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

Tonje Andreassen[⋆] and Jose J. Gonzalez[‡]

[⋆]The Norwegian Armed Forces Cyber Defence, Lillehammer, Norway
[‡]University of Agder, Dept. for ICT. josejg@uia.no

Abstract

The Norwegian Armed Forces are supposed to implement Network based Defence within the next couple of decades, but the implementation process is suffering from different obstacles, putting military operations at stake. The purpose of this research was to identify factors delaying the implementation process, and to investigate if the delay would have a negative impact on the users' perceived trust. Practical research consisting of interviews and questionnaires, and adapted system dynamic models from the oil sector were employed as methodologies to investigate the implementation process. The research identified inappropriate technological solutions, education of operators at random, complex information collection together with inadequate level of perceived trust among the operators as possible obstacles. The obstacles introduce gaps between technology implemented and knowledge needed to utilize it, possibly also affecting the operators' perceived trust. This paper suggests employing a full-fledged system dynamic model in parallel with the implementation process to ensure implementation in time, within the estimated cost and with reduced risk.

Keywords

Network Centric Warfare (NCW), military operations, situational awareness (SA), human factor(s), Network based Defence (NbF), trust.

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. Owing to budget pressure, 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 visualized as friend (blue spot) or foe (red spot) on an interactive map, or information delivered as intelligence directly from the soldiers via the networks.

This paper was presented at the NIK-2017 conference; see http://www.nik.no/.

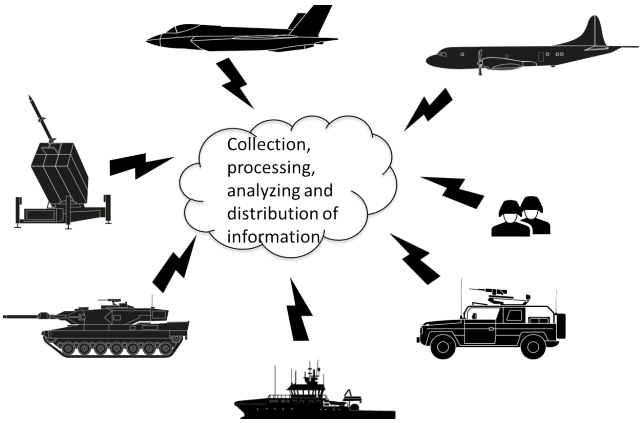

Figure 1: Conceptual model of Network Based Defence

The Norwegian Armed Forces are supposed to implement Network based Defence within the next couple of decades [7] to achieve information superiority and to enable speed of command during operations. The transition from traditional to Network based operations implicates a shift from platform based operations to network centric operations. The implementation is however suffering from different obstacles that are challenging and slowing down the process. Some operative units are impatiently adjusting solutions for testing of Network based Defence, but the Defence in total has lacking will and ability for implementation [20]. The delayed implementation affects the entire Norwegian Armed Forces, and can put soldier lives and operations at stake. The purpose of this research was to identify factors delaying the implementation process of Network based Defence. Another aspect of the research was to investigate if the delay would have a negative impact on the users' perceived trust. Practical research consisting of interviews and questionnaires was employed to investigate the implementation process of Network based Defence. In addition, adapted system dynamic models from the oil sector were employed to model the transition from traditional to network-based operations in the Norwegian Defence. This research identified several obstacles related to knowledge introducing gaps between technology implemented and knowledge needed to utilize it. This might in turn also affect the operators' perceived trust.

2 Background

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 [4]. 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 [16]. 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 [4]. The strategic objective of Network based Defence is to efficiently utilize technological infrastructure to support network based national operations and network based operations abroad [7]. A successful implementation relies on compatible systems, an excellent information infrastructure and intellectual capital [4]. 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 [6].

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 from 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 information 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.

Studied literature indicated that technology often is implemented much faster than relevant new knowledge, organization and doctrines are developed ([5] and [4]). Thus, there is a risk that technology, procedures and intellectual capital are not aligned also for Network based Defence. Comparable processes and consequences were found in a work done by Rich et al [19] and Qian [17]. They used system dynamic models to study Integrated Operations in the oil sector, modelling the transition from traditional to network-based operations. What they found, was if knowledge is not developed in parallel with the operation transition when technology is implemented, vulnerability is affected. As knowledge is an antecedent of trust and also a prerequisite to situational awareness ([21]), possible vulnerabilities introduced into the process might be inadequate level of trust and inappropriate situational awareness.

