LTE for military communication - business models and vulnerabilities

Bodil Farsund*, Anne-Marie Hegland**, Frode Lillevold*

*Norwegian Defence Research Establishment (FFI), Kjeller, Norway

**Kongsberg Defence & Aerospace, Asker, Norway

Bodil.Farsund@ffi.no, anne.m.hegland@kongsberg.com, Frode.Lillevold@ffi.no

***Abstract*— This document outlines security issues concerning military use of LTE. It illustrates implications of different business models, and outlines vulnerabilities that decision makers should be aware of in order to protect the assets; user payload, metadata and network availability. The article shows that control of base stations has a major security impact. Roaming further increases the vulnerability.**

***Keywords*— Security, LTE, IP, Military communication, Business models**

I. INTRODUCTION

There are several reasons why the interest in military use of LTE (Long Term Evolution) has increased. Most important are bandwidth, interoperability and cost.

In a situation with a growing number of international operations it is desirable that each nation is able to interoperate with the other partners using their own equipment. The current solution with proprietary waveforms and borrowing of equipment from the cooperating partners scales badly. There is a lack of commonly accepted military broadband interoperability standards, and military standardization is a slow process. It is therefore interesting to consider commercial standards such as LTE. Another factor is the cost. LTE is an open standard free from intellectual property rights issues and royalty claims. The standard is maintained by the 3GPP (3rd Generation Partnership Project) with large telecommunications organizations' support. The costs are spread over a large consumer base.

LTE is primarily an infrastructure-based technology. Building infrastructure covering a large area is very expensive. Consequently, it is not given that the armed forces should build and operate its own infrastructure. With limited budgets different business models are considered. The armed forces can own all, parts or none of the infrastructure components themselves, where the last two cases include cooperation with commercial network operators.

An important question is how the armed forces will utilize LTE. Possible application areas range from replacement of fixed office phones in peace time to tactical command and control systems in international operations. Different use cases will give different security issues. To perform a complete analysis of the security and vulnerabilities related to different business models, it is necessary to know the use cases.

This article gives an overview of different business models for the implementation of LTE, and highlights the implications for the assets and vulnerabilities associated with lack of control of parts of the infrastructure. It takes no position on whether the military should or should not use LTE or how it should be used, but aims to point out risk areas that should be studied more closely. The article may also serve as a framework for further discussions on the military use of LTE and the associated security challenges.

The article is organized as follows. The next two sections give an introduction to the LTE architecture and security. Sections IV and V defines the assets and discusses threats and threat vectors, respectively. The different business models are introduced in section VI, and section VII elaborates on the vulnerabilities associated with the different business models. Related work is found in section VIII. Concluding remarks and further work is summarized in section IX.

II. LTE ARCHITECTURE

Figure 1 provides an overview of the LTE architecture. The network in LTE is called EPS (Evolved Packet System). It is an all-IP network. All communication in EPS, both real-time services and other services are IP-based. EPS consists of two parts:

- E-UTRAN (Evolved UMTS Terrestrial Radio Access Network) which is the access network consisting of base stations.
- EPC (Evolved Packet Core) that denotes the underlying core network.

The UE (User Equipment) is the actual user device.

In tactical operations it is desirable to be able to communicate even without fixed infrastructure. LTE Advanced [1] specifies device-to-device communication over short distances. The connection can either be initiated via the fixed infrastructure, or can use the devices to establish connections through direct negotiation between them. The main focus of this article is the ordinary use of LTE with communication over fixed infrastructure components.

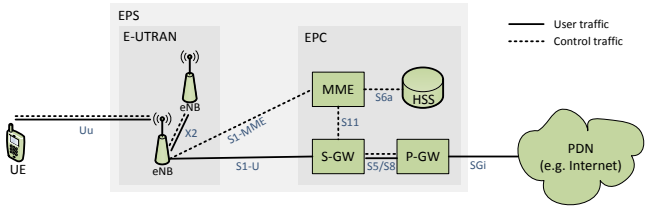

Figure 1. Outline of the LTE architecture

A. The Access Network (E-UTRAN)

The access network, E-UTRAN, consists of the base stations eNB (evolved-NodeB) that provides radio communication between the UE and the EPC. Each eNB controls UEs in one or more cells. They communicate over the interfaces (see Figure 1):

- *Uu*: interface to UE for user and control traffic.
- *S1*: interface to the EPC. S1-U transfers user traffic from/to the S-GW and S1-MME transfers the control traffic from/to MME.
- *X2*: interface to other eNBs. Used for control as well as user traffic during handover to another base station.

