# C4IS in the Norwegian Army

*-Are we keeping up with development?*

**KRIGSSKOLEN**

**Oddar Kristiansen**
OPERATIV, KULL LINGE
EMNE FORDYPNING
KRIGSSKOLEN
2016

Word count: 8842

Commanders intent – my purpose in writing this dissertation:

With this undergraduate dissertation I hope to simplify a quite complex problem within military technology. I wish to simplify the problem to a level where it makes sense to any 1st year army sergeant, regardless of said sergeant's specialisation. That is to say; one should be able to read and understand this dissertation as a layman, not having any specialisation within communications or informatics. Technical acumen will still be an advantage though.

With this goal in mind I will try to explain some of the underlying reasons for things being the way they are. And only after doing so, is it possible to discuss which things that are, that shouldn't be - and which things that aren't, that should.

I also wish to thank all those who were kind enough to give me time out of their busy days to discuss these topics with me.

# 1. Introduction

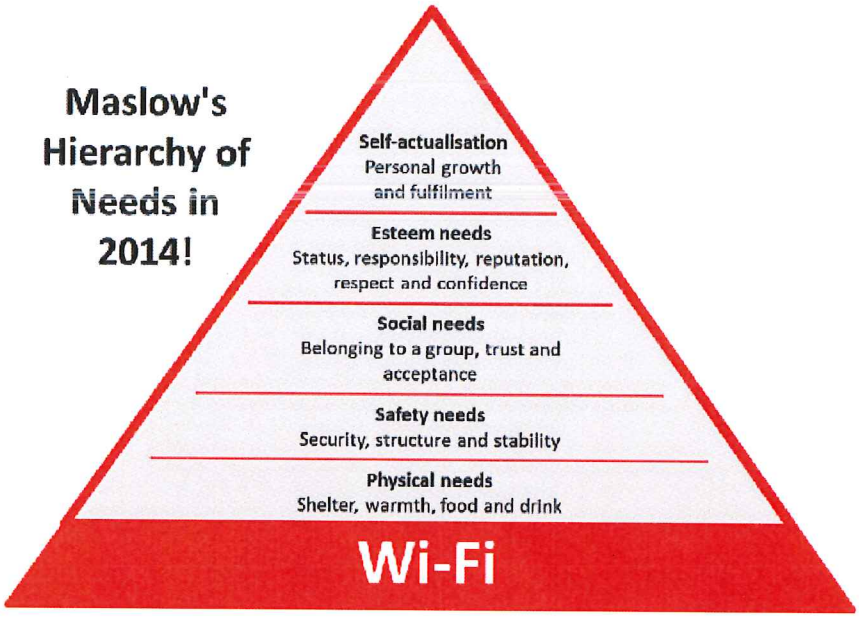
## 1.1 Definitions, disclaimers and background

There are so many acronyms and abbreviations in daily use within the armed forces and they are inescapable also in this dissertation. The most important one to know while reading this thesis would be C4IS: "Command, Control, Communications, Computer, Information Systems". C2IS is the acronym that is used most with regards to this, where the "Communications" and "Computer" are left out. In this dissertation the C4IS is the one that will be used the most, but that includes anything and everything C2IS or just C2 would entail, and then some.

A definition of C2 would be: "A basic function for planning and leading operations. C2 consists of the organisation, processes, procedures and systems that make military commanders capable to lead and control his forces." (Forsvaret, 2007, p. 170). The C4IS term is quite a wide one, but for this dissertation the focus will be largely on the technical implementation of information systems, and not too much on culture or processes.

It is worth mentioning that throughout the dissertation there is cited or paraphrased a few Norwegian books, doctrines, documents etc. Where the document that is paraphrased has no published translation into English, the reader can assume that I myself have translated it.

Background - In this day and age wireless communications are ubiquitous and pretty much a given wherever you are. There has even been made parodies of Maslow's Hierarchy of Needs, where "Wi-Fi" and/or "Battery life" has been added to the base of the pyramid.



While this is meant as a joke and a stab towards society's increasing dependency of always being online, it does portray a reality; also for the armed forces. For the armed forces the basal need may not be Wi-Fi per say, but connectivity for sure. The problem for the armed forces though, is that all their communications need to be secured.

The Norwegian agency with national responsibility for information security, the National Security Authority[1] (NSM), have to certify any communication solution or channel by which classified information is to be sent. This fact makes connectivity far less ubiquitous for the armed forces, when compared to the rest of society. The army is mostly dependent on its own communication systems built for them by the industry, just to abide to the demands of security. This makes the communication systems expensive, and therefore also more scarce. This scarcity decreases redundancy and availability. The Norwegian Army also states in a project trying to predict what the future holds, that: "Norway should base their communications- and encryption equipment on open standards, so that it in 2035 is possible to communicate securely across domains, agencies and nations." (Hæren, 2015). This is why I find it pertinent to ask the following question:

**Can we utilise 4G/LTE+ technology as a secure data carrier for information systems in the Norwegian Army?**

## 1.2 Scope

The scope of this dissertation is already somewhat limited by the phrasing of the question. It should be clear that this dissertation in principle seeks to answer the broad question whether or not we can utilise cheaper, commercially available data carriers for C4IS in general. However, that would be to great a task for this short dissertation. For that reason, there has been chosen one specific commercially available technology to discuss, namely 4G/LTE+. In the same way there are quite a few information systems within the armed forces one could discuss. This dissertation is limited to discuss only information systems in the Norwegian Army, and primarily the Norwegian Battle Management System (NorBMS).

Some topics will intentionally be omitted when it comes to discussing the NorBMS in the context of information security and its possible data. For instance, this dissertation will not discuss secure national Ecom[2] infrastructure as that would be classified. Military networking based on phone lines which makes up the lasting "back-end" of the system will be avoided for that reason.

---

[1] NSM – Norwegian: Nasjonal Sikkerhetsmyndighet.
[2] Ecom – Electronic communications

Economy will be mentioned at times throughout the dissertation and there will be no estimates of how much any of the suggested solutions would cost. The only comments will be with regards to whether or not something is cheap or expensive is not based on exact numbers, but rather a down to earth understanding as to the difference between i.e. a commercially sold iPhone and a military ruggedized hand-set tactical radio.

To match the scope, this dissertation mainly looks at Norwegian national doctrines and steers away from the NATO documents that applies to the same subjects. The Norwegian doctrines always base themselves on the NATO-doctrines to enable interoperability (Forsvaret, 2014, p. 15), so they might not differ too much. It is important to note that some of the expressions that also exist in NATO documents, might have a narrower definition in the national documents. For this reason, any expressions should be considered in light of the Norwegian doctrines and documents, and their definition.

