[41] Messel, E. Enhetlig presentasjon av stedfestet informasjon for forsvaret. Technical report, Forsvarets forskningsinstitutt (FFI), 2009.

[42] Saltzer, J. H. & Schroeder, M. D. 1975. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9), 1278–1308.

[43] Cherdantseva, Y. & Hilton, J. 2013. A reference model of information assurance & security. In *Availability, reliability and security (ares), 2013 eighth international conference on*, 546–555. IEEE.

[44] Bjørnstad, A. L. & Elstad, A.-K. Utvikling og evaluering av spørreskjema med fokus på organisasjon og bruk av samhandlingsteknologi. Technical report, Forsvarets forskningsinstitutt (FFI), 2015.

[45] ISO. 2016. *ISO/IEC 27000:2016. Information technology. Security techniques*. ISO.

[46] Senge, P. 1990. The fifth discipline. *New York: Currency Doubleday*.

[47] Business dictionary. 2017. Tacit knowledge. Available at (http://www.businessdictionary.com/definition/tacit-knowledge.html.

[48] English Oxford living dictionaries. 2017. Knowledge. Available at (https://en.oxforddictionaries.com/definition/knowledge).

[49] Yin, R. K. 2012. A (very) brief refresher on the case study method. *Application of case study research*, 3–20.

[50] Flyvbjerg, B. 2006. Five misunderstandings about case-study research. *Qualitative inquiry*, 12(2), 219–245.

[51] Stahlberg, M. 2000. Radio jamming attacks against two popular mobile networks. In *Helsinki University of Technology Seminar on Network Security*.

[52] Labaka, L. 2013. Resilience framework for critical infrastructures. *San Sebastian: University of Navarra*.

A Application for approval sent to NSD with receipt

MELDESKJEMA

Meldeskjema (versjon 1.4) for forsknings- og studentprosjekt som medfører meldeplikt eller konsesjonsplikt
(jf. personopplysningsloven og helseregisterloven med forskrifter).

1. Intro

Samles det inn direkte personidentifiserende opplysninger?	Ja ○ Nei ●	En person vil være direkte identifiserbar via navn, personnummer, eller andre personentydige kjennetegn. Les mer om hva personopplysninger. NB! Selv om opplysningene skal anonymiseres i oppgave/rapport, må det krysses av dersom det skal innhentes/registreres personidentifiserende opplysninger i forbindelse med prosjektet.
Hvis ja, hvilke?	□ Navn □ 11-sifret fødselsnummer □ Adresse □ E-post □ Telefonnummer □ Annet	
Annet, spesifiser hvilke		
Samles det inn bakgrunnsopplysninger som kan identifisere enkeltpersoner (indirekte personidentifiserende opplysninger)?	Ja ● Nei ○	En person vil være indirekte identifiserbar dersom det er mulig å identifisere vedkommende gjennom bakgrunnsopplysninger som for eksempel bostedskommune eller arbeidsplass/skole kombinert med opplysninger som alder, kjønn, yrke, diagnose, etc. NB! For at stemme skal regnes som personidentifiserende, må denne bli registrert i kombinasjon med andre opplysninger, slik at personer kan gjenkjennes.
Hvis ja, hvilke	Bostedskommune, arbeidsplass, alder	
Skal det registreres personopplysninger (direkte/indirekte/via IP-/epost adresse, etc) ved hjelp av nettbaserte spørreskjema?	Ja ○ Nei ●	Les mer om nettbaserte spørreskjema.
Blir det registrert personopplysninger på digitale bilde- eller videoopptak?	Ja ○ Nei ●	Bilde/videoopptak av ansikter vil regnes som personidentifiserende.
Søkes det vurdering fra REK om hvorvidt prosjektet er omfattet av helseforskningsloven?	Ja ○ Nei ●	NB! Dersom REK (Regional Komité for medisinsk og helsefaglig forskningsetikk) har vurdert prosjektet som helseforskning, er det ikke nødvendig å sende inn meldeskjema til personvernombudet (NB! Gjelder ikke prosjekter som skal benytte data fra pseudonyme helseregistre). Dersom tilbakemelding fra REK ikke foreligger, anbefaler vi at du avventer videre utfylling til svar fra REK foreligger.

2. Prosjekttittel

Prosjektittel	Factors affecting trust and trustwuthiness of military command and control systems	Oppgi prosjektets tittel. NB! Dette kan ikke være «Masteroppgave» eller liknende, navnet må beskrive prosjektets innhold.

3. Behandlingsansvarlig institusjon

Institusjon	NTNU	Velg den institusjonen du er tilknyttet. Alle nivå må oppgis. Ved studentprosjekt er det studentens tilknytning som er avgjørende. Dersom institusjonen ikke finnes på listen, har den ikke avtale med NSD som personvernombud. Vennligst ta kontakt med institusjonen.
Avdeling/Fakultet	NTNU i Gjøvik	
Institutt	Avdeling for informatikk og medieteknikk	

4. Daglig ansvarlig (forsker, veileder, stipendiat)

Fornavn	Jose	Før opp navnet på den som har det daglige ansvaret for prosjektet. Veileder er vanligvis daglig ansvarlig ved studentprosjekt. Daglig ansvarlig og student må i utgangspunktet være tilknyttet samme institusjon. Dersom studenten har ekstern veileder, kanbiveileder eller fagansvarlig ved studiestedet stå som daglig ansvarlig. Arbeidssted må være tilknyttet behandlingsansvarlig institusjon, f.eks. underavdeling, institutt etc. NB! Det er viktig at du oppgir en e-postadresse som brukes aktivt. Vennligst gi oss beskjed dersom den endres.
Etternavn	Gonzales	
Stilling	Professor	
Telefon	92031161	
Mobil		
E-post	jose.gonzalez@ntnu.no	
Alternativ e-post	jose.gonzales@ntnu.no	
Arbeidssted	NTNU Gjøvik	

Adresse (arb.)	Teknologivegen 22	
Postnr./sted (arb.sted)	2815 Gjøvik	

5. Student (master, bachelor)

Studentprosjekt	Ja ● Nei ○	Dersom det er flere studenter som samarbeider om et prosjekt, skal det velges en kontaktperson som føres opp her. Øvrige studenter kan føres opp under pkt 10.
Fornavn	Tonje	
Etternavn	Andreassen	
Telefon	99094832	
Mobil	99094832	
E-post	tonhaugen@gmail.com	
Alternativ e-post	tonjand@stud.ntnu.no	
Privatadresse	Holsjordet 67	
Postnr./sted (privatadr.)	2613 LILLEHAMMER	
Type oppgave	● Masteroppgave ○ Bacheloroppgave ○ Semesteroppgave ○ Annet	

6. Formålet med prosjektet

Formål	Hensikten med prosjektet er å identifisere eventuelle faktorer som påvirker brukernes tillit og troverdighet til militære kommando og kontroll systemer. Det kan antas at dette indirekte vil påvirke brukernes vilje til faktisk å benytte systemene.	Redegjør kort for prosjektets formål, problemstilling, forskningsspørsmål e.l.