Compared to previous generations of mobile networks, LTE has more functionality in the base stations. There is no central control unit; this functionality is included in the base stations to reduce the time to set up a connection and to do a handover.

The LTE base stations are responsible for dynamic allocation of radio resources and handover.

B. Core Network (EPC)

The core network in LTE – EPC – has a flat architecture with fewer levels than GSM and UMTS. The purpose is more efficient management of data traffic, as fewer network nodes are involved and conversion between protocols is avoided. User traffic and control traffic are separated in EPC, which makes it easier for operators to scale and customize the networks to their needs.

Central elements of the EPC are (see Figure 1):

- *HSS* (Home Subscriber Server) - the operator's central database where information about subscribers is stored. It is contacted by MME for authentication of UE at connection set up.
- *P-GW* (Packet Data Network Gateway) - handles user traffic between the LTE network and other networks. This may be the network operator's servers, the Internet or the IMS (IP Multimedia Subsystem). Central tasks are routing of packets, allocation of IP addresses to the UEs and to filter packets for each user.
- *S-GW* (Serving gateway) - handles user traffic. Its main task is to transport IP packets between the eNBs in a given area and the P-GW. Basically it works like a router. Each user device is associated with an S-GW. The S-GW changes if the user device moves out of the responsibility area of the current S-GW.
- *MME* (Mobility Management Entity) handles control traffic. Its main tasks are signaling for initiation of IP connections (contacts S-GW and P-GW), security, and features related to idle mode such as tracking and paging. An MME controls several eNBs in a given geographical area.

EPC has the following interfaces:

- *SGi*: user traffic between P-GW and other packet data networks.
- *S11*: Control traffic between the MME and S-GW for EPS-management including handover supported by MME and coordination in connection with paging. It is a many-to-many interface.
- *S6a*: Control traffic between the MME and HSS. It carries subscriber information for authentication and authorization of users.
- *S5/S8*: user and control traffic between the S-GW and P-GW.

C. User Equipment

The User Equipment (UE) consists of the actual mobile phone (ME, Mobile Equipment) and the UICC (Universal Integrated Circuit Card) as shown in Figure 2. The UICC is a smart card, issued by an operator, and runs the application USIM (Universal Subscriber Identity Module). USIM contains the IMSI (International Mobile Subscriber Identity), which is an identifier used to identify the Subscriber.

A USIM can only contain one IMSI, but UICC may contain multiple USIM – each with different IMSIs [6]. USIM also contains a security key, LTE K, which is used for authentication as described in section III.

A Mobile Equipment (ME) is uniquely identified by the identifier IMEI (International Mobile Equipment Identity). Whereas the IMSI is changed when the subscriber signs up with another operator; the IMEI identifier is inextricably linked to the equipment. Amongst other it is used to check if the device is stolen.

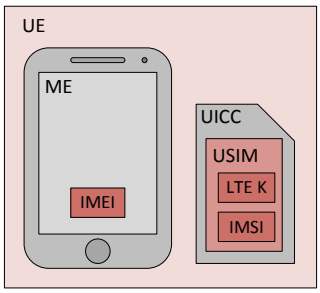

Figure 2. User Equipment (UE)

D. Roaming

Roaming is when a user associated with a specific mobile network operator uses a mobile network associated with another operator, usually because he stays outside of his operator's geographic coverage area. It is possible to have both national and international roaming.

A roaming user will always use the HSS of the home network, while E-UTRAN, MME and S-GW will always be in the visited/local network. P-GW can be in the home network or the visited network. Communication over the Internet usually goes via the P-GW in the home network using the S8-interface (see Figure 1). Voice communication on the other

hand, will usually go via P-GW in the visited network using the S5 interface. The benefits of this are that the user can make a local call without the need to go through the home network and emergency calls will be handled locally. HSS will indicate if the home network will allow the use of a local P-GW.