## 1.3 Dissertation structure

The dissertation is divided into four chapters discussing different aspects important to answer the question. Firstly, the Norwegian Armed Forces doctrinal bases to explain the view they have on warfare and how C4IS plays a role in it. Then it will discuss one specific C4IS; the NorBMS system. Further the dissertation will elaborate on information security and its principles. There will be quite an extensive elaboration on cryptography. This is simply because it is a difficult subject, but still a very important aspect to understand if you need to discuss information security. Then there will be a chapter to discuss where the 4G / LTE+ technology can fit into the C4IS, or if it can at all.

Thereafter there will be a short chapter on methodology and critique, and a chapter to summarise the conclusion of the dissertation.

# 2. Norwegian Armed Forces doctrine

## 2.1 Our way of thinking

There are three ideals that provide the bases for the Norwegian doctrine. These three ideals are effect-based thinking, the Manoeuvrist Approach, and network-based thinking (Forsvaret, 2007, p. 53).

Effect based thinking is all about starting with the end-state in mind, and then considering all the factors that could bring about this effect. This means considering the enemy not just as a military force, but as a complex system with many factors that are intertwined (Forsvaret, 2007, p. 54). With effect-based thinking one would chose to influence whichever factor that would bring about the desired effect. An example would be by applying political pressure to a neighbouring state to commit them to an economical embargo towards the enemy, to reduce his capabilities by means of attrition. Effect-based thinking is also dependent upon the availability of good intelligence (Forsvaret, 2007, p. 55).

According to the FFOD, the Manoeuvrist Approach is based on the tenet that warfare is a social endeavour where the psychological aspect is key. Warfare is a continuation of policy by other means and is considered a battle of wills. Warfare is chaotic, unpredictable and uncertainty permeates it. The Manoeuvrist Approach is embracing these aforementioned facts and it is not just about being able fight in the midst of it, but being able to turn it to one's own advantage. (Forsvaret, 2007, p. 56)

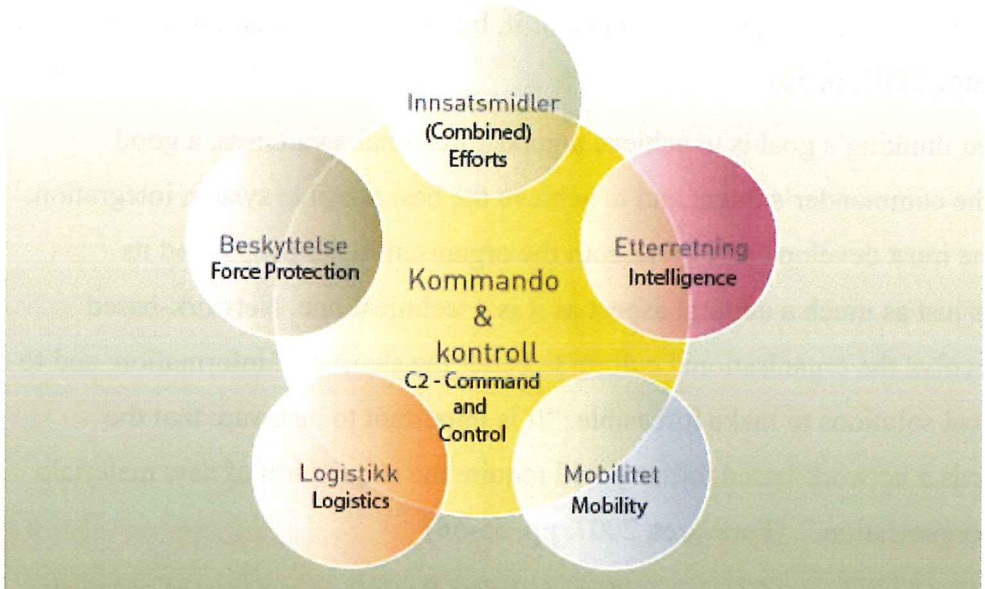
Network-based thinking's goal is to achieve a good situational awareness, a good understanding of the commander's intent and to achieve the best possible system integration. To achieve this, one must develop and evolve both the organisation, its people and its technology. This is just as much a cultural aspect as it is a technical one. Network-based thinking seeks to evolve the organisational culture to better the sharing of information, and to develop the technical solutions to make it feasible. "It is important to be aware that the development towards a network-based military will require the acquisition of new materials and new forms of organisation.". (Forsvaret, 2007, pp. 55-56)

With these three ideals as our bases we adhere to being flexible in our way of organising, and in our choice of method. There are three methods: the stabilising method, the manoeuvre method and the method of attrition (Forsvaret, 2007, p. 60). All of these methods require a functioning C4IS so the details of each method add little value to this dissertation.

## 2.2 Our tools of fighting.

The domain model depicts four domains where warfare can take place: the cognitive domain, the information domain, the social domain and the physical domain. The cognitive domain is about the individuals' thoughts and ideas, and in the end it is in this domain wars are lost or won. The information domain is where information is created and distributed and cyber warfare would belong in this domain. The social domain pertains to human interaction and the cohesion within the fighting parties. Lastly, the physical domain is of course the traditional battlespace with land-, sea-, air- and space-elements. This also includes the physical communication network. (Forsvaret, 2007, p. 70) The domain model shows where warfare takes place, but what about the how? This is where the combat functions enter the scene.

The Norwegian Armed Forces Joint Doctrine (FFOD[3]) of 2007 points out how military units are dependant on the six basal combat functions. The six combat functions are listed as intelligence, mobility, logistics/sustainability, force protection/survivability, efforts/lethality and lastly command & control (C2) (Forsvaret, 2007, p. 73). These combat functions are the basis for all military operations and it is paramount to get them all working seamlessly together. C4IS is the tool that makes it possible to tie all combat functions together, which is clearly shown in this figure from FFOD

