UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Marek Matsalu

The Development of Digital Forensics Workforce Competency on the Example of Estonian Defence League

Master's Thesis (30 ECTS)

Supervisor: Hillar Põldmaa, MSc.
Supervisor: Raimundas Matulevičius, PhD.

Tartu 2019

The Development of Digital Forensics Workforce Competency on the Example of Estonian Defence League

Abstract:

In 03.07.2014 Regulation No. 108 was introduced which regulates the conditions and procedure of the involvement of the Estonian Defence League (EDL) Cyber Defence Unit (CDU) in ensuring cyber security. This means that EDL can be brought in by the Information System Authority, Ministry of Defence or the authorities of its area of government within the scope of either of their tasks e.g. ensuring the continuity of information and communication technology infrastructure and in handling and solving cyber security incidents while applying both active and passive measures. In January 2018 EDL CDU's Digital Evidence Handling Group had to be re-organized and, thus, presented a proposal for internal curriculum in order to further instruct Digital Evidence specialists. While describing the CDU's tasks, it was noted that the CDU's partner institutions / organizations have not mapped out their specialists' current competencies. With this in mind, we set out to create a comprehensive list of needs and constraints (taking into account the community standards of DF) to develop a DF-based competence framework that supports the development of CDU professionals. Hence, we studied the current situation of CDU, their existing training program, and contemplated which features we need to consider and explore for further development. In order to assemble comparable results and to achieve the goal the model had to be able to solve the 5 following tasks: 1. Competency mapping, 2. Goal setting and reassessment, 3. Scheduling the training plan, 4. Accelerating the recruitment process, and 5. Promoting the continuous development of professionals. The framework was developed on the basis of the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), which was revised to meet the needs of DF specialists, including EDL CDU. Additions were supplemented in terms of levels, specialization, and job descriptions. The proposals included the DF limitations and standards introduced in the work, which ultimately resulted in a proposal for a Digital Forensics Competency ontology, EDL CDU structure change, Suggested Instructional Strategies for Digital Forensics Use With Each Level of revised Bloom's Taxonomy, a new DF standard subdivision – Unmanned Systems Forensics, and Digital Forensic Competency Model Framework. The list of tasks and skills were compiled from international certification distribution organizations and curricula, and their focus on DF Specialist Competencies. Mini-Delphi or Estimate-Talk-Estimate (ETE) techniques were applied to evaluate the proposed model. An initial estimation of competencies and priorities were given to the EDL CDU partner institutions for expert advice and evaluation. Considering the feedback, improvements were made to the model and a proposal was put forward to the CDU with a future work plan. In general, the proposed competence framework describes the expected scope of competence of an DF specialist in the EDL CDU to enhance their role as a rapid response team. The framework helps in defining the expected competencies and capabilities of digital forensics in practice and offers guidance to the experts in the choice of specialization. The proposed model takes into account the long-term effect (hire-to-retire). Due to the complexity of the model, the framework has a long implementation phase — the maximum time frame for achieving the full effect for the organization is expected to be 5 years. These proposals were approved by EDL CDU and the proposed plan was first launched in April 2019.

Keywords:

Criminal proceedings, Cyber Crime, permanent education, Cyber security, Information technology. CERCS: S281 - Computer-assisted education, S149 - Criminal proceedings, S280 - permanent education, P170 – Cyber security, Information technology.

Lühikokkuvõte:

03.07.2014 kehtestati Vabariigi Valitsuse määrus nr. 108, mis reguleerib Kaitseliidu kaasamise tingimusi ja korda küberjulgeoleku tagamisel. Seega võivad Kaitseliidu küberkaitse üksuse (KL KKÜ edaspidi KKÜ) kutsuda olukorda toetama erinevad asutused: näiteks Riigi Infosüsteemide amet (RIA), infosüsteemi järelevalveasutus või kaitseministeerium või selle valitsemisala ametiasutused oma ülesannete raames. KKÜ-d saab kaasata info- ja sidetehnoloogia infrastruktuuri järjepidevuse tagamisel, turvaintsidentide kontrollimisel ja lahendamisel, rakendades nii aktiivseid kui passiivseid meetmeid. KKÜ ülesannete kaardistamisel täheldati, et KKÜ partnerasutused / organisatsioonid ei ole kaardistanud oma spetsialistide olemasolevaid pädevusi ja sellele lisaks puudub ülevaade digitaalse ekspertiisi kogukonnas vajaolevatest pädevustest. Leitut arvesse võttes seati ülesandeks vajadustest ja piirangutest (võttes arvesse digitaalse ekspertiisi kogukonda kujudavaid standardeid) ülevaatliku pildi loomine, et töötada välja digitaalse ekspertiisi kompetentsipõhine raamistik, mis toetab KKÜ spetsialistide arendamist palkamisest pensionini. Selleks uurisime KKÜ ja nende olemasolevate koolitusprogrammide hetkeolukorda ning otsustasime milliseid omadusi peab edasise arengu tarbeks uurima ja kaaluma. Võrreldavate tulemuste saamiseks ja eesmärgi täitmiseks pidi koostatav mudel olema suuteline lahendama 5-t järgnevat ülesannet: 1. Oskuste kaardistamine, 2. Eesmärkide seadmine ja ümberhindamine, 3. Koolituskava planeerimine, 4. Värbamisprotsessi kiirendamine ning 5. Spetsialistide kestva arengu soodustamine. Raamistiku väljatöötamiseks võeti aluseks National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework) pädevusraamistik mida parendati digitaalse ekspertiisi spetsialistide, ja käesoleval juhul ka KKÜ, vajadusi silmas pidades. Täiendusi lisati nii tasemete, spetsialiseerumise kui ka ülesannete kirjelduste kujul. Parenduste lisamisel võeti arvesse töös tutvustatud digitaalse ekspertiisi piiranguid ja standardeid, mille lõpptulemusena esitati KKÜ-le Digitaalse Ekspertiisi Pädevuse ontoloogia, KKÜ struktuuri muudatuse ettepanek, soovitatavad õpetamisstrateegiad digitaalse ekspertiisi kasutamiseks (muudetud Bloomi taksonoomia tasemetega), uus digitaalse ekspertiisi standardi alajaotus – Mehitamata Süsteemide ekspertiis ja Digitaalse Ekspertiisi Pädevuse Mudeli Raamistik. Ülesannete ja oskuste loetelu koostati rahvusvaheliselt tunnustatud sertifitseerimis-organisatsioonide ja erialast pädevust pakkuvate õppekavade abil. Kavandatava mudeli hindamiseks kasutati mini-Delphi ehk Estimate-Talk-Estimate (ETE) tehnikat. Esialgne prognoos vajaduste ja prioriteetidega anti KKÜ partnerasutustele saamaks tehtud töö kohta ekspertarvamusi. Kogu tagasisidet silmas pidades tehti mudelisse korrektuurid ja KKÜ-le sai vormistatud ettepanek ühes edasise tööplaaniga. Üldiselt kirjeldab väljapakutud pädevusraamistik KKÜ spetsialistilt oodatavat pädevuse ulatust KKÜ-s, et suurendada nende rolli kiirreageerimisrühmana. Raamistik aitab määratleda digitaalse ekspertiisi eeldatavaid pädevusi ja võimekusi praktikas ning juhendab eksperte spetsialiseerumise valikul. Kavandatud mudeli juures on arvestatud pikaajalise mõjuga (palkamisest pensionini). Tulenevalt mudeli komplekssusest, on raamistikul pikk rakendusfaas – organisatsiooni arengule maksimaalse mõju saavutamiseks on prognoositud ajakava maksimaalselt 5 aastat. Antud ettepanekud on käesolevaks hetkeks KKÜ poolt heaks kiidetud ning planeeritud kava rakendati esmakordselt 2019 aasta aprillikuus.

Võtmesõnad:

Arvuti õpiprogrammide kasutamise metoodika ja pedagoogika, kriminaalõigus ja -protsess, elukestev õpe, küberturvalisus, infotehnoloogia.

CERCS: S149 – kriminaalõigus ja -protsess, S280 – elukestev õpe, P170 – küberturvalisus, infotehnoloogia.

