TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Haldo-Rait Harro 192539

Displaying Electronic Warfare Situation Awareness in Estonian Defence Forces

Master's thesis

Supervisor: Toomas Ruuben
Ph.D.

Tallinn 2021

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Haldo-Rait Harro

03.05.2021

Abstract

Electronic Warfare is a force multiplier that can enable asymmetric effects on the battlefield and in operations other than combat. In Electronic Warfare, technical assets are deployed to support achieving tactical, operational or even strategic goals. However, the people directing the military efforts usually do not possess engineering background. A risk of disconnect between the commanders responsible for achieving goals and Electronic Warfare specialists who operate and develop the capabilities exists.

In this thesis, Situation Awareness as a cognitive state was linked to Electronic Warfare as mastery over the electromagnetic spectrum through the concept of Data Fusion. Market research showed only a few available products designed to support Situation Awareness for the electromagnetic spectrum. These products seem to be mostly intended for Electronic Warfare experts and, without intuitive user interfaces are not suitable for supporting a tactical commander's ability to project future events.

The results of this thesis show a clear path towards improving displaying Electronic Warfare Situation Awareness in Estonian Defence Forces. Specific requirements were set for a missing feature as input for Estonian Defence Forces Situation and Battle Awareness System microservice development. Two mock-ups of value-added products were also prepared to visualize, what the service should be capable of.

This thesis is written in English and is 67 pages long, including 5 chapters, 19 figures and 18 tables.

Annotatsioon

Elektroonilisesõjapidamise olukorrateadlikkuse kuvamine Eesti kaitseväes

Elektrooniline sõjapidamine on jõukordistaja, mis võimaldab lahinguväljal ja lahinguvälistes operatsioonides saavutada asümmeetrilisi efekte. Suhteliselt väike üksus, mis kasutab elektroonilist sõjategevust, suudab saavutada ebaproportsionaalselt suuri tagajärgi juhtimise, luure, tulejõu ja väekaitse funktsioonides. Elektronilises sõjas kasutatakse taktikaliste, operatiivsete või isegi strateegiliste eesmärkide saavutamise toetamiseks tehnilisi vahendeid. Tavaliselt puudub sõjalisi operatsioone juhtivatel ohvitseridel inseneri haridus. Seetõttu eksisteerib oht, et eesmärkide saavutamise eest vastutavate ülemate ja võimete arendamisega tegelevate elektroonilise sõjapidamise spetsialistide vahel tekivad ebakõlad.

Selles lõputöös seostatakse olukorra teadlikkus kui kognitiivne seisund elektroonilise sõjapidamise kui elektromagnetilise spektri haldamine andmeühenduse mõiste kaudu. Luubi alla võeti olukorra teadlikkuse suurendamine elektroonilise sõja valdkonnas. Turu-uuringud näitasid vaid mõnda kättesaadavat toodet, mis on mõeldud elektromagnetilise spektri olukorra teadlikkuse toetamiseks. Näib, et need tooted on peamiselt mõeldud elektroonilise sõja ekspertidele ja ilma intuitiivse kasutajaliideseta ei sobi need toetama taktikalise ülema võimet tulevasi sündmusi ette näha.

Töö käigus tuvastati Eesti kaitseväelas üheksa kriitilist probleemi. Nende võimelünkade tähtsuse järjekorda seadmiseks viidi valitud tegevväelaste seas läbi küsitlus. Küsitluse tulemuste põhjal valiti edasiseks uurimiseks seadmete mõjualade kuvamise küsimus.

Selle lõputöö tulemused näitavad selget teed elektroonilise sõjaolukorra teadlikkuse tõstmiseks Eesti kaitseväes. Ühe puuduva funktsionaalsuse kohta esitati konkreetsed nõuded Eesti kaitseväe olukorra ja lahinguteadlikkuse süsteemi mikroteenuse arendamiseks. Koostati ka kaks lisaväärtusega toodete maketti, et visualiseerida, milleks teenus peaks olema võimeline.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 67 leheküljel, 5 peatükki, 19 joonist, 18 tabelit.

List of abbreviations and terms

No	Abbreviation	Meaning
1.	ADV	Adversary
2.	COP	Common Operational Picture
3.	CtQ	Critical-to-Quality
4.	DFSS	Design for Six Sigma
5.	DL	Design limitations
6.	DoS	Denial-of-Service
7.	EDF	Estonian Defence Forces
8.	EM	Electromagnetic
9.	EMS	Electromagnetic spectrum
10.	EW	Electronic Warfare
11.	HF	High Frequency
12.	HMI	Human-Machine Interface
13.	IDDOV	Identify, Define, Develop, Optimize, Verify
14.	ISTAR	Intelligence, Surveillance, Target Acquisition, and Reconnaissance
15.	LOS	Line-of-sight
16.	MANET	Mobile ad hoc Network
17.	NATO	North Atlantic Treaty Organization
18.	OE	operational environment
19.	OODA	Observe – Orient – Decide – Act
20.	RF	Radio Frequency
21.	SA	Situation awareness
22.	SRTM	Space Shuttle Radar Terrain Mapping Mission
23.	SWOT	Strengths, weaknesses, opportunities and threats
24.	TOC	Tactical Operations Centre
25.	UAV	Unmanned Aerial Vehicle
26.	VoC	Voice of the Customer
27.	VoP	Voice of the Process
28.	VoE	Voice of the Experts

Table of contents

1 Introduction 11
2 State of the art 12
2.1 Situation Awareness 13
2.1.1 Interface design and system compatibility 15
2.1.2 Complexity and automation 16
2.1.3 Abilities, experience and training 16
2.1.4 Goals, objectives and preconceptions 16
2.1.5 Situation Awareness in EDF 17
2.2 Data Fusion 18
2.2.1 Common Operational Picture (COP) 21
2.3 Electronic Warfare (EW) 25
2.3.1 Symbology 27
2.3.2 Jamming 28
2.3.3 Direction finding and geolocation 29
2.3.4 Emissions and communications analysis 30
2.3.5 Electromagnetic wave propagation models 30
2.3.6 EM wave properties 31
2.3.7 EM wave propagation models 32
2.3.8 Electronic Warfare in EDF 33
3 Gap of knowledge 36
3.1 Situation Awareness 36
3.2 Data Fusion 36
3.3 Electronic Warfare 37
3.4 Research question 37
4 Methods 38
4.1 Identify 38
4.2 Define and develop 39
5 Results and discussion 41

5.1 Identify 41
5.1.1 Voice of the Process 41
5.1.2 Design Limitations 43
5.1.3 Voice of the Experts 44
5.1.4 Voice of the Customers 47
5.1.5 Summary of Identify phase 55
5.2 Define and develop 56
5.2.1 Conclusions of problem analysis 56
5.2.2 Critical to Quality metrics 56
5.2.3 Goal statement 58
5.2.4 Develop 58
6 Summary 63
Bibliography 65
Appendix 1 - Non-exclusive licence for reproduction and publication of a graduation thesis 1
Appendix 2 – Questionnaire for the survey 2
Appendix 3 – Expert's statements affinity diagram 5

List of figures

Figure 1. Breakdown of the thesis concept. 12
Figure 2. Model of situation awareness in dynamic decision making [3] and OODA loop [6]. . 14
Figure 3. Framework for enhancing Situation Awareness with Data Fusion. [12] 18
Figure 4. User Experience Honeycomb. [15] 20
Figure 5. A TacELINT value-added product. [20] 23
Figure 6. mySPECTRA task-specific modules. [21] 24
Figure 7. Cyber Electromagnetic Activities. [25] 26
Figure 8. The relationship among the five domains and the electromagnetic spectrum. [25] 26
Figure 9. Generic EW intelligence process in EDF 42
Figure 10. Affinity diagram that produced the Area of Effect overlay focus area, input from expert A (left, black) and expert B (right, dark grey). 44
Figure 11. Affinity diagram that produced the network mapping and health monitoring focus area, input from expert B (left, dark grey) and expert C (right, grey). 45
Figure 12. Affinity diagram that produced the value-added products focus area, input from expert B (left, dark grey) and expert C (right, grey). 45
Figure 13. Affinity diagram that produced the COP system linked databases focus area, input from expert B. 46
Figure 14. Affinity diagram that produced regulations and processes focus area, input from expert C (left, grey) and expert D (right, light grey). 46
Figure 15. Response rate comparison between warfighting domains. 48
Figure 16. Response rate comparison between signals and operations specialists. 48
Figure 17. Percentage of responders who use CEMA related terms daily by group (grey), overall average of responders who use the terms daily (black) and the overall average of responders who never use a term (red). 49
Figure 18. Mock-up of Area of Effect value-added product for a case of jamming 59
Figure 19. Mock-up of an Area of Effect visualization value-added product for a case of direction finding. 60
Figure 20. Representation of the measurements taken in two directions at 10 m intervals from the transmitter. 61

List of tables

Table 1. Definitions of terms..... 13
Table 2. All symbols directly related to EW in NATO Joint Military Symbology APP-6(D) 2017..... 27
Table 3. Jammers can be divided by operating time, frequency or location. [26] [27] 29
Table 4. Empirical EM wave propagation models. [28] 33
Table 5. Criteria for selecting possible EW capabilities [33] 34
Table 6. SWOT analysis of the generic EW intelligence process..... 43
Table 7. reported use-rate of EW related terminology on the job..... 49
Table 8. Sizes and weights assigned to the for groups..... 50
Table 9. Answers to “How satisfied are you with SA regarding processing intelligence information”..... 51
Table 10. Satisfaction with symbology in CEMA domain 51
Table 11. Answers to statement “My work would be easier if there was more detailed documentation for CEMA”..... 52
Table 12. Answers to the question “How satisfied are you with currently available tools to visualize EM activities?”. 52
Table 13. Answers to the question “How satisfied are you with currently available tools to visualize Cyber activities?”..... 52
Table 14. Relative interest ratings group averages, overall average and weighted average 54
Table 15. Results of prioritization by the survey participants with group averages, overall average and weighted average. 55
Table 16. Comparison of rankings of outstanding use-cases based on relative interest and prioritization..... 56
Table 17. System requirements Critical to Quality for KOLT micro service 57
Table 18. Comparison of measured and theoretical changes in values for a jamming signal at 446.19 MHz. 62

1 Introduction

Electronic Warfare is a force multiplier that can enable asymmetric effects on the battlefield and in operations other than combat. A relatively small unit utilizing Electronic Warfare can realize disproportionately large effects in command, intelligence, fires and force protection functions. In Electronic Warfare, technical assets are deployed to support achieving tactical, operational or even strategic goals. However, the people directing the military efforts usually do not possess engineering background. A risk of disconnect between the commanders responsible for achieving goals and Electronic Warfare specialists who operate and develop the capabilities exists.

Academic research of Electronic Warfare in Estonia has mostly focused on specific capabilities, including aerial surveillance radars, jamming protection and electromagnetic signatures of military objects. Electronic Warfare assets in Estonia are almost exclusively deployed by Intelligence Centre, although our neighbouring nations have integrated such capabilities in all tactical level units. Military commanders on all levels could benefit from increased understanding of what is happening on the electromagnetic spectrum. Understanding comes from what is known as Situation Awareness. The question thus becomes, how to rise commanders' Situation Awareness of Electronic Warfare.

This thesis set out to provide an input to develop an Electronic Warfare display for Estonia's Defence Forces Situation and Battle Awareness system KOLT. In order to achieve this, gaps in Defence Forces Electronic Warfare Situation Awareness capabilities were highlighted and criteria and priorities for future development was described. Cyber security for proposed solution is not considered. These goals were supported by a scholarship from the Ministry of Defence of Estonia.

In this thesis, a state-of-the-art review is presented, giving an overview of three topics: Situation Awareness, Data Fusion and Electronic Warfare. Secondly, results from interviews with the experts in Electronic Warfare and Situation Awareness Systems in Estonian Defence Forces are presented on affinity diagrams. Thirdly, priorities for solving systematic problems are shown, based on a survey conducted on a sample of Estonian Defence Forces active-duty service members from operations or signals backgrounds. Finally, the requirements to solve one of the highest priority issues are defined and a mock-up of what a solution could look like is produced.

2 State of the art

In order to investigate the state of the art for Displaying Electronic Warfare (EW) Situation Awareness (SA) in Estonian Defence Forces (EDF) a thorough breakdown of the concept was necessary. This breakdown structure is illustrated in Figure 1, showing the order of chapters covering each element of the subject.

We firstly examine separately what is the scientific understanding of Situation Awareness in general and in Estonian Defence Forces. We then focus on how Data Fusion enables displaying Situation Awareness for creating a Common Operational Picture. Finally, we inspect the state of the art for Electronic Warfare in the world and in EDF.

Figure 1. Breakdown of the thesis concept.

In a cross-functional discourse the terminology and abbreviations can be easily mixed up. In the next section we will discuss concepts that are overlapping, but with significant differences in who are the main drivers of development in those areas. These concepts are Situation Awareness, Data Fusion and Common Operational Picture and their definitions that are used in this work are described in Table 1. To summarize, **Common Operational Picture** is displayed using **Data Fusion** Systems in order to create **Situation Awareness**. SA is the goal, COP and DF are tools to achieve it.

Table 1. Definitions of terms.

Common Operational Picture (COP)	**Data Fusion (DF)**	**Situation Awareness (SA)**
Visual representation of tactical, operational, and strategic information to support rapid assimilation and integration by team members. [1]	Utilising one or more **data sources** over time to assemble a **representation** of aspects of interest in an environment. [2]	**Perception** of the elements in the environment within a volume of time and space, the **comprehension** of their meaning and **projection** of their status in the near future. [3]

2.1 Situation Awareness

Situation Awareness (SA) was recognized as a crucial commodity for crews of military aircraft as far back as World War I. Direct research on SA itself is limited and has been conducted only as recently as 1990-s. [3]

Several definitions have been proposed for Situation Awareness, in this thesis the definition proposed by Mica Endsley, Former Chief Scientist of the U.S. Air Force will be used.

> *"Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future."* – Mica Endsley

Situation Awareness will be considered as a state of knowledge pertaining to the state of a specific dynamic environment. While the achievement, acquisition or maintenance of SA will be described as **situation assessment**. [3]

Firefighters, certain police units and military command personnel rely on SA to make their decisions. They must ascertain the critical features in widely varying situations to determine the best course of action. Inaccurate or incomplete SA in their environments can lead to devastating loss of life. In each of the domains described, operators must understand the integrated meaning of what they are perceiving in light of their goals. SA, as such, incorporates an operator's understanding of the situation as a whole, forming a basis for decision making. [3]

"Situation Awareness has been recognized as one of the important, yet unsolved, issues in many different domains, including human controlled and -monitored mobile communication networks, social networks, physical and cybersecurity systems, disaster monitoring and recovery, epidemic monitoring and control, intelligent transportation systems, financial and investment services, and tactical and operational battlefield command and control." [4]

Figure 2 shows how SA is tied to the general decision-making process of an individual and to the Orient-Observe-Decide-Act (OODA) loop, that is widely used in military education. [5] Several individual and system factors are shown to affect the forming of situation awareness. SA is built up from level 1 to level 3 during situation assessment. [3] Decision making is possible without attaining Situation Awareness just as walking in the dark is possible, without knowing where on is going.