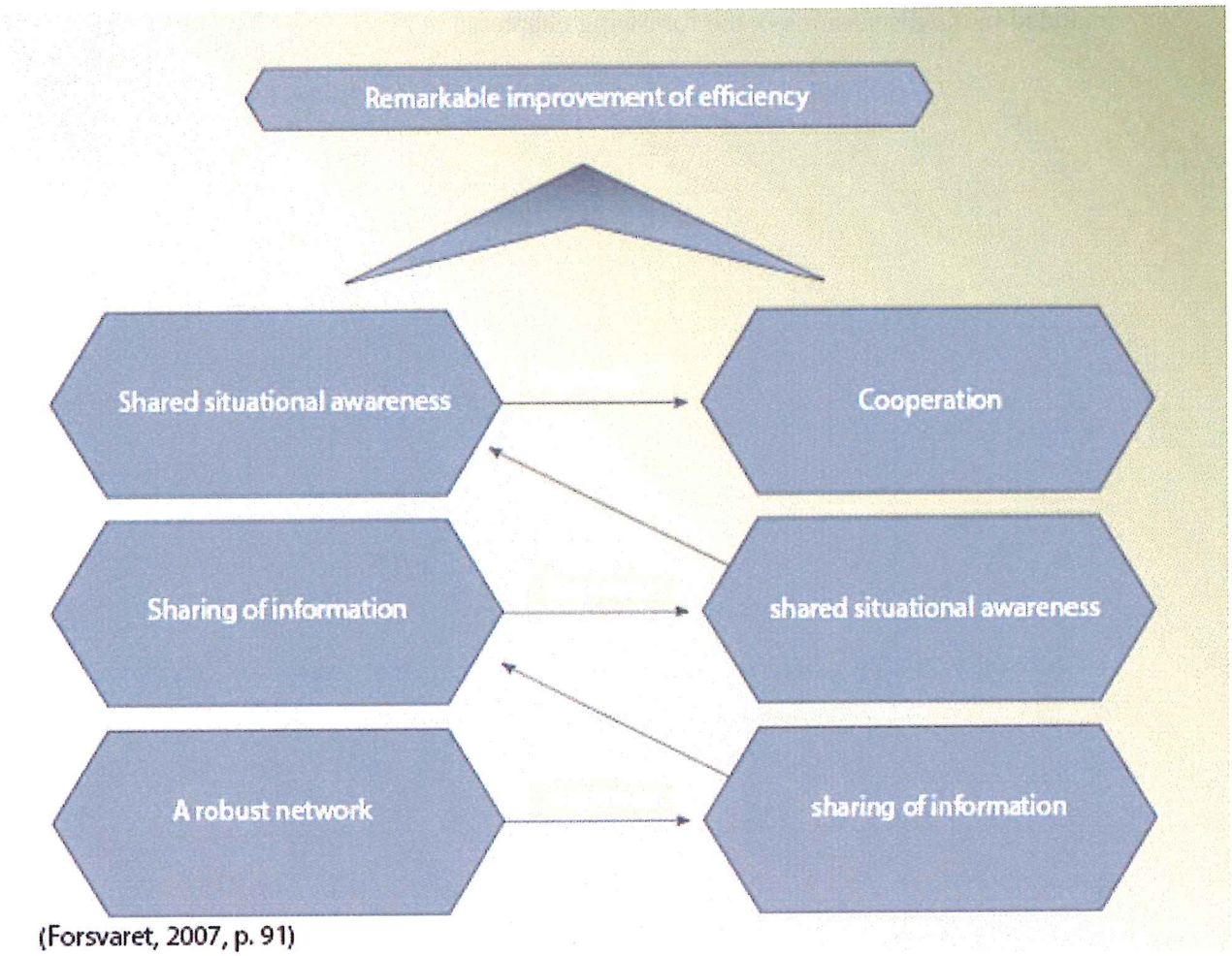


(Forsvaret, 2007, p.73) - English translations added to the figure.

[3] FFOD - Norwegian: Forsvarets FellesOperative Doktrine

## 2.3 Network-based defence

The C4IS provides the technical solution that enable these combat functions to work in synergy. FFOD explains how this synergy is made possible through network-based defence (NbF[4]). NbF provides increased flexibility and efficiency by making information readily available. By connecting sensors, effectors and decision makers in one robust network infrastructure it makes it easier to share information. This makes it easier to keep a correct and shared situational awareness, and make the correct decisions more quickly than before. Here is a model that shows this synergy effect of network-based defence, and in essence, the C4IS. (Forsvaret, 2007, pp. 90-91)



(Forsvaret, 2007, p. 91)

A robust network would arguably be one that delivers the information reliably and within reasonable time, but that means there are some requirements and perhaps challenges. I have earlier pointed out that network bandwidth is one challenge: "One of the biggest challenges for Norway's BMS during BQ11 was bandwidth on the radio." (Kristiansen, 2014). FFOD also points out challenges with NbF. The challenges are according to Forsvaret (2007, pp. 98-

[4] NbF – Norwegian: Nettverksbasert forsvar.

99) information management, bandwidth and transfer speeds, power supply, and increased use of centralised leadership could become an issue.

## 2.4 Conclusion doctrine

The Norwegian Armed Forces' doctrine shows clearly that command and control has a special role to play in combat, and that it is the combat function that ties the rest of them together. It is supposed to do that through a robust network and this is where the C4IS comes in. The technical implementation of C4IS in the army is what would make a robust network. There are two challenges from network-based defence that clearly should be discussed further, namely bandwidth and transfer speeds, and perhaps power supply. These will be included in the discussions in the following chapters.

# 3. Norwegian Battle Managment System – NorBMS.

*"No comms, no bombs!" – Unknown*

## 3.1 What is NorBMS?

**"Battlefield management system** (BMS) is a system meant to integrate information acquisition and processing to enhance command and control of a military unit." (Battlefield management system, 2016). BMSs has been in development as early as in the eighties, but from technical documents from the US Army it seems that it was mostly the map functionality that was under development. (U. S. Army Research Institute for the Behavioral and Social Sciences, 1988). In todays day and age technology has come so far that a BMS can do much more than just provide map tools.

> Battlefield Management Systems have been available for some time. A temporary Norwegian system (NORTaC BMS) has even been used in international operations, and the Norwegian army has recently selected Teleplan's NorBMS (formerly FACNAV) as its BMS. Thus, the technology for a "basic" BMS exists and is mature. (...) Apart from the basic BMS functionality, which comprises primarily map functions, blue force tracking (BFT) and data collection, more advanced functions will probably emerge in the near future. (Andås, Blix, Solheim, & Birkemo, 2013, pp. 20-21)

As one can see from this quote from FFI, the NorBMS is a C4IS and the system of choice for the Norwegian Army.

The capabilities of NorBMS include blue force tracking, information filtering, tactical navigation, alerts, message handling, 2D and 3D maps, battle log, terrain analysis, and planning tools to name a few. It also supports multiple communication systems and radio nets, and integration with weapon systems, sensors, and vehicles (Riisnæs, 2013).

To a layman, one can easily explain some of its capabilities by comparing it to that of the "radar" in a first-person shooter game. That is, it displays one's own position correctly on a detailed map, seeing friendly forces as well, and getting details about the enemy on the same map. (Kristiansen, 2014) The NorBMS is a vehicle mounted ruggedized computer. So since the NORMANS-projects C4IS solution was cancelled, the Norwegian Armed Forces lack the capability to track individual soldiers (Kristiansen, 2014). The NORMANS-project would have added these C4IS capabilities to the individual soldier and increased situational awareness significantly (Andås, Blix, Solheim, & Birkemo, 2013).