Trust is defined "to believe that someone is good and honest and will not harm you, or that something is safe and reliable" [3]. Trust is therefore tightly connected to the user's perception. As described by Jian et al [11], 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. Lee [12] 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. Too low trust in the system can affect the operator's willingness to employ it [2]. On the flip side, too high reliance on the system can result in the operator not noticing system fails. Inappropriate perceived trust, meaning both too high or too low trust in the system or to the information presented by the systems, can be caused by unreliable systems. In addition, inappropriate percieved trust can be caused by lack of competence and experience in employing the technical platform. Inadequate perceived trust and inappropriate competency might in turn result in inappropriate use of the technical platform and wrong interpretation of the information ([12] and [15]).

Research questions

Studied literature together with preliminary study of system dynamic models from Integrated Operations served as a basis to deduce five research questions:

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

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

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

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

RQ5: How will a system dynamic model simplify and reduce risk related to the integration

3 Methodologies

To investigate the five research questions, 2 different methodologies were used. System dynamic models from Integrated Operations in the oil industry were adapted and employed to model the transition from traditional to network-based operations in the Norwegian Armed Forces. This was based on the assumption that the processes related to transition to Integrated Operations and the transformation to Network based Defence shared the basics of introduction of new processes that required creation of new knowledge. Practical research including interviews and questionnaires were conducted in two different army units.

System dynamic models

System Dynamic (SD) models are high level descriptions of problem-relevant features of a reality domain. They are less complex and easier for humans to understand than the real world [23] and model a problem over time. Some details will be lost, but simplicity assists thinking and decision making. In addition the models serve as good communication tools. The methodology helps identifying unintentional effects acting against the stated objectives. This insight can be employed to understand how various problems can be solved. Qualitative SD models serve as a basis to develop quantitative models with the possibility to simulate future scenarios.

In this research, the objective was to find obstacles slowing down the implementation of Network based Defence. One assumption was 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 the implementation of Integrated Operations were identified by Rich et al [19] and further developed by Qian in her PhD work "Mitigating Information security risks during the Transition to Integrated Operations" [17]. 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 [9]. Because the transformation will include implementation of new technological equipment and information technology, there are no existing records of previous events [19]. In addition, Network based Defence and Integrated Operations share several similarities. Both systems include sensors, and they present current status based on reported inputs. If the inputs are wrong, the situational picture is also wrong. To utilize the system, the operators need proper education and training, and the user interface must be expedient ([19] and [4]). Lack of knowledge and misunderstandings might in both cases result in fatal consequences for ongoing operations. Historically, SD models were often employed in the safety domain, but the model is also applicable for problems related to information security ([8] and [22]). System dynamic models from Ying Qian's work related to Integrated Operations are therefore adapted in order to study the two processes of operation transition and knowledge development in Network based Defence in parallel.

The adapted SD models are denoted preliminary SD models of NbF. NbF is used as an abbreviation for Network based Defence (Nettverksbasert Forsvar in Norwegian spelling).

The practical research

The focus of this research was to investigate how knowledge is considered in relation to the implementation process of Network based Defence. Competence, training and experience are important prerequisites to situational awareness [21], and all of them are antecedents of trust. Practical research was therefore employed to investigate knowledge from 4 different angles, assuming to be of relevance for situational awareness and perceived trust among the users. The 4 focus areas were: 1) Knowledge for how to develop a technological platform supporting military operations. 2) The user's knowledge of how to utilize the technological platform. 3) Knowledge about the operational objectives and the situational picture. 4) If the user knew to what extent it is possible to trust information presented by the systems. In order to collect relevant information, an interview guide and a questionnaire were developed. In order to make the interview guide and the questionnaire more user friendly, the 4 focus areas were divided into 7 sub domains: Technical information systems, competence and training, information collection and sharing, obstacles to information sharing, situational awareness, trust and trustworthiness. Interviews and questionnaires were then carried out in two different army units. 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. 11 participants were interviewed and 17 persons participated in the questionnaire. Some participated in both, so the total number of participants were 22.

4 Results and discussion

This section includes a summary of the practical research. The results from the practical research is then compared with adapted preliminary SD models of NbF.

Summary of findings from the practical research

The results from the questionnaire can be found in figure 2, including both the actual questions and the responses. The interview guideline focused on the same main areas, but searched to find some deeper answers to the addressed issues. A summary from the practical research follows, looking into knowledge from 4 different angles. The results from the practical research include answers related to research question 2 and 3.