List of Acronyms and Definitions

CCDCOE	NATO Cooperation Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CIRC	Computer Incident Response Capability
CNSS	Committee on National Security Systems
CompTIA	The Computing Technology Industry Association
CSIRT	Computer Security Incident Response Team
DFFID	Digital Forensics Framework for Instruction Design
EASS	Estonian Academy of Security Sciences
EDL CDU	Estonian Defence League Cyber Defence Unit
ENFSI	European Network of Forensic Science Institutes
ENISA	European Union Agency for Network and Information Security
ESI	Electronically Stored Information
FBI	Federal Bureau of Investigation
FE	Functional Exercise
FSE	Full-Scale Exercise
GDPR	General Data Protection Regulation
HDD	Hard disk drive
HMS	Administrative Procedure Act
IoT	Internet of Things
IRT	Incident Response Team
ISACA	Information Systems Audit and Control Association
ISC2	The International Information System Security Certification Consortium
KAPO	Estonian Internal Security Service
KrMS	Code of Criminal Procedure
MoD	Ministry of Defence
MP	Military Police

NCIRC	NATO Computer Incident Response Capability
NICCS	National Initiative for Cyber security Careers and Studies
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OSINT	Open-source Intelligence
RIA	Estonian Information System Authority
RRT	Rapid Reaction Team
SANS	Escal Institute of Advanced Technologies
SERT	Security Emergency Response Team
TalTech	Tallinn University of Technology
TTX	Tabletop Exercise
UT	University of Tartu
VTC	Video Teleconferencing

Contents

1 Introduction

"Digital Forensics (DF) collects, processes, preserves, analyses, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations" (NICCS, 2016). DF as a field of cyber investigation branch is a diverse and fast-paced. This has been a suitable ground for creating off-the-shelf courses from internationally known institutions like SANS, ENISA, CompIT, ISACA, (ISC)2 and Mile2 that provide lectures, materials, trainings, workshops and give out internationally accepted certifications. Most of these courses take place in the United States and United Kingdom however there are courses which take place in Europe. Commonly for the international training audience, are virtual classrooms which are led by online instructors in pre-recorded videos or video teleconferencing (VTC). As these companies have been accredited by National Security Agency (NSA), Committee on National Security Systems (CNSS), NICCS, mapped with National Institute of Standards and Technology (NIST) cyber security workforce framework and also known to be preferred by FBI's (Federal Bureau of Investigation) Tier 1-3[1] trainings and in the United States Navy, Army, Air Force and law enforcement ranks. Highly ranked and wanted certifications means that they have acquired hefty price tags, for example 5 day Certified Digital Forensics Examiner Certification Course price range is 4,000.00 euros and some courses price tag reaching over 6,000.00 euros (Mile2, 2018). Nevertheless these aren't overall educational strategies.

Due to the Estonia's high level of development in the field of information technology we have made our infrastructure and high-tech lifestyle a potential platform for cyber-attacks and –incidents, which has increased the need for experts in this fast-paced evolving branch. According to new 2018 Global Digital suite (Kemp, 2018) of reports, out of 1.31 Million people in Estonia approximately 97% (1.27 Million) Estonia's population use the internet (see Figure 1), in which 88% use it every day, 10% at least once per week and 2% once per month (Kemp, 2018).

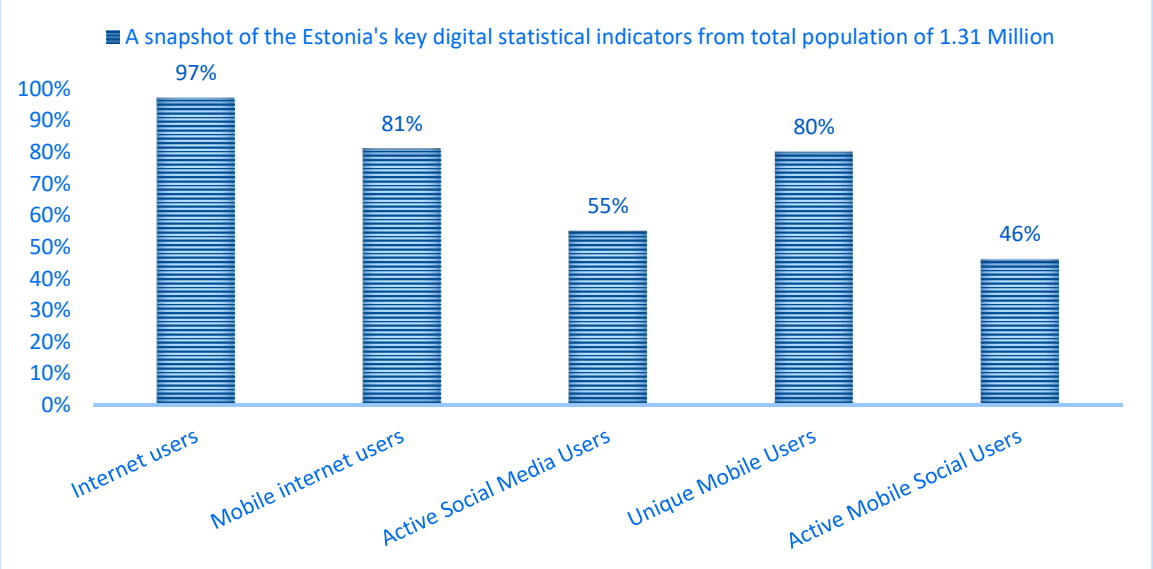

Figure 1 A Snapshot of the Estonia's key digital statistical indicators (Kemp, 2018)

[1] "Approval of the Federal Investigative Standards," signed by the Director of National Intelligence (DNI) as the "Security Executive Agent" and the Acting Director of the Office of Personnel Management (OPM) as the "Suitability Executive Agent." - William Henderson / Jul 23, 2009

It is safe to say that basically 97% (see Figure 2) of all of the adult population currently uses some kind of digital device in their everyday life, be it in e-commerce, managing diary or appointments, checking weather, taking photos or videos, reading book, etc.

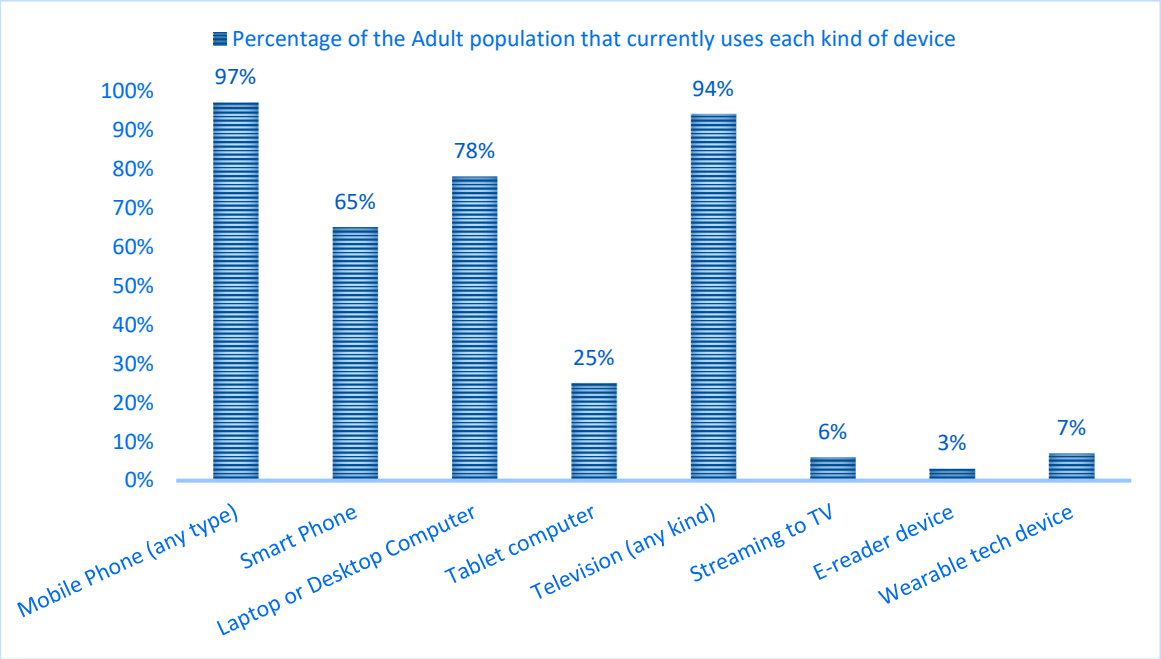

Figure 2 Device Usage in Estonia (Kemp, 2018)

The rapid development of information technology and the high number of smart devices, overall Internet of Things (IoT) and other portable "wearable" electronics leave digital traces that can be linked to suspicious acts. These traces most certainly include location information which in most investigations are key evidences. Formulating these electronic evidence (e-evidence[2] hence forward digital evidence) into presentable form do be decent and understandable enough for both leading investigators and stakeholders to carry out incident and crime investigations and present findings to court of law or other parties. For instances Estonian Academy of Security Sciences does not provide gathering and handling digital evidences courses for Police Officer, Police Service and Internal Security curriculums (EASS, 2018) which are in the forefront in collecting and processing digital evidences. That's why the need for to development of DF workforce competency based model for retaining and training purposes. This DF workforce development roadmap has to be both diverse and agile as technologies and devices that are being examined (Kiper, 2017).