7. Hvilke personer skal det innhentes personopplysninger om (utvalg)?

Kryss av for utvalg	□ Barnehagebarn □ Skoleelever □ Pasienter □ Brukere/klienter/kunder ■ Ansatte □ Barnevernsbarn □ Lærere □ Helsepersonell □ Asylsøkere ■ Andre	
Beskriv utvalg/deltakere	Utvalg vil omfatte ansatte og soldater i det norske forsvar i ulike avdelinger	Med utvalg menes dem som deltar i undersøkelsen eller dem det innhentes opplysninger om.
Rekruttering/trekking	Utvalget gjøres gjennom kontakt med aktuelle avdelinger og gjennom dialog med avdeling for å finne aktuelle kandidater.	Beskriv hvordan utvalget trekkes eller rekrutteres og oppgi hvem som foretar den. Et utvalg kan trekkes fra registre som f.eks. Folkeregisteret, SSB-registre, pasientregistre, eller det kan rekrutteres gjennom f.eks. en bedrift, skole, idrettsmiljø eller eget nettverk.
Førstegangskontakt	Gjøres av student gjennom først godkjenning hos avdelingsledelse, så gjennom dialog med de aktuelle kandidatene	Beskriv hvordan kontakt med utvalget blir opprettet og av hvem. Les mer om dette på temasidene.
Alder på utvalget	□ Barn (0-15 år) □ Ungdom (16-17 år) ■ Voksne (over 18 år)	Les om forskning som involverer barn på våre nettsider.
Omtrentlig antall personer som inngår i utvalget	50-100	
Samles det inn sensitive personopplysninger?	Ja ○ Nei ●	Les mer om sensitive opplysninger.
Hvis ja, hvilke?	□ Rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning □ At en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling □ Helseforhold □ Seksuelle forhold □ Medlemskap i fagforeninger	

Inkluderes det myndige personer med redusert eller manglende samtykkekompetanse?	Ja ○ Nei ●	Les mer om pasienter, brukere og personer med redusert eller manglende samtykkekompetanse.
Samles det inn personopplysninger om personer som selv ikke deltar (tredjepersoner)?	Ja ○ Nei ●	Med opplysninger om tredjeperson menes opplysninger som kan spores tilbake til personer som ikke inngår i utvalget. Eksempler på tredjeperson er kollega, elev, klient, familiemedlem.

8. Metode for innsamling av personopplysninger

Kryss av for hvilke datainnsamlingsmetoder og datakilder som vil benyttes	■ Papirbasert spørreskjema □ Elektronisk spørreskjema ■ Personlig intervju □ Gruppeintervju ■ Observasjon □ Deltakende observasjon □ Blogg/sosiale medier/internett □ Psykologiske/pedagogiske tester □ Medisinske undersøkelser/tester □ Journaldata (medisinske journaler)	Personopplysninger kan innhentes direkte fra den registrerte f.eks. gjennom spørreskjema,intervju, tester, og/eller ulike journaler (f.eks. elevmapper, NAV, PPT, sykehus) og/eller registre (f.eks.Statistisk sentralbyrå, sentrale helseregistre). NB! Dersom personopplysninger innhentes fra forskjellige personer (utvalg) og med forskjellige metoder, må dette spesifiseres i kommentar-boksen. Husk også å legge ved relevante vedlegg til alle utvalgs-gruppene og metodene som skal benyttes. Les mer om registerstudier her. Dersom du skal anvende registerdata, må variabelliste lastes opp under pkt. 15
	□ Registerdata	
	□ Annen innsamlingsmetode	
Tilleggsopplysninger	Den vedlagte samtykke erklæringen er et utkast som også kommer til å benyttes som basis for å lage samtykke skjema til intervjuene.	

9. Informasjon og samtykke

Oppgi hvordan utvalget/deltakerne informeres	■ Skriftlig ■ Muntlig □ Informeres ikke	Dersom utvalget ikke skal informeres om behandlingen av personopplysninger må det begrunnes. Les mer her. Vennligst send inn mal for skriftlig eller muntlig informasjon til deltakerne sammen med meldeskjema. Last ned en veiledende mal her. NB! Vedlegg lastes opp til sist i meldeskjemaet, se punkt 15 Vedlegg.
Samtykker utvalget til deltakelse?	● Ja ○ Nei ○ Flere utvalg, ikke samtykke fra alle	For at et samtykke til deltakelse i forskning skal være gyldig, må det være frivillig, uttrykkelig og informert. Samtykke kan gis skriftlig, muntlig eller gjennom en aktiv handling. For eksempel vil et besvart spørreskjema være å regne som et aktivt samtykke. Dersom det ikke skal innhentes samtykke, må det begrunnes.

10. Informasjonssikkerhet

Hvordan registreres og oppbevares personopplysningene?	■ På server i virksomhetens nettverk □ Fysisk isolert PC tilhørende virksomheten (dvs. ingen tilknytning til andre datamaskiner eller nettverk, interne eller eksterne) □ Datamaskin i nettverkssystem tilknyttet Internett tilhørende virksomheten □ Privat datamaskin □ Videoopptak/fotografi □ Lydopptak ■ Notater/papir □ Mobile lagringsenheter (bærbar datamaskin, minnepenn, minnekort, cd, ekstern harddisk, mobiltelefon) □ Annen registreringsmetode	Merk av for hvilke hjelpemidler som benyttes for registrering og analyse av opplysninger. Sett flere kryss dersom opplysningene registreres på flere måter. Med «virksomhet» menes her behandlingsansvarlig institusjon. NB! Som hovedregel bør data som inneholder personopplysninger lagres på behandlingsansvarlig sin forskningsserver. Lagring på andre medier - som privat pc, mobiltelefon, minnepinne, server på annet arbeidssted - er mindre sikkert, og må derfor begrunnes. Slik lagring må avklares med behandlingsansvarlig institusjon, og personopplysningene bør krypteres.
Annen registreringsmetode beskriv		
Hvordan er datamaterialet beskyttet mot at uvedkommende får innsyn?	Spørreskjemaene blir låst inn når de er utfylt. Forsvarets nett er sikret både med brukernavn og passord, samt tilgang til nettverket er fysisk sikret.	Er f.eks. datamaskintilgangen beskyttet med brukernavn og passord, står datamaskinen i et låsbart rom, og hvordan sikres bærbare enheter, utskrifter og opptak?