Knowledge for developing a military technological platform

Most of the respondents seem to be pretty satisfied with the technical information systems. Less of the participants seem to be satisfied with the technical support tools. Complexity, difficult user interfaces and continuous development challenge the use of the technological platform, requiring good, technical expertise which is a scarce resource. Lack of ownership and responsibility seem to result in lack of common solutions. Large and heavy equipment challenge the usability. The lack of interoperability within the system and with other nations also support the assumption of unadjusted solutions. In addition, technical challenges, functional errors, and systems not talking together, hamper the information sharing. Hence, more time has to be spent to follow up that messages are received and understood, stealing time from the actual operations. All the participants in

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

Figure 2: Results from the practical research including questions and responses.

the questionnaire more or less agreed that all the technical information systems enable faster task performance. The reliability seems however to be 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

The majority of the participants seem to 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. Less of the participants seemed to hold enough competence to fully utilize the technological platform. This can be explained by challenges related to turnover and competence transfer. Regular practice based on vested interest and curiosity is however 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.

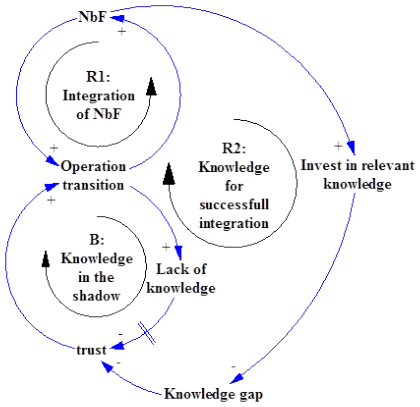

Figure 3: Parent model of Network based Defence implementation

Knowledge about operational objectives and the situation

The mission's objective seems obvious for all the respondents. All of the participants seem more or less aware of their own situation. The majority of the respondents find it more difficult to understand the enemy's situation. Education together with experience is necessary to achieve the required level of situational awareness, 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.

The user's trust in information presented by the systems.

The practical research indicates that the operators trust information presented by the communication system. Less of the participants seem to trust information presented by other technical systems to full extent. Most of the participants seem to be aware that information presented by the systems might be incorrect due to lacking details, that they are manipulated or wrong. The ordinary user however, tends to trust and depend on the graphical interface completely. In addition, the technical platforms are not employed properly due to complexity. Test and verification are not done before released, possibly resulting in reduced trust in the platform.

Practical results combined with preliminary SD models of NbF

To investigate the results from the practical research further, system dynamic models from integrated operations were adapted to the transformation process of Network based Defence. The SD models together with the results from the practical research served as a basis to answer four of the research questions further.

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

The SD model in figure 3 is an archetype, which is a short-hand version of system dynamic models. Archetypes are usually drawn as causal feedback loops, consisting of arrows

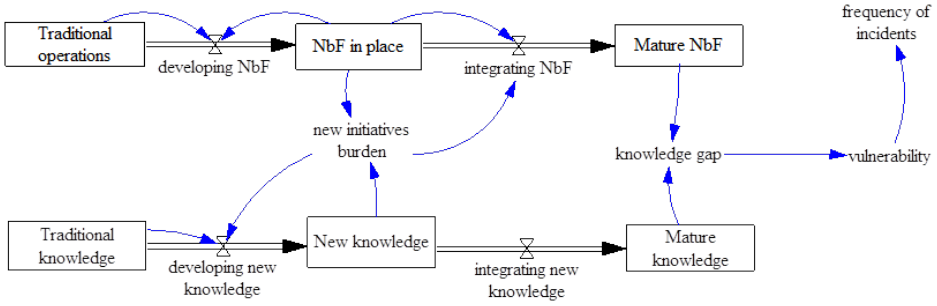

Figure 4: Conceptual model for the transition of NbF. Adapted from Qian [18]

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. The SD model in figure 3 serves as a parent model to explain the transformation from traditional operations to Network based Defence and visualizes the first research question. The objective is to transform more and more of the traditional operations to Network based Defence (NbF). This is visualized with the reinforcing loop, R1: Integration of NbF. R1 is reinforcing itself, and the speed of the transformation will increase when more of the operations are transformed into NbF. But when more of the operations are transformed, the operators lack knowledge and experience to conduct this new type of operations. Lack of knowledge will act as a constraint, and a knowledge gap will appear. The knowledge gap will most likely affect the operator's perceived trust. After a while, (delayed), the balancing loop, B: Knowledge in the shadow, will start acting against the intended outcome, reducing the operation transition. To reduce the constraints and increase the transformation speed, the organization needs to invest in relevant knowledge. This is illustrated with the reinforcing loop, R2: Knowledge for successful integration. If the organization fails to invest in relevant knowledge, the transformation process will be delayed, resulting in unexpected consequences.

