

20th ICCRTS

“C2, Cyber, and Trust”

Paper 071

**Seeing is believing; hearing is understanding:
Building real trust through virtual tools**

Topics:

Organizational Concepts and Approaches

Social Media

Data, Information and Knowledge

Arild Bergh

Norwegian Defence Research Establishment (FFI)

P.O. Box 25, N-2027 Kjeller, Norway

(+47) 63 80 73 27

arild.bergh@ffi.no

Point of Contact:

Arild Bergh

Norwegian Defence Research Establishment (FFI)

P.O. Box 25, N-2027 Kjeller, Norway

(+47) 63 80 73 27

arild.bergh@ffi.no

Seeing is believing; hearing is understanding: Building real trust through virtual tools

Arild Bergh

Norwegian Defence Research Establishment

Abstract

Joint operations between different military branches is a key element of modern conflicts that has to be facilitated through command and control. Officers may however, as is the case in the Norwegian Defence, have little exposure to other branches' ways of working, thinking and planning until late in their careers. This complicates joint operations as cultural issues impinge upon the shared awareness of the unfolding situation, and this can quickly erode officers' trust in other branches' abilities to address the situation as perceived by themselves.

The Norwegian Defence Research Establishment (FFI) ran a series of experiments to explore whether one can improve upon this lack of joint exposure at an early stage through a cyber environment. This involved cadets from air, sea and land in a geographically distributed setting working on a conflict scenario at the tactical level. A set of low-key HTML5 based collaborative technologies for communication, information discovery/sharing and social media were created and used together with a bare-bones virtual world to facilitate a basic C2 setup. The war game was played out in a command and staff training simulator.

The paper will discuss findings that relates to issues of trust. It suggests that there are several layers of trust that command and control in joint operations within a cyber environment need to consider. Trust in one self, trust in the digital tools and trust in others. It is also suggested that different communication tools have different affordances that affect the level and type of trust placed in them, and that these affordances must be factored in to any use cases. The mediating effect of the technology affects the participants' behaviour. They tend to factor in strengths and weaknesses of different tools, skilfully using relevant digital tools to create a collaborative environment that engenders trusts on all levels.

Introduction

In Norway cadet training is undertaken at the Royal Military, Air Force and Naval Academies, three academies based at different geographical locations. Given the increased importance of joint operations (Forsvarets stabsskole & Forsvarets høyskole, 2014; NATO, 2010) and the move towards a network based defence in the Norwegian Defence (Sunde, 2014), the Sinett project at the Norwegian Defence Research Establishment (FFI) undertook a series of exploratory experiments to determine whether it was feasible to give basic training in joint operations to young cadets through a cyber environment.

This environment would have to facilitate command and control (C2) in an online joint war game scenario. There is considerable discussion, not to say disagreement, as to what C2 entails and encompasses (Alberts & Hayes, 2006; Corps, 1996; Pigeau & McCann, 2002). [Understanding command and control]. That discussion was beyond the scope the Joint 2013 experiments. Instead the experiments focused on providing digital tools that enabled a subset of C2 that would help the cadets learn more about how they could work successfully with other branches. This included the building of shared situational awareness through

maps, documents and information sharing tools; agility of operations through the ability to arrange meetings and view information in a virtual world, the issuing of commands and tracking of progress through a range of planning and communication tools. The communication element included chat, wiki and email, whereas the planning tools covered basics such as mapping and combat logs. The actual wargame was played out in a lightweight staff training simulator. It was also decided to use a virtual world for meetings and information sharing.

Altogether these tools enabled "power to the edge" as defined by Alberts and Hayes (2003). This was a key point of the experiments for two reasons. Firstly, if implemented, such training will be undertaken in a geographically distributed setting where all participants should be able to participate fully. Secondly, we wanted all participants to be fully involved in a network based defence style online war game.

This paper is examining issues pertaining to trust and theorising how the different digital tools affected trust and collaboration. Lyons et. al. (2009) has emphasised the need for "better theoretical models to guide the development of novel collaborative tools", this paper hopes to contribute in some small way to this goal.

Experiment setup: Who, where and what digital tools

The experiments took place from 2010 to 2013 and were of an exploratory nature; rather than defining a hypothesis to confirm or disprove, there was an iterative process focusing on facilitating collaboration to answer the core research question. This question can best be summed up as "can cadets from different branches learn about other branches in a joint online war-game and will this add value to the cadets' current education, if so, how and what". As well as the cyber environment, Sinett provided a scenario for the wargame that presented a potential conflict situation with another country that would escalate into armed conflict.

Throughout the experiment series a range of digital tools, from online wikis to offline map creation tools, was tried out; I will return to these in detail below. Different cadet cohorts were involved at different times; all the experiments took place at FFI's campus. Various operational centre (OC) constellations were tried out, moving from physical co-location (but using digital tools to plan and communicate) to a fully distributed setup in the two final experiments. In those two experiments the cadets from each academy were in the same room, but were separated from the cadets from other academies who were in different locations on the FFI campus. Throughout the series cadets were organised into virtual ad-hoc teams where one cadet came from the branch that the team played in the game, whereas the rest came from other branches (see Figure 1). Thus a naval cadet could work in

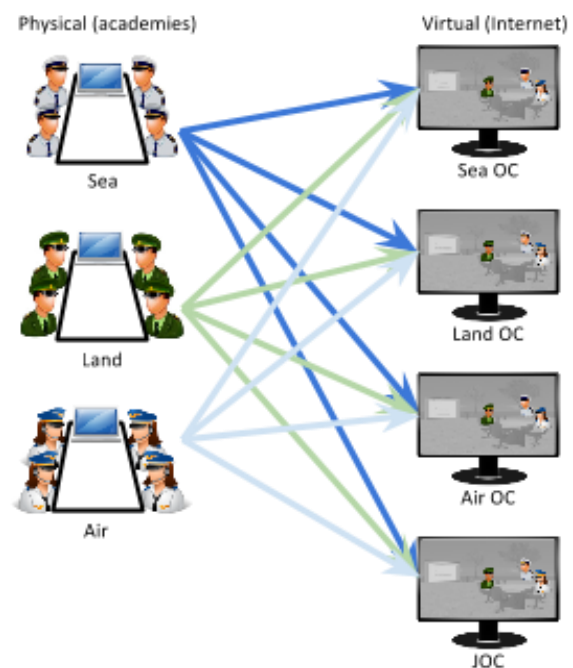


Figure 1 Physical and virtual cadet locations

an army OC, the purpose was to see whether taking on the role of others, not merely working with them in your usual role, i.e. "to walk a mile in others shoes" (Hafnor mfl., 2010) would add to the educational aspect of the experiments.