## 3.2 Advantages of a C4IS like NorBMS?

The FFI had run tests and state in their report that with the NORMANS C4IS system a dismounted unit would raise its effectiveness 20-40% over baseline (Andås, Blix, Solheim, & Birkemo, 2013, p. 16). The NorBMS and the NORMANS were interoperable and if the BFT-information could be sent as often as every 10th second for every individual soldier, there would be a drastic advantage on the battlefield. This advantage lies in having a reliable system for identifying friendly forces, and then being able to deliver indirect fire far more quickly in the vicinity of own forces. This would however require a much higher bandwidth and data transfer rate, than that in use today. (Andås, Blix, Solheim, & Birkemo, 2013)

The advantages with NorBMS continue as the integration with weapon systems and sensors increase. The level of fusion between these systems are dependent on using standard protocols interfacing between the systems, and on a higher data transfer rate. As FFI so eloquently put it; "Given radios with higher bandwidth, more functionality becomes available in a BMS. One could for instance request images from a UAV or other vehicle, or perhaps even live video." (Andås, Blix, Solheim, & Birkemo, 2013, p. 21)

All the benefits of network-based defence are technically supported by the NorBMS. Information can be shared to everyone who has a NorBMS client. It can be connected to multiple communication channels simultaneously, which would provide both redundancy and hopefully also better transfer speeds by choosing the best channel at the given time. Cellular network is one of the multiple communication channels the NorBMS can use, and the concept has been proven to work (E-mail correspondence between NOBLE[5] and J6 in the Norwegian Armed Forces Operative Headquarters, 07.November 2013).

## 3.3 Challenges with a C4IS like NorBMS bring?

The NorBMS is running on a proprietary ruggedized tablet computer running Microsoft Windows, all of which making it an expensive piece of hardware. Just like with the proprietary radios mentioned in the introduction, the NorBMS clients also become a scarce resource. So in addition to the NORMANS C4IS project being cancelled, there are not enough NorBMS clients for the mounted units either. The positive effect blue force tracking could have had when calling in indirect fires, is therefore not fully realised as of today.

The challenge of power supply is not necessarily a big problem with the NorBMS because it is meant to always be connected to power in the vehicles. The tablet solution does require quite a lot of power. So an unmounted solution using the tablet is not feasible on a

[5] NOBLE – Norwegian Battle Lab & Experimentation

large scale with the equipment of today. It is possible on a small scale though, by using Harris Radio batteries and a power adapter.

The transfer speeds can not be said to be a problem of the NorBMS software or hardware considering it is connected to a MRR[6], that admittedly has a maximum data transmission rate of 19.2kbps (Kongsberg Defence & Aerospace). The NorBMS itself would have a limit to its data transfer rate which is decided by the network interface it uses, which far exceeds that of the bottlenecking MRR.

The NorBMS is in this dissertation described as the technical implementation or the embodiment of network-based defence and the network-based thinking. The NorBMS therefore brings the same challenges that network-based defence does, including the cultural aspects that are not discussed in this dissertation.

## 3.4 Conclusion NorBMS

When it comes to the challenges from chapter 2; transfer speeds and power supply, only one of them is a limitation for the NorBMS. The power supply could be considered real challenge. Maybe not a challenge for the way it is used today, but because of it we are bound to use it like we do today. With a quickly waning battery and no viable portable charging solution, the DM8[7] based NorBMS hardware will have to be a vehicle mounted solution.

The NorBMS is a powerful tool, but it is in many ways held back by the low bandwidth of the Norwegian Army's primary radio. Future development and acquisition of a new primary radio should weigh high bandwidth as an important factor. Cellular networks can provide an alternate solution in the meantime.

The client in itself is stated to be expensive, and I suggest that this is a reason the Armed Forces don not have more of them. NorBMS is a software application built for Microsoft Windows, so it could be run on just about any Windows machine. Looking at alternate hardware could be a solution, at least for some of the users. E.g. most users in the Brigade HQ run their NorBMS on a regular non-rugged laptop, often virtualised from a local server in the HQ. Similar alternate solutions should be considered throughout the organisation.

---

[6] Multi Role Radio
[7] DM8 – Norwegian: DataMaskin 8

# 4. Information security

*"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." – Bruce Schneier*

## 4.1 The holy trinity of information security

Information security is divided into three parts in most literature that broach the subject. These three parts are often referred to as the CIA-triad. CIA stands for Confidentiality, Integrity and Availability in this context. Confidentiality refers to the concealment of the information, integrity to the information being immutable, and availability is simply that the information must be available to those who need it (Bishop, 2005). The Regulations of Information Security actually adds a fourth concept in its chapter on Information system-security, namely authenticity (Forskrift om informasjonssikkerhet, 2001). By authenticity it is meant that there should be an authentication of the user before they are able to access or send information, e.g., by requiring a username and password. In most theory the aspect of authentication is mentioned in the principle of integrity.

### 4.1.1 Confidentiality

Confidentiality is provided by the means of cryptography, which is defined as "the science of secret writing with the goal of hiding the meaning of the message." (Paar & Pelzl, 2010, p. 3). Hiding the meaning of the message has been of interest for ages and there are recorded usage of cryptography as far back as to the Egyptians 2000 B.C. The most well-known example of early usage of cryptography would be the Roman empire using the Caesar cipher. (Paar & Pelzl, 2010, p. 2)

#### *4.1.1.1 Symmetric algorithms*

The Caesar cipher is an example of perhaps the "simplest" form of encryption, namely the substitution cipher, using a symmetric algorithm. Symmetric algorithm is an algorithm where you do both encryption and decryption with the same secret key. Symmetric methods are the ones that have been used since ancient times and up until 1976. (Paar & Pelzl, 2010, p. 3). To understand the symmetric method one can use the Caesar cipher as an example:

Alice and Bob wishes to send each other secret messages without Eve[8] being able to eavesdrop on them. Let us say Alice and Bob are sending each other messages in letters via traditional mail. The last time they met, they agreed upon using the Caeser cipher with the secret key "3". The message "HELLO" would become "KHOOR" where each letter is

[8] In cryptography Eve is a common placeholder name for eavesdropper. The same way Alice and Bob are the usual placeholder names for the friendlies wanting to share information securely.

substituted by the letter coming three places after it in the alphabet. Below there is a substitution table that helps Alice and Bob to encrypt by going from top to bottom, and decrypt by going from bottom to top.

| X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

*Fig. Substitution table*

This example can shed light on some of the weaknesses to the symmetric methods. The secret key must be shared somehow. As Paar and Pezl (2010, p. 7) clearly states; "As always in symmetric cryptography, the key has to be distributed between Alice and Bob in a secure fashion.". This means Alice and Bob would have to be in the same location to share the secret key. A second problem is that it is easy to crack, at least with the secret key used in this example. It would probably take a human no more than 3 iterations to manually brute-force attack this ciphertext. Brute-force attacking means exhausting every possible solution.

It would be easy to add entropy[9] to a symmetric key by extending the length of the key, say if Bob and Alice agreed upon a key "4 – 5 – 2 – 16 – 25 – 0". Then "HELLO" would become "LJNBO", and they only used 5 of the 6 digits from the key. If the message had been longer they would repeat the key over and over. The problem with the repetition of the key is that although a brute-force attack may be foiled, a cryptanalysis based on the languages letter distribution would not be fooled. It is therefore still feasible to crack this given the computational power. The level of confidentiality provided by a symmetric key is decided by the strength(length) of the key. Symmetric keys can be as weak as the one in the previous examples, or reach the strength of perfect security.