Studied literature of Network based Defence identified gaps and incompatibilities between technology implemented and procedures and knowledge needed to utilize it. Similar obstacles were identified during the practical research. Insufficient technological solutions, education of operators at random and complex information collection and sharing suggest that technology, procedures and intellectual capital are not aligned to each other. The challenges are visualized in another preliminary SD model of NbF. The operation transition and knowledge development are modelled as two parallel processes as illustrated in figure 4. Both are developed through three stages, starting with the traditional operations, followed by operations and knowledge in place and at last, mature processes. In stage 2, operations and knowledge are in place, but not working properly. After a while, with the right use of resources, the operations and knowledge grow mature. But when implementing the two processes in parallel, this is a burden to people. The new initiatives trap transition to Network based Defence. Because change is difficult, the process is slowing down. The transition will affect the organizational structure and change the social structure. In addition, organizational change will in most cases meet some resistance. These factors increase the workload for the operators and reduce productivity of learning new type of operations. In addition, maturation of new knowledge takes time. It is easier to understand what to do, than how to do it. A knowledge gap will

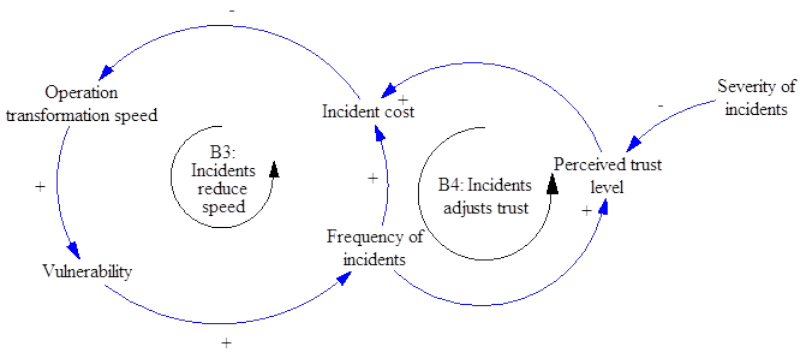

Figure 5: Causal loop diagram for incidents and transition speed. Adapted from Qian [17]

be introduced, resulting in increased vulnerability and increased number of incidents. Incidents in this context might be accidents or collateral damage on the battlefield.

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

Results from the practical research indicate that achieving appropriate situational awareness and adequate perceived trust are complicated, relying on information from several sources. The user's perceived trust in the technological platform is also challenged by poor test and verification procedures. In addition, the knowledge gap introduced as a result of unadjusted processes between the operation transition and knowledge development, will affect the operators' perceived trust, as knowledge is an antecedent of trust [21]. When the perceived trust is too high or too low, information and systems are not handled as expected to support Network based Defence and military operations. The result might be increased risk and delayed transformation process.

How will the perceived trust affect the implementation of Network based Defence?

The adapted preliminary NbF SD model in figure 5 shows that an increase in the transformation speed related to Network based Defence will increase the vulnerability, frequency of incidents and the incident cost. These factors together with severity of incidents are all factors affecting and adjusting the operator's perceived trust. It can be assumed that more severe incidents will have more significance. In addition, inappropriate perceived trust is a vulnerability together with inadequate situational awareness. To adjust the perceived trust and to learn from incidents, incidents and events must be registered. The lack of routines and procedures for registering incidents identified during the practical research, introduce challenges for the organization 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.

Without proper routines for registering incidents, the operators might not be aware that incidents happen. The perceived trust will not be adjusted, whether is it too high or too low. Hence, the operators are not aware that their perceived trust 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 process.

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

Based on the previous part of the discussion, there is a strong indication that knowledge development is not very well adjusted to the operation transition of Network based Defence. Post-mortem assessments of system dynamic models have shown significant cost-benefit utilization when employed in parallel with new technology adoption[14]. The costs related to delay and disruption for various projects are high, while the costs of modelling relatively low. Estimated benefit utilization in this context, is in the ratio 200:1 [10]. This paper 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 process to ensure implementation in time, within the estimated cost and with reduced risk.

5 Conclusion and future work

Based on the obtained results, there is a strong indication that the processes of operation transition and knowledge development in Network based Defence are not very well adjusted to each other, resulting in a knowledge gap. Insufficient technological solutions, education of operators at random and complex information collection and sharing challenge the implementation process, and will most likely result in increased vulnerability and increased number of incidents during military operations. The technological systems are complex, have difficult user interfaces and are under continuous development. Hence, there seems to be a lack of knowledge related to development of the technological platforms. The user's knowledge of how to utilize the technological platform is neither properly considered. Vested interest and curiosity is essential to employ the solutions properly and get insight into advanced functionality. In addition, the implementation process seems to lack a comprehensive approach related to education and development of procedures.