This Master's thesis focuses on combining this understanding and offers an in-depth competency based training and evaluation plan structure that is suitable for EDL CDU Digital Evidence Group. The main research question is "How to create an effective Digital Forensic workforce's competency based (competency structure) development and retainment model for the EDL CDU's staff?"

[2] "Electronic evidence is data stored in electronic form – such as IP addresses, e-mails, photographs, or user names – that is relevant in criminal proceedings. Often, this data is stored by service providers, and law enforcement and judicial authorities have to turn to them to obtain it" (Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017).

1.1 Research Questions

To get better overview we have created research questions which have been divided between chapters. The thesis main research question (**MRQ**) is:

MRQ – How to create an effective Digital Forensic workforce's competency based (competency structure) development and retainment model for the EDL CDU's staff? This question is broken down into several sub-research-questions (**SRQ**):

SRQ1 – What is the current emphasis and constraints of Digital Forensic workforce development and training within the ranks of EDL CDU? We will investigate the existing EDL CDU training program and decide which properties need to be considered for further development. Information will be gathered and modeled using GAP analyses and mini-Delphi method.

SRQ2 – How to develop and retain DF workforce competency in EDL CDU? We will introduce DF workforce competency model, revised DF standard taxonomy (see Annex **Digital Forensic ontology on the example of EDL CDU**) with additions to sub-disciplines (new sub-discipline into DF taxonomy) and proposal for new structural layout for EDL CDU.

SRQ3 – What are the means of validating the workforce competency development model? We will give the reader an overview of the evaluation procedures of the proposed model and remarks given by the leading experts and partner organizations on the DF field of work.

1.2 Research Method

The following research method is applied to provide a sufficient and detailed answer to the main research question (see MRQ in Section Research Questions):

1. State of the art – Investigate and research the existing frameworks and courses available based on the set of knowledge and skills acquired by DF expert.

By looking into different comparisons of Cyber Security based curricular frameworks we decided to continue with selected NICE framework. The decision was based on the frameworks focus on genres and topics – which framework was evenly distributed and if possible focused on DF field, after which we started to map different courses provided by national and international schools/trainers. As the problem statement was introduced to EDL CDU Digital Evidence Handing Group board and discussed with both NCIRC TC and EDF CIRC representatives, it was clear that the need for such a mapping and workforce development tool was justified. We saw, that the state of art had to include binding standards and restrictions of DF, both national and international cases although main focus should be in domestic use.

2. Analyze – Analyze the topics provided by the different courses and map the coherence of teachable topics and knowledge and skills mostly used/needed. We analyzed current EDL CDU workforce training and development plan and compared it to NICE framework and work out a proposal for sustainable model.

In the analysis, we monitored the coherence of training courses offered by training/education institutions with the most common ones and most needed. When mapping, we looked

at the topics of the different course providers, and we presented the mapping results to specialists in the field of DF.

3. Contribution – Propose DF competency based evaluation and training model to be used in the domain of DF. To provide qualitative skill and knowledge baseline through competency-based learning, developed for DF specialist education. Show how reference plan covers different Digital Forensic sub-disciplines and in sidelines, proposing NICE supportive structure model for the EDL CDU (Chapter Proposal for new EDL CDU specialization structure layout).

The full extent of the contribution is not only focusing on the competency framework however in the process of mapping the standards that are shaping todays DF field, we saw the opportunity to give our proposals for revised DF standard taxonomies and suggest them being taken into use for EDL CDU and other establishments as well. The main purpose of these proposals is to standardize DF workforce training opportunities and increase the reliability and efficiency of specialists handling digital evidence.

4. Validation – Assessment of the proposed workforce competency training and development model, while defining the full competencies spectrum of the DF field.

The aim of this research is to determine, on the basis of the sources and experts opinions, which boundaries and skills must be determined and what capacity should be given to organization such as the EDL CDU. To highlight the roles that DF units have to fulfill and eventually provide a Digital Evidence group with a training and management model that would ensure units integrity and reliability in incident management and investigations. The feedback and reviews were focusing on the mini-Delphi method, single round surveys and the feedback was given both by interviews and in written forms and answers represented to research questions are the conclusive reviews of the evaluators. This technique has been adapted for use in face-to-face meetings, and is then called mini-Delphi or Estimate-Talk-Estimate (ETE) Delphi. It differs from the classical Delphi method by the level of rounds of feedbacks and timeframe, as the normal time for tests in classical Delphi method is 30 years, in which period tests are repeated after every 5 years (Crisp, Pelletier, Duffield, Adams, & Nagy, 1997). The reason why we turned for Delphi method was its flexibility, as noted in "The Delphi Method for Graduate Research" by Skulmoski, Hartman and Krahn.

> It is a method for structuring a group communication process to facilitate group problem solving and to structure models (Linstone & Turloff, 1975). The method can also be used as a judgment, decision-aiding or forecasting tool (Rowe & Wright, 1999), and can be applied to program planning and administration (Delbeq, Van de Ven, & Gustafson, 1975). The Delphi method can be used when there is incomplete knowledge about a problem or phenomena (Adler & Ziglio, 1996; Delbeq et al., 1975). The method can be applied to problems that do not lend themselves to precise analytical techniques but rather could benefit from the subjective judgments of individuals on a collective basis (Adler & Ziglio, 1996) and to focus their collective human intelligence on the problem at hand (Linstone & Turloff, 1975). Also, the Delphi is used to investigate what does not yet exist (Czinkota & Ronkainen, 1997; Halal, Kull, & Leffmann, 1997; Skulmoski & Hartman 2002). *(Skulmoski, Hartman, & Krahn, 2007)*

The questions and model were distributed to chosen experts. These experts were chosen both Estonia (e.g. Estonian Police Service, Estonian Forensic Science Institute and other

organizations[3] in Estonia, as well as to private companies and abroad (e.g. NCIRC TC, Canada Armed Forces, USA West Point Military Academy and Naval Academy) and they were given key evaluation questions as well given the opportunity to give their own proposal ideas which are also being taken into account and are being presented in this thesis as conclusive remarks.

Furthermore we would like to provide input for future curriculums and training plans to create and enhance not only EDL CDU but entire DF community e.g. Estonia Police Service specialists or any specialists working in the DF expertise field.

In the next chapter (Chapter 2) we shall give overview of a state of art and setting the standards for DF. This is followed by constraints regarding DF and evidence handling. Chapter 3 describes the contribution – analysing and mapping the EDL CDU Forensic Groups skillset, improve unit's recruitment criteria and help to develop DF competency model. Followed by a proposal for DF group competency model to expert level with the restrictions in mind which have been provided by EDL CDU. Chapter 4 present assessment and validation of proposed workforce competency model and ultimately applying it to EDL CDU Digital Evidence group training. Finally, chapter 5 gives the concluding remarks and presents future works. In the appendix the reader will find proposal for a new structural model for EDL CDU, overview of standards regulating DF field, suggested instructional strategies for digital forensics use with each level of revised Bloom's taxonomy, suggested courses and curriculums, proposal for new DF discipline (unmanned systems forensics) and lastly DF model framework table (see Annex Proposal for Digital Forensic Competency Model Framework based DOL Competency Model).