The digital tools made available for the two experiments were as follows (Reitan, Bentsen, Bergh, & Gran, 2014):

Experiment 1	Experiment 2
Battle Command: simulator with maps of relevant areas, "engine" of the wargame. The simulator was operated manually by researchers and cadets who responded to blue force activities following a previously agreed storyboard/scenario, it had no automated elements.	
OpenQwaq: a virtual world with a basic setup. Used for Push To Talk (PTT) voice communication and organising meetings, each participant was represented with an avatar to move around. In meeting rooms one could display (and update, albeit with a lag) files such as a Word document or web pages.	
Wordpress: blogging platform, news stories relating to the wargame.	
Roundcube: webmail.	
MediaWiki: used to create and share plans and distribute background information such as scenario or Order Of Battle.	MediaWiki: used only to distribute background information such as scenario or Order Of Battle.
Overlaymaker: offline map creator, maps were integrated in Word documents or uploaded to Wiki.	Joint Communicator: custom made HTML5 solution which included planning maps, chat, timeline, combat log and documents. All these were updated in real time and could be used by any number of people. In addition it functioned as a portal to the services listed above with links to Wiki, email, etc.
Microsoft Office: offline word processor and presentation tools. Used for everything from drawing up plans to creating time lines.	
FMS: custom made Twitter like messaging system.	
Semantic Wiki: combat log.	

Table 1 Digital tools available

As we can see, in the second experiment most of the individual/offline tools were replaced with an integrated solution, Joint Communicator. The key difference was that in experiment 1, outside of the virtual world, information sharing was staggered in an *edit/save/share/read/[wait for response]* cycle. That is, information was generated/documented in isolation, then one or more of the digital tools was used to share the result, in some cases potential recipients also had to check for the information manually, either by refreshing a browser page or searching for files/web pages.

Data for this paper

In this paper I will focus on data from the two last experiments in October 2012 (hereafter known as experiment 1) and April 2013 (experiment 2). These had the same cadets present (unlike earlier experiments) but with a step change in the digital tools used. The final experiment used custom made, HTML5 based, real time tools for communication and planning whereas the earlier experiment had used existing digital tools packages/web based tools configured for the participants. Given that the same cadets were involved both times

this gave us rich data on how different digital tools affected the interactions within the war game.

Following the final experiment in depth, semistructured interviews were undertaken with all instructors (5 informants), observers (2 informants) and three to four cadets from each of the academies (11 informants). In addition we collected all written data that were produced by the cadets (emails, chats, wiki updates, planning maps, etc.). The interviews were then analysed using Nvivo using a grounded theory approach (Charmaz, 2006; Glaser & Strauss, 1967). Although exploring trust was not in itself a key element of the original research plan, we incidentally followed the ideas outlined by Riegelsberger, Sasse, & McCarthy (2003) for improving research on trust in computer-mediated communication by employing an asynchronous setting and using qualitative data collection.

Definition of trust

This paper will explore the role of trust in the cadets' interaction with each other and with the digital tools they used and how different types of digital tools affected how (and if!) users used and trusted them. Before discussing the data in detail it is useful to set out what is meant by trust in this paper.

Like many everyday concepts, the idea of trust is difficult to define once examined in detail. It is discussed at length in a wide range of academic disciplines that look at different aspects of trust (eg. Bjørnstad, Fostervold, & Ulleberg, 2011; Debra, Weick, & Kramer, 1995; Hall & McQuay, 2010; Hawley, 2012; J. B. Lyons, Stokes, Eschleman, Alarcon, & Barelka, 2011; J. Lyons mfl., 2009; Mcknight, Carter, Thatcher, & Clay, 2011). In this paper I will define trust relatively broadly, based on the aforementioned discussions. Trust is about relying on people or objects to fulfil certain expectations that one (rightly or wrongly) have of them, without being in a position to enforce these expectations. Trust thus implies a dependency on the trusted object(s)/person(s). In turn, this suggests an acceptance of a vulnerable position on behalf of the trusting person, coupled with a positive belief that there exists an intention (for people) and ability (for both people and objects) to fulfil their part of the (usually unspoken) trust arrangement.

Given the focus on digital tools in this paper, it is important to emphasise that by trust I do not refer to issues such as software to software security. This is typically concerned with issues of encryption, timely delivery of data and ensuring data is not corrupted (cf. eg. Thampi, Bhargava, & Atrey, 2013). In this paper trust is at the human level and from a human perspective; I follow Hall and McQuay's lead when they suggest that "*trust emanates from a person --- human centric*" (Hall & McQuay, 2010, s. 19), even if the trust is aimed at digital tools.

Summary of findings

In the official report from the Joint 2013 experiments (Elstad & Bergh, 2014), based on the same data as this paper as well as questionnaires filled in by all participants, it was clear that the cadets appreciated the concept that was being explored. Even from the experimental situation some of them were able to make use of what they had learnt in their general learning situation, often as a context for new things they learnt. They were also much more reflexive about the relationship between the different branches, and more open to the fact

that their way of working was not the only one. Most of them were interested in seeing something like Joint 2013 implemented at their academies and felt that it would contribute to the overall quality of their education. They also contributed practical ideas on how this could be achieved in terms of involving students in running of the wargame, developing the scenarios, etc. Clear ideas about what digital tools they liked and disliked using was also presented, and they discussed how this affected their work and what changes they would like to see. Most people liked the virtual world as it gave them a feel for where people were, it felt more "real", although some of the more experienced participants preferred plain chat with only a list of participants' names for communication. They also preferred the real time digital tools (Joint Communicator) over tools where the information flow was staggered. When it came to the idea of playing in a different OC than that of their own branch there were mixed feelings, some felt that being in their own branch, and using liaisons to talk to other branches would be more realistic and give them better outcome of future joint training sessions.

Trust - Person to person

Before moving on to the core issue of trust in relation to digital tools, it is worth examining trust between the cadets during the war game. In the interviews that were conducted, the term *trust* ("tillit" in Norwegian) was specifically mentioned primarily by a couple of the instructors. My analysis here is looking at what the cadets discussed that had an indirect bearing on trust, such as feeling that certain digital tools did not do facilitate was expected of them or worrying about the accuracy of information they received from other cadets.