III. LTE Security

Security in LTE includes security over the radio interface, as well as protection within the EPS. The big picture is that the control traffic between the user device and the LTE network will be integrity-protected, but not necessarily encrypted. User traffic can be encrypted, but will not be integrity-protected. Control traffic between different operators in the core network is integrity-protected, but within an operator's network neither integrity nor confidentiality protection are mandatory. Integrity and confidentiality protection of the user traffic in the core network are not specified.

Security over the radio interface is outlined in Figure 3, and consists of three main parts:

- *LTE-authentication*: mutual authentication between the UE (USIM) and the network. The procedure that is used for this takes place between the MME and USIM in the UE. Security is based on the symmetric key, *LTE K*, which is located in the user's USIM and the HSS. It is never exposed to other devices in the LTE infrastructure. MME therefore depends on HSS to authenticate the USIM. From LTE K a new key - K_{ASME} - is derived—which in turn is used to derive new keys for protection of user payload and control traffic. In contrast to LTE K, K_{ASME} and other keys are stored in ME outside the USIM.
- *NAS Security* (Non-Access Stratum): protection of control traffic between the UE and MME, based on the K_{ASME} key. This consists of mandatory integrity protection and optional encryption.
- *AS security* (Access Stratum): protection of control and user traffic between UE and eNB. This includes mandatory integrity protection and optional encryption of the RRC-signaling (Radio Resource Control) plus optional encryption of the user traffic. Integrity protection is not offered for the user payload. The keys used for AS-security is derived from the key K_{eNB} which is a derivative of the K_{ASME}-key.

In the core network and the X2- and S1- interfaces, it is the operator's responsibility to protect the control- and user traffic, except control traffic between different security domains. It is mandatory to integrity protect this control traffic with IPsec [2]. A security domain is defined as a network managed by the same authority, and operating on the same level of security in the case where there is more than one level. A security domain is usually equal to an operator's EPC, but in some cases, an operator may have multiple security domains.

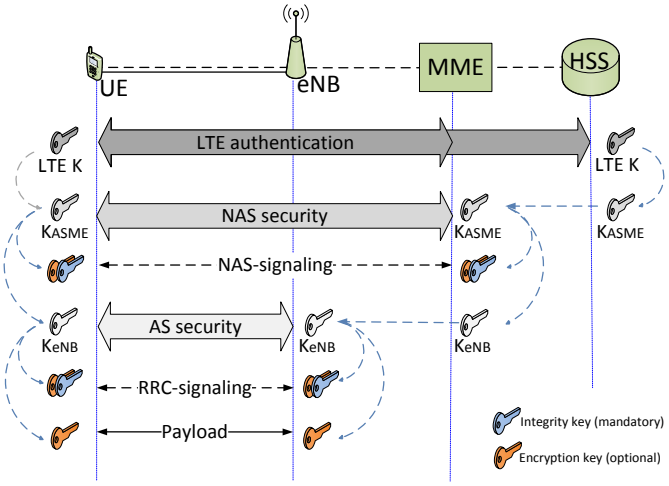

Figure 3. Overview of crypto keys and security between the user equipment (UE) and the LTE network (EPS)

IV. Assets

The following assets need protection: user payload, metadata and network availability.

User payload is here defined as any payload – including voice - that the end user either generates or consumes. User payload must be protected from unauthorized access and modification. Confidentiality and integrity protection of the user payload is important.

Metadata refers to information about where the user is, who he is, who he is talking to as well as communication patterns.

Network availability includes the availability of network components and network management traffic that is exchanged in order to keep the network service running. It requires high uptime and protection against unauthorized modifications of the network. Network availability must be maintained regardless of actual user payload on the network.

V. Threats and Attack Vectors

Attacks can be launched directly against the user device, the radio interface between the user device and base station, the LTE infrastructure, or via other connected networks.

A. User Equipment

Malicious software can be installed on the user device during the production or later by someone who have physical access to the user device. The device may also be infected through applications or other software received and installed via a network connection. It may come as an attachment, downloadable application or other. This is difficult to control and prevent. In addition, the USIM can be compromised.