Disclaimer:

- The views and opinions expressed in this thesis are those of the authors and do not necessarily reflect the official policy or position of any agency named in this thesis. Proposals within this thesis are focused mainly for EDL CDU use, however can be utilized in other agencies as well, if organization or agency personnel management approves it.
- Some names and identifying details have been changed or left out to protect the anonymity of individuals or the agencies/organizations.

[3] The complete list of institutions and persons shall not be made public due to the requirement to remain anonymous.

2 State of the Art

This chapter introduces the state of art for DF educational development and provide an answer to "What is the current emphasis and constraints of DF workforce development and training within the ranks of EDL CDU? (**SRQ1** in Section 1.1). To better answer this question, we break it down into four sub-questions:

1) Which standards are shaping the DF?
2) What are considered properties and emphasis for DF experts in Estonia?
3) What are the DF constraints in the legal space in Estonia?

We will begin by giving overview of the general requirements for DF experts and detailed insight to the characteristics and emphasis shaping the DF educational development. After this, subfields of DF are being looked into detail. Followed by overview of legal constraints regarding the digital evidence handling.

2.1 Background

The EDL according to Colonel Lieutenant Viktor Kalnitski, chief of Viru District, said that the EDL is a voluntary organization intended to contribute to Estonian national defence by supporting national institutions and structures on the basis of a wide broad approach to defence. The Estonian Defence Force's(EDF), the Police and Border Guard Board(PBGB), the Rescue Board and local governments are the main cooperation partners of the EDL. Although there is a willingness to help other national structures: hospitals, schools, etc. (Lamus-Tšistotin, 2018). In 03.07.2014 the Republic of Estonia established Regulation No. 108 (Conditions and procedure for involvement of the Defence League in ensuring cyber security, 2014), which regulates the conditions and procedure of the involvement of the EDL in ensuring Cyber Security. Thus the EDL Cyber Unit can be brought in by the Information System Authority(RIA) or by the Ministry of Defence (MoD) or the authorities of its area of government within the scope of either of their tasks. Since the unit is made up of volunteers with diverse backgrounds of knowledge and skills behind them, they still need ongoing training and deployment in the exercises and on-the-job training. In order to be at the required level, trainings and curricula of the leading certification centers must be taken as the benchmark, and a suitable workforce competency development model must be developed. As there are no right or wrong teaching methods for achieving these goals, we have to look at the scope of DF educational possibilities that are given. With such variety of International courses and complexity of retaining the feedback of how effective the course was and how did the student perform. Assessment cannot be done as "black-and-white" – did the specialist acquire the evidence needed or not, furthermore how did they acquire it and are these still applicable in court of law. We have decided to use European Union Agency for Network and Information Security (ENISA), Escal Institute of Advanced Technologies (SANS), The Computing Technology Industry Association (CompTIA), Mile2, Tallinn University of Technology (TalTech) and University of Tartu (UT), Estonian Academy of Security Sciences (EASS), NATO Cooperation Cyber Defence Centre of Excellence (CCDCOE) and many other curriculums, course materials and research papers (overview of courses suggested are listed in appendix VII). This chapter will be also covering the boundaries and constraints that are set for EDL CDU in providing digital evidence, regarding evidence collection and to be regarded as applicable in the investigations.

Recent study on forensication education done by J. Richard Kiper's "Forensication Education: Towards a Digital Forensics Instructional Framework" identified "the most effective instructional design features for a future entry-level DF course" (Kiper, 2017). The product

of this effort was the Digital Forensics Framework for Instruction Design, a comprehensive DF instructional framework meant to guide the development of future DF. Second most recent framework which was revised in August 2017 was National Initiative for Cyber security Education (NICE) the Cyber security Workforce Framework. The last document serves as a fundamental reference resource for describing and sharing information about cyber security work and the knowledge, skills, and abilities (KSA-s) needed to complete tasks that can strengthen the cyber security posture of an organization – purpose of this framework is to improve communication about how to identify, recruit, develop, and retain cyber security talents (Newhouse, Keith, Scribner, & Witte, 2017). Lastly we have taken the ontological model approach from five layer hierarchical structure specifying areas for certifying and specializing (Brinson, Robinson, & Rogers, 2006). By cultivating these three and comparing outcomes with revised Bloom's Taxonomy the end result will be put in use by EDL CDU by whom the research was ordered. The demarcation of this chapter will be the Standard 008.0 Digital Forensics (008.1- 008.6) version 1.1 written by the Netherlands Register of Court Experts (Nederlands Register Gerechtelijk Deskundigen, NRGD) and Register of Court Experts in Criminal Cases Decree (NRGD, 2018).

2.2 Research Protocol

In this research protocol we will present which properties of the curricular frameworks we consider for our research. What were the used methods of implementation and what were the constraints in our research.

2.2.1 Considered properties

The research is done from a cyber security workforce training and education perspective and thus we are considering the following properties:

1) Competency framework – we are implementing a modified United States of America Department of Labor (DOL) Competency Model Framework (developed by Employment and Training Administration) in the DF workforce perspective and we are layering it with the hierarchical structure from an ontological model. We suggest that these implementations should be included in DF curricular framework by introducing development plan for the future DF workforce. This whole proposal has been made with a direct focus in mind – to propose competency development model for EDL CDU Digital Evidence Group.
2) Knowledge areas – we are mapping and emphasizing topics of the frameworks that are being handled and identifying areas of focus.
3) Skills – we want to know which skills are needed and in which level should be developed and retained to support the workforce development model.
4) Services – we are listing a number of services (e.g. different vendors, universities and organizations) which provide different levels of training and education, supporting the DF workforce development model.
5) Standards – we are mapping the underlying standards that are shaping the DF community.

2.2.2 Scope

The scope of this thesis includes selected platforms of study and considered properties (skills, knowledge and abilities) for EDL CDU members. One of the main tasks of the EDL CDU is to share the knowledge and establish supportive capacities for crisis situations, thus the EDL CDU considers its mission to share their competence and knowledge in the area of information security. Members are not required to possess technical knowledge and skills

although it is beneficial to have basic knowledge in IT, because they will be given the chance to participate in different courses to acquire necessary the skillset. Although the EDL CDU uses four shared knowledge principals (transfer, exchange, collectivism and distribution of knowledge) the correct workforce development or training plan has not yet been drawn up, making it a problem for developing DF workforce inside the ranks. Similar problem was noted in the ranks of NATO Computer Incident Response Capability – Technical Center (NCIRC TC)[4]. PBGB also is facing the same problem with their investigators, who come across digital evidence on a daily basis, hence the need to map the roles and skills for DF specialists, first responders and other roles to start developing an organization wide workforce development plan.

It has to be mentioned that PBGB investigators go through EASS official curriculum, which is financed nationally. On the contrary, however the budget for EDL CDU training is smaller, than for EDF and PBGB counterparts, so the workforce training and educating has been done largely through self-study basis. The current principals for developing EDL CDU course materials have so far been done by taking into account the guidance materials for the development of the curriculum issued by the Archimedes Foundation. The current practice is to share knowledge principals, one member at the time. A unit's member learns a particular skill and then on a common study day it will be shared with others (Põldmaa, 2018). Although it may work to some degree, it is still necessary to draw up a list of roles for the EDL CDU and descriptions of the skills for each role. For example, the core knowledge for a DF specialist should be to know what to do upon first arriving on the site – initial operations at the incident site. This will be mainly focused for first responders, crime scene investigators, evidence collectors as the fundamental skill that everyone should know or be familiar with. Occupational competencies are technical and specific skills that shall be focused on more complicated skillsets, e.g. cloning HDD image, getting a memory dump, Android, iOS, Linux, Win forensics skills, - Administrating Windows and Linux based systems (command line).

2.2.3 Limitations

Today Estonia has taken the position in the forefront of digital and cyber space by applying e-Governance, Government Cloud, I-voting, State e-Services Portal and e-Cabinet and thus making them top of the digital society. On the other hand making them vastly dependant on different communication systems, IoT, smart devices and other forms of digital communication, meaning that every resident in Estonia and now after e-Residency almost everyone around the world will be leaving their mark in cyber space and therefore possibly creating digital evidence. These evidence materials have characteristics like being hidden, not constrained by national borders and jurisdiction, easily tampered and destroyed and sensitive to time factors. Similarly to physical evidence, the digital evidence is being used in any type of court, be it administrative cases, criminal proceedings or even civil matters. Thus the curricular frameworks and competency model should be reviewed and modified accordingly for the purpose of EDL CDU being called upon according to Code of Criminal Procedure (KrMS) § 109[1] as a qualified person. This states that a natural person or in this case specialist may be involved in procedural acts if he or she has specific expertise which is being needed. Many curricular frameworks are being developed and we will be focusing mostly on the use of digital evidence in a Criminal proceedings' context.