The participants in these experiments collaborated in *virtual ad-hoc teams*, in this case they were pre-allocated to their teams by the researchers at FFI before arrival. The only criteria used were that there should be at least one participant from each branch in each virtual OC, and that cadets did not participate in the same OC twice.

Research has explored what impedes trust in such teams, culture (often on the national level) being an issue that is often highlighted (Bjørnstad mfl., 2011). I believe that this was not an issue in the case of Joint 2013. The participants were all Norwegians and although each academy does try to foster a culture specific to their branch, in this case most of them were so young that their identity as cadets were more to the foreground and thus united them as fellow learners, and in this setting, fellow explorers. As one cadet said, "*we are all in the [Norwegian] Defence*".^{*} One aspect that would have affected the level of trust over time is the fact that the cadets did meet outside the virtual world through briefings before the experiments, during/after action reviews and a joint social arrangement in the evening of the first day. This was a result of the experimental setup (taking place on the FFI campus), and not a trust building exercise. If the type of training that was researched is eventually implemented, these meeting places would not exist. Here I will focus on the trust issues that emerged within the cyber environment during the online war game.

I would suggest that what we saw in the first experiment was mainly an example of *swift trust* (Debra mfl., 1995; Jarvenpaa & Leidner, 1998). This concept suggests that teams which meet up for a limited time with focus on a given task and are unlikely to work together repeatedly, start by showing considerable initial trust based on somewhat stereotypical

^{*} All interviews translated by author.

categories, rather than waiting to build up trust. I am therefore looking to see whether this trust was sustained, increased or reduced as a result of what took place within the joint online war game. In the second experiment this trust had added historical trust, they now knew each other to some extent and could make more personal judgements.

A key issue negatively affecting trust that were mentioned by several of the cadets was the possibility of incorrect learning caused by cadets from the other teams not being knowledgeable enough (yet) to know the full details of their own (real life) branch. The younger cadets were themselves worried about a potential knowledge gap on their behalf. This ties very much in with the idea that competence forms an important part of building trust (Hawley, 2012; McKnight, 2005; Mcknight mfl., 2011). Similarly, more experienced cadets pointed out that some planned the use/deployment of aircrafts and ships that the Norwegian Defence does not actually have, this affected how seriously one would take the plans being drawn up. One air force cadet pointed out that communication about the capacities of the different branches tended to be verbal within the virtual world, and not linked to proper documentation. This was quick, but would have to be taken on trust.

Another issue that was brought up by some of the cadets was miscommunication, often without a way to find out later who had misunderstood what. For instance, at one point the army moved in the wrong direction, not following clear orders from the JOC. As a result the army had to be told to turn around which left both the land OC and the JOC frustrated, no doubt reducing trust, at least temporarily. It was described as a human error, not caused by digital tools, but the cadet that discussed this incident also felt that the real time information sharing tools available in the second experiment could have helped.

More positively, as the war game progressed, and over the two experiments, all sides increased their understanding of how the other branches functioned, in particular in terms of the understanding of time (scales). Once the cadets realised the limitations that were imposed by material such as tanks (in terms of speed of deployment) and planes (fuel requirements) they also understood that a delay or rejection when requesting support was not a result of ill will, but a result of practical issues. As one cadet said, "*now I understand why the army is so slow*". This again ties in with notions of reliability and competence. By understanding the ins and outs of other branches perspective on planning and time, trust in the other branches ability and willingness to help increased. The correct(ed) expectations of what could be requested results in an ability to fulfil, and ability and intention to fulfil improves trust as discussed earlier.

Over time this also led to a less self centered outlook; initially each virtual branch prioritised themselves and how they could request aid from other branches, but over time they became more concerned with the whole of the operations. As one cadet put it, they started to play the game so the others performed better and was then willing to play so they could perform better. Thus increased trust in others' judgement acquired over time can result in better prioritisation for the overall task at hand.

A key aspect of the way the cadets communicated and learnt throughout the war game also revealed the level of (swift) trust that existed from the beginning. The informants repeatedly explained that the main method for learning more about the other branches, in particular about their capacities, was through questions over the voice channel. They clearly trusted the other person to not ignore, make fun, or lose patience with them. As one air force cadet

said, "I would not have had a problem asking someone next to me 'what kind of ship is this' for the fifth time". This trust increased over time as well, one cadet explained that in the second experiment there was a lower barrier to go and chat in the virtual world, thus the swift trust was enhanced with historical trust, that is, trust from experience.

An additional aspect of trust is worth examining, one that is often left out of work on trust in C2 contexts, namely trust in oneself (Hawley 2012:61). I already mentioned how some younger cadets in Joint 2013 distrusted their own knowledge, but more common was a distrust in one's own computer literacy. This distrust was often discussed rather defensively, either on the individual level ("I don't have much interest in [ICT], I have a Mac and that's it [...] but I'm not a computer person"), in generational terms (suggesting that the generation below you will have much better ICT skills) or with reference to your branch ("the second time [the digital tools] were much simpler [...] even me as an army person understood it"). A few cadets were highly skilled and were very network/game oriented. One of them pointed out that the problem, as he saw it, was it hadn't really developed a "network culture" among the cadets yet, and suggested that in the second experiment participants were more comfortable, not more competent, an important distinction. I personally observed how some cadets were unable to perform relatively basic but important tasks such as opening multiple tabs/windows in their web browser in order to, for instance, chat and edit a document at the same time.

People who do not trust their own ICT skills should be foremost in the thoughts of those designing C2 related digital tools. In an empirical study Thomas and Bostrom (2008) found that the successful adaptation of software by virtual teams led to increased trust within the teams. Thus C2 digital tools will have an effect not only on trust in the tools, but individuals trust in themselves.

JOINT COMMUNICATOR: 30 SEKUNDERS TUR


Joint Communicator er en portal til forskjellige Joint tjenester og informasjon.