These threats can potentially threaten all three assets. The malicious software can, for example, block the user device or contribute to DOS attacks (Denial of Service) on the infrastructure components so that also the network availability is threatened. It can also threaten the confidentiality and integrity of both user payload and metadata.

There is a vast amount of LTE user devices on the market

from a multitude of different vendors. It is hard to have confidence in all these terminals. One possibility is to find one or a few user devices that are trusted and allowed.

The user device can be a dedicated device owned by the armed forces handed out to the individual, and that is not used privately. There can also be restrictions on what applications are allowed to be downloaded. This way it will be possible to have some control with the user device. Another option is a bring-your-own-device solution where the users' own devices are used for both private purposes and military use. This solution makes it harder to have confidence in the user device. It is also possible to choose an intermediate solution where a dedicated phone is handed out and where the device can be used also for private purposes. Further details about vulnerabilities in the user device can be found in [8] and [10].

B. Radio interface

The radio interface can be exposed to both intelligent and unintelligent jamming. Many articles describe how to jam LTE [4][5][6]. Jamming equipment is cheap and easily available over the Internet [7]. Among other things, it is easy to disturb the synchronization signaling between the user device and the base station, and interfering with this makes it impossible to send data. Communication can also be blocked due to inadvertent interference with other systems such as Digital TV and S-band radar used in air traffic control [4]. Jamming and interference threatens first and foremost network availability.

The operator can choose not to encrypt traffic over the radio interface. This leaves the user payload more prone to attacks.

A fake base station can potentially threaten all of the assets. This attack is more difficult with LTE than by previous generations of mobile telephony, as LTE includes authentication of the base station. It may be easier to use a simple form of IMSI-catcher to get access to the IMSIs of the users in the area. Request and response messages regarding IMSI are unencrypted.

C. Access Network and Core Network

Interruption of the eNB, the MME, the S-GW or the P-GW logically or physically –intentionally or accidentally – threatens the availability of the network. The MME holds metadata such as IMSI, IMEI, geographical position, and encryption keys. Similarly, the eNB, S-GW and P-GW have access to the user traffic. Physical or logical access to the infrastructure components thus represents a threat to all of the assets.

HeNBs (Home eNB) and WiFi networks are cheap and easy to set up, and can be used to access internals of the LTE network. They can be exploited by attackers as a gateway to the LTE network. Altogether, there are more possible attack points in an LTE network than what was the case with previous generations of mobile telephony, and many of these points of attacks have limited physical protection.

D. Other Networks

Older mobile telephone systems with circuit-switched networks and limited data capacity were easier to control by the operators. They had simpler signaling and fewer connections to the outside world. In the all-IP LTE network with seamless roaming, the operators share the same threats since their respective infrastructures and services are linked to one aggregated service network. Such distributed networks and open architectures are prone to attacks. Vulnerabilities in a device or one interface can be exploited as a gateway for attackers who wish to compromise the entire LTE network. This is a threat to all three assets.

VI. BUSINESS MODELS

A mobile network operator does not necessarily own and operate the whole network. Different business models that include collaboration with more actors are common.

A. Mobile network operator (MNO)

A common definition of a mobile network operator (MNO) is that the operator has a license for the use of the appropriate radio frequencies as well as the necessary infrastructure to provide services to their subscribers over these frequencies. A MNO also typically holds the other elements that are necessary to provide the services to the end user, such as customer care, billing and marketing. In addition, an MNO may sell access to network services to mobile virtual network operators (MVNO).

Operating as an MNO, the armed forces would have control over the infrastructure and its localization. National borders put geographical limits for the development of coverage areas.

B. Mobile virtual network operator (MVNO)

A mobile virtual network operator (MVNO) is a service provider that neither has a license on the appropriate radio frequencies nor owns its own base station infrastructure.

There are many flavors of MVNOs. The simplest business model is the one where the MVNO is just a brand name. These companies have low investment costs and will in short time be able to be in operation. The most advanced MVNO operators possess all the functions necessary to deliver services in the mobile network apart from the physical network infrastructure and license to radio frequencies. Many virtual network operators produce their own UICC's.

C. Business models studied here

Four different business models are studied in the following: The armed forces as 1) MNO, 2) MVNO with control over the USIM and entire EPC, 3) MVNO with control over USIM and HSS and 4) Customer of a MNO.