[4] By the time that this thesis will be published, the Agency would have made significant progress in development of Talent Management program within its own structures. Changes that were made will not be reflected here.

2.3 Digital Forensics

In this section we will introduce standards that are shaping the DF community and ultimately answering the SRQ1 sub-questions:

1) Which standards are shaping the DF?
2) What are considered properties and emphasis for DF experts in Estonia?
3) What are the DF constraints in the legal space in Estonia?

We will begin by giving overview of the general standards for the DF community to get an insight to the characteristics and emphasis shaping the DF field.

2.3.1 Standards shaping the digital forensics community

On the 1st of January 2010 "Experts in Criminal Cases Act" was put to place in the Netherlands. Its sole purpose was to set legal requirements for the quality, reliability and competence of the experts (Henseler & Loenhout, 2018). In response to this the NRGD held a survey in 2014 amongst leading forensics and justice system experts (NRGD, 2018). The goal was to determine the need to acknowledge DF as a new field of expertise and to create standards for this particular field (Henseler & Loenhout, 2018). The result of this survey strongly suggested that the registration of new standards for the DF's field in the same year was needed. The standard's version 1.0 was fully codified in June 2015 as the 8th field:

1) DNA-analyses and interpretation;
2) Handwriting Examination;
3) Forensic Psychology;
4) Forensic Toxicology;
5) Drugs-analyses and interpretation;
6) Weapons and Ammunition;
7) Forensic Pathology;
8) Digital Forensics (Newly adapted).

This standard is now the basis of assessment for DF experts. The assessment is done by the Advisory Committee for Assessment (ACA) Board which consist of international experts (e.g. Germany, Italy, Netherlands, United Kingdom and South Africa) on the basis of this standard (Henseler & Loenhout, 2018). In 2014 and 2015 the project "Towards European Forensic Standardization through Best Practice Manuals (TEFSBPM)" was coordinated by the European Network of Forensic Science Institutes (ENFSI). The result was the 10 best practice manuals (BPM) one of which was "Forensic Examination of Digital Technology" (ENFSI, 2015). The need for BPMs was supported by the Prevention of and Fight against Crime Program of the European Commission (Security and Safeguarding Liberties - Prevention of and Fight against Crime, 2013). The concept of this was that the BPM's will enhance the quality of forensic services across the Europe and by doing so, encourage forensic standardization and cross-border cooperation (ENFSI, 2015). Cross-border cooperation has been in recent talks in the European Parliament and the Council for building stronger cyber security for the EU (Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017). Due to the complexity of DF being an expertise, the Advisory Committee of Standards (ACS) and the NRGD distinguishes in their standard the following subfields within the field of DF, as it also will be implemented it in our proposal. The expert must stipulate the subfield or fields from at least on one category (see Figure 3) (NRGD, 2018).

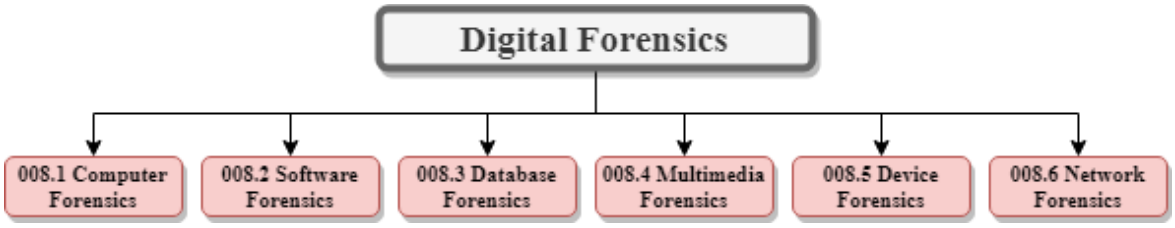

Figure 3 DF subfields (NRGD, 2018)

On the 24th of May 2018 version 1.1 was approved and took effect on the 5th of June 2018, its overall purpose being to ensure the confidence in the forensic expertise for stakeholders[5] (NRGD, 2018).

The development of international standards is important to enhance the reliability, transparency and confidence in collecting and handling evidence. These standards harmonize work practices between agencies and countries in response to cross border investigations. In case of losing or exhausting ones capabilities the support asked can be answered with services which fit to the purpose by the already adapted standards. As stated before by the NRGD, DF is a discipline of forensic sciences and therefore to be reviewed under ISO 21043, ISO 17025, BS 10008 and ISO 27K series, which promotes capturing forensics and investigation of evidence and digital evidence (International Organization for Standardization, 2018).

The goal is to internationally adopt similar if not identical approaches, making it easier for experts all over the world to compare and evaluate investigation finds and also be looked over and understood by different experts on other fields of expertise (International Organization for Standardization, 2018). These standards are not adopted by all local laws, however they provide detailed guidance on digital evidence. Overview of these standards is brought out in Annex Overview of standards regulating Digital Forensic community.

2.3.2 Basics of Digital Forensics

The core activities which each expert of any field of expertise must do is to first collect the evidence, secondly examine the evidence and thirdly do the analyses and write a detailed report. In DF the key procedural activities are all the same. In the first phase correct measures must be taken to validly copy and preserve digital footprints from media devices (e.g. hard drives, random-access memory, etc.). DF expertise in digital material must cover all aspects of digital systems, data entry, export, and processing. Digital information, the so-called digital fingerprint is found on an increasing number of sources such as hardware, software, or a combination of both. In the case of an investigation in a court, an expert must be prepared to answer questions and prove his/her competence in this area and, if necessary, justify how he performed his activities and what gives him the certainty that this certificate has not been tampered with. Every expert should be able to carry out all three core activities (Henseler & Loenhout, 2018).

Data Collection – involves the proceeding of correct methods used for copying, recording and preserving digital materials, thus expertise of various collection methods and software solutions for acquiring the evidence. Equal importance is knowledge of different systems and devices (tablets, smartphones, etc.), where to look for certain type of information. Although before we can start collecting data from the digital material, we have to recover the

[5] All stakeholders in the criminal justice system are involved in the development of quality improvement of expert opinions: the forensic expert and professional organisation, the Public Prosecution Service, judges, defence lawyers, the NRGD, the legislator and the European Commission. All are involved in drawing up quality frameworks for expert opinions. NRGD is only a part of this process (NRGD, 2018).

digital evidence from the actual scene and handle it accordingly. So it is in the vital interest of the investigation that the First Responder (e.g. police officer, evidence collection team, investigator), individuals or teams that in the early stages of an incident are responsible for protecting and preserving the crime scene, property, evidence, and the environment as intact and uncontaminated as possible and securing and documenting all the findings. This means that physical collection is equally important as data collection from these sources. In our case due to lack of manpower collecting may be the role of the EDL CDU forensics team members. Proper collecting can be managed only via correct and disciplined training and experience in evidence collection and preservation – crime scene management. This stage may be the most important and difficult, because if the evidence is tampered with during collecting, finds might end up being removed from the evidence list, thus making the specialists' skills questionable. This is where extra care and training comes into play. The training done for the experts should prepare them to be ready to answer questions relevant to the investigation, which will vary according to the stages of evidence handling (NRGD, 2018).

> *"The following questions - amongst others - are relevant for the data collection phase within the Digital Forensics field of expertise:*
> *1. Is the electronic equipment correctly secured?*
> *2. Is the bypassing of the access code correctly carried out?*
> *3. Is the data correctly safeguarded out of complex infrastructures like industrial control systems?" (NRGD, 2018).*

As collecting is done out there is a correct way of preserving the chain of custody and chain of events leading to the incident and chain of events leading to the discovery of a key proof for the case that would lead to a conviction and to patching up vital security flaws. To make sure that there will be no allegations of evidence being tampered with, the specialist would need to create an MD5[6] hash of the evidence. The MD5 hash can then be used to compare a hash of the original data to the copy. The hash values provide a unique digital fingerprint, which has now been accepted as an example in the Federal Rules of Evidence as a practical means of digital evidence validation. Previously there was the need to call in qualified witnesses and specialists who would have to authenticate ESI, however new FRE Rule 902 makes authentication easier for litigators (Michigan Legal Publishing Ltd., 2017).