The screenshot shows the Joint Communicator interface with several annotated features:

- Top navigation:**
 - "Klikk her for å komme tilbake hit" (Click here to come back here) points to the Joint Communicator logo.
 - "Tilgjengelige tjenester" (Available services) points to the "MELDINGER" (Messages) menu item.
 - "Ikon som åpner tjenesten i nytt vindu" (Icon that opens the service in a new window) points to the "DOKUMENTER" (Documents) menu item.
 - "Meny med tilgang til bakgrunnsinformasjon" (Menu with access to background information) points to the "INFO" dropdown menu.
- Left sidebar:**
 - "Søk gjeldende tjeneste" (Search current service) points to the search bar.
 - "Liste over dok., plan, etc. Klikk navn for meny" (List of docs, plans, etc. Click name for menu) points to the document list table.
 - "Chat med andre som jobber med samme dokument/plan" (Chat with others working on the same document/plan) points to the chat window.
- Main content area:**
 - "Arbeidsområde, trykk høyre museknapp for meny" (Work area, click right mouse button for menu) points to the "PLANKART" (Map) area.

Name	Land	Luft	Sj	Ter
Live/BFT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-
Plan A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Plan C	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Testing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kopi av Plan A	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 2 Joint Communicator start page

In the second experiment icons showing a stylised "window" with a plus sign () to open a link in a new tab/window were specifically added. This alleviated the behaviour observed in the first experiment. At the same time the front page of Joint Communicator had a "learn Joint Communicator in 30 seconds" image (see Figure 2). In the debrief after the second experiment a cadet who had voiced her worries about the tools in the first experiment and pointed out that she was not skilled in ICT said that it was so easy to use Joint Communicator that she understood it in, yes, 30 seconds. Thus simple cues and aids based on input from users or empirical observations can make a great difference to someone's self trust in connection with digital C2 tools.

Trust - In and through digital tools

The Joint 2013 experiments utilised a wide range of digital tools. Rather than discussing how each of these affected trust on their own, I will examine a set of issues that each deal with one or more aspects of enhancing or depleting trust. These trust aspects were either trust in other people through the use of the C2 related digital tools or trust in the tools themselves. Following this I will discuss in detail **how** the digital tools were able to affect trust.

Before starting this, it is worth briefly highlighting how trust in digital tools differ from trust between people. Hall and McQuay (2010) has suggested that whereas people (can) have mutual trust, interaction with computer systems is mainly about people finding the system trustworthy. Hawley (2012) defines trustworthiness as the ability to meet commitments, this is a rather useful way of thinking about the digital tools; if one expects a tool to record and share a combat log, does it actually do this? Thus, trust is bidirectional for people, and unidirectional for digital tools, i.e. digital tools has no concept of trusting a person in response to being trusted themselves, at least not the type of tools used in Joint 2013. However, this does not mean that these tools do not affect trust, in themselves or in people on either side of the communication/collaboration tool(s), i.e. self-trust and trust, as discussed above.

It is also worth noting that I will not discuss trust in the content carried by the tools. The content was primarily information from other users, however I will look at how content was shaped by digital tools. Furthermore, I will not discuss outright failures of tools. There were examples of this in the Joint 2013 experiments, in particular the FMS "Twitter clone" needed to be restarted several times and was very slow at times. Such faults certainly affect trust in the system as a whole and will slow down work/communication, but tend to affect binary responses. When the tools are not working they are the object of much complaints, but when they are back online they are used pretty much as before. For instance, one cadet pointed out that errors in the simulator (a vehicle could get stuck due to faulty software) would stop the flow of the game as one had to focus on fixing the software problem. Once rectified however, this error did not affect the plans being made.

Unlike the swift trust exhibited between cadets, their trust in digital tools was more about history (either in the experiments or from personal history prior to the experiments) or the cadets disposition, as discussed above regarding those lacking in ICT skills. As with people, when trustworthiness is breached, it is difficult to get it back. Lyons et. al. (2011, s. 221) put it this way:

Given the proliferation of computers, it is likely that many if not most people in modern societies have preexisting attitudes about using computers. When these computer systems perform in anomalous ways, individuals' expectations may be violated, resulting in tension or, in this case, suspicion.

Roger that: Confirmation and virtual teams

The ability to get confirmation as to whether a message was received and, ideally, read, was unsurprisingly high on the agenda for many cadets. For this reason voice communication within the virtual world was often the preferred communication method, or it was used to check if information sent with other digital tools had been received. Email was used quite a lot in the second experiment, but not at all in the first, and although this offered a simple "message received" request, it was not possible to say if it had been read. Thus there were some worries, i.e. distrust, in regard to how reliable it was in terms of getting the information across. In some cases people were requesting manual receipts within the email to handle this issue. Tools like MediaWiki or the FMS Twitter clone were problematic in that they were first and foremost publishing platforms rather than communication tools. In the logs of chats I found some "copy" confirmations, but no standard way of confirming that it was read seems to have been used.

In addition to simple confirmation, voice communication also gave cadets a way to immediately check if they had understood correctly, or to clarify terms that were new to them, which, as we saw above, helped with the learning outcome.

Give me a cue: Presence in the virtual world

Receiving additional cues about people one interacts with can also support in situ confirmation and build trust. Lyons (2009, s. 37) has discussed how

non-verbal cues such as facial expressions, verbal tone, gestures, etc., may be better for promoting trust because of the increased availability of this relational information. This supplementary information may be especially useful in ad-hoc virtual teams [...].

In Joint 2013 voice was the only non-mediated communication method available. One cadet felt that voice was a must as one "cannot hear irony in a text message", and as discussed above, most cadets liked using voice communication. Riegelsberger et. al., when discussing a meta-review by Sally, supports the importance of voice communication when they say that for computer-mediated communication the fact that frequent verbal communication increases trust is the most relevant factor (Sally, 1995 in Riegelsberger et. al. 2007 pg. 7).

The virtual world designed for Joint 2013 was (deliberately) very sparse. It had "rooms" that were simply spaces surrounded by fields, with an entrance and a number of panels for sharing information from local documents on a users PC or web pages. Each cadet had a very basic avatar that could be manoeuvred into the rooms, and once in a room one could use push to talk to contact others in the room. Despite this simplicity several of the cadets felt that this made it feel more real, and appreciated the use of rooms and avatars to see who were present and whether they were busy (talking to others, looking at information, etc.).

Several informants suggested that they would like to have a video conference before such virtual joint training and felt this would make them acquainted before starting the war game. In line with Lyons' suggestion this would probably increase trust in later stages.

Ease of (ab)use: The right tool for the right job

As discussed above, for the second experiment the *Joint Communicator* digital tools were created that focused on ease of use and providing real time information sharing and discussion, without requiring any explicit actions from the cadets. Most cadets supported the view that these tools were considerably easier to use than the tools available in the first experiment. However, it became clear that making something very easy to use can be something of a double edged sword.