Samles opplysningene inn/behandles av en databehandler (ekstern aktør)?	Ja ○ Nei ●	Dersom det benyttes eksterne til helt eller delvis å behandle personopplysninger, f.eks. Questback, transkriberingsassistent eller tolk, er dette å betrakte som en databehandler. Slike oppdrag må kontraktsreguleres.
Hvis ja, hvilken		
Overføres personopplysninger ved hjelp av e-post/Internett?	Ja ○ Nei ●	F.eks. ved overføring av data til samarbeidspartner, databehandler mm. Dersom personopplysninger skal sendes via internett, bør de krypteres tilstrekkelig. Vi anbefaler for ikke lagring av personopplysninger på nettskytjenester. Dersom nettskytjeneste benyttes, skal det inngås skriftlig databehandleravtale med leverandøren av tjenesten.
Hvis ja, beskriv?		
Skal andre personer enn daglig ansvarlig/student ha tilgang til datamaterialet med personopplysninger?	Ja ● Nei ○	
Hvis ja, hvem (oppgi navn og arbeidssted)?	Roger Johnsen og Ivar Kjærem, ansatte i Forsvaret, Cyberforsvaret Jørstadmoen, Lillehammer	
Utleveres/deles personopplysninger med andre institusjoner eller land?	● Nei ○ Andre institusjoner ○ Institusjoner i andre land	F.eks. ved nasjonale samarbeidsprosjekter der personopplysninger utveksles eller ved internasjonale samarbeidsprosjekter der personopplysninger utveksles.

11. Vurdering/godkjenning fra andre instanser

Søkes det om dispensasjon fra taushetsplikten for å få tilgang til data?	Ja ○ Nei ●	For å få tilgang til taushetsbelagte opplysninger fra f.eks. NAV, PPT, sykehus, må det søkes om dispensasjon fra taushetsplikten. Dispensasjon søkes vanligvis fra aktuelt departement.
Hvis ja, hvilke		
Søkes det godkjenning fra andre instanser?	Ja ● Nei ○	F.eks. søke registereier om tilgang til data, en ledelse om tilgang til forskning i virksomhet, skole.
Hvis ja, hvilken	Søke om/få tillatelse fra avdelingsleder i aktuell avdeling i Forsvaret om å få lov til å gjennomføre forskning i avdelingslederens avdeling.	

12. Periode for behandling av personopplysninger

Prosjektstart Planlagt dato for prosjektslutt	15.01.2017 01.06.2017	Prosjektstart Vennligst oppgi tidspunktet for når kontakt med utvalget skal gjøres/datainnsamlingen starter. Prosjektslutt: Vennligst oppgi tidspunktet for når datamaterialet enten skalanonymiseres/slettes, eller arkiveres i påvente av oppfølgingsstudier eller annet.
Skal personopplysninger publiseres (direkte eller indirekte)?	□ Ja, direkte (navn e.l.) □ Ja, indirekte (bakgrunnsopplysninger) ■ Nei, publiseres anonymt	NB! Dersom personopplysninger skal publiseres, må det vanligvis innhentes eksplisitt samtykke til dette fra den enkelte, og deltakere bør gis anledning til å lese gjennom og godkjenne sitater.
Hva skal skje med datamaterialet ved prosjektslutt?	■ Datamaterialet anonymiseres □ Datamaterialet oppbevares med personidentifikasjon	NB! Her menes datamaterialet, ikke publikasjon. Selv om data publiseres med personidentifikasjon skal som regel øvrig data anonymiseres.Med anonymisering menes at datamaterialet bearbeides slik at det ikke lenger er mulig å føre opplysningene tilbake til enkeltpersoner. Les mer om anonymisering.

13. Finansiering

Hvordan finansieres prosjektet?	Gjennom Forsvaret	

14. Tilleggsopplysninger

Tilleggsopplysninger		

Jose Julio Cabeza Gonzalez
Avdeling for informatikk og medieteknikk NTNU i Gjøvik

7004 TRONDHEIM

Vår dato: 19.01.2017 Vår ref: 51490 / 3 / ASF Deres dato: Deres ref:

TILBAKEMELDING PÅ MELDING OM BEHANDLING AV PERSONOPPLYSNINGER

Vi viser til melding om behandling av personopplysninger, mottatt 07.12.2016. Meldingen gjelder prosjektet:

51490	*Factors affecting trust and trustwuthiness of military command and control systems*
Behandlingsansvarlig	*NTNU, ved institusjonens øverste leder*
Daglig ansvarlig	*Jose Julio Cabeza Gonzalez*
Student	*Tonje Andreassen*

Personvernombudet har vurdert prosjektet og finner at behandlingen av personopplysninger er meldepliktig i henhold til personopplysningsloven § 31. Behandlingen tilfredsstiller kravene i personopplysningsloven.

Personvernombudets vurdering forutsetter at prosjektet gjennomføres i tråd med opplysningene gitt i meldeskjemaet, korrespondanse med ombudet, ombudets kommentarer samt personopplysningsloven og helseregisterloven med forskrifter. Behandlingen av personopplysninger kan settes i gang.

Det gjøres oppmerksom på at det skal gis ny melding dersom behandlingen endres i forhold til de opplysninger som ligger til grunn for personvernombudets vurdering. Endringsmeldinger gis via et eget skjema, http://www.nsd.uib.no/personvern/meldeplikt/skjema.html. Det skal også gis melding etter tre år dersom prosjektet fortsatt pågår. Meldinger skal skje skriftlig til ombudet.

Personvernombudet har lagt ut opplysninger om prosjektet i en offentlig database, http://pvo.nsd.no/prosjekt.

Personvernombudet vil ved prosjektets avslutning, 01.06.2017, rette en henvendelse angående status for behandlingen av personopplysninger.

Vennlig hilsen

Kjersti Haugstvedt

Amalie Statland Fantoft

Kontaktperson: Amalie Statland Fantoft tlf: 55 58 36 41

Dokumentet er elektronisk produsert og godkjent ved NSDs rutiner for elektronisk godkjenning.

Vedlegg: Prosjektvurdering

Kopi: Tonje Andreassen tonhaugen@gmail.com

Personvernombudet for forskning

Prosjektvurdering - Kommentar

Prosjektnr: 51490

INFORMASJON OG SAMTYKKE
I følge meldeskjemaet skal deltakerne i studien informeres skriftlig og muntlig om prosjektet og samtykke til deltakelse. Informasjonsskrivet er godt utformet.

METODE
Det skal innhentes personopplysninger gjennom intervju og papirbasert spørreskjema. Observasjoner skal i følge studenten være anonyme og opplysninger fra observasjon skal registreres som feltnotater. Likevel skal de som observeres informeres om prosjektet. Dette har studenten bekreftet på e-post mottatt 19.01.2017.

INFORMASJONSSIKKERHET
Personvernombudet legger til grunn at dere behandler alle data og personopplysninger i tråd med NTNU sine retningslinjer for innsamling og videre behandling av forskningsdata og personopplysninger. Studenten skal i følge e-post mottatt 19.01.2017, avklare oppbevaringen av datamaterialet.

PROSJEKTSLUTT OG ANONYMISERING
I meldeskjemaet har dere informert om at forventet prosjektslutt er 01.06.2017. Ifølge prosjektmeldingen skal dere da anonymisere innsamlede opplysninger. Anonymisering innebærer at dere bearbeider datamaterialet slik at ingen enkeltpersoner kan gjenkjennes. Det gjør dere ved å slette direkte personopplysninger, slette eller omskrive indirekte personopplysninger og slette digitale lydopptak.