> *"(13) Certified Records Generated by an Electronic Process or System. A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).*
> *(14) Certified Data Copied from an Electronic Device, Storage Medium, or File. Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11)" (Michigan Legal Publishing Ltd., 2017).*

Data Examination – involves the investigation, tracing, filtering and evaluation of gathered and extracted hidden evidence without interpreting the resultant findings in the context of the case (NRGD, 2018). Thus, a specialist can create his own experiment in which he intends

[6] message digest 5, is a simple algorithm to implement, and provides a digital „fingerprint" (Rollins, 2018)

to prove which evidence is relevant to this investigation and is eligible in court and ready for further analyses. In this phase the expert will come across volatile evidence, meaning the evidence needs constant power supply for storage. Often digital devices contain information crucial to investigation in the internal memory. It is therefore vital that such devices are charged or kept behind a power source, until the expert has recovered the required information. The volatile data that could be lost upon removal of a device from the power source could have key importance in court cases, that's why it should not be discounted as non-important or non-relevant as it often can be a crucial argument in testimonies (Data Recovery Services Ltd, 2018).

"The following questions - amongst others - are relevant for the data examination phase within the Digital Forensics field of expertise:
1. What data concerning the crime can be found on what exhibit, what is the location of the data and by what means can it be retrieved?
2. Was the data accessible by use of software available to the suspect?
3. Can it be ascertained when the retrieved data has been stored on the data carrier when the data has been accessed, modified and/or changed?
4. In case of deleted information like text messages, photos and videos, has such information been correctly retrieved?
5. Is the exchange of data, captured in a network trace, correctly made visible?" (NRGD, 2018).

Data Analysing – this involves cleaning, remodeling, inspecting and discovering useful information and interpreting them as the evidence which was gathered from digital resources. Analysing should be done on a duplicate copy of the evidence, so that the original would not be tampered with. The experts aim is to give professional review and assessment in which he or she will have to support the decision-making in court hearings (NRGD, 2018).

"Questions relating to reconstruction
1.a. Is digital evidence present on the material to be examined?
1.b. What is the nature of the digital evidence on the material to be examined?
1.c. How did the digital evidence end up on the material to be examined?
These questions are aimed at providing a reliable reconstruction of how digital evidence ended up on the material to be examined. After all, digital evidence can be produced in various ways.
Questions relating to interpretation
2.a. Does the read data match a scenario outlined in advance?
2.b. Given alternative hypotheses, what can you say about the evidence that was found?
2.c. Given the evidence that was found, what can you say about the alternative hypotheses?
Questions aimed at providing a qualitative opinion
3.a. How much knowledge and skill in the field of digital technology is required in order to achieve a particular result?
3.b. Is a particular event or action technically difficult?" (NRGD, 2018).

These questions give a relatively good overview of what a DF specialist is up against in case of being involved in the investigations. We suggest that these questions should be included in training practices for DF specialists on each taken upon case.

2.3.3 Subdivision of Digital Forensics

As stated before, due to the complexity of DF as expertise, we have taken NRGD Digital Forensic Standard 1.1 and detailed ontology for DF disciplines published in 2014 in Journal of forensic sciences to establish and assist the development of professional specialization. The detailed proposal with improved ontology for EDL CDU can be found later in the thesis. The DF is divided into 6 sub-units (Computer, Software, Database, Multimedia, Device and Network forensic) as previously presented in Figure 3.

Computer forensics

Computer forensics uses different methods for pertaining the evidence from desktops, laptops and servers. Search will be carried out after the incident has been happened. Evidence is in most cases stored on the computers' hard drive that also stores operating system's data (e.g. log files) and application/user's data (see Figure 4).

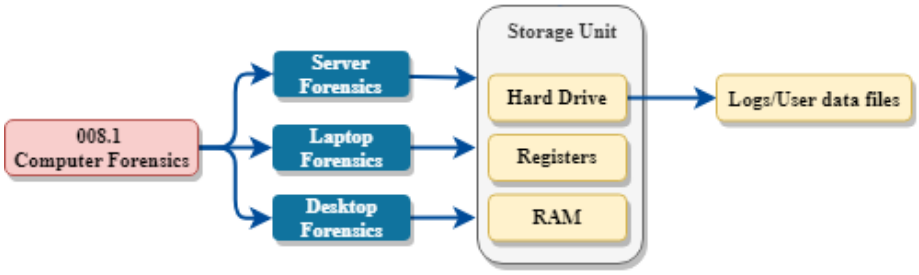

Figure 4 Computer Forensics subfields (NRGD, 2018) (Karie & Venter, 2014)

The Random Access Memory (RAM) investigation and evidence collection must be done as soon as possible, considering of the value of data that may be lost by powering down a device (Karie & Venter, 2014). Collected data is emails, documents, deleted files as well as metadata - nformation about the files, like creation date, when was it last edited, saved or printed.

Software forensics

The goal of software forensics is to examine potential evidence inside a software code. Software forensics covers operation systems, software applications, forensics' tools and malware (see Figure 5). Software forensics (furthermore known as software forensics' engineering) can address other problems, like finding point of failure in software's running critical infrastructure, which can have major effects in case of accidents or incidents[7].

As people have their own linguistic features so does the company or programmer who produces the source code or the architectural design of the software. The code can reflect the so-called generation (by showing the complexity and how and when it was devised) and type or form (functionality). This said the source code can be viewed in forensic viewpoint as well as its counter part, hand writing. This branch primarily focuses on the concerns of discovering potential evidence from a binary code[8] of the software or application, furthermore it is used to test the DF tools. This is for legitimacy purposes, so that the instruments that are being used to retrieve evidence, are valid. The four methods that are being used for source code analyses for determining authorship are Author Discrimination, Identification, Characterization and Intent determination.

[7] July 23 2012 train crash, with over 40 dead in Wnzhou China was caused by railway software failure.
[8] A code whose application results in a code element set whose elements are formed from an alphabetic *[numeric] *[alphanumeric] *[binary] character set. (Institute of the Estonian Language, 2018)

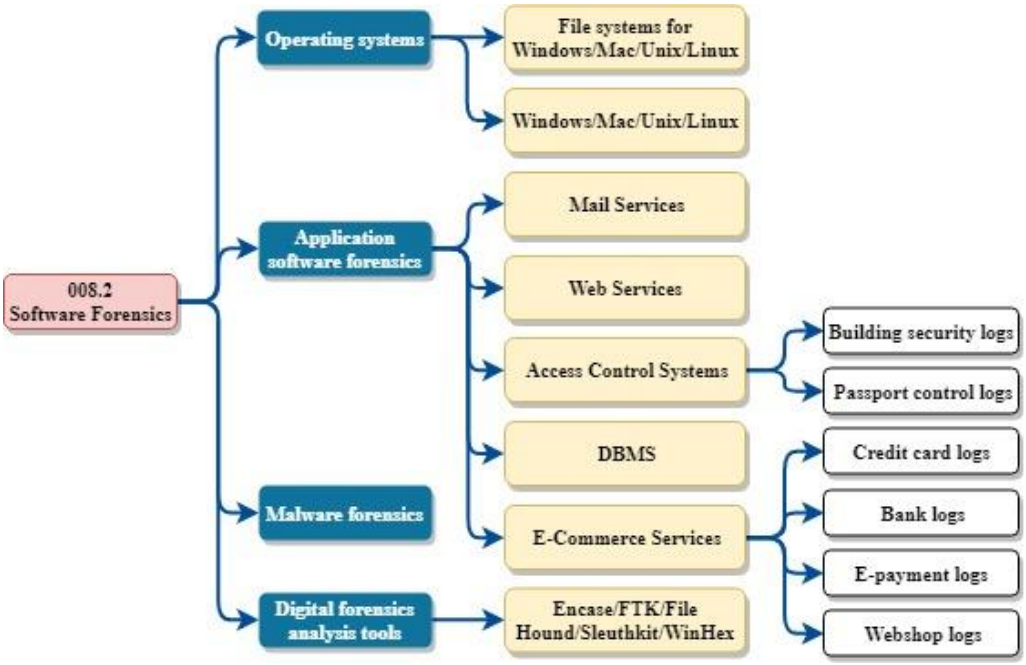

Figure 5 Software Forensics subfields (NRGD, 2018) (Karie & Venter, 2014)

Firstly the Author Identification method is being used for determining the author of a code or a piece of code, if the program was done by multiple authors. In this method it is necessary to have samples from said authors previous works to compare the codes. Secondly the Author Characterization method, which is further more known as profiling, is done by analysing the author's code for characteristics, such as education, personality, cultural and religious beliefs and background. And thirdly Author Intent Determination method, the purpose of which is to determine if software has errors or flaws, whether they have been written for intentional malice or a random error.