Firstly, there was some "misuse" of tools. As the word processor in *Joint Communicator* updated the document for all users who viewed/worked on it in real time, some cadets started using the document itself as a space for chat. This was despite the fact that there was a proper chat easily accessible next to every document. Although chatting in the word processor did work, it lacked the time and user stamp that a proper chat has, so it would be difficult to see who said what and when. Furthermore, this meant that "chat text" within the document could be (and was) deleted, making it untrustworthy as a proper chat tool by not facilitating tracking.

More problematic was the fact that the cadets starting making several overlapping documents, particularly planning maps. An air cadet pointed out that

An interesting challenge was that several people could start writing the same document at the same time, or parallel documents with the same or similar names. However, that was really the cadets' responsibility [...] to have some templates and standard [procedures] on how we should do this.

Another cadet concurred and explained that "*there were a lot of maps there, perhaps our own fault as we gave them a lot of strange names, so a bit messy*". An instructor also felt that this had a problematic side:

Making a common picture, I don't know how they 'hacked' the common picture [...] they didn't make a simple map that stated 'now we are here, even if a lot of things happen in Battle Command, this is our common picture, [...] and this we know for sure.

Overall this meant that it would be difficult for the cadets to be sure of which plan were the one to use, and if the one they had open was the one to trust.

A more insidious issue was the underlying belief that if something was easy to use, it would improve communications. Most cadets preferred to use the PTT voice option in the virtual world for communication as it provided quick communication and confirmation without having to type. But its ease of use seems to have lead to a mistaken trust in the tool, which could lead to misunderstandings. A simple example was the helicopter NH-90 (pronounced *enn-ho nitti* in Norwegian), later non air force cadets mistakenly referred to this by the number 91 (pronounced *en-o-nitti* in Norwegian). Although many informants disliked chat due to the slowness of typing or the lack of in built confirmation option, it would have been a more trustworthy communication method for messages that required high accuracy. This seemed to be appreciated by more experienced participants who had used chat when deployed in Afghanistan.

Thus we can see that easy to use tools can also create confusion and cause misunderstandings and duplication of work. These are both elements that can reduce trust over time.

It's now or never: Sharing information

The methods for sharing information varied greatly between the different digital tools explored in Joint 2013. It went from the Wiki/Office/offline tools in experiment one that required a staggered edit/save/share/read/[wait for response] cycle and the Joint Communicator tools in the second experiment which were designed for real time, automated sharing. The key issue that emerged is that trust in tools that introduced a time lag (for whatever reason) rapidly deteriorated and cadets would quickly resort to workarounds such as asking each other directly for information outside the cyber arena. This would be unrealistic in a proper implementation of joint cyber training tools, but it did expose the lack of trust that delayed updates could result in.

Another important aspect of sharing information was the ability to access/view multiple sources of information at the same time. Although Joint Communicator would allow multiple tabs to be open at the same time, one would have to flick through them to look at different information sources. For this reason the panels for sharing applications/web pages in the virtual world were often used. One army cadet emphasised that this ensured that everyone in the OC saw the same information at the same time, thus improving shared situational awareness, a key to reliable planning in virtual teams. However, these displays were very slow in being updated when documents were amended (a problem of OpenQwaq), a naval cadet explained that *"it is not particularly user friendly to share information in that virtual world [...] if you made a plan and make it as a picture and hang it up on some wall, and then, five minutes later it is irrelevant"*.

Finally, the ease of (or automated) sharing was crucial, one cadet explained that in the first experiment with he ended up sharing documents only with himself as it was so difficult.



Figure 3 Snapshot of virtual world Poom⁴ with shared information panels

How are digital tools able to affect virtual interactions?

So far I have examined different aspects of working with different digital tools in virtual teams in a C2 context, with a focus on cadets' feedback related to trust issues. Lyons et. al. point out that *"the military must overcome the limitations that pervade computer-mediated interactions by identifying features of collaborative tools that facilitate trust development"* (J. Lyons mfl., 2009, s. 38). To do so, we also need to develop a theoretical foundation that attempts to understand the mechanisms of such facilitations, and move towards a framework that can be applied to examine digital tools, new or old, and ask the question, "how will this affect interactions"?

One approach to this that I believe can prove fruitful is the application of the actor-network theory (ANT). ANT do not understand objects (be they digital tools or furniture) as neutral, "dead" entities, but suggest that they are a part of (social) networks that are formed through the combination of the human and the object. Both parts are actors that in combination achieve more than they can do in isolation. Properties of the objects therefore influence the social actions that they are a part of and take on the role of a mediator. Latour (1999) who developed this concept takes the example of a gunman, the combination of a person and a gun. On their own a person cannot shoot anyone, and only in rare circumstances will a gun kill someone on their own. It is the network of the person and the gun that "creates" the gunman. By applying such an approach to our analysis we will learn more about the *connection* between the cadets and the digital tools they used, in other words, how did they mesh to produce an effect.

Taking this as our foundation, we then need to understand how digital tools affected the human actors within the person/digital tool network. We know that digital tools such as the ones used in Joint 2013 do not possess any will of their own (they are not programmed to have artificial intelligence), nor do they have any cognitive faculties. Instead, the digital tools "afforded" certain actions/uses. The concept of affordance of objects was defined by the psychologist Gibson as a way to explain how people perceive meanings and values of objects around them, and how it suggests possible actions, i.e. what it offers the subject, in this case the cadets (Gibson, 1977, s. 127). A simple example of affordance would be a chair. It affords sitting (more than other actions) by the way it is shaped and a common, local understanding of what a chair is. However, this does not stop the chair from being used as a weapon or as a ladder, so affordance is not a fixed diktat but a "most likely action(s) of many" that this object can be used for.