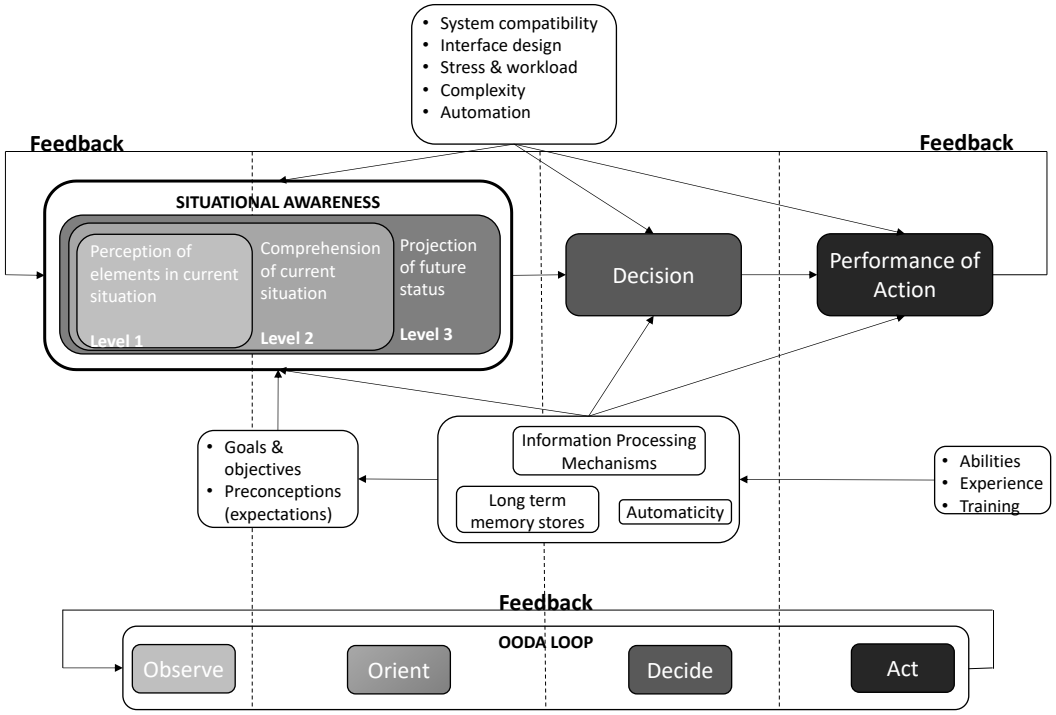


Figure 2. Model of situation awareness in dynamic decision making [3] and OODA loop [6].

SA is therefore based on perceiving information, comprehending the meaning of that information in an integrated form, comparing it with operator goals, and providing projected future states of the environment that are valuable for decision making. [3] The model in Figure 2 is a more fleshed out and detailed description related to Russel John Boyd's famous OODA loop that describes

tactical engagements and means of adjusting strategies in constant coevolution with one's strategic environment. [6] As SA is only one part of the overall decision-making process, it must be stated that good SA can increase the probability of good performance but cannot necessarily guarantee it. SA is significantly related to performance only for those who have the capabilities to take advantage of such knowledge and will not necessarily lead to poor performance if lack of SA is realized and risks are mitigated by corrective actions. [3]

2.1.1 Interface design and system compatibility

An operator's supply of attention is limited. More attention to some elements, resulting in improved SA of these elements may mean a loss of SA on other elements once the limit is reached. An operator's SA is also limited by personal available working memory. [3]

A system cannot possess all information needed for a complete SA because of technical limitations and the system architect's limited understanding of required information. Firstly, all information acquired by the system cannot be displayed for the operator, because limitations of the interface. Secondly, the transmission to the human operator will be inaccurate because perceptual, attentional and working memory constraints. [3] Furthermore, SA is a mental phenomenon, and is understood to be about human minds. SA is not a computer system or a screen display - it is a state of human awareness. [7] Thus, it is also saddled with human constraints. However, advanced knowledge of the characteristics, form and location of information can significantly facilitate the perception of information [3], making interface design a crucial part of an SA system.

Global Situation Awareness should be preferred when designing systems and interfaces. When in conflict with the possibility of information overload, goal orientation and level of processing and integration for level 2 and 3 SA requirements should be weighed. This means that information should not be filtered from human-machine interface (HMI) off hand. Rather, the relation to the operator's goals should be considered first. If possible, the raw information should be processed and integrated to provide level 2 or 3 Situation Awareness. [3]

2.1.2 Complexity and automation

System complexity is hypothesized to negatively affect operator workload and SA, increasing the amount of mental work required to achieve a given level of SA. When demand exceeds a person's capabilities, SA will suffer. [3]

Automatic processes tend to be fast, autonomous, effortless, and unavailable to conscious awareness [8]. With automaticity certain features of cognitive processing occur below conscious awareness. Automaticity could be a mechanism for overcoming human information-processing limitations, however, it creates a risk of reducing responsiveness to new stimuli. While fully automatic systems have been shown to decrease SA, automating unnecessary manual work and data integration may provide benefit to both SA and workload. [3] When introducing automation, tasks that the operator needs to complete for situation assessment should not be automated.

2.1.3 Abilities, experience and training

Experienced operators have mental models built up, with existing scripts for achieving regular goals in familiar situations. Repeated experience in an environment allows one to develop expectations about future events. [3]

It is well known that distress reduces a person's ability to build SA. However, stressors are only detrimental to the extent that they are perceived as dangerous or threatening. Complex tasks with multiple input sources appear to be particularly sensitive to the effects of stressors [3]

Thus, an experienced operator who is not sensitive to regular stressors in their environment and has a good mental model will build SA much easier than a novice.

2.1.4 Goals, objectives and preconceptions

SA is integrally linked with the context and the decisions linked to a person's goals. When scripts are available for executing a selected plan, they will be deployed. Otherwise, actions will have to be devised to allow achievement of goals. [3]

The key to achieving SA is to recognize **critical cues** that map to key features in an individual's preconceived understandings. The classification of information into understood representations forms level 1 SA and provides the basic building blocks for the higher levels of SA [3].

2.1.5 Situation Awareness in EDF

The closest thing the Estonian Defence Forces have to a Doctrine is the Estonian Defence Forces Land Warfare Principles (*Eesti kaitseväe maaväe lahingutegevuse alused*) by Enno Mõts, 2010. Other high-level manuals for the application of Situation Awareness or Electronic Warfare in Estonian Defence Forces were not found in the public or unclassified domains.

Land Warfare Principles focuses heavily on the concept of the OODA loop (Figure 2), originally described by John Boyd. OODA loop begins with the **Observation** of the operational environment (level 1 for SA model). The second step is to **Orient** yourself by organizing and structuring the available information and generating possible courses of action, predicting the future state (level 2 and 3 for SA model). The third step is to **Decide** on a course of action and finally the fourth step is to **Act**. Everybody is in the process of going through the OODA loop. The goal of a military commander is to take the initiative by disrupting the loop for the adversary, forcing them to go back to the first step, before they can act. [5]

Situation Awareness is mentioned briefly in the Land Warfare Principles. It is stated that by creating Situation Awareness, a commander sees patterns in the operational environment, their dissipation and re-emergence. These patterns enable him to direct his unit's actions, aligning them with friendly units, civilian organizations, the adversary, the terrain and the population. The success of leadership and the operation/battle is founded on the commander's ability to acquire, maintain and refine his understanding of the situation. A Tactical Operations Centre (TOC) must operate non-stop in order to maintain Situation Awareness. [5]

Two research documents on SA were also produced in cooperation with EDF in 2018 and 2019. The first "Modelling Complex System-Of-Systems for Creating Situation Awareness" puts together a suite of models for behavioural details of a cyber-physical-social system-of-systems. [9] The second "Mapping the Information Flows for the Architecture of a Nationwide Situation Awareness System" shows how the mapping of information flows between governmental institutions allows development of an SA system and continuously improve it by optimizing the movements of information. [10].

2.2 Data Fusion

Data fusion is the process of utilising one or more data sources over time to assemble a representation of aspects of interest in an environment. A simplified, high level illustration of a Data Fusion System can be found on Figure 3, that shows how data is gathered about the world by sensors, is transmitted via connector interfaces to a Data Fusion engine. The Data fusion engine can send the fused information directly to a user interface or to another connector, where supportive tools can enhance situation assessment by the user. In order to understand how Situation Awareness is achieved with the help of technology a brief look at human-machine Data Fusion systems is necessary. A complete fusion system needs to integrate both human Situation Awareness and machine Data Fusion, including a means of interfacing between the two. [2]

"Situation Awareness can be understood as the human counterpart to machine Data Fusion, while Data Fusion can be conceived as the machine counterpart to Situation Awareness" - Dale A. Lambert [11].

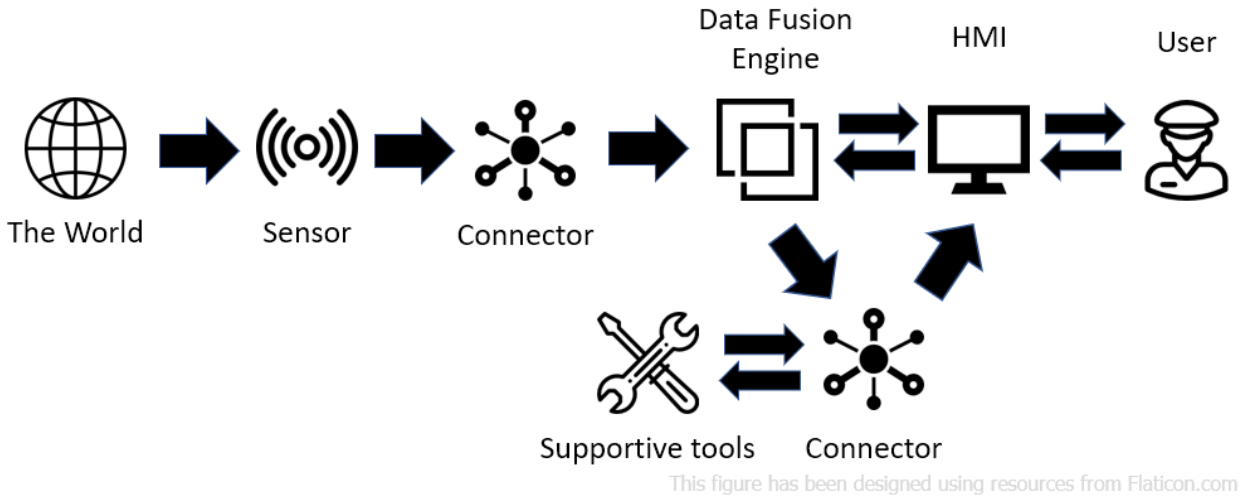


Figure 3. Framework for enhancing Situation Awareness with Data Fusion. [12]

How fast the data is delivered between the nodes shown in Figure 3 can be roughly divided into three categories. Real-time means there is a minimal and known latency between data being generated and received, usually under a second. Near-real-time is more ambiguous, but generally means the data is sent as soon as practically possible and any delays are insignificant compared to the speed of the whole process. Near-real-time can mean that data is sent and received from within

seconds to minutes. Finally, most manual data entries are batch deliveries, when data is collected int a batch and then sent or only received when the system or operator requests for an update. [13]

“All system designs are not equal in their ability to convey needed information or in the degree to which they are compatible with basic human information-processing abilities.” [3] this creates a dependency on the systems used for generating the display. The design of a Data Fusion System must be considered holistically.

In 2003 Dale A. Lambert formulated five grand challenges for information fusion:

1) **System Challenge**: How should we manage information fusion systems formed from combinations of people and machines?
2) **Paradigm Challenge**: How should the interdependency between sensor fusion and information fusion paradigms be managed?
3) **Semantic Challenge**: What symbols should be used and how do those symbols acquire meaning?
4) **Epistemic Challenge**: What information should we represent and how should it be represented and processed within the machine?
5) **Interface Challenge**: How do we interface people to complex symbolic information stored within machines to provide decision support? [2]

When designing a Data Fusion system, the first challenge should be met by creating a system schematic, where desired integration between humans and machines is described. The second challenge by describing, how the system supports transitioning between the levels of SA (level 1 to 3). The third challenge should be met by designing symbology that describes the sensory input (level 1), its relation to the world (level 2) and possible effect on the operator goals (level 3). The fourth challenge should be met by describing the whole system in a process schematic including the machine and human actors. Then deriving the form of information representation from the compatibility requirements apparent in the process. The final challenge should be met by selecting from available interfaces, a suitable combination. Auditory, visual, contextual, tactile etc. interface should be considered [14] based on facets of the user experience illustrated in Figure 4. The User Experience Honeycomb illustrates the various facets of user experience design. [15]

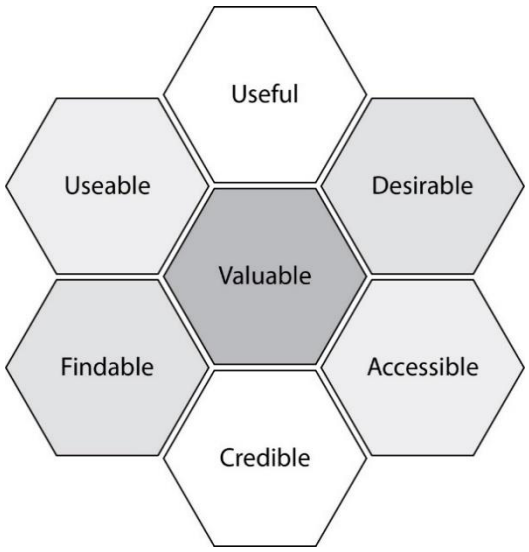


Figure 4. User Experience Honeycomb. [15]

Each facet of user experience design can be defined by this diagram as such:

- **Usable**: Systems should be designed in a way that is familiar and easy to understand and learning curve for a user should be as shallow and painless as possible.
- **Useful**: A product or service needs to fill a need. If the product or service is not fulfilling user's wants or needs, then there is no real purpose for the product itself.
- **Desirable**: The visual aesthetics of the product, service, or system need to be attractive and easy to translate. Design should be minimal and to the point.
- **Findable**: Information needs to be findable, and the system should be easy to navigate. If a user has a problem, they should be able to quickly find a solution. The navigational structure should also be set up in a way that makes sense.
- **Accessible**: The product or services should be designed so that even users with disabilities can have the same user experience as others.
- **Credible**: The company and its products or services need to be and appear trustworthy.

[15]

The understanding of goals and tasks for humans is referred to as a mental model. For computers, we call these models computer models. Both can be viewed as types of cognitive models. A

computer system that supports awareness needs to include a model of the environment. This model defines what is relevant about the environment, provides for dynamic information prioritization, and provides a mechanism for integration of low-level data to create meaning, for example projections of possible and likely future situation states. [4]

Firstly, such a model needs a process of active learning to maintain and refine it as new things about the system are encountered. In addition, encountering familiar situations, they need to be linked to the model for rapid processing of well-defined situations. [4]

Secondly, to be successful, these models need to capture an understanding of relevant goals. Goals define information's relevance (separating signal from noise) and let meaning be established regarding that information. [4]

Finally, the computer model will need to include a mechanism for goal prioritization, along with knowledge of which data states are pertinent for indicating which goals are the most critical at a given time. [4]

A real-world example of data fusion system to support SA in for military personnel was developed from 2010 to 2013 for European Defence Agency by a multinational group of stakeholders. The project was called "Cardinal" and the purpose was to "design and implement a system for supporting and coordinating information flow, in the form of a mobile workstation that provides support in planning and performance of tactical missions of military units operating in urban environments". [16]

2.2.1 Common Operational Picture (COP)

"COP is a term used to describe a visual representation of tactical, operational, and strategic information to support rapid assimilation and integration by team members. It is used as an information tool in command-and-control centres to generate situational awareness [1]" COP is not inherently digital, but can be created by drawing, using markers or connecting strings with pins and so on. Digital systems that support situation assessment and display COP are called by very different names. Possible descriptions include:

1. Automated Planning System
2. Situational Awareness System
3. Automated Digital Data System
4. Tactical Command and Control System
5. Command, Control and Intelligence System
6. Manoeuvre Control System
7. Command Information System
8. Tactical Data System [17]
9. Situation and Battle Awareness System [18]

All these systems can be on some level or another called Data Fusion Systems. It is found that Data Fusion Systems allow a commander to focus more on real-time command and less on information analysis (European Defence Agency, 2013).