VII. VULNERABILITIES OF DIFFERENT BUSINESS MODELS

Vulnerabilities of different business models are in the following related to the components of the LTE network and whether the armed forces will have control over the component or not with the given business model. Control here

refers to that the component is acquired, used and operated by the armed forces or others with similar trust.

Ideally, you should also have control with the production. We have chosen not to take this into consideration, as some of the idea with using LTE in the armed forces is to be able to use commercial off-the-shelf. One should nevertheless be aware that commercial off-the-shelf can contain inline vulnerabilities that will be able to pose a threat.

The article relies on a trust model that distinguishes between two main categories of actors: "Trusted" and "Non-trusted." The first group includes the military's own personnel, as well as other actors with national security clearance and the necessary authorizations. It includes both legitimate users and administrators of the system. The second group covers external actors who are not trusted or authorized. The assumption is that this last group can include actors who may not act friendly in all situations, and who thus may threaten one or more of the assets. It is possible to define several sub-categories with varying degree of trust within both main categories. However, the simple trust model with two categories has been considered sufficient for giving an overview highlighting the generic vulnerabilities in LTE.

Threats with different business models are visualized with a color-coding of the affected infrastructure components. Green indicates that the component is in control of the armed forces. Yellow indicates partial control. Red means that this component is outside the armed forces control.

Likewise, the asset symbols are colored green if the asset is protected as the armed forces are in control of the components that affects this asset. Yellow indicates partially protected and red means that the asset is threatened.

The models use only three colors to indicate the control and the vulnerability level. This is done to bring out the big picture and to give an overall overview of the differences and the similarities between business models. The downside is that it may conceal some finer distinctions.

The article assumes that commercial user equipment and infrastructure components are used, and the assessment of vulnerability assumes that one can rely on such equipment. This is probably a strong simplification as shown in section V. Without confidence in the infrastructure components and user equipment, all assets in all business models would be threatened, and it would be harder to illustrate the differences between the business models.

A. Armed forces as an MNO

With this business model the military forces is the operator of the network, and control all parts of the infrastructure, even during the acquisition. There are no other MNOs or MVNOs involved in the network. This is illustrated in Figure 4. All components of E-UTRAN and EPC are under the control of the armed forces or other personnel with corresponding trust and are thus colored green. It is assumed that ME is a dedicated unit owned by the armed forces, and only for military use. It is therefore green. It is also assumed that the USIM is issued by the armed forces.

Figure 4 shows two cases. The first have no link to the Internet or roaming agreements with other operators, only an intranet under the control of the armed forces. The second case includes Internet connections and roaming with other operators.

In the first case you are left with the intrinsic vulnerabilities of LTE such as bad jamming resistance and vulnerabilities associated with the use of an infrastructure-based communication technology. This business model provides good control of user payload and metadata. The network availability is as good as it can be with commercial LTE technology. The assets are therefore colored green in the upper case in Figure 4.

Roaming and connection to the Internet introduce vulnerabilities. The control is still good within the armed forces' network, although not as good as in the first case. If a user on the other hand is roaming, the control of all the assets is lost because the communication goes through infrastructure components in the visited network. This can be compared with the business model where one neither has control of the eNB nor EPC. The assets at the bottom of Figure 4 are therefore colored yellow.

In international operations or exercises abroad, the armed forces must either bring their own mobile eNBs or use a local operator in the operation area. In principle, the armed forces can still use their own EPC. Abroad the armed forces can either replace their national USIMs with local USIMs, or establish roaming agreements with local operators in the same way as other commercial operators do. The vulnerabilities are then similar to those in the business model where the armed forces are an MVNO that controls the USIM and HSS.