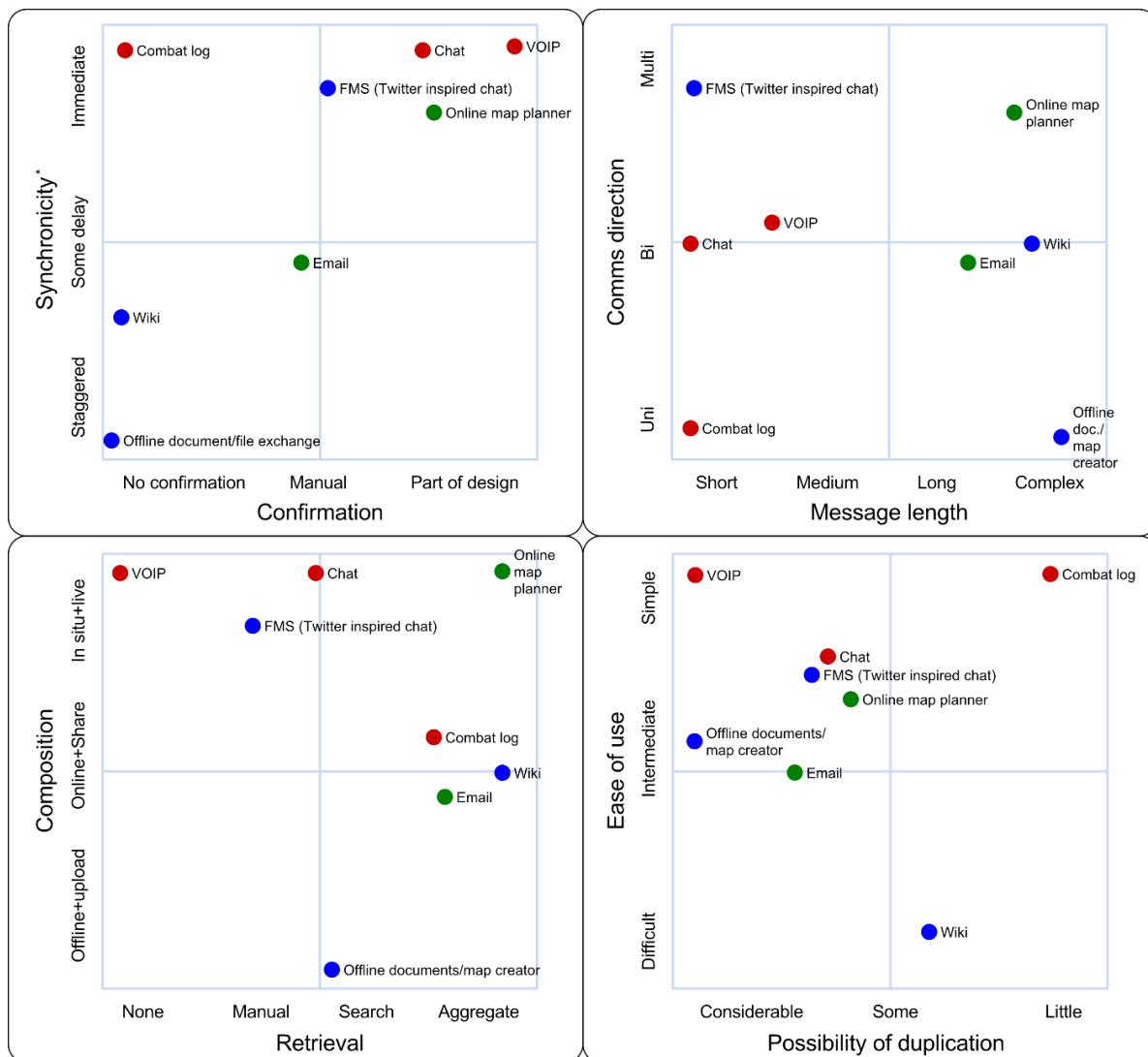
It is also important to understand that the affordance of a tool is not the same as the features of the tool, a chat may have a timestamp feature, but it is what this timestamp affords/enables in terms of human actions that is of interest to us.

Enabling, limiting and influencing: affordances of digital tools

To help us think about the affordances of different digital tools I will use four basic 2x2 matrices (see **Error! Not a valid bookmark self-reference.**) that look at some properties that are of interest in a C2 context. Such properties are what underpins affordances. Similar analysis has been undertaken regarding, for instance, a typology of virtual communities (Porter, 2006).

The positioning in these matrices are based on an evaluation that stems partly from personal experience and partly from the observation of their (logged) use in the Joint 2013 experiments. The properties evaluated relate to the implementation of these tools as used in Joint 2013, there may be other implementations available with different abilities. As such they represent a broad brush approach to exploring some aspects of the digital tools in a specific context, and not a definitive version. Yet this is a valuable exercise to understand more about digital tools and their affordances. Following on from this I can discuss the affordances of the digital tools, and how this affected their use by the cadets in the network.

* Synchronicity is the degree to which a medium enables real-time interaction (Dennis & Valacich, 1999).



● Only used in exp. 1 ● Only used in exp. 2
 Figure 4 Some properties of interest from digital tools used in Joint 2013

What we see here is that different digital tools, as we have all experienced at some time or another, perform some tasks better than others. Thus they have different affordances, positive and negative. Tools that are easy to use for instance, but offer no means of easily retrieving old communication, affords duplication more than other tools. Similarly, an air force instructor discussed the problematic side of chat in terms of keeping an overview of what is happening:

We used chat a bit in [HQ in Afghanistan] it worked well as few few people were connected, Chat is very difficult to keep track of, incredibly difficult. If you don't have chat groups and are very well organised [...] in a small world it is OK to keep track of it, in a more complex [setup] it can soon take all your time to keep track of who one is chatting with.

The affordance(s) of the digital tools were discussed indirectly by the cadets in different contexts. One air force cadet explained that “[email] can be very good for posing the slightly larger, clarifying questions in [a planning phase]” but at the same time warned that email “works in the planning phase, but as you get less and less time, the more dangerous it is to have the email [there]”. Another air force cadet felt that email entailed more responsibility to check, understand and receive longer messages, whereas with chat it was too easy to “just write things”. The same cadet also discussed how using voice communication meant he

talked in the present and one was not able to think so much, whereas the combat log and the real time document tools helped to learn procedures and make it more structured. Along the same line, an air force cadet felt that something written, even just a chat conversation, felt more like an order (even if it was not meant as one), whereas on voice it was easier to have a dialog.