Attacks against average digital device users and companies through computer fraud, viruses[9], worms[10], logic bombs[11], trojan horses[12], plagiarism, patent infringements and other intellectual property theft are still active. In 2017 two cases, Cisco v. Arista[13] (Cisco Systems Inc. accused Arista Networks Inc. for allegedly copying the command line interfaces of Cisco software used to manage ethernet switches) and Zenimax v. Oculus[14](Facebook subsidiary Oculus VR Inc. was accused of copying the software architecture of a virtual reality video game publisher ZeniMax Media Inc.), are good examples of court cases where software forensics was put in use.

Database forensics

Servers store massive amounts of sensitive data. Database forensics look at who accessed the database and what actions were performed. Although the figures have been decreasing

[9] A program that propagates itself by modifying other programs to include a possibly changed copy of itself and that is executed when the infected program is invoked. (Institute of the Estonian Language, 2018)
[10] A self-contained program that can propagate itself through data processing systems or computer networks. (Institute of the Estonian Language, 2018)
[11] Malicious logic that causes damage to a data processing system when triggered by some specific system condition. (Institute of the Estonian Language, 2018)
[12] An apparently harmless program containing malicious logic that allows the unauthorized collection, falsification, or destruction of data. (Institute of the Estonian Language, 2018)
[13] Cisco v. Arista, Case No. 5:14-cv-5344-BLF (N.D. Cal. NC)
[14] Zenimax v. Oculus, Case No. 3:16-mc-00098 (N.D. Tex.)

year-by-year, almost 1.4 billion records were exposed in 686 breaches during the first quarter of 2018 which is a big improvement compared to previous years 1442 incidents with over 3.4 billion records exposed. Database forensics is investigating unlawful disclosure, modification and/or thefts of data within a database to track down any perpetrators with such malicious intent (Karie & Venter, 2014). Specialists must search for motives and methods to try to identify suspects. Threat vectors differ from accidental exposes, outside attacks to inside malicious, last being the most likely vector of incident (Risk Placement Services, Inc., 2018).

> "66.9% of incidents and 16.9% percent of exposed records are the result of outsider activity. It is worth noting that the threat vector for one incident exposing over 1 billion records cannot be definitively classified, making the number of records attributed to Unknown unusually high. The most likely vector for the incident is Inside-Malicious" *(Risk Placement Services, Inc., 2018).*

Forensic examination of database involves investigation of the timestamps (meta-data) to verify the actions of a database user (DBMS), transactions information (content) within a database system or application with specific time period in order to identify any fallacious transactions (see Figure 6) (NRGD, 2018).

Figure 6 Database Forensics subfields (NRGD, 2018)

Experts need to be informed in almost all aspects of database development and use. As they come across standard, out of the box, custom-built solutions that cannot be taken to office for analyses.

Multimedia forensics

Multimedia forensics is a perfect example of distrusting the idiom "seeing is believing"[15]. As we need concrete evidence, we cannot trust our eyes anymore because the photographic images, video and audio material have lost their innoscence. With the diffusion of digital media, the validity of photos as witness of a real events has now been lost. Multimedia forensics has to resolve the three categories fields in the DF tree (see Figure 7).

Figure 7 Multimedia Forensics subfields (NRGD, 2018) (Karie & Venter, 2014)

[15] Only physical or concrete evidence is convincing, as in seeing is believing. This idiom was first recorded in this form in 1639.

Alteration of images, videos and audio recordings has been around since photography, film making and sound recording has existed. Retouching, cropping and compiling all these files can be done for many reasons, to improve the aesthetics, to carry out fraud or conceal traces and evidence. This form of investigation has become a fast changing and growing trend. Adoption of smart devices with high bandwidth, larger storage capabilities and a market with large number of new applications and programs which allows new methods of media manipulation, has provided the internet with vast amounts of multimedia content. It has become part of our everyday life and a basic human activity to record videos and take pictures of our daily activities. As we have entered the era of digital lifestyle we are greeted with the rise of fake news in different forms. Social media, fake news sites, video-sharing and streaming sites are full of altered media, causing the visitor of these site to question themselves, what is real and what is not. Today anyone can obtain sophisticated technology which allows an inexperienced user to photoshop to a level in which it is nearly impossible to identify the counterfeited work. Multimedia forensics uses signal processing such as audio, speech, image and video signal processing to identify the source and whether these recordings have been altered or manipulated. For instance in image forensics the image with the use of computer algorithms can show us a specific fingerprint of the device, which the picture was taken with. This fingerprint consist of such properties as systems color sensor, optical system type, etc. All commercially used cameras use metadata tags in their photos. This metadata information is rather simple to be acquired from the image. It allows to determine the mark and model of the device, which was used to take the photograph and even the location where it was taken. However these tags can furthermore be manipulated, however signal processing allows other means to identify the digital acquisition of digital devices (color sensor patterns, sensor imperfections (Dirik & Karakücük, 2014).

Device forensics

Every criminal investigation involves information that can be captured from a digital device, including phones and tablets. To understand what information can be obtained from these devices, as well as how to collect and preserve the information legally is critical. By understanding how wireless and cellular networks operate, and review data and information that can be obtained from these devices, we can build together a solid profile of the user and collect the necessary evidence if needed. Device forensics is divided into six major device groups - peripheral devices, network-enabled devices, storage devices, large-scale devices, small-scale devices, and obscure devices (see Figure 8) (NRGD, 2018) .

Peripheral devices are system expanding devices that range from internal to external peripherals (mouse, keyboard, printer, CD-ROM). Network-enabled devices are network based telecommunication devices such as hubs, routers, wireless access points etc. Storage devices are basically any hardware that can store information (DVD, CD, RFID tags Micro SD cards). Large-scale devices are devices that deal with large (multiple terabyte-sized storage) data sets. Today the border between large scale and average storage device forensics gets distorted because new hard drives become cheaper and it is quite usual to find 2 terabyte hard drives in consumer computers. Small-scale devices are small and versatile handheld devices. The list of small-scale devices is yet to be finalized because of the development of even newer technologies in the age of IoT. Obscure devices are devices that cannot be classified under any of the other disciplines. Some examples of these are camcorders, surveillance cameras (CCTV) and gaming devices (Karie & Venter, 2014). With now over 4 Billion users connected to the internet worldwide as of January 2018 (Central Intelligence Agency, 2018), which is well over half of the world's population and nearly 6 times the devices, approximately 23.14 Billion devices are now online (Columbus, 2016) not to mention offline devices.