B First draft of the questionnaire, interview guide and agreement

Spørreskjema

Bakgrunn

Alder:		
Bostedskommune:		
Militær grad:		
Antall år i Forsvaret:		
Høyeste utdanningsnivå:	Militært:	Sivilt:

Tekniske informasjonssystemer

Indiker i hvilken grad du er enig eller uenig i følgende påstander:	Uenig (1)	Delvis uenig (2)	Delvis enig (3)	Enig (4)	Vet ikke (5)
Systemenes funksjonalitet er godt tilpasset vår avdeling					
Jeg forstår godt hvordan systemene fungerer					
Jeg forstår godt hvordan systemene kan støtte mitt informasjonsbehov					
Jeg forstår godt hvordan systemene henger sammen					

Kompetanse og kompetanseoppbygging

Indiker i hvilken grad du er enig eller uenig i følgende påstander:	Uenig (1)	Delvis uenig (2)	Delvis enig (3)	Enig (4)	Vet ikke (5)
Jeg har nødvendig kompetanse for å utføre mine oppgaver					
Jeg har nødvendig kompetanse og erfaring til å utnytte de tekniske systemenes funksjonalitet					
Jeg forstår nødvendigheten av å benytte systemene slik de er tenkt					
Jeg har tilstrekkelig erfaring til å forstå og analysere den informasjonen systemene presenterer					
Jeg har utdanning/kurs på alle systemene					
Jeg har utdanning/kurs på enkelte av systemene					
Jeg har utdanning/kurs for å forstå hvordan systemene henger sammen					
Jeg har utdanning/kurs for å forstå hvordan systemene kan støtte mitt informasjonsbehov					
Min erfaring gjør at jeg kan forstå hvordan systemene kan støtte mitt informasjonsbehov					
Min avdeling benytter tilstrekkelig tid til internopplæring på systemene					
Internopplæringen fokuserer også på hva som er viktig og nødvendig informasjon					
.. og hvorfor det er viktig å registrere riktig info					

Informasjonsinnhenting og deling

Indiker i hvilken grad du er enig eller uenig i følgende påstander:	Uenig (1)	Delvis uenig (2)	Delvis enig (3)	Enig (4)	Vet ikke (5)
Jeg vet hva slags informasjon som er viktig å detektere					
Jeg vet hvordan jeg skal detektere viktig informasjon					
Jeg vet hvordan jeg skal verifisere at detektert informasjon er riktig					
Jeg vet hvordan jeg skal registrere viktig informasjon på systemene					
Jeg får passe mengde informasjon					
Jeg er fornøyd med informasjonen jeg mottar					
Jeg er fornøy med informasjonen jeg gir					
Jeg søker informasjon etter behov					
Jeg sender informasjon i tide					
Mottatt informasjon er oppdatert og nøyaktig					

Hinder for informasjonsdeling

Indiker i hvilken grad du er enig eller uenig i følgende påstander som hinder for informasjonsdeling:	Uenig (1)	Delvis uenig (2)	Delvis enig (3)	Enig (4)	Vet ikke (5)
Tekniske utfordringer					
Funksjonelle mangler					
Systemer som ikke snakker sammen					
Tidsbegrensninger					
Sikkerhet					
Usikkerhet omkring hvem som har behov for informasjon					
Ulik prioritering internt relatert til samme oppgave					

Situasjonsforståelse

Indiker i hvilken grad du er enig eller uenig i følgende påstander:	Uenig (1)	Delvis uenig (2)	Delvis enig (3)	Enig (4)	Vet ikke (5)
Jeg har en klar oppfatning av vår egen situasjon					
Jeg har en klar oppfatning av fiendens situasjon					
Jeg vet hva operasjonens målsetning er					
Det skjer ofte misforståelser					
Vi er usikre på hvordan felles oppgaver skal utføres					
Vi kjenner hverandres ansvarsområder					
Min erfaring gjør at jeg kan lese egen situasjon ut i fra systemene					
Jeg klarer fint å lese egen situasjon selv med mangelfull og forsinket informasjon					
Min erfaring gjør at jeg kan lese fiendens situasjon ut i fra systemene					
Jeg klarer fint å lese fiendens situasjon selv med					

mangelfull og forsinket informasjon					
Jeg klarer fint å forutse fiendens handlemåte ut i fra tilgjengelig informasjon					
Jeg klarer fint å planlegge neste fase ut i fra tilgjengelig informasjonen					

Tillit

Indiker i hvilken grad du er enig eller uenig i følgende påstander:	Uenig (1)	Delvis uenig (2)	Delvis enig (3)	Enig (4)	Vet ikke (5)
Jeg kan stole på den informasjonen som presenteres av systemene					
Jeg vet i hvilken grad jeg kan stole på systemene					
Jeg vet hva systemene kan støtte meg med					
All registrert informasjon er riktig					
Registrert informasjon kan være mangelfull					
Registrert informasjon kan være manipulert					
Registret informasjon kan være feil					
Jeg kan stole på at jeg får tilgang til nødvendig informasjon gjennom systemene					

Troverdighet

Indiker i hvilken grad du er enig eller uenig i følgende påstander:	Uenig (1)	Delvis uenig (2)	Delvis enig (3)	Enig (4)	Vet ikke (5)
De tekniske systemene gjør at arbeidsoppgavene blir utført raskere					
De tekniske systemene gjør at arbeidsoppgavene blir utført enklere					
Jeg kan stole på de tekniske systemene avdelingen benytter					
De tekniske systemene er pålitelige					
De tekniske systemene er funksjonelle					

Spørreskjemaet er nå fullført!

Takk for ditt bidrag!

Intervjuskjema

Bakgrunn

Alder:		
Bostedskommune:		
Militær grad:		
Antall år i Forsvaret:		
Høyeste utdanningsnivå:	Militært:	Sivilt:

Tekniske informasjonssystemer

1. I hvilken grad mener du de tekniske systemene er tilpasset operative behov i egen avdeling?

2. I hvilken grad har du oversikt over hvordan de tekniske systemene fungerer? Hvordan henger systemene sammen? (Avhengigheter)?

3. På hvilken måte kan systemene støtte ditt informasjonsbehov?

Kompetanse og trening

4. Føler du at du har nødvendige trening og erfaring i å benytte de tekniske systemene? Hva er det som eventuelt mangler?

5. Føler du at du har nødvendig trening og erfaring i å forstå og analysere den informasjonen systemene presenterer? Hvorfor/hvorfor ikke?

6. Har du gjennomført kurs/utdanning på noen/alle systemene? Evt hvilke?

7. Har du gjennom utdanning lært hvordan systemene henger sammen og hvordan de kan støtte ditt informasjonsbehov? Eller er dette noe du evt har fått gjennom erfaring?

8. Gjennomfører avdelingen internopplæring på systemene? I tilfelle hvordan? Og hva er hovedfokus? (Fokus på nødvendig/riktig informasjon og hvorfor dette er viktig)

Informasjonsinnhenting og deling

9. Har du en klar oppfatning av hva slags informasjon som er viktig å se etter og hvordan du skal gjøre dette?

10. Hvordan kan du verifisere at denne informasjonen er korrekt? Og hvordan registrerer du dette på systemet?

11. Mener du selv at du får nødvendig informasjon for å utføre dine funksjoner i operativ sammenheng? Utdyp hvor denne informasjonen kommer i fra, og eventuelt hvilken del som er mangelfull i forhold til informasjonsbehovet ditt.