Affordances of different tools can also complement each other. A naval cadet discussed how the selection of communication tools in the Joint 2013 experiments could be combined according to needs:

“the last time, when you were [talking to] someone, had agreed with someone over voice for instance, to meet up such and such a place, you could switch over to [chat] to continue to monitor the situation [while] one or two persons who were tasked with something could continue to produce a plan”

What he is discussing here is, in effect, the optimal use of digital tools' affordances. Other cadets from air and sea also felt that using the chat next to a document/plan in progress helped cut down on overload on the voice communication, whereas another naval cadet felt that chat was more important within the staff room, as it *“was more difficult to use voice in small rooms”*. In terms of trust in the digital tools, this very much mirrors how we apply and limit our trust when dealing with people. We may trust a friend to help us move house, but not to perform brain surgery (Hawley, 2012).

Some negative affordances of tools were highlighted in connection with the virtual world. Users found it slow to "go" (i.e. move their avatar) from room to room to find out where someone was.[†] As voice communication was implemented as "push to talk" operated, they could not work on a document whilst clarifying something on voice, thus the attempts by the virtual world to feel realistic reduced the speed of collaborative work. One user felt that this created a higher threshold for talking to people, partly as PTT could interrupt an existing conversation, although the fact that you could see if people were busy was seen as a boon.

Affordances affect the use, content and frequency of information processing, production and sharing. Such affordances are not necessarily obvious to all users, particularly for the less experienced users. A chair has certain physical properties that aid ones understanding of its use. Digital tools on the other hand are not only two dimensional, thus reducing the cues regarding their affordance(s); they may also have a lot of functionality presented in a small physical display unit. Furthermore, they often co-exist on a piece of hardware that is the same for a wide range of digital tools (e.g. a PC), so the cues for their use are even more impoverished. This is something that needs to be carefully considered when developing new digital tools for virtual teams in C2 contexts.

The human (f)actors

So far I have focused on one of the two actors in the C2 cyber environment discussed here, the digital tools. These tools are, as discussed above, in many ways double edged sword, the easier the communication or information production became, the more was shared or produced. This is another example of how affordances of tools can lead to good or bad actions, it is therefore important to also understand the human (f)actors, their actions and

[†] There were shortcuts available, but the cadets were not aware of them.

reactions related to the digital tools as ultimately they decide the outcome of the use of these tools.

One result discussed earlier related to the ease of use of the digital tools, and how they resulted in more document being created. This overproduction and/or duplication of information is not necessarily linked only to ease of use. Another cause may have been the fact that in real time online editing tools found in Joint Communicator, everything is visible all the time. This may have resulted in a need to "show off",

a focus on producing paper, admittedly electronic, but that plans should be forthcoming [...] a lot of focus on having something visible before anyone else. That is something of an illness in the defence, where one tries to satisfy the extreme information needs of those above oneself

as one naval cadet put it. When one is more concerned with output than (also) receiving information and/or processing it, the outcome and quality of the communication will obviously be affected, over time eroding trust in the material produced.

Furthermore, this focus on the "reader on your shoulder" can affect concentration and content when creating the document(s). This can cause stress, as one cadet put it:

[I] felt that it was a lot easier [with offline map tool] because I could work on it separately, no-one could get into what I was working on my PC before it was finished. But in [the second experiment] everyone could keep track of the fact that I madet his plan, fair enough, but it perhaps not everybody understood that it was not completely finished yet.

Inexperienced users who do not trust themselves fully (yet), may prefer to polish what one is working on before showing it to others. This is not possible to do in real time editing tools such as those found in Joint Communicator. In turn this can afford an unwillingness to share information and/or develop a plan.

Worrying about being observed all the time (whether it happens or not), particularly in the virtual world, can be a general problem that is afforded by virtual tools. One air force cadet explained that

in real life when an instructor shows up [...] it is very visible [but] in the virtual rooms [...] suddenly there are five avatars there [...]. So one feels a bit monitored [...] not a big issue but a source for some distraction.

Generally speaking the cadets were happy to receive input from the instructors, whether in the virtual world or in real life meetings. So this was not about a rejection of the need for instructors, but a slight uneasiness about whether there was someone in the background, which they could not know for sure. Thus we can say that while the virtual world on one hand increased trust through the affordance of the avatars that made it feel more real, it also added some, not exactly distrust, but a slight undermining of trust in one self. This was due to the affordance for monitoring without the monitored person knowing for sure due to the avatars always being visible, but not showing if the person the avatar represented looked at the screen at that point.

A final point on the human aspect of working in virtual teams is the danger that when working on your own you can forget the others you are working with, or the overall goals you are working towards. This, as a naval cadet explained, doesn't happen in real life. This was something that the virtual world helped to alleviate, but which could happen with tools where sharing and collaboration was staggered or real time tools where partners left the document

to work on something else. This worry was supported by a naval cadet who felt that one could easily “*sit in their own dream world for 10-15 minutes to write a plan [...] that would never be read by anyone afterwards, and then upload it*” when using the Wiki based solution in experiment one.

Conclusion

We have seen how different digital tools can affect the trust people have in themselves, in their collaboration partners and in the digital tools. This comes about through the affordance of different actions that may reduce or enhance initial trust people place in one another. When the level of trust goes down, the chances of misunderstandings, duplication of work or inability to track what is happening can lead to negative outcomes in the war games. Trust as discussed in this paper is a multi-layered and changing process, not a static entity (Hall & McQuay, 2010), where each layer may change independently of other layers. Thus improvements in trust in, for instance, a particular digital tool may or may not affect collaboration positively to engender more trust in those one work with.

Alberts and Hayes (2006) have suggested that if we are to move towards a truly networked organisation “*we need to develop new approaches to Command and Control. These include the creation of robust socio-technical networks that rely upon human behaviors that are facilitated and supported by technical means*”. This paper attempts to contribute to this vision by examining the role of digital tools used in an online war game for C2 purposes to teach cadets joint operations. I have theorised how these tools may affect communication and collaboration outcomes by suggesting that cadets and tools are both actors in a network and the concept of affordance can explain why and how digital tools have an effect on collaborative C2 work. This is in line with Lyons et. al. (2009) call for improvement in the theoretical models used when developing new collaboration tools. By developing theoretical models, in this case grounded in empirical data, we can move beyond the view of digital tools’ features as simple checklist items to be implemented at will, and move towards seeing the affective power of the behaviours of the digital tools. This should make the tools more suitable for real life usage, and more potent in real use.

This paper has presented a tentative look at how digital tools can affect interactions and trust in a C2 context, using data from joint training in a cyber environment. Further research is needed to learn more about how affordances can be examined and considered when developing new software, and how to measure this in practical use, this needs to take a bottom up approach to be of real value. The Sinett project plans to develop the Joint Communicator tools further by taking into consideration feedback from participants in the experiments discussed here, and explore how trust building aspects can be built directly into the software.