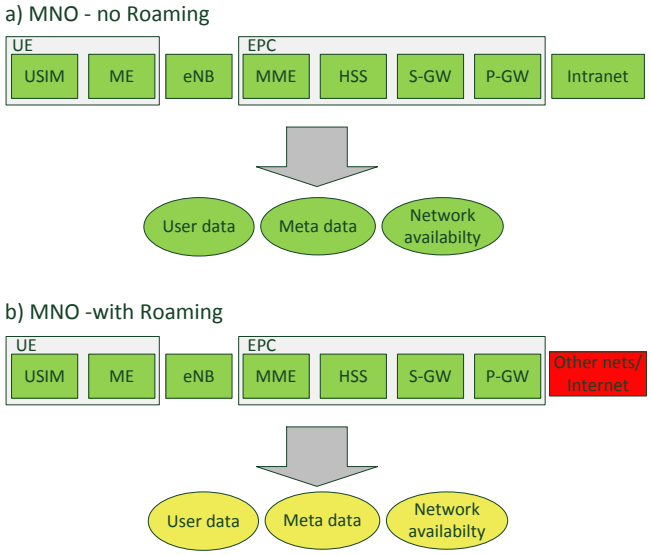

Figure 4. Armed forces as an MNO: a) with no roaming or Internet link, b) with roaming and Internet link

B. Armed forces as an MVNO with control of the USIM and the entire EPC

In this business model the armed forces operate and control

all components apart from the eNBs, and do not have their own frequencies. The eNBs and frequencies are provided by a commercial mobile operator. See illustration in Figure 5.

The eNB is here red. Internet connection and roaming are also assumed. The user device is in yellow. It is assumed that the user devices are provided by the armed forces, but can also be used for private purposes. The armed forces have therefore only partial control over the devices.

In addition to the vulnerabilities discussed in the previous business model, new vulnerabilities are introduced as a result of not having control over the base stations. This makes it harder to protect network availability. Anyone who controls the base station is able to prevent network access. Furthermore, encryption of traffic from the user device is terminated in the base stations. The user payload can therefore be read, changed, or stopped. The base station may also introduce false data without being detected. Whereas much of the signaling traffic between the UE and the MME is encrypted, the base station will at least have some metadata such as the approximate location of the user. The user device is colored yellow as the armed forces have limited control over the device. This means that all the assets could potentially be threatened.

With these vulnerabilities both user payload and network availability become red and metadata yellow as shown in Figure 5.

For operations abroad it may – depending on scenario – be possible to establish an MVNO agreement that enables use of other operators' eNBs, but own EPC. A simpler solution is a roaming agreement. Another alternative is replacing the USIM with a local one.

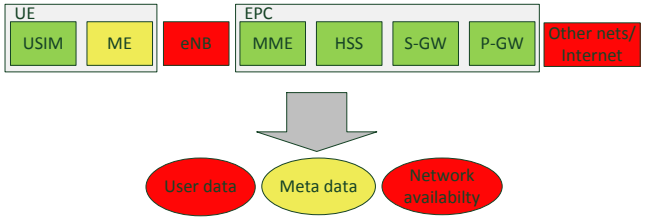

Figure 5. Armed forces as an MVNO that controls USIM and EPC

C. *Armed forces as an MVNO with control of the USIM and HSS*

With this business model the armed forces operate as a MVNO that rely on a commercial operator to provide everything apart from the HSS and the USIM. In this way, the armed forces control all LTE K keys, even if most of the infrastructure is provided and controlled by another party. This business model is illustrated in Figure 6. Only the USIM and the HSS are green. It is here assumed in the same way as in the previous model that the user device is a dedicated unit provided by the armed forces, and the user device is also used for private purposes. It is therefore yellow.

This business model has all the vulnerabilities from the previous model. In addition, the armed forces will lose control over the metadata as the MME is a component outside of the armed forces control. Although the armed forces has control of the LTE K key, they will not have control on the derived keys used to protect user traffic and control traffic. They will also lose control of the infrastructure components where this traffic is sent in plaintext. Both the assets user payload and metadata are therefore colored red.

Relying on an external party to provide the entire infrastructure except for the HSS, increases the vulnerability associated with the network availability. As control of many of the critical nodes in the network is missing, the availability will be more vulnerable here than with the previous business models. Network availability is therefore red in this model.

Roaming has little additional impact on the vulnerability.