12. Har informasjonen den nødvendige kvaliteten? Hva er det som eventuelt er bra/dårlig?

13. Hva er det som eventuelt hindrer effektiv informasjonsutveksling? Går det på tekniske utfordringer eller mer på mellommenneskelige utfordringer?

Situasjonsforståelse

14. I hvor stor grad oppfatter du egen og FI situasjon korrekt i en operativ setting?

15. Skjer det ofte misforståelser? Hvis ja; kan du utdype hva slags misforståelser?

16. I hvor stor grad mener du egen erfaring og utdanning er avgjørende for riktig oppfattelse av situasjonsbildet? Klarer du å lese situasjonen selv med mangelfull og/eller forsinket informasjon?

17. I hvilken grad klarer du å forutse fiendens handlemåte ut i fra tilgjengelig informasjon?

18. Er presentert informasjon tilstrekkelig til å planlegge neste fase?

Tillit og troverdighet

19. Har du tillit til den informasjonen som blir presentert av de tekniske systemene? Hvorfor/hvorfor ikke?

20. Gir systemene deg tilgang til nødvendig informasjon? I hvilket format er da informasjonen?

21. I hvilken grad er du avhengig av de tekniske systemene for å utføre dine egne oppgaver?

22. Er de tekniske systemene pålitelige og funksjonelle? Hvor/hvorfor ikke?

Generelt

23. Har det skjedd uhell som følge av mangler/feil ved den tekniske plattformen eller at denne ikke er tilpasset operative behov? Evt pga menneskelige feil som følge av mangel på kompetanse/erfaring?

24. Hvis du skulle ønske deg en ting som burde vært forbedret relatert til den tekniske løsningen i din avdeling, hva ville det vært?

25. Er det noe jeg ikke har spurt om, men som du ønsker å tilføye?

SAMTYKKE FOR DELTAGERE I UNDERSØKELSEN

Om undersøkelsen
Dette spørreskjemaet er en del av et forskningsarbeid relatert til implementasjon av en teknologisk plattform for understøttelse av militære operasjoner. Arbeidet har som mål å identifisere faktorer som påvirker i hvilken grad den enkelte bruker er villig til å bruke systemet slik det er tenkt og i hvilken grad brukeren stoler på systemet og de data det produserer. Resultatene fra undersøkelsen skal danne grunnlag for å vurdere hvordan en felles teknologisk plattform kan implementeres raskere og sikrere. Datainnsamlingen foregår ved hjelp av dette spørreskjemaet i tillegg til felt observasjoner og komplementerende intervjuer blant militært personell i Hæren og ved Forsvarets Ingeniørhøgskole. Arbeidet utføres som en del av en Master studie i regi av NTNU og skal ferdigstilles 1.juni 2017.

Deltagelse i undersøkelsen
Ved å være deltager i undersøkelsen, kommer du til å være med på en spørreundersøkelse som består av 57 spørsmål fordelt på 7 forskjellige emner relatert til bruk av militær samhandlingsteknologi og i hvilken grad denne benyttes etter hensikten. Hvert spørsmål skal besvares ved hjelp av 4 valgmuligheter skalert fra uenig(1) til enig (4), evt vet ikke (5). Undersøkelsens varighet er beregnet til ca 30 minutter.

Hva skjer med informasjonen vi får fra deg?
Spørreskjemaet skal besvares skriftlig ved bruk av papir og penn. Opplysningene vil bli behandlet konfidensielt, og personidentifiserbar informasjon vil kun være tilgjengelig for student og veileder for dette prosjektet. Notater fra undesøkelsen vil bli tilintetgjort etter at undersøkelsen er avsluttet.

Frivillig deltagelse
Det er frivillig å delta i undersøkelsen, og man kan trekke seg fra undersøkelsen så lenge den pågår uten å oppgi noen grunn. Dersom du trekker deg vil alle data fra ditt intervju bli tilintetgjort og fjernet fra den endelige rapporten.

Undersøkelsen er meldt inn til Personvernombudet for forskning, NSD – Norsk senter for forskningsdata iht Personopplysningsloven §31.

Ved eventuelle spørsmål rundt undersøkelsen, vennligst kontakt Tonje Andreassen på e-post tonhaugen@gmail.com eller telefon 9909 4832. Resultatene fra undersøkelsen vil også være tilgjengelig for de som er interessert ved henvendelse til oppgitt kontakt person.

Samtykke erklæring

Jeg har mottatt informasjon om undersøkelsen og er villig til å delta

---

(Signatur deltaker, dato)

SAMTYKKE FOR DELTAGERE I UNDERSØKELSEN

Om undersøkelsen

Intervjuet er en del av et forskningsarbeid relatert til implementasjon av en teknologisk plattform for understøttelse av militære operasjoner. Arbeidet har som mål å identifisere faktorer som påvirker i hvilken grad den enkelte bruker er villig til å bruke systemet slik det er tenkt og i hvilken grad brukeren stoler på systemet og de data det produserer. Resultatene fra undersøkelsen skal danne grunnlag for å vurdere hvordan en felles teknologisk plattform kan implementeres raskere og sikrere. Datainnsamlingen foregår ved hjelp av intervju i tillegg til felt observasjoner og spørreskjema blant militært personell i Hæren og ved Forsvarets Ingeniørhøgskole. Arbeidet utføres som en del av en Master studie i regi av NTNU og skal ferdigstilles 1.juni 2017.

Deltagelse i undersøkelsen

Ved å være deltager i undersøkelsen, kommer du til å være med på intervju relatert til bruk av militær samhandlingsteknologi og i hvilken grad denne benyttes etter hensikten. Undersøkelsens varighet er beregnet til ca 60 minutter.

Hva skjer med informasjonen vi får fra deg?

Det gjøres opptak av intervjuet, samt notater underveis. Opplysningene vil bli behandlet konfidensielt, og personidentifiserbar informasjon vil kun være tilgjengelig for student og veileder for dette prosjektet. Notater fra undesøkelsen vil bli tilintetgjort etter at undersøkelsen er avsluttet.

Frivillig deltagelse

Det er frivillig å delta i undersøkelsen, og man kan trekke seg fra undersøkelsen så lenge den pågår uten å oppgi noen grunn. Dersom du trekker deg vil alle data fra ditt intervju bli tilintetgjort og fjernet fra den endelige rapporten.

Undersøkelsen er meldt inn til Personvernombudet for forskning, NSD – Norsk senter for forskningsdata iht Personopplysningsloven §31.

Ved eventuelle spørsmål rundt undersøkelsen, vennligst kontakt Tonje Andreassen på e-post tonhaugen@gmail.com eller telefon 9909 4832. Resultatene fra undersøkelsen vil også være tilgjengelig for de som er interessert ved henvendelse til oppgitt kontakt person.