References

- Alberts, D. S., & Hayes, R. E. (2003). *Power to the edge: command, control in the information age*. Washington, DC: CCRP Publication Series.
- Alberts, D. S., & Hayes, R. E. (2006). *Understanding command and control*. DTIC Document. Hentet fra <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA457162>
- NATO. (2010, desember). Allied Joint Doctrine NATO. NATO. Hentet fra https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33694/AJP01D.pdf

- Bjørnstad, A. L., Fostervold, K. I., & Ulleberg, P. (2011). Effects of cultural diversity on trust and its consequences for team processes and outcomes in ad hoc distributed teams. *Scandinavian Journal of Organizational Psychology*, 3(2). Hentet fra <http://sjop.no/index.php/sjop/article/view/192>
- Charmaz, K. (2006). *Constructing grounded theory : a practical guide through qualitative analysis*. London : SAGE.
- Corps, U. M. (1996). Command and control. *Marine Corps Doctrine Publication*, 6, 45–47.
- Debra, M., Weick, K. E., & Kramer, R. M. (1995). Swift trust and temporary groups. *Trust in organizations: Frontiers of theory and research*, 166.
- Dennis, A. R., & Valacich, J. S. (1999). Rethinking media richness: Towards a theory of media synchronicity. I *Systems Sciences, 1999. HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference on* (s. 10–pp). IEEE. Hentet fra http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=772701
- Elstad, A.-K., & Bergh, A. (2014). *Om nettbasert fellesoperativ samarbeidslæring mellom krigsskolene - tilbakemeldinger fra kadetter og instruktører* (FFI Rapport No. 2014/01450). Kjeller, Norway: FFI. Hentet fra <http://rapporter.ffi.no/rapporter/2014/01450.pdf>
- Forsvarets stabsskole, & Forsvarets høyskole. (2014, oktober). Forsvarets fellesoperative doktrine. Forsvarsstaben. Hentet fra <http://brage.bibsys.no/xmlui/bitstream/handle/11250/224031/5/FFOD%202014.pdf>
- Gibson, J. J. (1977). The Theory of Affordances. I R. Shaw & J. Bransford (Red.), *Perceiving, Acting, and Knowing*. Michigan: Lawrence Erlbaum Associates.
- Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Aldine Pub. Co.
- Hafnor, H., Bentsen, D. H., Gran, C. J., Reitan, B. K., Valaker, S., Wold, R., ... Waade, S. W. (2010). *Joint Experiment 2010 - om det å samarbeide med noen som ikke er lik en selv* (FFI Rapport No. 2010/01923). Kjeller, Norway: FFI.
- Hall, S., & McQuay, W. (2010). Review of trust research from an interdisciplinary perspective-psychology, sociology, economics, and cyberspace. I *Aerospace and Electronics Conference (NAECON), Proceedings of the IEEE 2010 National* (s. 18–25). IEEE. Hentet fra http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5712918
- Hawley, K. (2012). *Trust: A very short introduction*. Oxford University Press.
- Jarvenpaa, S. L., & Leidner, D. E. (1998). Communication and trust in global virtual teams. *Journal of Computer-Mediated Communication*, 3(4), 0–0.
- Latour, B. (1999). *Pandora's Hope: Essays on the Reality of Science Studies*. Harvard University Press.
- Lyons, J. B., Stokes, C. K., Eschleman, K. J., Alarcon, G. M., & Barelka, A. J. (2011). Trustworthiness and IT Suspicion An Evaluation of the Nomological Network. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 53(3), 219–229. <http://doi.org/10.1177/0018720811406726>
- Lyons, J., Stokes, C., Garcia, D., Adams, J., & Ames, D. (2009). Trust and decision-making: An empirical platform (CCP 204). *IEEE Aerospace and Electronic Systems Magazine*, 24(10), 36–41. <http://doi.org/10.1109/MAES.2009.5317785>
- McKnight, D. H. (2005). Trust in information technology. *The Blackwell encyclopedia of management*, 7, 329–331.
- McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems (TMIS)*, 2(2), 12.
- Pigeau, R., & McCann, C. (2002). Re-conceptualizing command and control. *Canadian Military Journal*, 3(1), 53–64.
- Porter, C. E. (2006). A Typology of Virtual Communities: A Multi-Disciplinary Foundation for Future Research. *Journal of Computer-Mediated Communication*, 10(1), 00–00. <http://doi.org/10.1111/j.1083-6101.2004.tb00228.x>

- Reitan, B. K., Bentsen, D. H., Bergh, A., & Gran, C. J. (2014). *Joint 2013: Spillininfrastruktur og nettverkskonsept – utvidbart, fleksibelt og NbF'ish* (FFI Rapport No. 2014/01417). Kjeller, Norway: FFI. Hentet fra <http://www.ffi.no/no/Rapporter/14-01417.pdf>
- Riegelsberger, J., Sasse, M. A., & McCarthy, J. D. (2003). The researcher's dilemma: evaluating trust in computer-mediated communication. *International Journal of Human-Computer Studies*, 58(6), 759–781.
- Sally, D. (1995). Conversation and cooperation in social dilemmas a meta-analysis of experiments from 1958 to 1992. *Rationality and society*, 7(1), 58–92.
- Sunde, H. (2014). *Forsvarets IKT-strategi*.
- Thampi, S. M., Bhargava, B., & Atrey, P. K. (2013). *Managing Trust in Cyberspace*. CRC Press. Hentet fra http://books.google.com/books?hl=en&lr=&id=MyMtAgAAQBAJ&oi=fnd&pg=PP1&dq=%22Gupta,+Padam+Kumar,+and+Ajith%22+%22A+Survey+of+Trust+and+Trust+Management+in+Cloud+Computing+.....%22+%22Trust+Models+for+Data+Integrity+and+Data+Shredding+in+Cloud+.....%22+&ots=rr3KZOGsKF&sig=R_R1YoBnz9t_aq7Ho7YxpiENzoA
- Thomas, D., & Bostrom, R. (2008). Building Trust and Cooperation through Technology Adaptation in Virtual Teams: Empirical Field Evidence. *Information Systems Management*, 25(1), 45–56. <http://doi.org/10.1080/10580530701777149>