#### *4.1.1.2 The One-Time Pad – perfect security*

As Bruce Schneier (1996) tells us "Believe it or not, there is a perfect encryption scheme. It's called a **one-time pad**, and was invented in 1917(...)" (Schneier, 1996, p. 15). He goes on to explain that it is as "simple" as having a truly random secret key, and the key must be as long as the message itself.

The key generation must be based on true randomness, and not pseudo-random generators. The random generators available in a personal computer is pseudo-random. True

[9] Entropy – unpredictability of information.

randomness is therefore hard to implement with automation. A coin-toss done by a human is an example of true randomness, but not automated and thus not a scalable solution. Scalable solutions do exist and usually they are created with esoteric hardware using sensors to read static from the electromagnetic spectrum or better yet, from a decaying isotope of radioactive material. So while true randomness is possible, it is not easy and not cheap. With access to true randomness the key generation would begin. (Paar & Pelzl, 2010, pp. 34-38) (Schneier, 1996, pp. 44-47)

The second factor of perfect secrecy is having a key that is as long as the message itself, meaning no repetition of the key. The key is only used to encrypt one message, and then the key is destroyed. When this technique has been used the keys were printed on pads where they would use a pad and then discard it, hence the name. If Alice and Bob uses a One-Time pad based on true randomness and the key is successfully kept a secret, then Eve or Oscar would not be able to decipher it ever. This is the definition of perfect secrecy or unconditional security; that it can not ever be cracked even with infinite time and computational resources. Important note is that Eve might be able to decipher it with infinite computational resources, but she would have no way of knowing when she has. All messages imaginable in the world of that particular length, are equally probable to be the message and hence – perfect secrecy. (Paar & Pelzl, 2010, pp. 34-38) (Schneier, 1996, pp. 44-47)

#### *4.1.1.3 Asymmetric algorithms*

Asymmetric algorithms, also known as public-key algorithms, are based on an encryption key that works one-way, and then needing another key entirely to decrypt the message. The encryption key can be distributed publicly, hence the name public-key, because it provides no possibility to decrypt the message. The decryption key is called the private key, (Schneier, 1996, p. 4)

This algorithm is based on hard mathematical problems and so-called one-way functions, meaning that given the answer of the function one could never know what the input of the function was. Understanding the mathematics behind this particular function is luckily not at all necessary to understand the benefits it could yield. These benefits will be discussed later.

#### *4.1.1.4 Kerckhorffs' Principle*

> Kerckhorffs' Principle: A cryptosystem should be secure even if the attacker (Oscar) knows all details about the system, with the exception of the secret key. In particular, the system should be secure when the attacker knows the encryption and decryption algorithms (Paar & Pelzl, 2010, p. 11).

This principle is a key take away from the subject of cryptography. There are several examples where cryptosystems have been created and used on the basis of security through obscurity. An open-source system showing all the details of how it works is far more secure through being scrutinised and tested by others. Relying on a cryptosystem should mean relying on the strength and the secrecy of the key, and not the obscurity of how the system is set up.

#### *4.1.1.5 Advantages and disadvantages*

Confidentiality is a requirement and a concept that keeps the military safe by providing operational security through information security. There are a few disadvantages that follow confidentiality worth mentioning. Cryptosystems can be onerous to use and they are not always user-friendly or intuitive. Depending on the algorithm and its implementation the data increases in size after encryption, meaning it takes requires more bandwidth than the original message.

The primary advantage of the symmetric key is that it is not based on complex mathematics using large primes or hard-to-compute functions. This makes a symmetric key require very little processing resources when it is used. The symmetric key's shortcomings is that one would have to meet in person to safely exchange keys. One would also have to produce a different key to use with different people increasing the key exchange problem, and creating a key management problem. There is no integrity check in a symmetric algorithm so Alice could send a message, and then say that it was Bob that sent it. The principle of preventing this is called non-repudiation and needs an asymmetric key to be achieved. (Paar & Pelzl, 2010, pp. 150-151)

Asymmetric keys solve the problem of non-repudiation by adding a integrity check with a personal cryptographic signature. The asymmetric algorithm also solves the problem of key distribution because the encryption key is public. The encryption key is made to be shared and the open-source asymmetric solution Pretty Good Privacy (PGP) is a good example where they have gone to the step of creating a central database to share your public key. The clear disadvantage is that the algorithm is based on hard-to-compute functions and requires more resources and time to compute. (Paar & Pelzl, 2010) (Schneier, 1996, pp. 47-52) (Paar & Pelzl, 2010, pp. 150-157)

Perfect security has the clear advantage of being unconditionally secure, but the key management problem would increase to a level where it is not feasible to use on a large scale. Small communities and contingency solutions could use the one-time pad.

Asymmetric and symmetric algorithms fulfil each other when it comes to their advantages and disadvantages and they are used together in hybrid solutions all the time. A simplified example of net-banking: Alice logs onto her internet banking account. Behind the scenes the connection is made to the bank using a public-key algorithm when authenticating that Alice is not Eve. After the authentication process has been done there is an open communication channel between the bank and Alice's computer based on an asymmetric key. Through that secure tunnel the bank shares a secret symmetric key with Alice's computer. While browsing the bank the connection is now secured with the symmetric key that requires far less resources to compute. After Alice logs off or the connection times out, the shared secret key is deleted and the bank will require a new authentication and creating a new key.

### 4.1.2 Integrity

Integrity is all about the integrity of the information. Has the message that Bob received from Alice been changed by Eve? Kluge (Informasjonssikkerhetsmessige utfordringer i Forsvaret, 2003, p. 9) has an excellent example from the military context where the enemy makes a recording of chatter on the radio and later plays it back on the radio. With the voice being a familiar one it is easy to fall for it being a real message and this would be the moment to use the authentication table that has been distributed before the operation. (Kluge, 2003)

When it comes to modern network data the integrity is confirmed using one-way functions to provide a so-called signature. As long as Bob sees Alice's signature he knows it is from her. This is done to prevent what you call a man-in-the-middle attack where Eve hijacks the public key exchange between Alice and Bob. In such an attack Eve makes Bob think he received Alice's public key while he in fact received Eve's public key. (Schneier, 1996, pp. 30-57)

The inner-workings of key authentication and safe key exchange falls somewhat outside the scope of this dissertation, simply because we as a military organisation keep true to basing our cryptosystem on shared secret keys. By staying true to pre-shared secret keys the costs do build up, but man-in-the-middle attacks or other public-key problems are of no concern.

### 4.1.3 Availability

Having the information needed available for the correct people at the right time. Both confidentiality and integrity can negate availability if implemented poorly. In informatics a good example of an attack on availability is a denial of service-attack. A classic military example of attacking availability would be jamming (Kluge, 2003). In a military organisation there is also the concept of need-to-know. This concept has the purpose of providing operational security and to avoid an overload of information on the individual. This concept

can at times be in the way of availability, especially if the method to implement it is by classifying the material.