In order to succeed, a COP system needs a clear and specific set of requirements. In the absence of such requirements a rigorous discipline in systems engineering processes is necessary. Failure to produce either can result in constant changes to underlying systems and significant delays in delivering functionality. [19]

In 2019 Spring Storm exercise Estonian Defense Forces fielded a new version of its COP system "KOLT" (*kaitseväe olukorra ja lahinguteadlikkuse süsteem* – EST). The system was developed cooperatively by reservists and active-duty service members. [18]

Examples of solutions that bring Electronic Warfare into the Common Operational Picture are TacELINT Situational Awareness Prototype from Electronic Warfare and Radar Division Defence Science and Technology Organisation in Australia [20] and mySPECTRA from German company LS telcom [21].

In TacELINT Situational Awareness Prototype, so-called value-added products shown in Figure 5 use information resources from a central database, including geographic information, to provide specific details of the capabilities and context of detected entities. This illustration of detection ranges (shown as red shaded areas) and lethality ranges (shown as dark red circles) uses values for

"maximum" detection and effective range from a database. The blue areas are related to own forces, and the green are mission waypoints. [20]

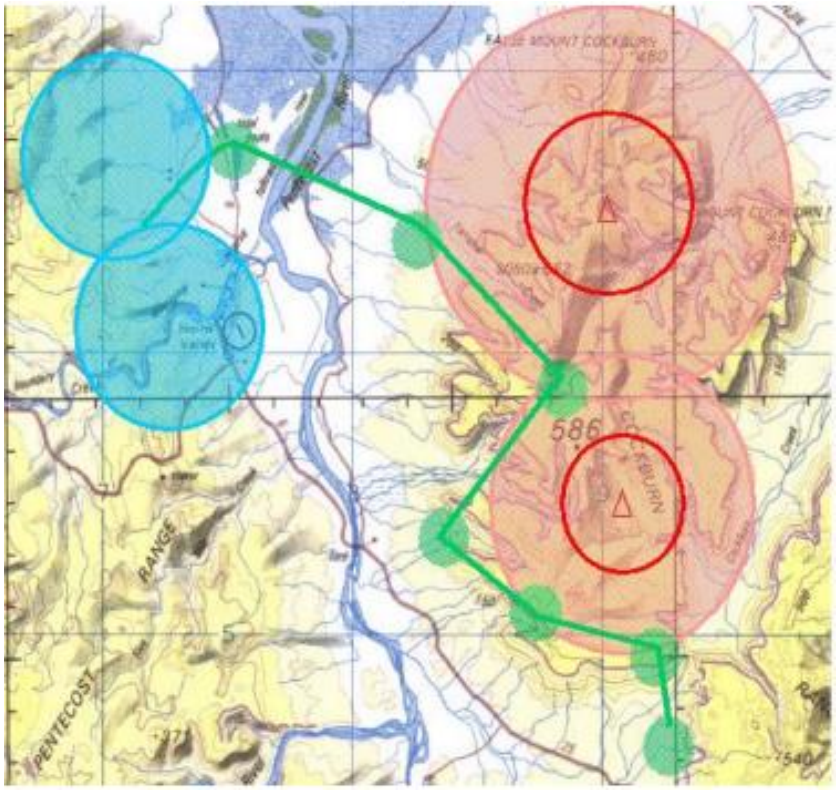


Figure 5. A TacELINT value-added product. [20]

MySPECTRA is a Military Automated Spectrum Management & Electronic Warfare System marketed by German Company LS telcom. MySPECTRA is based on a central database for spectrum data and includes task specific software modules shown in Figure 6. The software claims to support:

- Spectrum Situation Awareness
- Electronic Warfare
- Spectrum, Mission and Battle Space planning
- Tactical communications
- Frequency assignment and allocation
- Host nation and international coordination, mutual interference or jamming mitigation
- Spectrum sharing

[21]

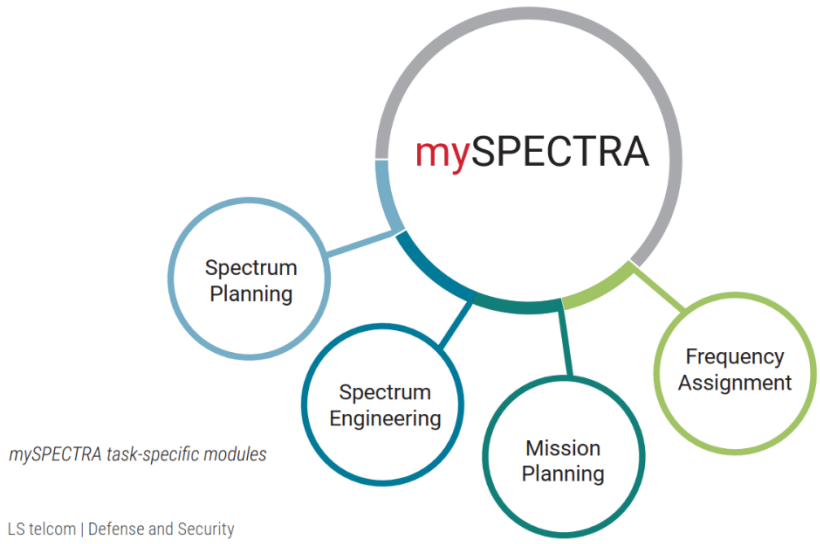


Figure 6. mySPECTRA task-specific modules. [21]

Based on the material available about the product, it remains unclear how mySPECTRA reconciles the five grand challenges of Data Fusion system or if the user interface is designed with the facets of the user experience honeycomb in mind.

There have recently been some developments in developing a common operational picture for electromagnetic (EM) domain in NATO. The efforts began with a centralized database. "The NATO Emitter Database (NEDB) was established as a NATO database and information sharing tool on electromagnetic systems over 25 years ago. It is NATO's primary platform for EW mutual support and exchange of the best emitter data available in both peacetime and periods of crisis. Therefore, it is one of the most important sources of information to enable C2 of EW. Since its inception, the NEDB has been continuously expanded to facilitate the description of new electromagnetic systems and associated platforms." [22]

However, NEDB has not been used widely in EDF and a database alone cannot enhance situational awareness. A Next Generation (NG) version for the database is being developed and is compatible with more modern platforms and networks. "The NEDB-NG will be delivered during the first increment of C2 of EW. It was developed as a web-based capability, with advanced data storage and near-real-time data-sharing capabilities, which can be deployed in a federated infrastructure of a system of systems. All existing NEDB data will be migrated into NEDB-NG which will be available and run on the NATO Secret Wide Area Network. It will also be accessible through Battlefield Information Collection and Exploitation Systems (BICES) networks to all NATO

nations. Each NATO nation may also have national instances of NEDB-NG running on their own National networks." [22]

There are plans for further development that will start to create some enhancement for situational awareness. "The NATO Recognised Electromagnetic Picture (REMP) aims to visualize EM activity in time and space (3D tracking) in a manner that is relevant to enhance Situation Awareness and the effective conduct of Allied EM operations. NATO REMP seeks to compile all electronic operations information for own, adversarial and neutral entities within the Joint Operations Area. The NATO REMP will utilize NATO Core Geographical Information Services to visualize geographically referenced EM information for dissemination and storage. As such it will provide a seamless sharing of the REMP into the NATO Common Operational Picture, increasing the awareness of Electromagnetic Operations across the Joint Force" [22]

2.3 Electronic Warfare (EW)

Electronic warfare has a few definitions, while some professionals colloquially only use the term EW to mean Electronic Attack, most publications use a broader definition.

The US military that has published much of the material available on the subject defines Electronic Warfare as "Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. [23]" They expand on this definition further bay stating "Electronic warfare (EW) is essential for protecting friendly operations and denying adversary operations within the electromagnetic spectrum (EMS) throughout the operational environment (OE) [23]"

Although, USA is part of NATO, USA sometimes uses separate definitions, the definition of EW for NATO is referenced on NATO official web page. "Electronic Warfare (EW) is the military action that exploits electromagnetic energy to provide Situation Awareness and achieve offensive and defensive effects. [24]" In the NATO definition, the importance of EW for situation assessment is highlighted.

It is widely accepted that EW consists of three functions: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). These functions are referred to as divisions

in US military joint doctrine. [25] Richard Poisel covers the details of EW extensively in his excellent book "Introduction to Communication Electronic Warfare Systems" published in 2002 by Artech House, London. Only a brief overview of relevant concepts is covered in this thesis. [26]

In the last decade, the concept of Cyber Electromagnetic Activities (CEMA) has been adopted in many NATO forces. "Cyber electromagnetic activities are activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system. CEMA consist of cyberspace operations (CO), electronic warfare (EW), and spectrum management operations (SMO)" [25] As such CEMA can be seen as an umbrella domain that EW is a part of. Figure 7 depicts how CO, EW and SMO make up CEMA and explains the principles of each domain. It should be noted that EW and SMO are very tightly linked together. While EW is concerned with the use and control of EMS, SMO is responsible for planning, coordination and management of the EMS. Figure 8 illustrates how EMS enables the use of Cyberspace that ties the rest of the five natural domains together.

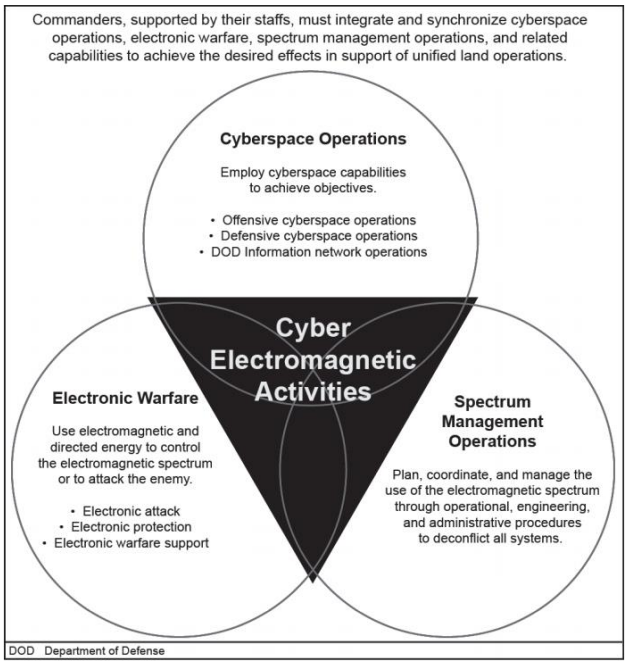


Figure 7. Cyber Electromagnetic Activities. [25]

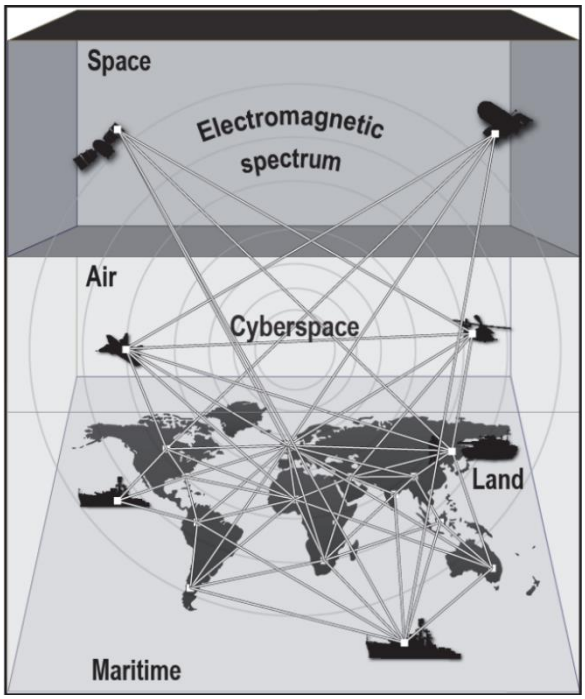


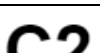
Figure 8. The relationship among the five domains and the electromagnetic spectrum. [25]

While air, land and sea exist naturally without any human interference, cyberspace only exists because of humans. Cyberspace connects most modern warfighting platforms; however, these connections are only possible due to human's ability to manipulate the electromagnetic spectrum. These manipulations include, but are not limited to electricity generation, optical or radio frequency (RF) communication over wired and wireless mediums, radar ranging and imaging systems, weapons guidance systems *etc*. Modern life would simply not exist as we know it without the utilization of the EMS.

2.3.1 Symbology

In NATO documentation there are limited resources to visualize EW units, equipment, effects or activities. All symbols directly related to EW in NATO Joint Military Symbology APP-6(D) 2017 can be seen in **Table 2**.

Table 2. All symbols directly related to EW in NATO Joint Military Symbology APP-6(D) 2017.

Meaning	Symbol	Meaning	Symbol
Electronic Warfare		Jamming	
Command and Control		Signals intelligence	
Electronic Ranging		Broadcast Transmitter antenna	
Radar		Radio	
Direction finding		Radio relay	
Search (reconnaissance or intercept)		Tactical satellite (satellites have 9 more variations, non are EW specific)	
Sensor		Computer system	
Sensor emplacement		Laser	

Although there are many other symbols created to depict EM activities, these are not documented on NATO or EDF level and thus not “official”.

2.3.2 Jamming

“Jamming radio signals has been around almost as long as radio signals themselves.” [26] Jamming is a kind of attack that consists of intentionally or unintentionally interfering with the communication medium to keep it occupied or to corrupt data in transit causing a denial of service (DoS). It is the most common type of electronic attack. Jammers can be divided into types based on how much of their operating time is spent transmitting, how they interact with operating frequencies and where they are located. These categories are illustrated in Table 3. [27] Submersed jammers are not common, because EM waves do not penetrate water very well, however sea surface jammers operate in the same way as ground-based jammers. Space based jammers are also currently not common but would operate much the same way flying jammers do.