To achieve appropriate situational awareness, information must be collected from several sources. Even if the users are aware that presented information can be incorrect, the operators tend to trust most of the information. Perceived trust is also affected by the introduced knowledge gap. Inadequate perceived trust might result in inappropriate use of the technological platform or wrong interpretation of presented information. Identified, lacking routines for registering incidents challenge the ability to adjust the processes of operation transition and knowledge development to each other. It is also difficult to learn from incidents and to adjust the perceived trust among the operators. Hence, it is difficult to understand the risks related to the operation transition of Network based Defence and to identify factors challenging the implementation process. In order to ensure implementation in time, within the estimated cost and with reduced risk, this paper suggests employing a full-fledged system dynamic model in parallel with the implementation process of Network based Defence.

Future work

In order to enhance the process of implementing Network based Defence, this research recommend to implement a living SD model of NbF to follow the implementation process

in parallel. The SD model can e.g. be supported by the Delphi method [13] to verify obtained results. The process must consist of domain experts including a cross sectional group from The Norwegian Armed Forces to extend the selection from this research. First, a proactive full SD model of NbF can be developed investigating possible scenarios and conduct what-if studies. This model can be further developed to a customized, living system dynamic model. By developing a living model in parallel with the implementation process, solutions can be simulated 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.

6 Acknowledgements

This research was conducted as a Master's thesis [1] and Jose J. Gonzalez was principal supervisor as adjunct professor at NTNU. Ying Qian permitted reuse and adaption of developed system dynamic models from her PhD "Mitigating Information security risks during the Transition to Integrated Operations" [17]. Ivar Kjærem and Roger Johnsen from the Norwegian Defence helped with guidelines and support related to the military context. All contributions are highly appreciated.

References

[1] Tonje Andreassen. The role of trust when implementing network based defence in the norwegian armed forces. Master's thesis, Norwegian University of Science and Technology, Gjøvik, 2017.

[2] Robert S Bolia, Michael A Vidulich, and W Todd Nelson. Unintended consequences of the network-centric decision making model: Considering the human operator. Technical report, DTIC Document, 2006.

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

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

[5] Egil Daltveit, Jan Frederik Geiner, and Palle Ydstebø. Trends in military operations. (Trender i militære operasjoner). Technical report, Norwegian Defence Research Establishment (FFI), 2010.

[6] Defence Security Department. *Security concept for Network based Defence (Sikkerhetskonsept for et nettverksbasert forsvar)*. 2011.

[7] Department of Defence. Implementation letter for the Norwegian Defence 2010 (2009). (Iverksettingsbrev for Forsvaret gjennomføringsåret 2010). Available at `https://www.regjeringen.no/globalassets/upload/fd/budsjettdokumenter/ivb-2010_18-des-2009.pdf` (15.11.2016), 2009.

[8] Farhad Foroughi. The application of system dynamics for managing information security insider-threats of it organization. In *Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.*, 2008.

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

[10] James. System dynamics applied to project management: A survey, assesment, and directions for future research. In *International System Dynamics Conference*, 2007.

[11] Jiun-Yin Jian, Ann M Bisantz, and Colin G Drury. Foundations for an empirically determined scale of trust in automated systems. *International Journal of Cognitive Ergonomics*, 4(1):53–71, 2000.

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

[13] Harold A Linstone, Murray Turoff, et al. *The Delphi method: Techniques and applications*, volume 18. Addison-Wesley Publishing Company, Advanced Book Program, 2002.

[14] James M Lyneis and David N Ford. System dynamics applied to project management: a survey, assessment, and directions for future research. *System Dynamics Review*, 23(2-3):157–189, 2007.

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

[16] William A Owens. The emerging US system-of-systems. Technical report, DTIC Document, 1996.

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

[18] Ying Qian, Yulin Fang, and Jose J Gonzalez. Managing information security risks during new technology adoption. *computers & security*, 31(8):859–869, 2012.

[19] Eliot Rich, Jose J Gonzalez, Ying Qian, Finn Olav Sveen, Jaziar Radianti, and Stefanie Hillen. Emergent vulnerabilities in integrated operations: a proactive simulation study of economic risk. *International Journal of Critical Infrastructure Protection*, 2(3):110–123, 2009.

[20] Frode Rutledal, Håvard Fridheim, Tone Danielsen, and Stein Malerud. Support to the Norwegian Defence NbF-development - final report (Støtte til Forsvarets NbF-utvikling – sluttrapport). Technical report, Norwegian Defence Research Establishment (FFI), 2015.

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

[22] Finn Olav Sveen and Jose J. Gonzalez. Cascading effect affecting situational awareness in power cut failures. *The Norwegian Information Security Conference (NISK) 2009*, 2009.

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