Samtykke erklæring

Jeg har mottatt informasjon om undersøkelsen og er villig til å delta

____

(Signatur deltaker, dato)

C Adjusted questionnaire and interview guide

Spørreskjema

Bakgrunn

Alder:		
Bostedskommune:		
Militær grad:		Bransje (O/T/F):
Antall år i Forsvaret:		
Høyeste utdanningsnivå:	Militært:	Sivilt:

Tekniske informasjonssystemer

Indiker i hvilken grad du er enig eller uenig i følgende påstander:	Uenig (1)	Delvis uenig (2)	Delvis enig (3)	Enig (4)	Vet ikke (5)
1. Tale sambandet er godt tilpasset vår avdeling					
2. Det grafiske kartsystemet passer godt til vår avdeling					
3. De tekniske støtteverktøyene er godt tilpasset vår avdeling (støtteverktøy for utvikling av ordre og operasjoner, oppfølging av personell/vedlikehold)					
4. Eventuelle kameraer, GPS eller sensorer* hjelper til med å holde oversikt på situasjonen					
5. Jeg forstår godt hvordan ovennevnte systemer fungerer					

* = sensorer kan for eksempel være innbrudds system, radar, deteksjon av innbrudd i nettverk, værføler ol.

Kompetanse og kompetanseoppbygging

Indiker i hvilken grad du er enig eller uenig i følgende påstander:	Uenig (1)	Delvis uenig (2)	Delvis enig (3)	Enig (4)	Vet ikke (5)
6. Jeg har nødvendig utdanning og erfaring til å utføre mine oppgaver					
7. Jeg har nødvendig utdanning og erfaring til å utnytte de ovennevnte systemers funksjonalitet					
8. Jeg har tilstrekkelig erfaring til å forstå og analysere den informasjonen systemene presenterer					
9. Jeg har utdanning/kurs på alle systemene					
10. Jeg har utdanning/kurs på enkelte av systemene					
11. Jeg har utdanning/kurs for å forstå hvordan systemene henger sammen					
12. Jeg har utdanning/kurs for å forstå hvordan jeg kan få tilgang til nødvendig informasjon					
13. Min erfaring gjør at forstår hvordan jeg kan få tilgang til nødvendig informasjon					
14. Min avdeling benytter tilstrekkelig tid til internopplæring på ovennevnte systemer					
15. Internopplæringen fokuserer også på hva som er viktig og nødvendig informasjon					

Informasjonsinnhenting og deling

Indiker i hvilken grad du er enig eller uenig i følgende påstander:	Uenig (1)	Delvis uenig (2)	Delvis enig (3)	Enig (4)	Vet ikke (5)
16. Jeg vet hva slags informasjon jeg skal søke etter					
17. Jeg vet hvordan jeg skal søke etter viktig informasjon					
18. Jeg vet hvordan jeg skal kontrollere at informasjonen er riktig					
19. Jeg vet hvordan jeg skal registrere viktig informasjon på systemene					
20. Jeg får passe mengde informasjon					
21. Jeg er fornøyd med informasjonen jeg mottar					
22. Jeg er fornøyd med informasjonen jeg gir					
23. Jeg søker informasjon etter behov					
24. Jeg sender informasjon i tide					
25. Mottatt informasjon er oppdatert og nøyaktig					

Hinder for informasjonsdeling

Indiker i hvilken grad du er enig eller uenig i følgende påstander som hinder for informasjonsdeling:	Uenig (1)	Delvis uenig (2)	Delvis enig (3)	Enig (4)	Vet ikke (5)
26. Tekniske utfordringer					
27. Funksjonelle mangler					
28. Systemer som ikke snakker sammen					
29. Tidsbegrensninger					
30. Sikkerhet					
31. Usikkerhet omkring hvem som har behov for informasjon					

Situasjonsforståelse

Indiker i hvilken grad du er enig eller uenig i følgende påstander:	Uenig (1)	Delvis uenig (2)	Delvis enig (3)	Enig (4)	Vet ikke (5)
32. Jeg har en klar oppfatning av vår egen situasjon					
33. Jeg har en klar oppfatning av fiendens situasjon					
34. Jeg vet hva operasjonens mål er					
35. Det skjer ofte misforståelser					
36. Vi er usikre på hvordan felles oppgaver skal utføres					
37. Vi kjenner hverandres ansvarsområder					
38. Min erfaring gjør at jeg kan forstå egen situasjon					
39. Jeg klarer fint å forstå egen situasjon selv med mangelfull og forsinket informasjon					
40. Min erfaring gjør at jeg kan lese fiendens situasjon					

41. Jeg klarer fint å lese fiendens situasjon selv med mangelfull og forsinket informasjon					
42. Jeg klarer fint å forutse fiendens handlemåte ut i fra tilgjengelig informasjon					
43. Jeg klarer fint å planlegge neste fase ut i fra tilgjengelig informasjonen					

Tillit

Indiker i hvilken grad du er enig eller uenig i følgende påstander:	Uenig (1)	Delvis uenig (2)	Delvis enig (3)	Enig (4)	Vet ikke (5)
44. Jeg kan stole på den informasjonen som rapporteres via tale sambandet					
45. Jeg kan stole på den informasjonen som presenteres på det grafiske kartsystemet					
46. Jeg kan stole på den informasjonen som presenteres ved hjelp av sensorer, GPS, kamera					
47. Jeg vet hva systemene kan støtte meg med					
48. All registrert informasjon er riktig					
49. Registrert informasjon kan være mangelfull					
50. Registrert informasjon kan være manipulert					
51. Registret informasjon kan være feil					

Troverdighet

Indiker i hvilken grad du er enig eller uenig i følgende påstander:	Uenig (1)	Delvis uenig (2)	Delvis enig (3)	Enig (4)	Vet ikke (5)
52. Tale sambandet gjør at arbeidsoppgavene blir utført raskere og enklere					
53. Det grafiske kartsystemet gjør at arbeidsoppgavene blir utført raskere og enklere					
54. Kameraer, GPS og sensorer gjør at arbeidsoppgavene blir utført raskere og enklere					
55. Tale sambandet er pålitelig og funksjonelt					
56. Det grafiske kartsystemet er pålitelig og funksjonelt					
57. Kameraer, sensorer og GPS er pålitelig og funksjonelt					

Spørreskjemaet er nå fullført!

Takk for ditt bidrag!

Intervjuskjema

Bakgrunn

Alder:		
Bostedskommune:		
Militær grad:		Bransje (O/T/F):
Antall år i Forsvaret:		
Høyeste utdanningsnivå:	Militært:	Sivilt:

Tekniske informasjonssystemer

1. I hvilken grad mener du de tekniske systemene er tilpasset operative behov i egen avdeling? (Tale samband, grafiske kart system, sensorer, kamera, GPS..)

2. I hvilken grad har du oversikt over hvordan de tekniske systemene fungerer? Hvordan henger systemene sammen? (Avhengigheter?)