Table 3. Jammers can be divided by operating time, frequency or location. [26] [27]

Operating time	**Frequency**	**Location**	
Constant: The basic strategy is to continuously transmit on the channel to occupy the transmission channel for a certain time. However, from an attacker's point of view, this strategy consumes a lot of energy and is easily identifiable.	**Narrow band**: A jammer that attacks the target's carrier frequency only.	**Ground based**: Ground-based systems are most useful when extended ranges are not required. The advantage of ground-based systems is their all-weather capability.	
Random: This method allows the attacker to save energy by going from an active state to a sleeping state at random time intervals.	**Barrage**: emits a broad range of frequencies simultaneously.	**Flying:** usually an UAV, minimal vulnerability due to constant motion, smaller power requirements, but more expensive.	
Reactive: This tactic aims to minimize the risk of being detected. Therefore, the attacker jams the channel only upon detecting transmission. This strategy reduces attack time and increases its effectiveness because the attacker no longer blindly jams the network.	**Follower**: detects the frequency of the target, identify that as the target of interest, and then apply narrowband jamming power to that frequency.	**Standoff**: operates from within the friendly held battlespace.	**Stand-in**: operates within an adversary's held battlespace

Some communications are more resilient to jamming attack than others. "Analog voice, either AM or FM, for example, requires significantly more jamming power than most digital communications. /---/ A bit error rate of 0.5 can be achieved against a continuously broadcast digital signal (with adequate signal levels) by only jamming 50% of the time" Approximately 30% of analogue voice signal or 1% of digital signal needs to be interrupted for jamming to be considered successful. A single narrowband jammer can switch or sweep between frequencies in what is called "time-sharing" to jam multiple frequencies. [26]

2.3.3 Direction finding and geolocation

Geolocating communication emitters, known as position fixing, is one of the more important functions of Electronic Support (ES) systems. The amassing of units in a close area, detected and located by EW means, might indicate a specified type of activity. The location of emitters,

however, does not necessarily mean the location of the target. It is possible to position the transmitting antenna of an emitter quite a distance from the target itself. [26]

One of the most common ways to accomplish emitter geolocation is by triangulation. In this, the direction of arrival of an incoming wave front is determined at two or more sites. Estimated location of the emitter is at the intersection of these bearings. [26]

2.3.4 Emissions and communications analysis

Electronic Support measures can support generation of the common operational picture (COP), not only by geolocating targets, but also in some cases, identifying those targets by unit type, or even by identifying the specific unit. The latter can only occur if specific emitter identification is accurate enough. COP could display the up-to-date disposition of adversary forces as well as possibly show interconnected networks. If a target was intercepted previously and the technical capability is present to recognize it, then the system can automatically indicate that the same target is present. If the target is in a new location, then this can contribute to the COP by indicating its movement, intentions. [26]

Certain weapon platforms or units sometimes have unique combinations of emitters that can be intercepted and geolocated indicating that specific weapon platform or unit is present. It also can sometimes indicate that they are in a particular state, for example, preparing to fire artillery. This also contributes to the COP generation and maintenance function. [26]

2.3.5 Electromagnetic wave propagation models

Most EMS manipulation in Electronic Warfare is conducted in the air environment. In order to rise Situation Awareness for EW we must first investigate how we can predict or model the range of EMS manipulation in free space.

Before diving into different models for predicting the reach of electromagnetic waves in EW, we shall quickly examine what are the factors that contribute to the algorithms. Aron Haljase's master's thesis provides an excellent overview on this subject already, especially from a military perspective, so we will be brief and focus only on the essentials.

2.3.6 EM wave properties

The following paragraphs are not referenced as they describe the basic physics of electromagnetism that can be found in many textbooks.

An electromagnetic wave has some polarization and phase angle describing the direction of oscillations in its amplitude. EM waves in vacuum travel at the speed of light in a straight line or so-called "line of sight" (LOS). However, EM waves can reflect, refract, diffract and change polarization and phase. In vacuum an EM wave has a specific frequency f determined by its wavelength λ $f = \frac{c}{\lambda}$, where c is the speed of light. Waves that meet will add together to create interference. Each of these qualities effect the propagation of the wave. The speed of propagation is affected by the substance of the environment called the medium.

Reflected waves change polarity with each pounce, while creating multiple paths for the same wave to take from the transmitter to receiver. A signal traveling a longer path will reach the receiver later. If the signal duration is long, then the reflected wave can join back with the original to strengthen it with constructive interference or reducing it with destructive interference. Reflection quality of EM waves enables non-line of sight propagation.

Multi path propagation can be predicted to be destructive or constructive based on the position of the reflective surface. The most significant destructive effect comes from objects located in the space called the first Fresnel zone. The Fresnel zones are prolate ellipsoidal regions of space between and around a transmitter and a receiver. Between two points, the height of the first Fresnel zone r can be calculated from $r = \frac{1}{2}\sqrt{\lambda \cdot d}$, where λ is the wavelength and d is the distance between two points.

Diffraction causes a wave to "bend" slightly behind obstacles, reducing the effect of shadowing from large objects that would block a beam that travels only in a straight line. This also enables a wave to propagate beyond line of sight.

Refraction also "bends" an EM wave due to the change of the medium the wave is traveling through. For example, because the speed of light is different in lower atmosphere than in the

stratosphere, high frequency (HF) waves beamed into the sky can bend back down towards the earth, making very long-distance propagation possible.

2.3.7 EM wave propagation models

In “Military Communications and Information Technology: A Trusted Cooperation Enabler” volume 2 there is a table of well-known empirical propagation models suitable for variety of frequency bands, distances, transmitter and receiver heights shown in Table 4. Unfortunately, none of the models apply very well to parameters used in most military applications, where the most common frequency bands in use are 30-88 MHz and 225-400 MHz and the antennaes are mostly 1.5-10 m in height. [28] Additionally, John Egli’s model has been added to the table, that is in fact designed to take irregular terrain into account. [29]

The empirical models do not consider the real terrain in the operational environment. However, there exists a more complex collection of propagation models, including the Egli model, called Longley-Rice model. “The Longley-Rice method considers atmospheric absorption including absorption by water vapor and Oxygen, loss due to sky-noise temperature and attenuation caused by rain and clouds. It considers terrain roughness, knife-edge, (with and without ground-reflections), loss due to isolated obstacles, diffraction, forward scatter and long-term power fading.” It is designed to apply for 20-20 000 MHz frequencies and in seven different pre-configured climate environments. The model is computationally demanding and requires dedicated software and relatively powerful computer. [30] Real terrain can be taken into account by using software tools (*e.g.* LS Telcom or Radio Mobile software) that combine terrain models with propagation models to create more realistic predictions of RF propagation. Radio Mobile is a free propagation simulation program written by Roger Coudé. [31]

Longley-Rice is the preferred model for predicting the effects EM manipulations in military applications. While proprietary software for using the Longley-Rice model for EM wave propagation predictions may be superior, the best open-source software for simulating the radio environment in Radio Mobile [32]

Table 4. Empirical EM wave propagation models. [28]

Author	Frequency (MHz)	Distance (km)	Transmitter height (m)	Receiver height (m)
Y. Okumura	15-1920	1-100	30-1000	
M. Hata	150-1500	≥ 1	30-200	1-10
COST 231	800-2000	0.02-5	4-50	1-3
H. Xia	900, 1900	0.001-2	3.2, 8.7, 13.4	1.6
V. Erceg	1956	0.01-0.5	3.3, 6.6	1.5
D. Har	900, 1900	0.06-2	3.2, 8.7, 13.4	1.6
A. Kanatas	1890	0.02-0.18	4	1.7
H. Masui	3350, 8450, 15750	0.02-0.5	4	2.7
Y. Oda	457-15450		≥ 20	
T. Rao	200, 400, 450	0.5-10.5	≥ 20	3
N. Blaunstein	902-928		7	2-3
W. Yong	150, 450, 800, 3700	0.108-16.3	138	2
J. Egli	**40-1000**	**0.15-50**	**1.5-1500**	**1.5-300**

2.3.8 Electronic Warfare in EDF

The Estonian Defence Forces Land Warfare Principles states that Combat Support Elements include Fire Support and Air Defence, ISTAR[1] and Electronic Warfare Elements but also Military Police and Engineers and some Air Forces assets. [5]

A units EW capability is derived from both a unit's own assets but also their ability to minimize the effects of an adversary's EW activity. Employing Electronic Warfare to enable achieving warfighting goals is considered a part of the Firepower combat function. A geographic area or corridor where EW is used to force the adversary to change their course of action is designated as a Target Area of Interest. [5]

[1] Intelligence, Surveillance, Target Acquisition, and Reconnaissance

While high-level doctrinal approach to EW is scarce, Electronic Warfare has been the subject of some study in the Estonian Defence Forces. Three dissertations from Estonian Defence Academy and one master's thesis from Tallinn Technical University by a EDF officer stand out.

One of the academic works approached Electronic Warfare holistically. In the dissertation "Electronic Warfare Capability in a Small Country" by Ott Mihailov, 2013 EW concepts and the structure of EDF are described in detail. Mihailov also suggests criteria and their application for selecting Electronic Warfare Capabilities shown in Table 5. All these criteria should be considered when selecting new EW capabilities for development. [33]

Table 5. Criteria for selecting possible EW capabilities [33]

Criteria group 1	**Criteria group 2**	**Criteria group 3**	**Criteria group 4**
EW subdivisions and their capabilities	Protection of a weapons platform	Derived from organic forces warfighting capabilities	Land
	Targeted electronic attack, support or defence	Derived from allied forces warfighting capabilities	Air
		Derived from adversary's warfighting capabilities	Sea

Other works focused more on Electronic Protection for wireless communication. In 2007 Ivo Kõiv authored the dissertation "The Feasibility of Protecting 1st Infantry Brigade's Radio Communications in an Environment of Communication Electronic Warfare", Kõiv lays out how spectrum management, geographical planning, dynamic transmit power and encryption can enable protecting an infantry unit from jamming, signal and communication intelligence operations. Kõiv outlines the need for a software solution to enable Electronic Protection in 1st Infantry Brigade. [34]

Aleksei Biller's thesis from 2016 is titled "Testing the Jamming Resistance of Radio Station Harris RF-5800V-MP" explored protecting radio communications further by investigating Harris™ RF-5800V-MP hopping algorithm QUICKLOOK 1A tolerance towards growing jamming factor for both voice and data broadcasting. [35]

“Simulation of battlefield radio communications’ situation for determining radio network coverage and signal propagation distances” was the title of Aron Haljaste’s master’s thesis. While he did not focus directly on Electronic Warfare, the principles he outlines for simulating battlefield signals situations and analysing them are applicable for EW purposes. [32]

3 Gap of knowledge

In this chapter we organized the knowledge from the state-of-the-art overview to reflect what parts seem to have the greatest gaps. In order to keep the scope more manageable we focus on aspects that are more related to Estonian Defence Forces. Having identified the gaps of knowledge we formed those into research question to be answered by this thesis.

Once again, we followed the structure outlined in Figure 1, starting with Situation Awareness, then moving on to look at Data Fusion and finally looking at Electronic Warfare. Finally presenting our research question. In order to narrow the scope, Estonian Defence Forces were used as a case study for all three sections.

3.1 Situation Awareness

From all the research reviewed we can conclude that Situation Awareness has not been rigorously studied in EDF. Some research has been conducted in Estonia in general. In EDF, the concept is mostly connected to the simplified model of OODA loop. Although the importance of Situation Awareness is acknowledged by E. Mõts in Land Warfare Principles, there are no documents describing how SA can be achieved, measured or maintained or how systems should be designed to support it. We can therefore conclude that research into the condition of SA in EDF is justified and necessary.

More generally, there is a gap of knowledge in what, how and when to present to a commander in order to support situation assessment in other words, how to display **Situation Awareness**. Furthermore, the question is how to automate information processing to build level 2 and 3 SA while not depriving the commander from detailed understanding of the underlying reality.

3.2 Data Fusion

Modern understanding of Situation Awareness seems to be integrally linked to data fusion solutions such as COP systems. There are many COP systems including EDF's KOLT, however few can be said to have dedicated services to support situation assessment in CEMA domains. There are some prototypes and proposed solutions to build a COP system that supports EM

operations, however those in the public or EFD unclassified domains do not fully resolve the five grand challenges for a Data Fusion System. The central gap of knowledge seems to be how to convey EM activities to commanders with COP systems or in other words how to **display** Situation Awareness.

3.3 Electronic Warfare

Electronic warfare knowledge and capabilities are extremely classified in Estonian Defense Forces. Because of this, it is hard to identify gaps of knowledge in this area. However, EW symbology used by NATO countries is released to public and here we can identify some gaps. There are no common symbols for frequency, bandwidth, interference, waveforms, RF propagation, networks, encryption, passive antennae, directional antennae, radio links, servers or databases. To summarize, the question is, how to display **Electronic Warfare** activities, effects and equipment.

3.4 Research question

Goals set at the start of this project were to:

1. Provide an input to develop an Electronic Warfare display for Estonia's Defence Forces Situation and Battle Awareness system KOLT.
2. Highlight gaps in Defence Forces Electronic Warfare capabilities
3. Describe criteria and priorities for future developments.

From the three sections above we synthesized the heading of this thesis: **Displaying Electronic Warfare Situation Awareness in Estonian Defence Forces**. The central research questions are:

1. What are the problems for experts working on Electronic Warfare and situation assessment in EDF?
2. How are the problems prioritized by EDF stakeholders?
3. How to create a value-added product that addresses the prioritized problems?

4 Methods

The Design for Six Sigma (DFSS) framework called Identify, Define, Develop, Optimize and Verify abbreviated to IDDOV was selected to tackle the research questions. Design for Six Sigma (DFSS) is an engineering process used by businesses to design a quality product from scratch. IDDOV in DFSS provides the necessary framework for product development and emphasizes the step-by-step phases to achieve quality There are five phases called Identify, Define, Develop, Optimize and Verify (IDDOV). [36]

However, the scope of this thesis was to lay the fact based, detailed groundwork for developing a solution that addresses the most severe problems related to Electronic Warfare Situation Awareness. Thus, only Identify and Define phases were carried out. Due to *force major* COVID-19, the define phase could not be completed in its entirety and instead a step from Develop phase was completed. Final development, optimization and final verification of a comprehensive product would be subject of subsequent projects.

4.1 Identify

In the identify phase, the goal was to understand the opportunity. We identified the customer requirements and prioritized their needs. It is considered the most important phase since all future activities of the projects depends on this phase. [36]

1. The phase starts with process analysis in order to understand how the current process is set up and record any limitations or dependencies inherent in the process itself. This step is called the "**Voice of the Process**".
2. The second step is to analyse design limitations. What standards need to be applied if any and what are the existing inputs and expected outputs for the system from a technical standpoint. This step is called the "**Design Limitations**".
3. The third step is to conduct interviews with experts in the field. The purpose of this step is to understand the main issues with the current process. An affinity diagram is constructed from the ideas, issues and solutions from the stakeholders. This step is called the "**Voice of the Experts**".

4. The fourth step is to conduct a survey on the customers and/or users of the system being designed. This is done in order to clarify priority and expectations for any future solution. This step is called the "**Voice of the Customers**".

A three-part survey questionnaire was compiled to investigate the focus areas developed in Voice of the Experts step. the survey can be found in Appendix 2. The first part of the questionnaire focused on gauging the customer's satisfaction with the current situation in CEMA. The second part was designed to assess the customer's need for possible future solutions. The third section was meant to create a clear prioritization of possible use-cases, identified with experts.

A sample of 98 Estonian Defence Forces and Defence League active-duty service member was selected for the survey. 39 people were in operations sections of tactical or joint units, 31 people were in signal's section of tactical or joint units. 18 were from CIS or CO units. 10 were experts from unique units.

In order to weigh the responses, the customers were asked to rank their utilization of the terms "Cyber Domain", "Electromagnetic Spectrum", "Electronic Warfare", "Communication Network" and "Operational Area" in their daily work. This ranking was then used to divide the responders into four groups and a weight of 1x, 2x, 3x and 4x multipliers were applied accordingly. Both weighted and unweighted results were then analysed and compared.

4.2 Define and develop

In the define phase we translated the customer's priorities and expectations into a problem statement. We produced design requirements to solve the problem stated by creating Critical to Quality (CtQ) metrics. From those metrics a specific, measurable, attainable and relevant goal for the solution was set. The collection of CtQ metrics, problem statement and goal statement can be considered Requirement Specifications for the solution.

This phase also should have contained benchmarking the current process *versus* a mock-up of a value-added product made to Requirement Specifications. The experiment was prepared over 12 days to take place in the EDF Main Command Post Exercise Griffin Lighting 21 EST. However, due to COVID-19 the exercise was scaled back, and the experiment was cancelled. "According to

the chief of the exercises Estonian part /---/, due to the spread of the coronavirus, the initial ambitions of the Defence Forces had to be scaled back and it was not possible to implement everything planned in full.” [37]

5 Results and discussion

The results are presented and discussed in phases: Identify, Define and Develop. The main effort of this thesis was to identify the problems for people working with EW SA in EDF, to prioritize them and to develop a mock-up of a value-added product that would address the most valuable missing feature.