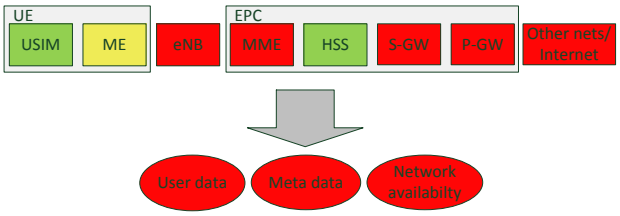

Figure 6. Armed forces as an MVNO that controls USIM and HSS

D. *Armed forces as costumer of a commercial MNO*

Everything is here outsourced to a commercial mobile operator.

This business model inherits all the vulnerabilities discussed in the previous business model. In addition, the control over the LTE K key is lost. If the LTE K is distributed to any unauthorized party it may be exploited both for passive eavesdropping as well as spoofing.

This business model is illustrated in Figure 7. We have here assumed a bring-your-own-device solution where the armed forces have even less control over the user devices than in the previous models. It would not make any significant difference for the assessment if a dedicated user device had been used instead. All central components in the network are red with this business model.

All assets were considered threatened and colored red in the previous business model. All assets are therefore red also here.

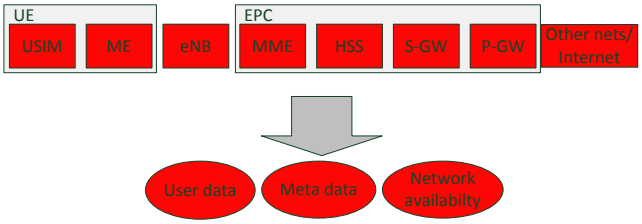

Figure 7. Armed forces as a costumer of a commercial MNO

E. *Discussion*

The previous subsections show - not unexpectedly - that the armed forces as an MNO with no roaming business model provides the lowest vulnerability. However, this is probably an unrealistic model as the investment cost for a nationwide LTE network is extensive. The procurement of frequencies

that alternatively would have been sold to commercial operators comes in addition. Using frequencies that are not in the LTE standard is not considered here, since both the base stations and user devices must be adapted, and most of the economic gains of using commercial technology would disappear. Furthermore, a system without roaming or link to the Internet will probably not give the end-users the expected service. A more realistic business model is the one where the armed forces use mobile eNBs to provide coverage in a specific area in a tactical operation. The challenges here will probably be access to frequencies and possible interference with other players operating in the same area using the same frequency range.

This review furthermore shows that control over the eNBs plays an important role. It is first and foremost the network availability asset that is threatened. Confidentiality of the user payload will also be threatened, since the encryption is terminated in the base station. Some information about users will also be available, as the eNB will have an overview of the approximate geographical position of users and who they communicate with.

As a non-commercial actor, the armed forces operating as MVNO will probably be able to establish roaming agreements with multiple commercial operators operating in the same area, as the armed forces do not act as a competitor. This may give increased coverage and robustness compared to what a commercial actor would be able to achieve.

The differences between the last two business models where the armed forces are either an MVNO with control over USIM and HSS or an ordinary customer of a commercial operator, are not so big. An external party has in either case access to both metadata and user payload since they control the infrastructure components. An important observation is that the same applies for all business models when users are roaming. The roaming users are connected to infrastructure components that the armed forces have no control over.

VIII. Related work

In [9], J. Cao & al. provide a comprehensive survey of security aspects of LTE and LTE-Advanced. The article gives an overview of security features of these standards, and elaborates on the vulnerabilities. The article also reviews existing solutions to these problems and outlines topics for further study. Differently from this work, J. Cao & al. does not address military use of LTE in particular, and they do not consider different business models.

Reference [11] describes security and privacy architecture between existing and next generation public protection and disaster relief (PPDR) networks from the European seventh framework programme project SALUS. The report elaborates on components and interfaces and discusses possible roadmaps for the evolution of PPDR networks. The roadmaps resemble the business models discussed in this article. One roadmap is legacy PPDR networks connected a commercial LTE operator using dedicated terminals. Another roadmap is the PPDR operating as an MVNO, and the last one is the PPDR organization operating as an MNO. The first roadmap is applicable for non-mission critical data. Mission critical services over LTE are included in the last roadmap. The evaluation criteria encompass who controls the authentication procedures, the LTE network, and QoS assurance. Metadata is not considered.

IX. Concluding remarks and further work

A final assessment will have to include the intended use of LTE in the Armed Forces. The benefits of using LTE must outweigh the vulnerabilities it introduces.