Kompetanse og kompetanseoppbygging

3. Føler du at du har nødvendig utdanning og erfaring i å benytte de tekniske systemene? Og for å utføre egne oppgaver? Hva er det som eventuelt mangler? (Separer mellom de ulike systemene, også ikke tekniske/mennesker)

4. Føler du at du har nødvendig trening og erfaring i å forstå og analysere den informasjonen systemene presenterer? Hvorfor/hvorfor ikke?

5. Har du gjennomført kurs/utdanning på noen/alle systemene? Evt hvilke?

6. Har du gjennom utdanning lært hvordan systemene henger sammen og hvordan de kan støtte ditt informasjonsbehov? Eller er dette noe du evt har fått gjennom erfaring?

7. Gjennomfører avdelingen internopplæring på systemene? I tilfelle hvordan? Og hva er hovedfokus? (Fokus på nødvendig/riktig informasjon og hvorfor dette er viktig?)

Informasjonsinnhenting og deling

8. Under en operasjon: Har du en klar oppfatning av hva slags informasjon som er viktig å se etter og hvordan du skal gjøre dette?

9. Hvordan kan du verifisere at denne informasjonen er korrekt? Og hvordan registrerer du dette på systemet?

10. Mener du selv at du får nødvendig informasjon for å utføre dine funksjoner i operativ sammenheng? Utdyp hvor denne informasjonen kommer i fra, og eventuelt hvilken del som er mangelfull i forhold til informasjonsbehovet ditt.

11. Har informasjonen den nødvendige kvaliteten? Hva er det som eventuelt er bra/dårlig?

12. Hvordan er du fornøyd med den informasjonen du selv gir?

13. Hva er det som eventuelt hindrer effektiv informasjonsutveksling? Går det på tekniske utfordringer eller mer på mellommenneskelige utfordringer? Konkretiser gjerne.

Situasjonsforståelse

14. I hvor stor grad oppfatter du egen og FI situasjon korrekt i en operativ setting?

15. Skjer det ofte misforståelser? Hvis ja; kan du utdype hva slags misforståelser?

16. I hvor stor grad mener du egen erfaring og utdanning er avgjørende for riktig oppfattelse av situasjonsbildet? Klarer du å lese situasjonen selv med mangelfull og/eller forsinket informasjon?

17. I hvilken grad klarer du å forutse fiendens handlemåte ut i fra tilgjengelig informasjon?

18. Er presentert informasjon tilstrekkelig til å planlegge neste fase?

Tillit og troverdighet

19. Har du tillit til den informasjonen som blir presentert av de tekniske systemene? Hvorfor/hvorfor ikke? (Separer mellom de ulike systemene)

20. Gir systemene deg tilgang til nødvendig informasjon? I hvilket format er da informasjonen (tale, posisjoner, tekst..)?

21. I hvilken grad er du avhengig av de tekniske systemene for å utføre dine egne oppgaver? Hvordan støtter de dine oppgaver?

22. Er de tekniske systemene pålitelige og funksjonelle? Hvor/hvorfor ikke? (Separer mellom de ulike systemene)

Generelt

23. Har det skjedd uhell som følge av mangler/feil ved den tekniske plattformen eller at denne ikke er tilpasset operative behov? Evt pga menneskelige feil som følge av mangel på kompetanse/erfaring?

24. Hvis du skulle ønske deg en ting som burde vært forbedret relatert til den tekniske løsningen i din avdeling, hva ville det vært?

25. Er det noe jeg ikke har spurt om, men som du ønsker å tilføye?

D Results from preliminary research at The Norwegian Defence University College of Engineering - Telematics

Spørreskjema til veileder ifm støtte til Masterprosjekt

Indiker i hvilken grad du er enig eller uenig i følgende påstander:	**Uenig (1)**	**Delvis uenig (2)**	**Delvis enig (3)**	**Enig (4)**	**Vet ikke (5)**
Informasjonen studentene søker er relevant for oppdraget			3	7	
Informasjonen studentene søker er oppdatert og riktig			4	6	
Studentene kvalitetssikrer innhentet informasjon		3	5	1	1
Studentene klarer ved hjelp av innhentet informasjon å skape seg god og riktig situasjonsoversikt		3	7		
Metode for ordregivning påvirker i stor grad LFs/leders situasjonsforståelse (*)	1		3	3	3
Metode for ordregivning påvirker i stor grad samhandling i laget		1	1	8	
LFs/leders personlighet påvirker i stor grad samhandling i laget (**)				10	
LFs/leders personlighet påvirker i stor grad tilliten til LFs ordre og føringer			1	6	3
Bruk av tekniske hjelpemidler øker samhandlingen i laget		2	5	2	1
Bruk av tekniske hjelpemidler øker LFs situasjonsforståelse			5	4	1
Angrep via nettverk blir detektert på et tidlig tidspunkt	3			4	1
Angrep via nettverk blir håndtert på en god måte	1	2	4	2	1
Jamming av radiosignal blir detektert raskt				3	4
Jamming av radiosignal blir håndtert på en god måte				3	4

(Antallet i hver rute angir hvor mange av respondentene som har krysset av for dette valget)

Tilleggsopplysninger respondentene besvarte skriftlig:

(*) Hva var det evt ved metode for ordregivning som påvirket situasjonsforståelse/samhandling?

(**)Hva var det ved LFs personlighet som evt påvirket tillit/samhandling?

Utfyllende informasjon relatert til ovennevnte punkter:
Hvor henter studentene informasjon til oppdragene? (Gjennom datasystemene, via radio, hos foresatte, hos andre lagsmedlem, andre i staben)

Hvordan kvalitets sikrer evt studentene innhentet informasjon (eks oppdateringstidspunkt, fra hvem kommer info, oppklarende spørsmål ved usikkerhet, diskusjon internt i laget for å skape større forståelse/klarhet)

Med ulike metoder for ordre giving menes for eks ordre personlig fra troppssjef, ordre som melding via datasystem, tekstmelding, ordre muntlig via radio osv.

Andre utfyllende kommentarer som ikke framkommer gjennom spørreskjema ovenfor:

(Svar fra respondentene er lagt i eget vedlegg som ikke vil bli publisert)

Resultats from questionnaire conducted at FIH:

Questionnaire	Disagree	Partly disagree	Partly agree	Agree	I don't know
Technical information systems					
1. The system's functionality is well adjusted to your unit	0	1	7	7	0
2. I understand well how the systems work	0	2	6	7	0
3. I understand well how the information systems can support my need of information	0	2	2	11	0
4. I understand well how the systems are connected	0	1	6	8	0
Competence and training					
5. I hold the necessary competence to perform my duties	0	2	6	7	0
6. I hold the necessary competence and experience to utilize the technical platform	0	3	10	2	0
7. I understand why it is necessary to employ the systems in a proper manner	0	0	6	9	0
8. I have necessary experience to understand and analyze information presented by the systems	0	2	8	5	0
9. I have education/course for all the systems	1	3	8	3	0
10. I have education/course for some of the systems	0	0	4	11	0
11. I have education/course in order to understand how the systems are connected	2	4	3	5	1
12. I have education/course in order to understand how the systems can support my need of information	1	3	5	5	1
13. My experience help me to understand how the systems can support my need of information	1	1	6	7	0
14. My unit spends enough time for internal learning on the technical platform	0	6	7	2	0
15. The internal learning focuses on finding important and necessary information	0	5	5	4	1
16. .. and why it is important to register correct information	1	3	5	3	3
Information collection and sharing					
17. I know what kind of information to detect	0	2	11	2	0
18. I know how to detect important information	0	4	10	1	0
19. I know how to verify collected information	1	8	5	0	1
20. I know how to register important information into the system	0	2	9	3	1
21. I receive enough information	1	2	7	4	1
22. I am satisfied with received information	0	2	11	0	2
23. I am satisfied with the information I deliver	0	1	11	2	1
24. I seek information on demand	0	1	5	9	0
25. I send information in time	1	4	5	2	3
26. Received infromation is updated and correct	0	4	8	1	2
Obstacles to information sharing					
27. Technical challenges	0	3	10	2	0
28. Functional errors	0	5	7	2	1
29. Systems not talking together	0	2	7	4	2
30. Time limitations	0	1	7	6	1
31. Security	0	3	7	3	2
32. Uncertanties related to who will need the information	0	4	6	4	1
33. Different internal prioritizing related to the same task	0	3	3	3	6
Situational awareness					
34. I am very well aware of our own situation	0	1	9	5	0
35. I am very well aware of our enemy ituation	1	6	8	0	0
36. I know the operation's objectives	0	2	6	7	0
37. Misunderstandings happen a lot	0	7	4	4	0
38. We do not know how to solve common tasks	0	7	6	0	2
39. We know each others responsibilities	0	2	8	5	0
40. My experience helps me to understand our situation based on information from the systems	1	3	7	4	0
41. I understand our situation even with lacking and delayed information.	0	7	6	0	2
42. My experience helps me to understand the enemy's situation based on information from the systems	0	6	9	0	0
43. I understand the enemy situation even with lacking and delayed information.	1	9	3	0	2
44. I am able to predict the enemy's next move based on available informationn	0	10	4	0	1
45. I am able to plan the next phase of the operation based on available information	0	2	7	4	2
Trust					
46. I can trust the information presented by the systems	0	1	13	1	0
47. I know to what extent I can trust the systems	0	1	6	8	0
48. I know how the systems can support me	0	1	6	8	0
49. All registered information is correct	2	9	1	2	1
50. Registered information can lack details	0	0	2	12	1
51. Registered information can be manipulated	0	2	5	7	1
52. Registered information can be wrong	1	0	4	9	1
53. I know that the systems will feed me with necessary information	0	2	11	2	0
Trustworthiness					
54. The technical systems enable faster task performance	0	1	9	5	0
55. The technical systems make the tasks easier to accomplish	0	3	6	6	0
56. I can trust the technical systems employed by the unit	0	3	6	6	0
57. The technical systems are reliable	1	3	9	2	0
58. The technical systems are functional	0	2	8	5	0

E Questionnaire army unit 1 and 2

Resultats from questionnaire conducted in two different army units:

Questionnaire	Disagree	Partly disagree	Partly agree	Agree	I don't know
Technical information systems					
1. The communication system is well adjusted to your unit	1	2	5	9	0
2. The graphical map interface is well adjusted to your unit	0	0	5	12	0
3. The technical support tools are well adjusted to your unit	0	0	7	8	2
4. Cameras, sensors or GPSs help me to keep track of the situation	0	0	5	10	2
5. I understand well how the systems work	0	2	4	9	2
Competence and training					
6. I hold the necessary education and experience to perform my duties	0	0	4	13	0
7. I hold the necessary competence and experience to utilize the technical platform	0	1	10	6	0
8. I have necessary experience to understand and analyze information presented by the systems	0	2	5	10	0
8. I have education/course for all the systems	5	3	8	1	0
10. I have education/course for some of the systems	0	2	4	10	1
11. I have education/course in order to understand how the systems are connected	1	3	6	7	0
12. I have education/course in order to understand how the systems can support my need of information	2	4	2	9	0
13. My experience help me to understand how the systems can support my need of information	0	2	4	11	0
14. My unit spends enough time for internal learning on the technical platform	1	5	9	2	0
15. The internal learning focuses on finding important and necessary information	0	2	11	4	0
Information collection and sharing					
16. I know what kind of information to search for	2	0	8	7	0
17. I know how to search for important information	1	2	5	9	0
18. I know how to verify collected information	1	0	7	8	1
19. I know how to register important information into the system	1	3	4	7	2
20. I receive enough information	1	2	9	4	1
21. I am satisfied with received information	1	1	10	5	0
22. I am satisfied with the information I deliver	1	1	11	4	0
23. I seek information on demand	0	0	4	13	0
24. I send information in time	0	1	8	8	0
25. Received infromation is updated and correct	0	3	9	5	0
Obstacles to information sharing					
26. Technical challenges	0	1	9	7	0
27. Functional errors	0	3	10	3	1
28. Systems not talking together	0	4	8	4	1
29. Time limitations	2	7	5	1	2
30. Security	2	8	3	2	2
31. Uncertanties related to who will need the information	3	6	5	1	2
Situational awareness					
32. I am very well aware of our own situation	0	0	9	8	0
33. I am very well aware of our enemy ituation	0	4	10	2	1
34. I know the operation's objectives	0	0	2	15	0
35. Misunderstandings happen a lot	3	6	7	1	0
36. We do not know how to solve common tasks	7	7	3	0	0
37. We know each others responsibilities	0	0	7	10	0
38. My experience helps me to understand our situation	0	0	4	13	0
39. I understand our situation even with lacking and delayed information.	0	2	10	5	0
40. My experience helps me to understand the enemy's situation	0	5	9	2	1
41. I understand the enemy situation even with lacking and delayed information.	1	8	6	2	0
42. I am able to predict the enemy's next move based on available informationn	1	7	5	3	1
43. I am able to plan the next phase of the operation based on available information	0	2	8	4	3
Trust					
44. I can trust the information presented by the communication system	0	0	2	15	0
45. I can trust the information presented by the graphical map interface	0	1	9	7	0
46. I can trust the information presented by sensors, cameras and GPS	0	1	7	9	0
47. I know how the systems can support me	0	0	4	13	0
48. All registered information is correct	4	5	6	2	0
49. Registered information can lack details	0	0	11	6	0
50. Registered information can be manipulated	1	4	6	4	2
51. Registered information can be wrong	0	2	8	6	1
Trustworthiness					
52. The communication system enables faster task performance	0	0	11	6	0
53. The graphical map interface enables faster task performance	0	1	6	10	0
54. Sensors, cameras and GPS enable faster task performance	0	1	10	5	1
55. The communication system is functional and reliable	1	4	5	7	0
56. The graphical map interface is functional and reliable	0	2	10	5	0
57. Sensors, cameras and GPS are functional and reliable	0	3	9	4	1