The content of results and discussion is considered “For official use only” for five years until 03.05.2026 under Estonian Public Information Act § 35 p (1) section 10: “information on technological solutions if disclosure of such information would damage the interests of the holder of information or if classification of such information as internal is prescribed in a contract entered into with a person in private law;”

5.1 Identify

In this phase we selected a use-case that we expect will help our customers the most for further investigation. However, many other use-cases are also identified that should also be implemented in order to improve Estonian Defence Forces Cyber and Electromagnetic Activities Situation Awareness.

5.1.1 Voice of the Process

The first step was to understand the current process for building Electronic Warfare Situation Awareness in Estonian Defence Forces. Currently this is achieved mostly based on intelligence reports. A process flow for a generic EW intelligence reporting was drawn, shown in Figure 9. This was based on observations of EDF Main Command Post operating procedures and consultations with an EDF Cyber Command Tactical Communication Systems Architect and an Intelligence Centre EW expert.

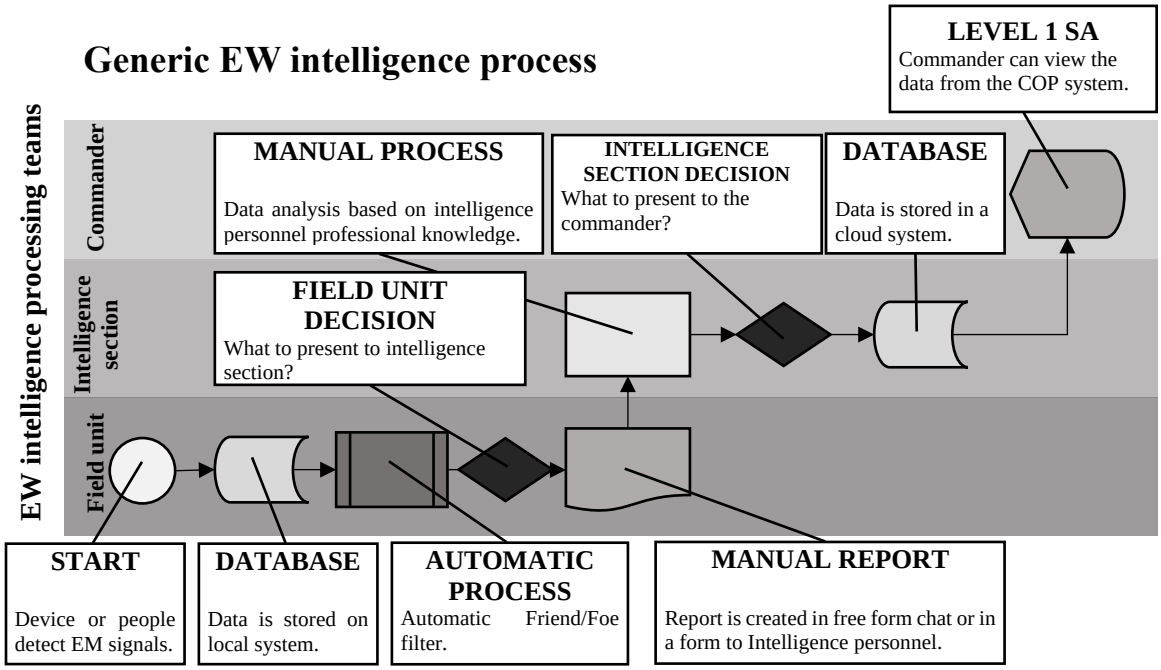


Figure 9. Generic EW intelligence process in EDF

Next, we analysed the strengths, weaknesses, opportunities and threats (SWOT) of the current process as shown in Table 6. Three main takeaways can be observed.

Firstly, while the main strength of the current process seems to be that it is very straightforward, it does not provide feedback to the field unit, if they are providing useful information nor the context of how their information looks in the bigger picture.

Secondly, although the detection, storing and friendly signals filtering is done automatically, the report must still be manually created by the field unit to be sent up the chain. Then the intelligence section must manually process this report to display useful information to the commander.

Finally, the processed product allows the commander to perceive what is happening on the EM spectrum, but the current tools do not aid comprehending the meaning nor predict future events based on this knowledge. In this regard the commander must only rely on their personal experience and expertise.

Table 6. SWOT analysis of the generic EW intelligence process

Strengths	**Weaknesses**
• Straightforward. • 4/9 steps are automated.	• No feedback. • Bach delivery speed • Manual reporting. • Manual processing from the report to the cloud database. • Enables only level 1 SA (perception).
Opportunities	**Threats**
• A loopback from the commander to the field unit to refine operational plans. • Automate reporting from field unit to intelligence section to approach near-real-time updates from operational area. • Added-value products on COP system to help the commander to comprehend (level 2 SA) and project the future (level 3 SA) the EW situation and how it effects the operation.	• Field unit will not change priorities as the situation develops. • Field unit ignores clues that only make sense in context. • Situation changes faster than manual processes can keep up. • Commander will not comprehend the EW information perceived from COP.

5.1.2 Design Limitations

For this step, the scope was narrowed to the main COP system employed by EDF. One limitation and one opportunity were identified from analysing the current design of the COP system KOLT.

For security reasons, currently the EW sensory system must be air-gaped from the cloud-based COP system. This means that automatic report generation will be extremely hard to implement. It would either require advanced security protocols to upload to the central system or the report needs to be printed out and scanned into the main COP system, where image processing would translate the scan back into processable format. In any case, real-time or near-real-time data delivery is not possible with current policies.

The COP system KOLT is being re-designed to be modular and allow micro services. This creates an opportunity to develop an EW plugin separately from the KOLT development cycle and without burdening users without the need for such a tool.

5.1.3 Voice of the Experts

This step began with individual interviews with four key stakeholders to identify what they see as the main issues with building Situation Awareness in Electronic Warfare context. Names of the specialists have been redacted for security reasons. Interview were conducted with:

1. The architect of Estonia's COP system KOLT. (Expert A, black)
2. An Electronic Warfare specialist from EDF Intelligence Centre. (Expert B, dark grey)
3. An Electronic Warfare specialist from Estonian Cyber Defence League. (Expert C, grey)
4. The Chief of Joint Operations Centre of EDF Main Command Post. (Expert D, light grey)

Based on the interviews, an affinity diagram was created. The full diagram is presented in Appendix 3. The affinity diagram produced five focus areas to be investigated further in the next step. These five focus areas are (1) Area of Effect (AoE) overlay, (2) network mapping and health monitoring solution, (3) value-added products, (4) COP system linked databases and (5) regulations and processes.

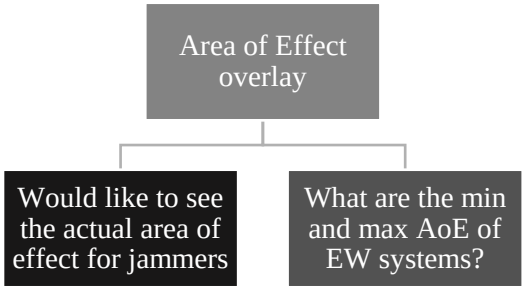


Figure 10. Affinity diagram that produced the Area of Effect overlay focus area, input from expert A (left, black) and expert B (right, dark grey).

The first focus area was derived from two statements by the experts, illustrated in Figure 10. Expert A expressed a need to display actual Areas of Effect based on RF propagation models. Expert B voiced a similar desire for a feature that would help visualize the minimum and maximum area of effect for an EW asset.

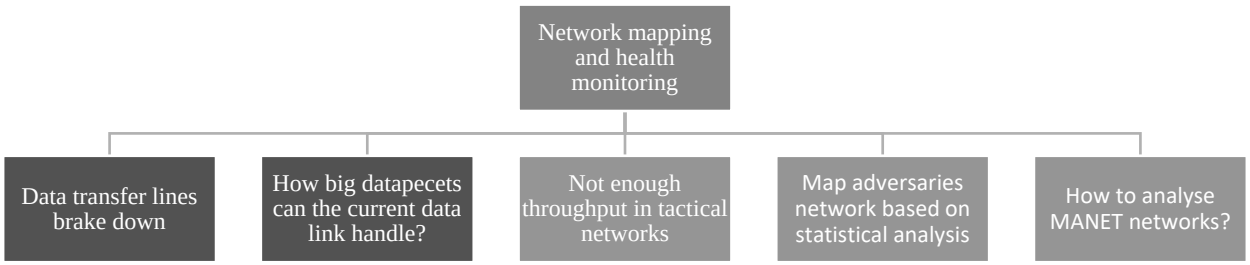


Figure 11. Affinity diagram that produced the network mapping and health monitoring focus area, input from expert B (left, dark grey) and expert C (right, grey).

The second focus area was derived from six statements by the experts, illustrated in **Figure 11**. Expert B raised the pain point that data transfer lines brake down disrupting the dissemination of EW intelligence products, this could be mitigated if there was an indicator, how big data files the current connection can handle.

Expert C also pointed out that the throughput of tactical networks is hindering sharing products currently produced by their units. They also highlighted a missing feature that would allow statistical analysis to be conducted on adversary's wireless network activity to map out a likely organizational structure and the concern that mapping adversary networks will become impossible with current methods, once they start using MANET networks.

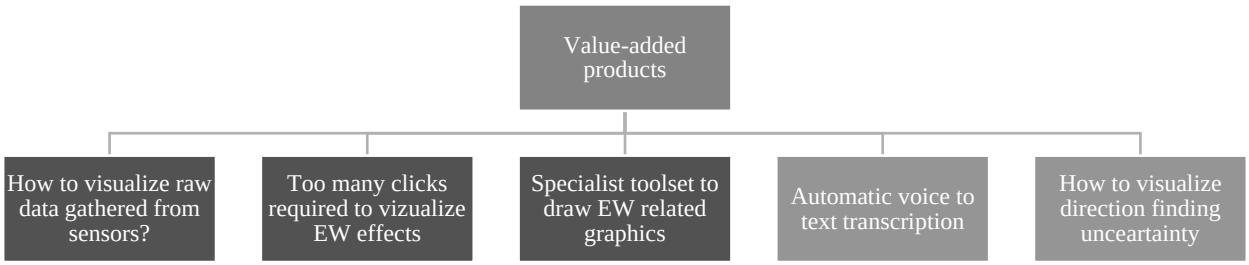


Figure 12. Affinity diagram that produced the value-added products focus area, input from expert B (left, dark grey) and expert C (right, grey).

The third focus area was derived from five statements by the experts illustrated in **Figure 12**. Expert B raised the issue of visualizing raw data gathered from sensors automatically, stating that

it takes around 30 clicks to produce a representation of the EW effect manually with current methods. A specialist toolset is also a missing feature that would mitigate this issue.

Expert C was more specific, stating that one of the automated procedures cold be a transcriber that converts recorded voice to text. They also brought out that as direction finding cannot pinpoint a transmitters location, it is sometimes hard to convey that uncertainty to the client.

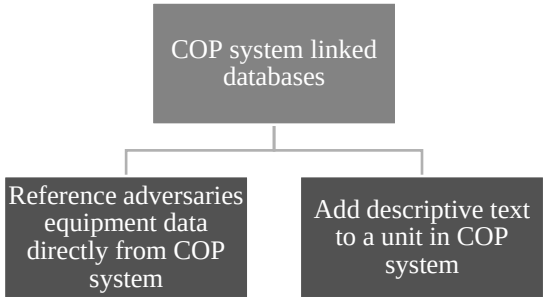


Figure 13. Affinity diagram that produced the COP system linked databases focus area, input from expert B.

The fourth focus area was derived from two statements by expert B, who expressed a need to sometimes add descriptive text to a unit's or equipment's icon in COP system. Also, similarly it would be beneficial if an icon could link directly to an information snippet that described the capabilities of the selected unit or equipment in detail. The statements are illustrated in **Figure 13**.

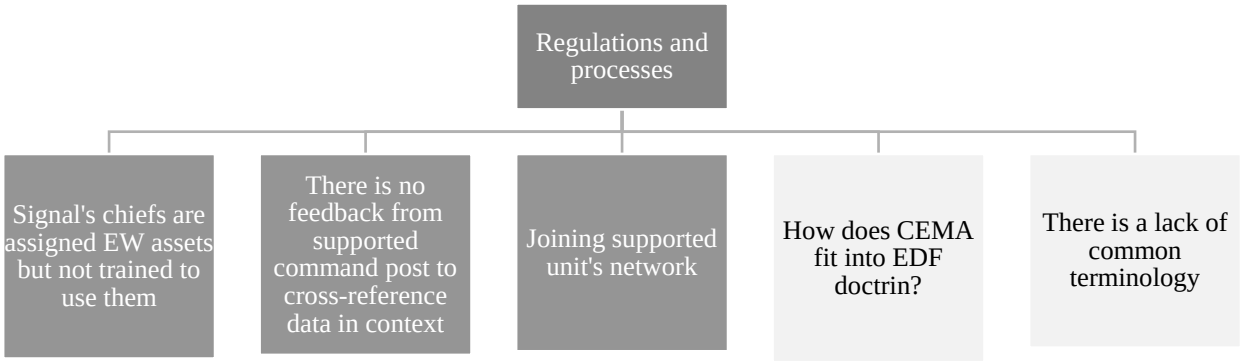


Figure 14. Affinity diagram that produced regulations and processes focus area, input from expert C (left, grey) and expert D (right, light grey).

The fifth focus area was derived from five statements by the experts illustrated in Figure 14. Expert C described an issue when EW assets are assigned to a tactical unit, the commander usually has

the signal's chief take charge of utilizing the asset in operations. However, signal's officers do not receive training in the current curriculum to plan EW effects or activities. Cooperation is also hampered by lack of standard operating procedures for an EDL EW unit joining a supported unit's network. Thirdly, the supported command post does not provide feedback on the intelligence products or the development of the operational environment, as illustrated in Figure 9.

Expert D highlighted that there is currently no documentation describing how Cyber and Electromagnetic Activities (CEMA), including EW fit into EDF's doctrine. Also, that there is a lack of common and agreed terminology, with stakeholders from different background not agreeing on the definition of words and phrases.

5.1.4 Voice of the Customers

38% (37 people) of the 98 people selected to the survey sample responded to the questionnaire. The highest response rate among warfighting domains, 50% (9 people), was from Cyber Command, followed by 44% (4 people) from the Navy and 43% (3 people) from the Air Force. Only 27% (14 people) of Land Forces personnel selected to the sample responded to the survey (**Figure 15**). 70% (7 people) from the various specialized units responded. The response rate when comparing signals vs operations specialisation was close with 39% and 36% respectively (**Figure 16**).

Based on the response rate we can say that **the land forces may be underrepresented, but the overall number of answers was significant and sufficient for drawing conclusions**.

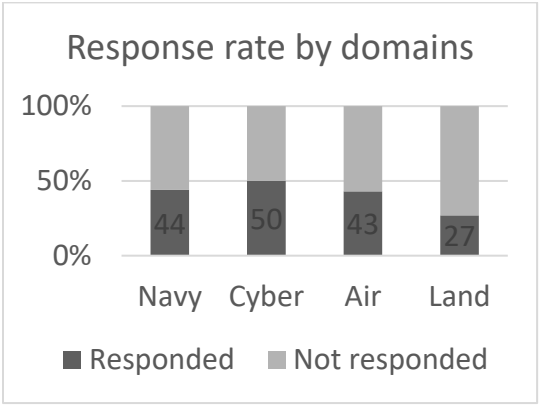


Figure 15. Response rate comparison between warfighting domains.