## 4.2 Information security and NorBMS

The NorBMS is classified as BEGRENSET, which is the equivalent of NATO RESTRICTED. This means it falls within the realm of information security and the realm of the NSM. How the security is upheld and what legalities pertains to it because of this will be discussed briefly in chapter 6. For now, let's see how the NorBMS lives up to the holy trinity.

The confidentiality is secured using a cryptosystem. The Norwegian Army has its own organisational elements that generate symmetric keys and the keys are distributed using couriers. The keys are loaded onto the primary radio and anything sent on the radio is encrypted. The NorBMS is connected to the radio and sends its data through it. The NorBMS is not the machine doing the encryption so any data carrier that is connected must either provide a secure and encrypted channel, or the data must be passed through an encryption box before it is connected to the unsecured data carrier. This last solution is what makes using 4G and unsecured cellular networks possible.

The integrity is as good as it can be with secret keys. It is integrity through successful confidentiality. Alice knows that Bob is Bob because he is the only one who has the shared secret key. The same principle goes for the NorBMS and the radios it is connected to. The basic assumption is that anyone sending a message must be friendly because the secret key has not been shared outside the organisation. Understanding this fragility to our security concept, it may be easier to appreciate the extreme lengths the Army goes to to the secret keys safe. This is the reason we define equipment as CCI[10] and keep perfect track of it, and the reason we do not leave it unguarded.

Availability for the NorBMS is about being connected to the network. If the keys are not correct, there is no availability. If the radio does not have coverage, there is no availability. The fact that the NorBMS has no encryption makes it cheaper, but completely dependent upon a secure channel. This means that the only way for the NorBMS to have availability is by using the primary radio as a data carrier with a valid shared secret key, and being within the radio coverage that is provided by the Signal Battalion.

---

[10] Cryptographic ComSec Item – Cryptographic equipment that has certain regulations on how to store it, keep track of it, and use it.

All three principles of information security are important to consider when considering the data carrier of a C4IS. With this understanding of information security in the context of NorBMS and C4IS it is worth trying to look at how LTE as a data carrier will affect it.

# 5. 4G / LTE+ technology

*"There is but one mind-set you need to have in the Home Guard; and that is to buy cheap commercially available solutions that just work right out of the box!" – Inspector General and Chief of the Home Guard, Tor Rune Raabye*

## 5.1 What is 4G / LTE+?

4G means 4th generation and is a label used in telecommunications to say something about what to expect of the networks capabilities, i.e. bandwidth. There are two types of 4G technologies; WiMAX and Long Term Evolution (LTE). Long Term Evolution Advanced (LTE+) is the standard that is taking over for LTE. (4G, 2016)

## 5.2 Why 4G / LTE+?

There are two technologies providing sufficient network bandwidth, that could be argued to be readily available; LTE and WiMAX. While both should be discussed in depth, that would go far beyond the scope of this dissertation. The Norwegian Defence Research Establishment[11], henceforth only referred to by their acronym FFI, have written a report on both WiMAX and LTE. In this report it is stated that WiMAX is rapidly spreading in its availability, but that it is more likely to be built in places where older mobile technologies aren't present (Farsund, 2010; Hveem, 2011). The average mobile user will have observed that since 2010 LTE has been the technology of choice among the service providers in Norway.

The LTE has theoretical download speeds of 50-100 Mbit/s and is purely IP based. The technology will provide a bandwidth fitting for multimedia streaming other demanding applications. (Hveem, 2011, pp. 64-65) According to Hveem (2011, p. 65) the service providers' biggest challenge with this new technology will be to "offer this adequately cheap". The bandwidth is an excellent reason to consider it a viable data carrier for the NorBMS. The fact that it uses the IP-standard makes it easy to use with the NorBMS, which is IP based today. With LTE as a data carrier the availability would increase dramatically because it is provided commercially. It is of course in the service providers' best interest to have the best coverage to have on advantage on their competitors.

Hveem (2011) offers a thorough description of the information security aspects of the technology in her report, but it would be farfetched to think the cellular network in general would be certified for classified information so the Armed Forces still need their own security. There are ways of doing man-in-the-middle attacks on cellular networks by using

---

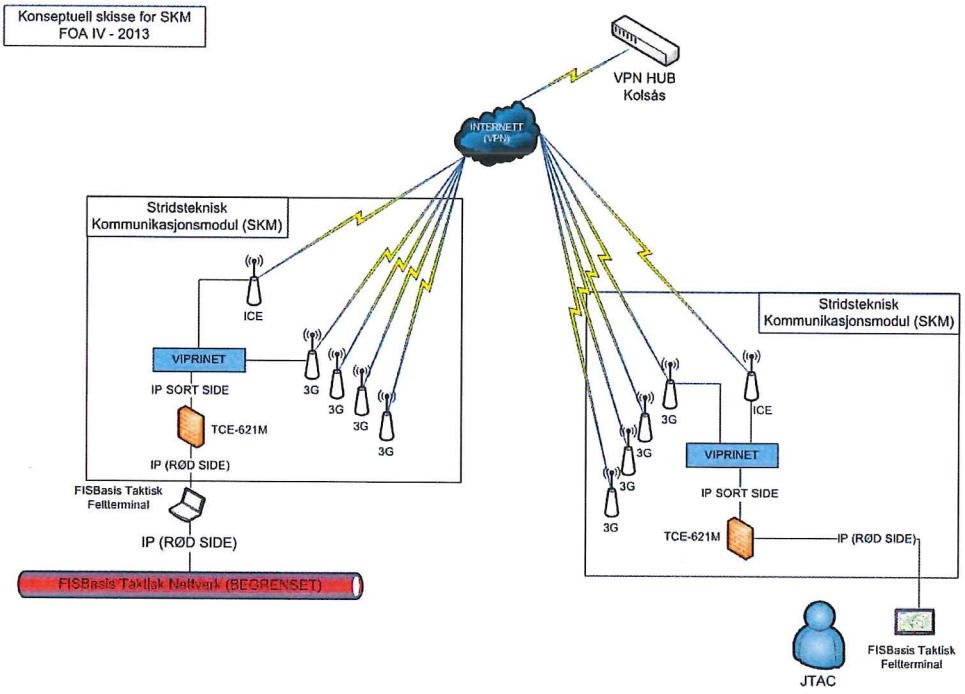
[11] FFI – Norwegian: Forsvarets ForskningsInstitutt

IMSI-catchers. It would be like Eve putting up her own cellular base station and makes Alice and Bob think they are connected directly through their service provider, while in fact the call goes through Eve's base station.