The inherent vulnerabilities of LTE such as low jamming resistance and dependency upon infrastructure apply to all business models. There are also additional external vulnerabilities. As an example, the LTE network will be vulnerable to attack that affects the power grid. Another observation is that LTE does not offer integrity protection of user payload at all.

The work has revealed several areas for further studies. One is applications for LTE in the military context. Infrastructure based systems such as LTE is more vulnerable than traditional autonomous military radio systems. This may have a bearing on where and how the military should use LTE. Another natural topic for further studies is how the different assets can be better secured.

3GPPs standardization of device-to-device functionality makes LTE less dependent on infrastructure components over a short distance. Custom military LTE-infrastructure components are also emerging on the market, and maybe some of these will have better built-in security. The drawback is that this can be more expensive than the purely civilian equipment.

For securing user payload it may be appropriate to use end-to-end application-layer encryption such as with SCIP (Secure Communication Interoperability Protocol). The use of commercial user equipment for classified information and how security can be hardened is another objective that needs further investigation. This applies regardless of the business model.

To what extent metadata can be hidden from unauthorized entities will largely depend on the chosen business model. A possibility might be to use many IMSIs for each user. How effective this is depends amongst other things on what components of the infrastructure the armed forces have control over.

There are several ways to enhance network availability with each of the business models. One possibility is to establish agreements with several independent operators, add stronger security requirements to the infrastructure components and software in the core network, own mobile base stations-with or without built-in EPC, more advanced network monitoring, and better protection of the power grid. It is also important to provide a good overview of the vulnerabilities and attack vectors within the E-UTRAN access network and the EPC

core network to find ways to improve availability.

The effect of these measures must be analyzed in more detail, and the costs have to be weighed against the benefits. For example, introducing mobile base stations will only help on availability in a limited geographical area. Likewise, end-to-end encryption of user payload still provides opportunities for traffic analysis since the address information will be sent in plaintext.

To summarize; each business model studied here has its pro's and con's. Control over the eNBs has a large impact on the vulnerability. How LTE shall be used needs to be clarified in order to choose the best business model. Hopefully this article can serve as a framework for further discussions on security and vulnerabilities related to the use of LTE within the armed forces.

REFERENCES

[1] Universal Mobile Telecommunications System (UMTS); LTE; Proximity-based Services (ProSe); Security aspects, 3GPP TS 33.303 version 13.2.0 Release 13, ETSI TS 133 303, Jan, 2016.

[2] S. Kent and K. Seo, Security Architecture for the Internet Protocol, RFC 4301, IETF, December 2005.

[3] Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Network Domain Security (NDS)M IP network layer security, 3GPP TD 33.210 version 12.2.0 Release 12, ETSI TS 133 210 V12.2.0 (214-10).

[4] N. Mahmud, Vulnerabilities of LTE and LTE-Advanced Communication, White Paper, Rohde & Schwarz, 2014.

[5] M. Lichtman, J. H. Reed, T.C. Clancy, and M. Norton, Vulnerability of LTE to Hostile Interference, IEEE Global Conference on Signals and Information Processing (GlobalSIP), 2013.

[6] R. P. Jover, J. Lackey, and A. Raghavan, Enhancing the security of LTE networks against jamming attacks, EURASIP Journal on Information Security, Springer, 2014.

[7] Jammerfromchina Co,Ltd, 4G Cell Phone Jammer Wholesales, available URL:http://www.jammerfromchina.com/categories/4G%7B47%7DLoJack%7B47%7DXM_Jammers/

[8] F. Mancini, Modern mobile platforms from a security perspective, FFI-rapport 16/00319, 2016.

[9] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, A Survey of Security Aspects for LTE and LTE-A Networks, IEEE Communications Surveys & Tutorials, Vol.16, No. 1, First Quarter, 2014, pp. 283-302.

[10] B. Michau, and C. Devine, How to not break LTE crypto, SSTIC 2016.

[11] Deliverable 5.2, PPDR Security Architecture, end-to-end security, privacy mechanisms and intrusion detection approach – Intermediate, SALU, EU seventh framework programme, project number: 313296, Version 1.3, Jan 2015.