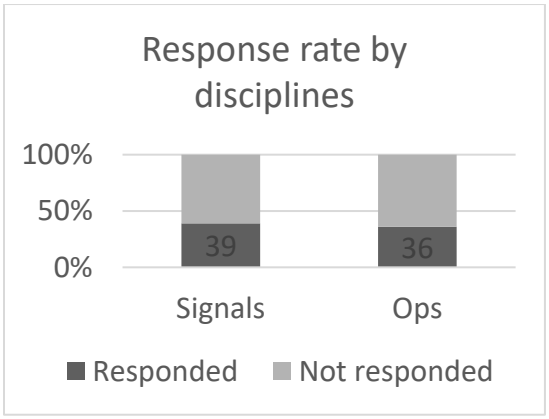


Figure 16. Response rate comparison between signals and operations specialists.

In the first part of the survey, we asked the responders to rank how often they use CEMA (Cyber and Electromagnetic Activities) related terminology on a scale of "daily", "often", "rarely" and "never". Overall, the term "Cyber Domain" was used the least with 35.1% never using it. The most used term was "communication network", with 37.8% using it daily and only 2.7% never using the term. The least daily users (5.4%) are reported for the term "Electronic Warfare". Highlights from the statistics are shown in **Table 7**.

Table 7. reported use-rate of EW related terminology on the job.

	Cyber Domain	Electronic Warfare	Electromagnetic Spectrum	Communications network	Operational Area
Daily	18.9%	**13.5%**	16.2%	**37.8%**	27.0%
Never	**35.1%**	5.4%	29.7%	**2.7%**	8.1%

Based on this data we can assume that the terms "Operational Area" and "Communication network" belong to the active dictionary of the sample. The term "Electronic Warfare" is well known but rarely utilized on the job. The terms "Cyber Domain" and "Electromagnetic Spectrum" are only used by specialists and most of the sample uses these terms rarely, if ever.

In order to give more weight to the opinions of customers, who have more stake in building EW SA the responders were sorted into four groups as shown in **Table 8**. The groups were formed based on how often the individuals use all the terms in the survey. A detailed look on how the groups are characterized is shown in Figure 17.

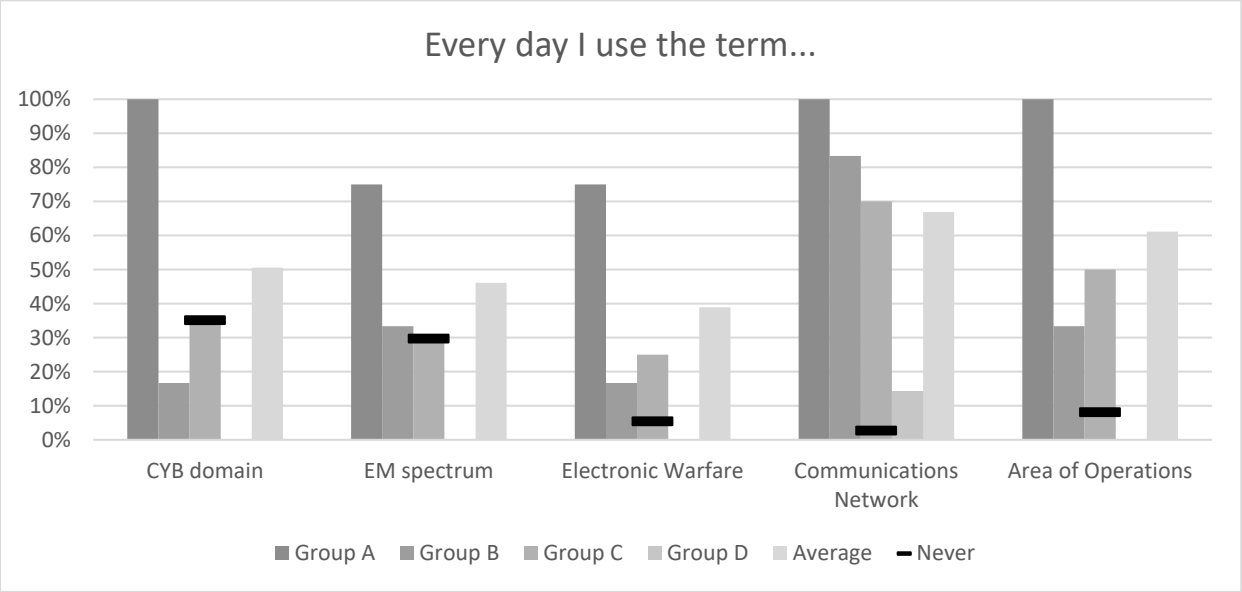


Figure 17. Percentage of responders who use CEMA related terms daily by group (grey), overall average of responders who use the terms daily (black) and the overall average of responders who never use a term (red).

Group A is made up of three cyber and one joint domain officers. Group B consists of three cyber branch representatives, one intelligence representative, one Navy officer and one Land Forces

representative. Group C is made up of 11 Land Forces, 5 Cyber Command, 2 Navy and 2 Airforce personnel. Finally, group D counts 3 Cyber Command, 2 Land Forces, 1 Navy and 1 Airforce persons. The make-up of the groups is shown in Table 8.

Table 8. Sizes and weights assigned to the for groups.

Group	Cyber	Intelligence	Navy	Airforce	Land Forces	Joint	Weight multiplier	No. of participants
Group A	3					1	4x	4
Group B	3	1	1		1		3x	6
Group C	5		2	2	11		2x	20
Group D	3		1	1	2		1x	7

Conclusions from these results indicate that the state EW is not yet an everyday aspect of EDF operations and is not considered. Cyber as a new warfighting Domain has been accepted by experts in the field, but not even considered by most of EDF operations and signals personnel. A critical vulnerability of EDF may be exposed by this revelation, because if CEMA are not considered in training and planning for operations a **CEMA actor could exploit this oversight to inflict asymmetrical harm the EDF forces**, while EDF is not prepared to mitigate CEMA threats. Further study may be warranted into the actual state of Cyber and Electromagnetic Activities in Estonian Defence Forces training and planning procedures.

In the next section we asked to responders to evaluate the current situation. No one reported that they are completely satisfied with the Situation Awareness they have during exercises regarding processing intelligence information but 43.2% were mostly satisfied. A brake down of satisfaction with SA by group is shown in Table 9.

Table 9. Answers to "How satisfied are you with SA regarding processing intelligence information".

Evaluation	Overall	Group A	Group B	Group C	Group D
Do not know	8.1%	0%	0%	10%	14.3%
Sufficient SA	**0%**	**0%**	**0%**	**0%**	**0%**
Mostly sufficient SA	43.2%	25%	66.7%	45%	28.6%
Insufficient SA	43.2%	75%	33.3%	40%	14.3%
Absolutely insufficient SA	5.4%	0%	0%	5%	14.3%

It seems that the biggest experts are also those, who miss SA the most, 75% say SA is insufficient to process intelligence information in group A. In other groups satisfaction is much higher.

Next, the participants were asked to evaluate their satisfaction with symbology used in Cyber Domain, EM spectrum monitoring and EW. While almost a third of the participants were satisfied with symbology for EW, the overall trend was that EDF personnel do not know about CEMA related symbology. This also reflects that **EDF may not be very well prepared to conduct CEMA operations or respond to CEMA threats**.

Table 10. Satisfaction with symbology in CEMA domain

	Cyber Domain	EM spectrum monitoring	EW
Do not know	**54.1%**	**62.2**	**48.6**
Absolutely satisfied	2.7%	0%	0%
Mostly satisfied	16.2%	16.2%	**29.7%**
Mostly not satisfied	18.9%	18.9%	16.2%
Absolutely not satisfied	8.1%	2.7%	5.4%

Regarding regulation and processes the participants were asked if more thorough documentation of CEMA procedures would help them conduct their duties better. 35.1% said that they do not know but the majority, altogether 43% saying that more detailed documentation would benefit them. The interest in groups is shown in Table 11.

Table 11. Answers to statement "My work would be easier if there was more detailed documentation for CEMA".

	Overall	Group A	Group B	Group C	Group D
Do not know	35.1%	25%	33.3%	25%	71.4%
Absolutely agree	18.9%	25%	0%	25%	14.3%
Agree	**24.3%**	**50%**	**50%**	**30%**	**0%**
Do not agree	16.2%	0%	0%	15%	0%
Absolutely do not agree	5.4%	0%	16.7%	30%	14.3%

We observed that 75% of participants in group A, 50% in Group B, 55% in group C and 14% in group C see a need for more detailed documentation. **This highlights the experts need for a doctrinal approach to CEMA in EDF**.

The tools currently available to visualize Cyber and Electromagnetic Activities do not satisfy the users with 75% of group A and mostly not satisfied with tools for Cyber Operations and 50% of group A and 66.7% group B mostly not satisfied with the tools for EM activities. A detailed brake down is shown in Table 12 and Table 13.

Table 12. Answers to the question "How satisfied are you with currently available tools to visualize EM activities?".

	Overall	Group A	Group B	Group C	Group D
Do not know	45.9%	25%	16.7%	40%	100%
Absolutely satisfied	13.5%	0%	0%	0%	0%
Mostly satisfied	13.5%	25%	16.7%	15%	0%
Mostly not satisfied	**29.7%**	**50%**	**66.7%**	**25%**	**0%**
Absolutely not satisfied	10.8%	0%	0%	20%	0%

Table 13. Answers to the question "How satisfied are you with currently available tools to visualize Cyber activities?".

	Overall	Group A	Group B	Group C	Group D
Do not know	45.9%	25%	50%	55%	71.4%
Absolutely satisfied	13.5%	0%	0%	0%	0%
Mostly satisfied	13.5%	0%	33.3%	5%	0%
Mostly not satisfied	**29.7%**	**75%**	**16.7%**	**40%**	**28.6%**
Absolutely not satisfied	10.8%	0%	0%	0%	0%

These results indicate that **there should be significant interest to improve the tools available for CEMA operators to visualize their plans and operations**. This interest is mostly driven by experts, with less engaged people mostly unaware of the current capabilities.

Finally, the participants were asked to rate their personal need to map adversary's communication networks. Unsurprisingly this was rated as critical by group 75% of group A, but as relatively unnecessary by the other groups. This indicates that **while developing better tools for mapping an adversary's communication network may provide high value, the final users of such features would be very few**.

Based on the affinity diagram from the Voice of Experts, nine use-cases were created to be presented to customers for prioritization. The affinity diagrams are broken down in Figure 10, Figure 11, Figure 12, Figure 13 and Figure 14. These use-cases were:

1. Visualizing the speed of network connections (Link speed visualisation)
2. Visualizing the stability of network connections (Link stability visualisation)
3. Visualizing the history of network connections (Link history visualisation)
4. Visualizing the adversary's network structure (ADV wireless network mapping)
5. Linking tactical-technical information directly to the COP system (Specification on-the-fly integration)
6. Visualizing minimum and maximum Area of Effect of units/equipment (Area of Effect)
7. Visualizing Cyber Operations tactical tasks (Task visualisation in CYB domain)
8. Visualizing Electromagnetic Activities tactical tasks (Task visualisation in EM domain)
9. Visualizing the uncertainty around a marker's location in COP system (Approximate unit location visualisation)

The participants of the survey were first asked to indicate how necessary they thought such features would be in their current jobs in the future. The scores were normalized based on the highest scoring use-case to create relative interest ratings shown in Table 14. The weighted averages use the weights assigned to the groups in Table 8. Visualizing minimum and maximum Area of Effect of units/equipment received the highest relative interest rating overall meaning this use-case has

wide appeal. However, among the more experienced users in groups A and B visualizing the stability of network connections was seen as the most valuable feature, thus bringing it to the top of weighted average score board.

Table 14. Relative interest ratings group averages, overall average and weighted average

#	Use-case	Relative interest rating					
		Group A	Group B	Group C	Group D	Overall average	Weighted average
1.	Link stability visualisation	**100,0**	**100,0**	90,8	69,6	97,7	**100,0**
2.	Specification on-the-fly integration	87,5	95,0	97,6	91,3	99,8	96,1
3.	Task visualisation in CYB domain	91,7	90,0	93,5	86,2	97,4	95,3
4.	Area of Effect	87,5	85,0	**100,0**	**100,0**	**100,0**	94,4
5.	ADV wireless network mapping	87,5	90,0	94,5	73,0	93,0	92,3
6.	Link speed visualisation	81,3	**100,0**	90,8	69,6	91,8	91,2
7.	Task visualisation in EM domain	91,7	85,0	83,3	60,9	87,1	89,4
8.	Approximate unit location visualisation	91,7	75,0	90,4	76,1	90,2	89,3
9.	Link history visualisation	81,3	80,0	77,5	65,9	82,4	82,5

Then the participants were asked to prioritize the nine use-cases, the results are shown in Table 15. Linking tactical-technical information directly to the COP system was top priority overall and also after weights had been applied. The popular AoE visualization use-case ranked third overall and fifth by weighted average. Visualizing the stability of network connections that had the highest weighted interest rating only ranked 6th in weighted average priority.

Table 15. Results of prioritization by the survey participants with group averages, overall average and weighted average.

#	Use-case	Priority					
		Group A	Group B	Group C	Group D	Overall average	Weighted average
1.	Specification on-the-fly integration	2	4	3	**1,5**	**2,6**	**2,8**
2.	Link speed visualisation	4,5	2	5	**1,5**	3,3	3,6
3.	Task visualisation in CYB domain	**1**	5	7	6	4,8	3,9
4.	ADV wireless network mapping	6	3	**1**	5	3,8	4,0
5.	Area of Effect	4,5	6,5	2	3,5	4,1	4,5
6.	Link stability visualisation	8	**1**	4	3,5	4,1	4,7
7.	Task visualisation in EM domain	3	8,5	9	8	7,1	6,4
8.	Link history visualisation	9	6,5	6	7	7,1	7,5
9.	Approximate unit location visualisation	7	8,5	8	9	8,1	7,9

5.1.5 Summary of Identify phase

All-in-all three use-cases stand out as both high priority and high interest, they are compared in Table 16. The first of these, linking tactical-technical information directly to the COP system is a purely software development project and can be solved without any understanding of CEMA. Use-cases #2 and #3 rank equally and are both directly tied to CEMA. However visualizing minimum and maximum Area of Effect of units/equipment is more connected to Electronic Warfare and Visualizing the stability of network connections to Cyber Operations. Thus, for this thesis, it makes the most sense to look more closely at **visualizing minimum and maximum Area of Effect of units/equipment**.

Table 16. Comparison of rankings of outstanding use-cases based on relative interest and prioritization.

#	Use-case	Interest		Priority		Result
		Overall	Weighted	Overall	Weighted	
1.	Specification on-the-fly integration	#2	#2	**#1**	**#1**	Most critical
2.	Area of Effect	**#1**	#4	#4-5	#5	Critical
3.	Link stability visualisation	#3	**#1**	#4-5	#6	Critical

5.2 Define and develop

The problem statement was formulated to describe the situation the Electronic Warfare Situation Awareness solution must address. Critical to Quality metrics were defined to specify the requirements and a goal was phrased.

5.2.1 Conclusions of problem analysis

Based on all inputs from literature, experts and Estonian Defence Forces service members, a problem statement was formulated:

Electronic Warfare is not a daily aspect of Estonian Defence Forces operations. Current Electronic Warfare intelligence products do not support achieving level 2 or 3 of Situation Awareness. EDF is at risk of being unprepared to conduct Electromagnetic Activity operations or respond to those threats. However, there is significant interest for improved tools that help visualize plans and operations.