## 5.3 How to use 4G / LTE+ securely

### 5.3.1 Proprietary crypto solutions

There is a solution today that is certified by the NSM and that is used to some degree in the Armed Forces today. Norwegian Battle Lab & Experimentation (NOBLE) made this solution to transfer information securely through any commercial network by means of end-to-end encryption. It requires a box called MINIP provided by Thales to do the encryption and decryption. (E-mail correspondence between NOBLE[12] and J6 in the Norwegian Armed Forces Operative Headquarters, 07.November 2013). This solution encrypts all data before it connects to the "unsecure" data carrier, which in this is example is a 3G cellular network.




This is an excellent solution with regards to confidentiality where one can stay true to using a shared secret key and increasing availability of the C4IS. It is of course in use, but not so widely as to reap the benefits that a C4IS could provide. The challenge is the cost of a proprietary encryption box from the industry, of which one would need 1 unit per user. On top of that comes the cost to the service providers using the cellular network. This fulfil the need of confidentiality by using a solution approved by the NSM. It fulfils the need of integrity the

[12] NOBLE – Norwegian Battle Lab & Experimentation

same way our current system does, meaning that the security organisation must be maintained and the routines must be kept as strict regarding CCI. Availability is increased drastically, but arguably the army have less control of its availability and less knowledge on how availability can be attacked during a conflict. It is of course obvious that in the physical domain the service providers' base stations can be attacked. How the service can be attacked in the information domain is outside the control of the Army.

### 5.3.2 Mobile phones as modems or mobile broadband modems

In the previous example it was not just the MINIP from Thales that was needed. There was also the need of mobile broadband modems. Is it not possible to use cellular phones to save cost? Everyone has a smartphone so that could be a possible solution. It is of course the security implications that stop this from being possible.

First of all, a mobile phone in close proximity to other secured comms would be a breach of TEMPEST. TEMPEST is an expression dating back to the 50s. All electronic equipment emit electromagnetic radiation and if this radiation can be analysed to distil classified information, that would be TEMPEST. (NSM, n.d.). There are also other ways in which a smartphone can be compromised and used as a espionage tool.

All modern smartphones have cameras and microphones these days. If someone is able to hack the phone, then they would be able to activate both the camera and the microphone. So using a smartphone as the data carrier for a secure system provides serious implications to the security of its system. It is therefore easier to use a mobile broadband that firstly, does not have neither camera nor microphone, and second, a lot more difficult to hack without physical access than a smartphone.

## 5.4 Conclusion 4G / LTE+

It is clear that yes, we can in fact utilise the 4G/LTE technology as a data carrier for C4IS in the Norwegian Army, and we do of course. It is however not widely in use, but as a supplementary data carrier for key units. The full power and all the advantages of a C4IS will not be fully realised until every system is on the network with an adequate bandwidth. Where the threshold for adequate bandwidth should be, would probably require a dissertation in itself to answer, but todays primary data channel of 19kbps is surely too narrow. The reason for the Army not using LTE more, is likely to be because of the costs and possibly because many consider it irresponsible to "be dependent upon civilian infrastructure". Use of civilian of civilian infrastructure is an important question worth researching, but what I can say based on the research done within my scope is that it is not the only option.

The US Army has 4G relays mounted on vehicles like we have radio relay. Australian Signals Officer and Engineer Kurt Brown has written a paper on "Enhancing battlefield communications through 4G LTE+ cellular technology". That paper was based on the premise that the army would provide the cellular network for itself. (Brown, 2015). Perhaps a hybrid solution where one could use both commercial and ones own cellular network. This way availability would be many times better, and the rest of the CIA triad would be basically equal to our system today.

# 6. Method and methodology

"My methodology is not knowing what I'm doing and making that work for me." – Stone Goddard

The problem that this dissertation seeks to answer is in many ways a technical one, and by that, a purely scientific one. However, the issue is discussed in the context of the social constructs of both warfare and legalities. This puts the dissertation in both the realm of the natural sciences and the realm of social sciences. When it comes to the technical particulars of the issue it has to be observed from the position of the natural sciences. This can strengthen the thesis by supporting the factors with hard sciences and near undisputable facts.

At the same time the core of the question is not a hypothetical one, but a pragmatic one. Meaning that whether or not it is hypothetically possible to use 4G securely, it is actually irrelevant if the National Security Authority won't approve it. Therefore, it is in the end a question that should be considered from the view of the social sciences. The methodology used is therefore very much in the tradition of the social sciences.

This method of research has been qualitative and based mainly on literature. I say mainly because it is also based on conversations with various experts in the field. Trying to narrow down a research question for the dissertation I had conversations with experts within the information security environment and the Norwegian military industry. I talked to people from Teleplan Globe, Thales, Kongsberg Defence and Aerospace, Telenor, Nasjonal Kommunikasjonsmyndighet[13], and of course some people from the NSM. These discussions were informal and none of them were transcribed or taped and they are not used as evidence in this research, but rather just a means to find the research question. From there I did a systematic search of relevant libraries to find a fitting theoretical basis.

## 6.1 Weaknesses to this dissertation

The literature used to answer is mainly narrow scope and is about the technologies, but somewhat wider when it comes to military doctrine. Quite a few of the sources are collected online, but that is mainly the reports from FFI who are renowned and accredited researchers. There are a few resources in the bibliography I expect to be critiqued on choosing, so I'll elaborate a bit on these.

Three sources that I base a lot of the research on is Bishop, Schneier, and Paar & Pelzl. Both Bishop and Schneier can be said to be too old considering that the field is informatics, and they are used to argument in relation to very modern technology. The parts used from

[13] Norwegian Communication Authority

both Bishop and Schneier were basic principles of computer security and cryptography, and not things that have likely changed since. That has of course been confirmed by other sources.

Citing my own work could of course be seen as an example of bias, or an attempt to support my arguments on foundations of which I could not find any proper sources. Most of those references however are observational on how the NorBMS works and what capabilities it has. While any argument made with reference to that work, is backed up with other credible sources.

The choice to include so much of the Norwegian Armed Forces Joint Doctrine of 2007, instead of the new one from 2014 can seem a bit weird. It is important to understand that even though the doctrines are revised so thoroughly, they don't really loose their validity. The military theory the Norwegian Armed Forces consider important has not changed. The doctrine of 2014 describes it as "changing focus" and it is apparent that the 2007 is not automatically void and there is no doubt that network-based thinking is still important. The 2007 edition was chosen because it explains more simply how network-based defence fits into the military theory.

## 6.2 Further research

Throughout the dissertation there came up quite a few interesting questions and themes beyond its scope that had to be omitted. I chose to highlight a few of the most interesting ones, that would be fitting as recommendations towards further research:

- It would be interesting to see if LTE could be implemented as the data carrier on all levels in the Norwegian Army, especially from a financial point of view.
- Having LTE is a logical choice in Europe, but what about Africa and the places where WiMAX is the 4G technology of choice. Do we need both capabilities in the case of future deployments to such regions?
- Could we systematically provide encryption on our unclassified devices in the Armed Forces, and build the infrastructure needed for such a project?
- Is it viable to completely base a communication plan on civilian infrastructure and what are the risks?

# 7. Conclusion - summary

There should be little doubt that network-based thinking is one important part of our Norwegian Armed Forces doctrine. It is not the only way of thinking that holds importance, but the way it is connected to effective command and control makes it a precursor for the other combat functions. The combat functions are intelligence, effects, mobility, logistics, force protection and the one keeping them all together, command & control.

NorBMS is a C4IS used in the Norwegian Army and can be thought of as the technical tool by which network-based thinking and network-based defence is realised. It increases situational awareness, but its potential is somewhat underutilised. This is mainly because the C4IS is not available to all units, probably for economic reasons. It is also because the NorBMS in itself is limited to a very low bandwidth because the primary radio has such a low bandwidth. An alternate communication channel with higher bandwidth would add capabilities to the C4IS such as live video streaming, sensor integration and weapon integration. This would further add to both situational awareness and operative capability.

Information security is a requirement to communications in the military to keep a level of operational security. The National Security Authority is the authority on information security in Norway and decide which systems can be certified for sending classified information. Information security is enabled by making sure its key concepts confidentiality, integrity and availability are upheld. Confidentiality is provided by using cryptography. In the Norwegian Armed Forces confidentiality is based on a symmetric secret key with high entropy. This requires a solid security organisation with strict regulation of the keys and CCI. In the army integrity is not checked systematically, but it is assumed all users having the secret key are authorised. This confirms the importance of being strict with the regulations. Availability is considered low in the Army because the availability of the network is based primarily on own infrastructure.

4G / LTE technology would provide the NorBMS enough bandwidth to add the capabilities mentioned earlier. While the 4G is quite secure compared to all the previous generations of cellular technology, there are too many uncertainties for the NSM to certify the technology in itself. The implementation of LTE, and the network architecture can also vary from service provider to service provider, and therefore the security would also differ. Adding end-to-end encryption to the LTE channel is a viable solution to make it secure enough for classified information. NOBLE created a concept of using 3G-cellular modems and a certified end-to-end encryption box with keys that were certified up to Norwegian SECRET. The same solution is possible to use with 4G.

Using this solution provides a proper level of confidentiality already approved by the NSM. Checking integrity would be based on the same system as today with very strict control of the key and the physical access to the CCI. Availability on the other hand would increase dramatically, but in Norway it would as of now be based solely on civilian infrastructure. If cooperating with other NATO forces, they might provide a military 4G network.

There is no doubt that it is perfectly possible to utilise 4G as a secure data carrier for C4IS in the Norwegian Army. The solution exists today, and it is in use within the army. It would be interesting to further research how it is possible to get 4G on every NorBMS unit, what it would cost, and what consequences it could have.

## Accronyms and abbreviations

4G – 4th generation cellular technology.

Bandwidth – In this dissertation used with the meaning of the colloquial for data transfer rate in mind (download speeds).

C2 – Command and control

C2IS – Command, control, Information Systems

C4IS – Command, control, communications and computer information systems

Ecom – Electronic communications

FFOD – Norwegian: Forsvaret Fellesoperative Doktrine. Norwegian Armed Forces' Joint Doctrine

MRR - Multi Role Radio

NbF – Norwegian: Nettverksbasert forsvar. Network-based defence

NOBLE – Norwegian Battle Lab & Experimentation

NorBMS – Norwegian Battle Management System

NSM – Norwegian: Nasjonal SikkerhetsMyndighet. National Security Authority

LTE – Long Term Evolution

## Works Cited


Andås, H. E., Blix, T. A., Solheim, S. O., & Birkemo, G. A. (2013, 06 05). *FFI.no.* Retrieved 02 10, 2016, from Miltech report 2012: http://www.ffi.no/no/Rapporter/13-01139.pdf

4G. (2016, 04 13). *Wikipedia.* Retrieved 04 14, 2016, from https://en.wikipedia.org/wiki/4G

Battlefield management system. (2016, 04 10). *Wikipedia.* Retrieved 04 12, 2016, from https://en.wikipedia.org/wiki/Battlefield_management_system

Bishop, M. (2005). *Introduction to Computer Security.* California: Addison Wesley Professional.

Brown, K. (2015, 11). Enhancing Battlefield Communications through 4G LTE+ cellular technology. *Journal of Battlefield Technology, 18*(3), 5-16.

Farsund, B. H. (2010, 06 23). *WiMAX - teknologi, funksjonelle egenskaper og sikkerhet.* Retrieved 01 16, 2016, from Forsvarets Forskningsinstitutt: http://www.ffi.no/no/Rapporter/10-01347.pdf

Forskrift om informasjonssikkerhet. (2001, 07 01). *Lovdata.* Retrieved 03 02, 2016, from Lovdata: https://lovdata.no/dokument/SF/forskrift/2001-07-01-744/KAPITTEL_5-4#KAPITTEL_5-4

Forsvaret. (2007). *Forsvarets fellesoperative doktrine* (1 ed., Vol. 1). Oslo: Forsvarsstaben.

Forsvaret. (2014). *Forsvarets Fellesoperative Doktrine.* Oslo: Forsvarsstaben.

Hæren. (2015). *Hæren - Visjon 2035.* Oslo: Hæren.

Hveem, A. P. (2011, 04 05). *Mobilt bredbånd med LTE – teknologi, sikkerhet, tjenester og utbygging* . Retrieved 01 16, 2016, from Forsvarets Forskningsinstitutt: http://www.ffi.no/no/Rapporter/11-00709.pdf

Kluge, G. (2003). *Informasjonssikkerhetsmessige utfordringer i Forsvaret.* Krigsskolen. Oslo: Krigsskolen.

Kongsberg Defence & Aerospace. (n.d.). *Kongsberg Gruppen.* Retrieved 04 05, 2016, from MRR VHF: http://www.kongsberg.com/~/media/KDS/Files/Products/Defence%20Communication/MV_MP300%20datasheet.ashx?la=en

Kristiansen, O. (2014, 11 13). *C4IS.army.* Retrieved 04 14, 2016, from http://c4is.army/about/miltek.pdf

NSM. (n.d.). Retrieved 04 02, 2016, from https://www.nsm.stat.no/tjenester/sikker-kommunikasjon/tempest/

Paar , C., & Pelzl, J. (2010). *Understanding Cryptography - A Textbook for Students and Practitioners.* Berlin, Germany: Springer-Verlag.

Riisnæs, R. (2013, 01 17). *NorBMS - Quick overview.* Retrieved 11 13, 2014, from https://kgv.doffin.no/app/docmgmt/downloadPublicDocument.asp?DVID=82176&FMT=1&AT=15&ID=15314

Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms and Source Code in C* (2nd edition ed.). Indianapolis, Indiana, USA: John Wiley & Sons.

U. S. Army Research Institute for the Behavioral and Social Sciences. (1988, 07 01). Retrieved 04 02, 2016, from http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA201189