5.2.2 Critical to Quality metrics

Starting to solve the problem stated above begins with creating requirements for a possible solution. These requirements are critical to the quality of any solution. Eight Critical to Quality metrics can be identified from the previous steps shown in Table 17.

Table 17. System requirements Critical to Quality for KOLT micro service

#	Step	Requirement	How?
1.	VoP	Provide context	Highlight effected units, civilians or equipment, describe the effect.
2.	VoP	Predict future events	Alert to possible incoming attacks or adversary's movement.
3.	VoP	Automatic reports	Generate automatic reports to be presented to a commander.
4.	DL	KOLT microservice	AoE value-added products work as an add-on to KOLT and do not burden the main instance running on less powerful tactical systems.
5.	VoC	Visualizing min/ max AoE	Weapons or equipment AoE is visualized on a map as minimum and maximum effective ranges.
6.	VoC	Symbology from APP-6 (D)	Symbology from NATO standard document APP-6 (D) is used
7.	VoE	Propagation modelling	Signal strength is modelled on the specific terrain.
8.	Literature	Fulfils Data Fusion challenges	The solution design fulfils the five grand challenges of Data Fusion

All the requirements above should be satisfied in a product designed to solve the problem. However, this is not an exhaustive list. Some opportunities for improvement were not considered due to design limitations. These are:

1. Feedback from the commander to the field unit to refine operational plans.
2. Automated reporting from field unit to intelligence section to approach near-real-time updates from operational area.

5.2.3 Goal statement

We created a goal statement that is specific, measurable, attainable and relevant. According to our research, a specific microservice developed for the KOLT COP system is necessary. This service must provide context for a commander who is not intimately familiar with EM activities specifics. It must help them comprehend the meaning of what is shown, and project future events based on this understanding, thus achieving level 2 or 3 of Situation Awareness. We could not identify design limitations that would prevent the development of such a service. There is significant interest for this feature, and it is rated as above average priority by both experts and non-experts. The goal can be summarized as such:

Develop a KOLT microservice that supports tactical and operational level commanders and signals specialist to achieve level 2 and 3 Situation Awareness by modelling the propagation of EM fields of Electronic Warfare assets and visualizing the results on a map with description of the expected effect.

5.2.4 Develop

Two mock-ups of value-added products were created to make it easier to develop the microservice (Figure 18 and Figure 19). In the first mock-up we can see an adversary's jamming station with basic specifications attached. Based on the capabilities of the jammer the Area of Effect is calculated using propagation modelling over terrain. The area is two-tiered, with red overlay indicating areas that would be more affected and yellow overlay over areas where the signal strength would be lower. Both friendly units that could be affected are highlighted with an exclamation mark. The operator can click on the exclamation mark to open a callout that gives more context. We can see a friendly mine warfare ship near Prangli island, whose radar system may be at risk. A friendly port installation is shown in Muuga harbour that could be affected. Civilians living in the area of effect may have their mobile devices disrupted. In the case of the anti-air radar platoon, there is also a prediction that if the radar system is jammed it could indicate an imminent air strike. The infantry company to the south, however, is unlikely to be significantly affected and no indicator is displayed. The symbols used to denote nodes of interest are from APP-6 (D).

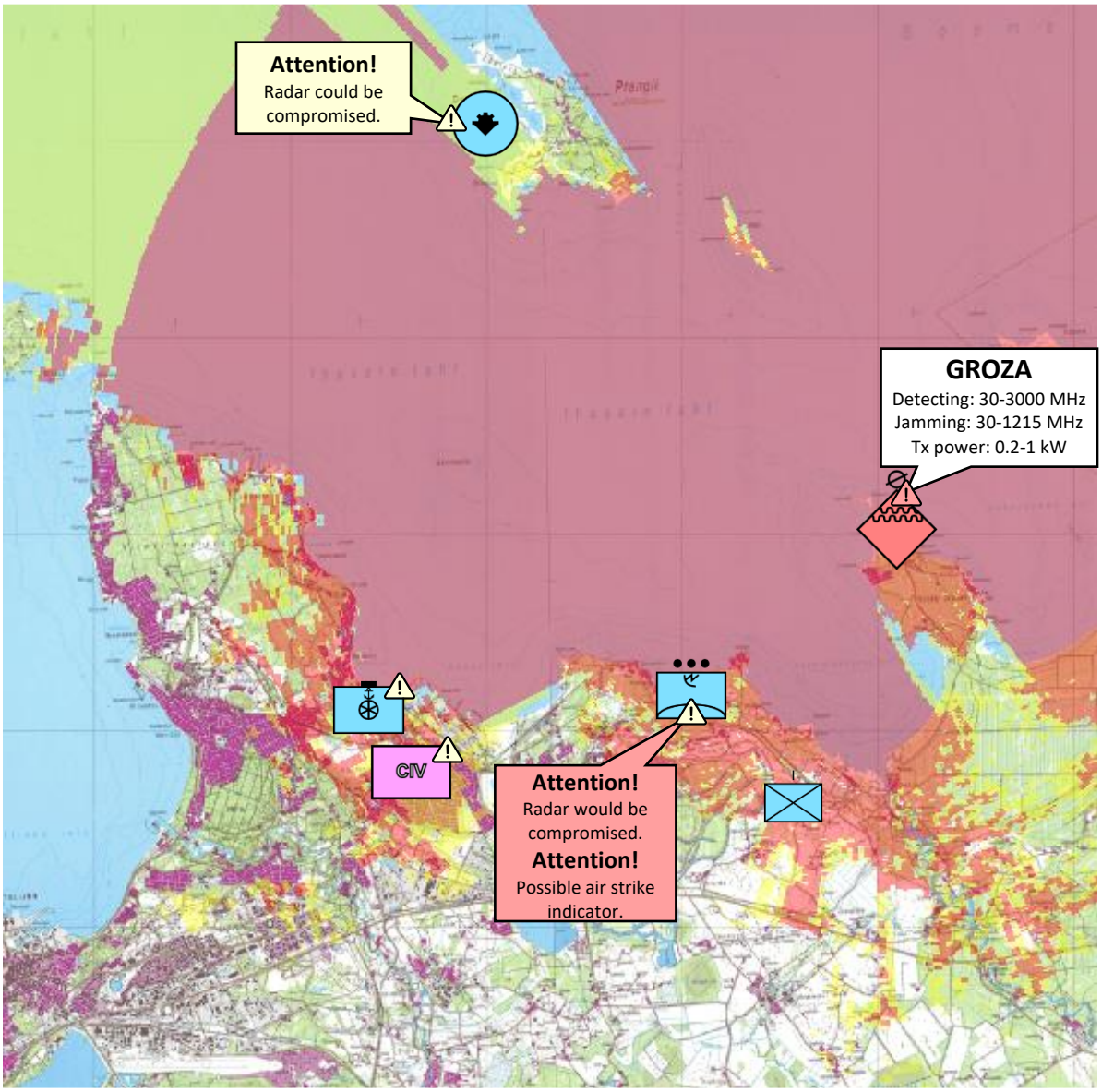


Figure 18. Mock-up of Area of Effect value-added product for a case of jamming

In the second mock-up, two friendly direction finders are set up on high ground near Kambja, in southern Estonia. RF propagation modelling over terrain is used to create coverage analysis and areas where coverage for both direction finders intersect are coloured in to show areas, where adversary units can be detected. Red arrows show how two intersecting bearings can then be used to triangulate the position of a possible adversary unit. Amber arrow indicates a case, where only one direction finder detects a signal and triangulation is not possible.

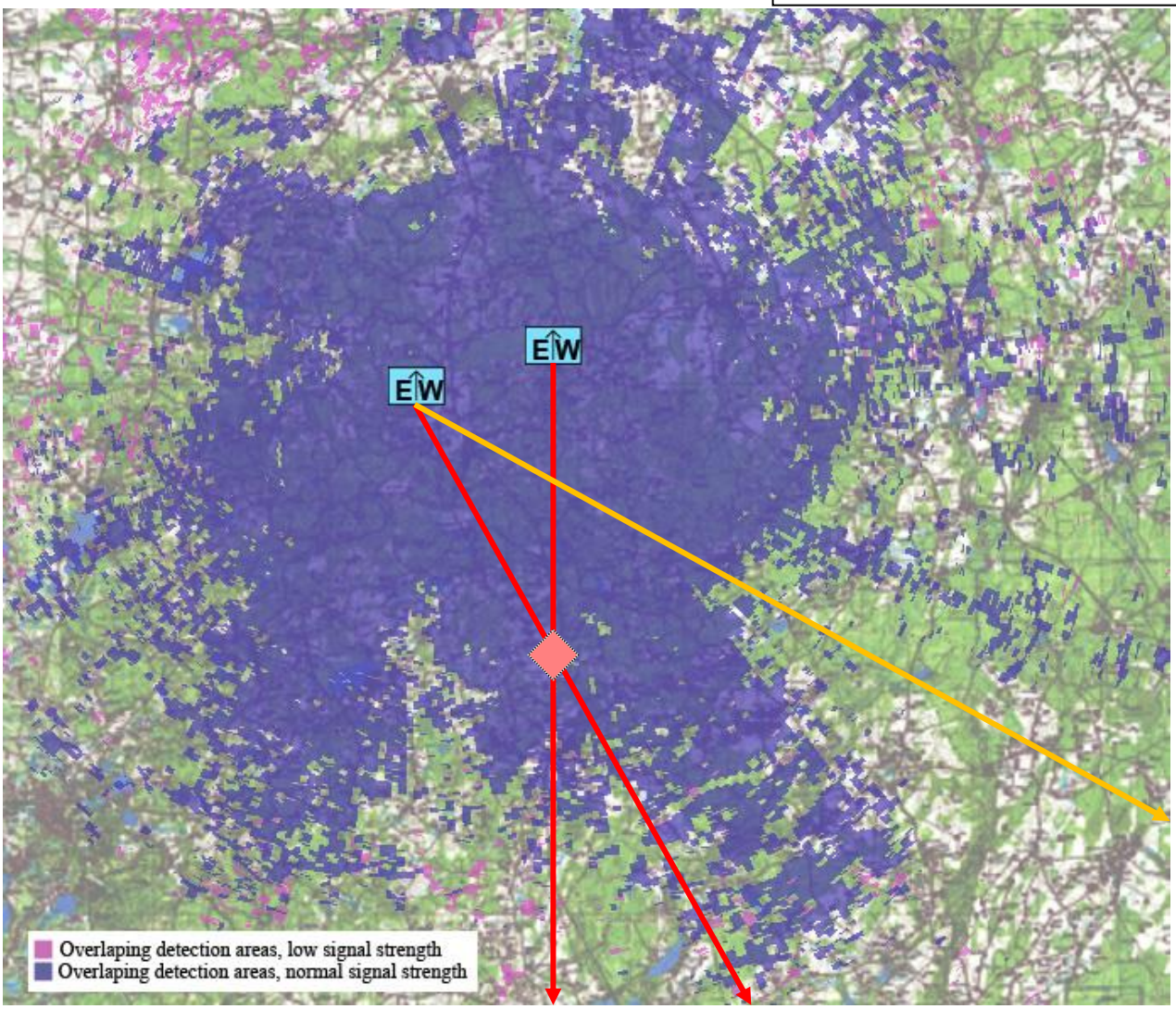


Figure 19. Mock-up of an Area of Effect visualization value-added product for a case of direction finding.

These mock-ups were created using Radio Mobile (https://www.ve2dbe.com/) software for Area of Effect visualization. Radio Mobile uses the Longley-Rice Irregular Terrain propagation model. Space Shuttle Radar Terrain Mapping Mission (SRTM) terrain. VHF band from 30 to 107 MHz with vertical polarization over continental temperate terrain, with surface reflectivity of 301, ground conductivity of 0.0005 S/m and relative ground permittivity of 15 used in the simulations. The map is “Map of Estonia 1:50 000 1997-2000” from Estonia’s Land Board website (https://xgis.maaamet.ee/). The NATO icons are taken from Spatial Illusions Unit Generator

(https://spatialillusions.com/unitgenerator/). The exclamation marks are taken from https://www.flaticon.com/.

A small experiment was conducted to compare predictive models for RF propagation with real world measurements. A jamming signal was broadcast at 446.19 MHz. The signal strength was measured in two directions from the transmitter at 10 m intervals up to 100 m from the transmitter illustrated in Figure 20.

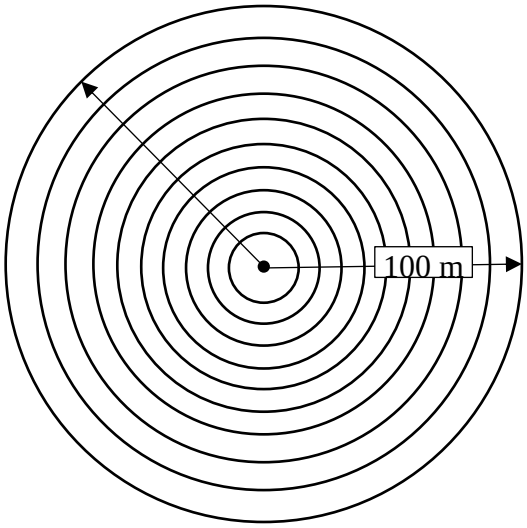


Figure 20. Representation of the measurements taken in two directions at 10 m intervals from the transmitter.

At such close ranges and low frequencies there are no good models to work with. The free space path loss was selected. In order to make the measurements more comparable the difference between distances not absolute values were considered. Direction 1 was completely open and direction 2 was more wooded. The results are shown in Table 18. There are interesting artefacts around 30 to 60 m where the measured signal's strength drops very suddenly and recovers one dB later. The predictions are more accurate further away from the transmitter. The experiment illustrates the problems with relying on predictive modelling and how it can be very inaccurate. Many aspects of RF propagation highlighted in the state-of-the-art review may be behind the anomalies witnessed in the experiment, thus in may be prudent to include some indicators of reliability to Areas of Effect shown in a COP system, based on empirical testing with real equipment.

Table 18. Comparison of measured and theoretical changes in values for a jamming signal at 446.19 MHz.

Distance	Theoretical	Direction 1	Direction 2
10 to 20 m	-6.02 dB	-3 dB	-8,1 dB
20 to 30 m	-3.52 dB	-4 dB	-6,1 dB
30 to 40 m	-2.5 dB	-1,6 dB	**-9,1** dB
40 to 50 m	-1.94 dB	**-10,5** dB	-3,5 dB
50 to 60 m	-1.58 dB	-3,1 dB	+1 dB
60 to 70 m	-1.34 dB	5,6 dB	-4,6 dB
70 to 80 m	-1.16 dB	-1,9 dB	-2,9 dB
80 to 90 m	-1.03 dB	-1,2 dB	-2 dB
90 to 100 m	-0.91 dB	-1,2 dB	-2 dB

6 Summary

By composing this thesis, input to develop an Electronic Warfare display for Estonia's Defence Forces Situation and Battle Awareness system KOLT was produced. Furthermore, gaps in Defence Forces Electronic Warfare Situation Awareness capabilities were highlighted and many avenues for further research were opened. Additionally, criteria and priorities for future developments were described.

Through our research, Situation Awareness as a cognitive state was linked to Electronic Warfare as mastery over the electromagnetic spectrum through the concept of Data Fusion. Enhancing Situation Awareness in the Electronic Warfare domain was inspected. As a result, a significant gap of knowledge in the area of creating valuable displays was identified. Market research showed only a few available products designed to support Situation Awareness for the electromagnetic spectrum. These products seem to be mostly intended for Electronic Warfare experts and, without intuitive user interfaces are not suitable for supporting a tactical commander's ability to project future events.

A Design for Six Sigma framework was chosen as a tool for starting to fill the gap of knowledge. From the framework, the steps of identifying the root causes of problems and defining a comprehensive solution were completed. Through interviews with four Electronic Warfare and Common Operational Picture experts, nine problems for Estonian Defence Forces were identified. Then a sample of 98 active-duty service members was selected and a survey was conducted to prioritize the issues. 39 responses were received and analysed, with the results showing a general need for more training in Electronic Warfare, but also outlining the most critical missing features for Situation Awareness. While three critical issues were identified, one was addressed in detail in this thesis, although most of the problems found during the research merit separate projects. The issue of displaying Areas of Effect for equipment was selected, as it best fit the researcher's profile.

A list of criteria for the solution and a goal statement was formulated as input for Estonian Defence Forces Situation and Battle Awareness System's microservice development. Two mock-ups of value-added products were prepared to visualize, what the service should be capable of.

The results of this thesis show a clear path towards improving displaying Electronic Warfare Situation Awareness in Estonian Defence Forces. Specific requirements were set for one of the missing features, and mock-ups of the service was created for reference. Further research and development should be conducted based on the prioritization of the problems highlighted in this work. There is a clear need and interest for some solutions, including:

1. A manual for bringing Cyber and Electromagnetic Activities together with Estonian Defence Forces doctrine.
2. Developing a service that allows monitoring the health of communication lines across Operational Environment.
3. Compiling a database of tactical-technical specifications for military equipment and making it available in the COP system.

Bibliography

[1] M. D. McNeese, P. M. S., E. S. Connors, J. F. Obieta, I. S. Terrell and a. M. A. Friedenberg, "Multiple Vantage Points of The Common Operational Picture: Supporting International Teamwork," *PROCEEDINGS of the HUMAN FACTORS AND ERGONOMICS SOCIETY 50th ANNUAL MEETING,* vol. 50, no. 3, pp. 467-471, 2006.

[2] D. A. Lambert, "Grand Challenges of Information Fusion," in *Sixth International Conference of Information Fusion, 2003.*, Cairns, QLD, Australia, 2003.

[3] M. R. Endsley, "Towards a Therory of Situation Awareness in Dynamic Systems," *Human Factors Journal,* vol. 1, no. 37, pp. 32-64, 1995.

[4] M. K. Mieczyslaw and M. R. Endsley, "Situation Awareness and Cognitive Modeling," *Intelligent Systems Magazine,* pp. 91-96, May/June 2012.

[5] E. Mõts, Eesti kaitseväe maaväe lahingutegevuse alused, Tartu: Kaitseväe Ühendatud Õppeasutused, 2010.

[6] R. J. Boyd, "The essence of Winning and Losing," 1995.

[7] D. Lambert, "Situations for Situation Awareness," Salisbury, 2001.

[8] G. D. Logan, "Automaticity, resources, and memory: Theoretical controversies and practical implications," *Human Factors,* no. 30, pp. 583-598, 1988.

[9] L. Motus, K. Taveter and V. Dieves, "Modelling Complex System-Of-Systems for Creating Situation Awareness," *IEEE Conference on Cognitive and Computational Aspects of Situation Management,* pp. 168-170, 2018.

[10] H. Bahs¸i, V. Dieves, T. Kangilaski, P. Laud, L. Motus, J. Murumets, I. Ploom, J. Priisalu, M. Seeba, E. Taks, K. Tammel, P. Tammpuu, K. Taveter, A. Trumm, T.-T. Truusa and T. Vihalemm, "Mapping the Information Flows for the Architecture of a Nationwide Situation Awareness System," *IEEE Conference on Cognitive and Computational Aspects of Situation Management,* pp. 152-157, 2019.

[11] D. A. Lambert, "The State Transition Data Fusion Model," in *High-level Information Fusion Management and Systems DEsign,* Boston, Artech House, 2012, pp. 33-79.

[12] European Defence Agency, "Cardinal End Meeting," Łukasiewicz Research Network – Industrial Research Institute for Automation and Measurements PIAP, Brussels, 2013.

[13] C. Cundius and R. Alt, "Real-Time or Near Real-Time? - Towards a Real-Time Assessment Model," in *Thirty Fourth International Conference on Information Systems,* Milan, 2013.

[14] D. A. Lambert, A. Saulwick and K. Trentelman, "Consensus: a Comprehensive Solution to the Grand Challenge of Information Fusion," in *18th International Conference on Information Fusion,* Washington, DC, 2015.

[15] P. Morville, "User Experience Design, Semantic Studios," 21 June 2004. [Online]. Available: http://semanticstudios.com/user_experience_design/. [Accessed 30 March 2021].

[16] Łukasiewicz Research Network, “CARDINAL,” Łukasiewicz Research Network – Industrial Research Institute for Automation and Measurements PIAP, 2021. [Online]. Available: https://piap.pl/en/research-projects/cardinal/. [Accessed 15 April 2021].

[17] R. S. Hager, “Current and future efforts to vary the level of detail for the common operational picture,” Naval Postgraduate School, Monterey, 1997.

[18] Estonian Defence Forces, “Kevadtormil arendavad küberväejuhatuse ajateenijad IT-lahendusi,” 2019. [Online]. Available: https://mil.ee/uudised/kevadtormil-arendavad-kubervaejuhatuse-ajateenijad-it-lahendusi/. [Accessed 22 April 2021].

[19] J. R. J. Coliens, “Theater Battle Management Core System Lessons for Systems Engineers,” *20 IEEE A&E SYSTEMS MAGAZINE,* pp. 15-20, March 2007.

[20] K. Mason, “Enhancing Tactical Situation Awareness,” Edinburgh SA, 2002.

[21] LS telcom, “Defense and Security,” 2021. [Online]. Available: https://www.lstelcom.com/fileadmin/content/lst/marketing/brochures/LS_Brochure_Military_en_web.pdf. [Accessed 3 May 2021].

[22] E. Bamford and M. von Spreckelsen, “Future Command and Control of Electronic Warfare,” *JAPCC Journal,* no. 28, 2019.

[23] Joint Chiefs of Staff, Electronic Warfare, Joint Publication 3-13.1, Washington D.C.: U.S. military, 2012.

[24] NATO, “The 107th NATO Electronic Warfare Advisory Committee (NEWAC) convenes in Brussels,” 26 November 2019. [Online]. Available: https://www.nato.int/cps/en/natolive/news_171280.htm?. [Accessed 20 April 2021].

[25] Department of the Army , Cyber Electromagnetic Activities, Washington, DC: Headquarters, Department of the Army , 2014.

[26] R. Poisel, Introduction to communication electronic warfare systems, London: ARTECH HOUSE, INC, 2002.

[27] E. Bout, V. Loscrì and A. Gallais, “Energy and Distance evaluation for Jamming Attacks,” Prague, 2020.

[28] M. Suchański, P. Kaniewski, R. Matyszkiel and P. Gajewski, “Dynamic Spectrum Management in Legacy Military Communication Systems,” in *Military Communications and Information Technology: A Trusted Cooperation Enabler*, Warsaw , MUT Publishing House, 2012, pp. 151-160.

[29] J. J. Egli, “Radio Propagation above 40 MC over Irregular Terrain,” *Proceedings of the IRE,* vol. 45, no. 10, pp. 1383-1391, 1957.

[30] V-Soft Communications, “Propagation Prediction White Paper,” V-Soft Communications, Olathe, 2014.

[31] I. D. Brown, Radio Mobile An Illustrated Hanbook, Santa Maria: Telecommunications Commission of Colegio de Ingenieros de Chile, 2011.

[32] A. Haljaste, “Lahinguvälja sideolukorra simuleerimine võrkude sidekauguste ja levialade määratlemiseks,” Tallinn Technical University, Tallinn, 2018.

[33] O. Mihailov, “Elektroonilise võitluse võimekus väikeriigis,” Kaitseväe Ühendatud Õppeasutused, Tartu, 2013.

[34] I. Kõiv, “1. Jalaväebrigaadi raadioside kaitsmise võimalikkus sidealase elektroonilise,” Kaitseväe Ühendatud Õppeasutused, Tartu, 2007.

[35] A. Biller, “Raadiojaam Harris RF-5800V-MP segamiskindluse testimine,” Kaitseväe Ühendatud Õppeasutused, Tartu, 2016.

[36] Bright Hub PM, “IDDOV in DFSS (Design for Six Sigma) - The Framework for Product Development,” 29 September 2010. [Online]. Available: https://www.brighthubpm.com/six-sigma/89186-the-iddov-lifecycle-in-design-for-six-sigma-dfss/. [Accessed 4 May 2021].

[37] Estonian Defense Forces, “Õppusel Griffin Lightning harjutatakse regiooni sõjalist kaitset,” 9 March 2021. [Online]. Available: https://mil.ee/uudised/oppusel-griffin-lightning-harjutatakse-regiooni-sojalist-kaitset/. [Accessed 4 May 2021].

Appendix 1 - Non-exclusive licence for reproduction and publication of a graduation thesis

I Haldo-Rait Harro

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Displaying Electronic Warfare Situation Awareness in Estonian Defence Forces, supervised by Toomas Ruuben.
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology after expiration of confidentiality period on 03.05.2026, until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology after expiration of confidentiality period on 03.05.2026, until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

03.05.2021

Appendix 2 – Questionnaire for the survey

Lugupeetud vastaja,

Palun märgista enda valitud vastus trükkides vastavasse kasti „X“ v.a küsimus nr 9, kuhu on vaja vastata kirjutades kasti järjekorra number.
Vastaja nimi:

1. **Kui sageli kasutad järgnevaid termineid enda töös?**
   0 – ei kasuta üldse, 1 – kasutan harva, 2 –kasutan sageli, 3 – kasutan igapäevaselt.

	0	1	2	3
küber domeen				
elektromagnet spekter				
elektrooniline sõjapidamine				
sidevõrk				
operatsiooniala				

2. **Saan õppustel piisava ülevaate lahinguruumis toimuvast, et minu kätte koondunud luureandmeid tõlgendada ja/või valideerida.** 1 – ei nõustu üldse, 2 – pigem ei nõustu, 3 – pigem nõustun, 4 – nõustun täielikult, 0 – ei oska öelda

1	**2**	**3**	**4**	**0**

3. **Hetkel kasutusel olevad tingmärgid rahuldavad minu teenistuslikke vajadusi…**

1 – ei nõustu üldse, 2 – pigem ei nõustu, 3 – pigem nõustun, 4 – nõustun täielikult, 0 – ei oska öelda

	1	2	3	4	0
…küber domeenis					
…elektromagnetilise spektri jälgimisel (monitooring)					
…võimaldavate, ründavate või kaitsvate elektroonilise sõjapidamise tegevuste jaoks (EW)					

4. **Minu teenistusülesannete täitmine oleks lihtsam kui küber- ja elektromagnetspektri tegevuste eeskirjad oleksid detailsemalt dokumenteeritud.** 1 – ei nõustu üldse, 2 – pigem ei nõustu, 3 – pigem nõustun, 4 – nõustun täielikult, 0 – ei oska öelda

1	**2**	**3**	**4**	**0**

5. **Kuivõrd rahuldavad hetkel olemasolevad tööriistad minu vajadusi <u>elektromagnetspektri</u> tegevuste visualiseerimisel?** 1 – ei rahulda üldse, 2 – piirangutega, 3 – rahuldavad vajadused, 4 – võimalusi on üle ootuste, 0 – ei oska öelda.

1	2	3	4	0

6. **Kuivõrd rahuldavad hetkel olemasolevad tööriistad minu vajadusi <u>küber</u> tegevuste visualiseerimisel?** 1 – ei rahulda üldse, 2 – piirangutega, 3 – rahuldavad vajadused, 4 – võimalusi on üle ootuste, 0 – ei oska öelda.

1	2	3	4	0

7. **Kuivõrd on minu praeguste teenistusülesannete täitmisel vajalik vastase sidevõrkude kaardistamine.** 1 – ei ole üldse vajalik, 2 – ei ole eriti vajalik, 3 – on vajalik, 4 –on kriitilise tähtsusega, 0 – ei oska öelda.

1	2	3	4	0

8. **Hinda kui vajalikuks pead nimetatud kasutusvõimaluse olemasolu <u>tulevikus</u>, sinu <u>praeguste</u> teenistusülesannete täitmiseks.** 1 – ei ole üldse vajalik, 2 – ei ole eriti vajalik, 3 – on vajalik, 4 –on kriitilise tähtsusega, 0 – ei oska öelda.

8.1. Side visualiseerimine	1	2	3	4	0
8.2. Näen visualiseeritud kujul sidevõrgu ühenduste kiirust…					
8.2.1. …ainult oma sidevõrgu kohta					
8.2.2. …kogu operatsiooniala ulatuses					
8.3. Näen visualiseeritud kujul sidevõrgu ühenduste järjepidevust…					
8.3.1. …ainult oma sidevõrgu kohta					
8.3.2. …kogu operatsiooniala ulatuses					
8.4. Näen visualiseeritud kujul sideühenduste ajalugu…					
8.4.1. …ainult oma sidevõrgu kohta					
8.4.2. …kogu operatsiooniala ulatuses					
8.5. Näen visualiseeritud kujul kuidas vastane sidet peab					
8.6. Tehnika kujutamine	1	2	3	4	0
8.7. Näen digitaalsel kaardil tehnikat tähistavat tingmärki ja saan sellel ikoonil klikkides taktikalis-tehnilist informatsiooni (sh pilte)					
8.8. Saan digitaalsele kaardile tehnikat tähistavat tingmärki lisades viidata taktikalis-tehnilisele informatsioonile, mis on kasutajale otse kaardilt ligipääsetav					

8.9. Näen visualiseeritud kujul tehnika minimaalset ja maksimaalset mõjuala (laskekaugus, segamisulatus vms.)					
8.10. Eriala tööriistad	1	2	3	4	0
8.11. Näen visualiseeritud lahingtoiminguid küber domeenis					
8.12. Saan kiirvalikust joonistada lahingutoiminguid küber domeenis					
8.13. Näen visualiseeritud lahingtoiminguid elektromagnetspektril					
8.14. Saan kiirvalikust joonistada lahingutoiminguid elektromagnetspektril					
8.15. Näen täpselt teadmata asukohaga üksuse tingmärgi ümber visualiseeritud ala, milles üksus tõenäoliselt asub					
8.16. Saan ise visualiseerida ala, kus võib asuda täpselt teadmata asukohaga üksus					

9. Palun reasta kõik need funktsioonid sinu jaoks olulisuse järjekorras.

Kasutusvõimalus:	**# 1-9**
1) Sidevõrgu ühenduste kiiruste visualiseerimine	
2) Sidevõrgu ühenduste järjepidevuse visualiseerimine	
3) Sideühenduste ajaloo visualiseerimine	
4) Vastase sidevõrgu visualiseerimine	
5) Taktikalis-tehnilise info liidestamine lahinguinfo süsteemi (näiteks KOLT)	
6) Tehnika minimaalset ja maksimaalset mõjuala visualiseerimine	
7) Küber domeeni lahingutoimingute visualiseerimine	
8) Elektromagnetspektril lahingutoimingute visualiseerimine	
9) Hägusa asukohaga üksuse tingmärgi ümber tõenäolise asukoha ala visualiseerimine	

Appendix 3 – Expert's statements affinity diagram