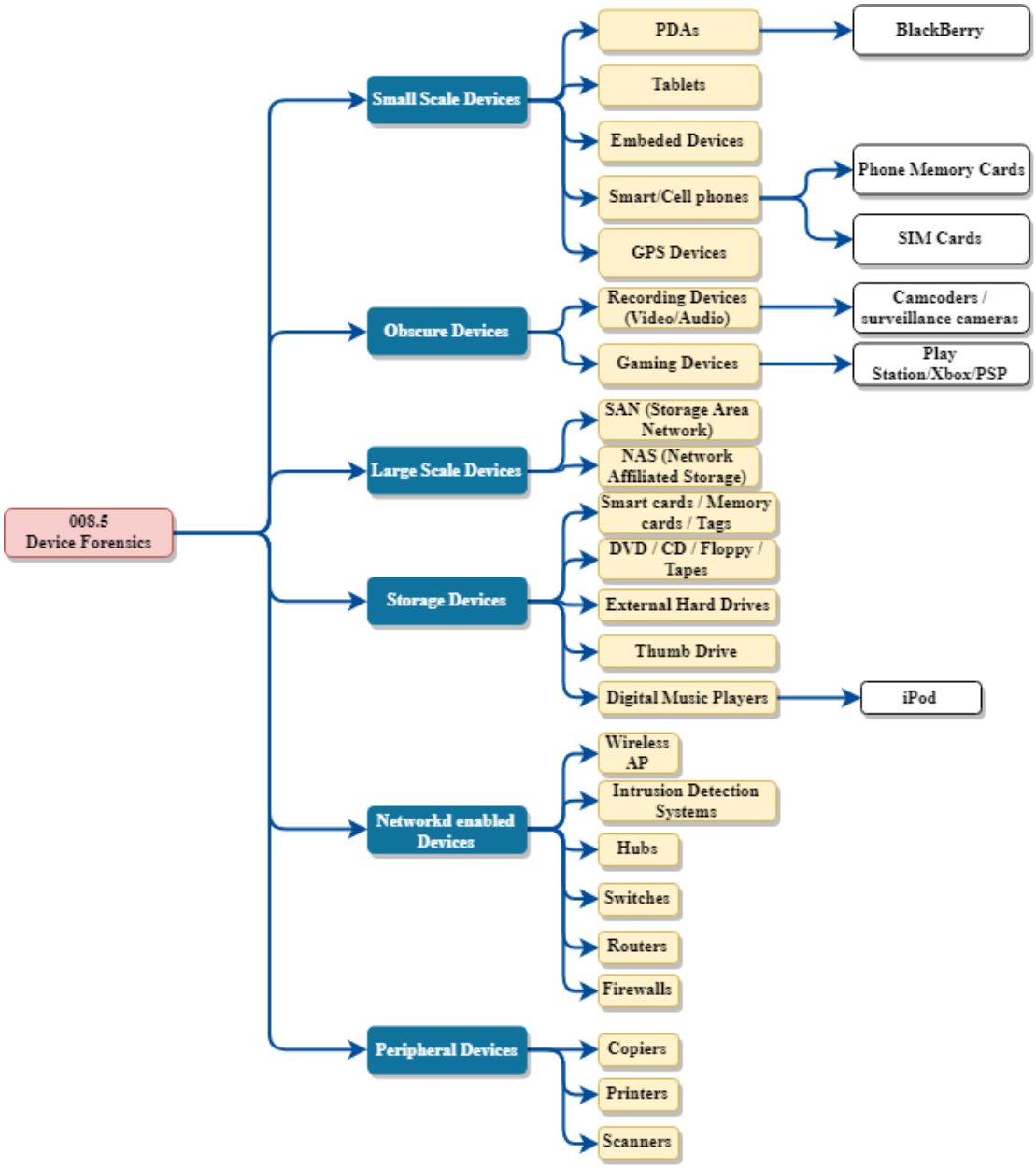

Figure 8 Taxonomy of Device Forensics (NRGD, 2018) (Karie & Venter, 2014)

Digital has become an essential part of our everyday life. We spend an average of 6 hours each day in internet however keep our devices connected and running 24/7. We are using connectivity in almost every aspect of our lives, chatting with friends, finding love on dating apps, playing games, searching product information, keep track of our health and movement habits via smart watches and streaming shows that were missed during being at work etc. For example in January 2018 year-on-year statistical overview showed 4% growth (+218 Million) in unique mobile users world-wide, rising to 5.135 Billion unique mobile users. In Estonia the total population is approximately 1.31 Million and the annual digital growth has been since 1% January 2017 (+11 thousand users) bringing the total of 1.05 Million unique mobile device users (Kemp, 2018) .

Network forensics

Network forensics is a sub-discipline of DF relating to the monitoring and analyses of computer network traffic for the purposes of information gathering, legal evidence, or intrusion

detection (NRGD, 2018). On network we deal with volatile and dynamic information, as traffic can be cut, making it often a pro-active investigation (Yan, 2017). The network traffic evidence might help even if host machine logs have been erased by the attacker, therefore be the only evidence available for forensic analyses (Hjelmvik). Captured network traffic is used for collecting transfered files and searching for keywords from captured communications, by capturing network data via "catch it as you can" and "stop - look - listen" method (Parate & Nirkhi, 2012). All this collection of information like tweets and user / device relationship generated info (log data containing text, images etc.) is called big data. To get the grasp of the shere size of big data, let's try to visualize it, just consider the 2.38 billion people active on Facebook since March 31, 2019. Every 60 seconds on Facebook: 510,000 comments are posted, 293,000 statuses are updated, and 136,000 photos making approximately 300 million photos uploaded every day (Noyes, 2019). These photographs alone comprise over 557.5 billion bits of information, which just microscopic in the world of big data (Jeffers, 2018).

Network forensics is divided into Cloud, Telecom, Internet and Wireless network forensics (see Figure 9).

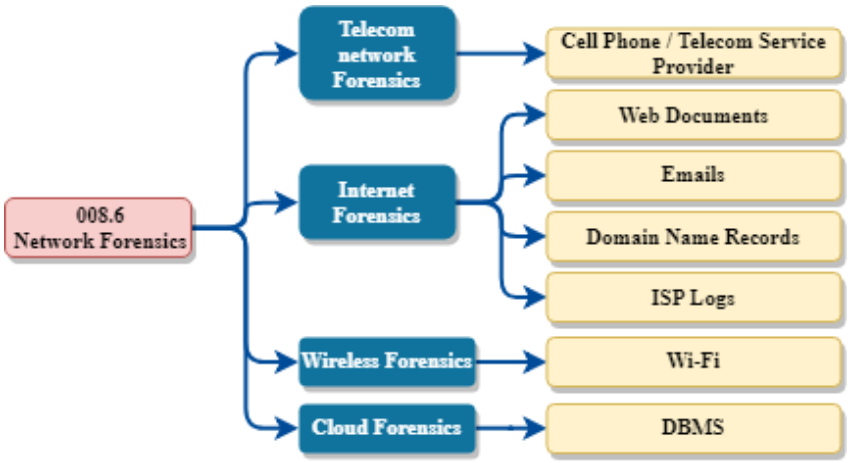

Figure 9 Network Forensics subfields (NRGD, 2018)

Cloud computing is reckoned to be the most radically changing and developing IT service. Telecom network forensics can be summed up basically as "phone tapping", especially now with the widespread in voice-over-IP (VoIP) systems. In Estonia for example, last year 4,596 calls were tapped from Telia Eesti. Although you need to go through a complex process to obtain a court permit for this type of evidence collecting. Estonian government has information acquisition permit. This meaning that security agencies are additionally pursuing our citizens, in fact, without any suspicion of crime, for the reasons of national security. The circumstances for this conduct are state secrets. Furthermore the total volume which this acquisition is taking place is considered as a state secret (Nääs, 2018) . Internet forensics consist of commerce, business information, transactions etc. Internet shops are constantly becoming victims to internet attacks, most notably fraud (e.g. credit card fraud) and identity theft. The goal here is to uncover origins, content, patterns and transmission paths, as well as browser history to extract information that might contain potential evidence. Wireless forensics on other hand tries to capture data which is being exchanged over the wireless network. Evidence here can correspond to plain data or even voice conversations (Karie & Venter, 2014).

2.3.4 General requirements and restrictions for forensics experts in Estonia

The Forensics Examination Act was passed in Estonia on the 30th May 2001, the scope of which was to give a legal status for DF' specialists and forensics' institutions to be regarded as experts in criminal, civil, administrative and misdemeanor proceedings. They will be providing scientific expert opinions on the presented evidence materials. Forensics Examination Act Chapter 1 § 4 states that "an expert is a person who uses non-legal expertise in the forensics examination and legal expertise in cases provided by law" (Forensic Examination Act, 2002). The act further states that forensics' expert can be an officially certified expert or any other person who has been appointed by bodies, who are conducting the proceedings. According to the Act (§ 6), forensics' expert for the EFSI can be anyone who has filled the following criteria:

---

1) *Has to have active legal capacity;*
2) *Has to be proficient in Estonian to the extent established by law or on the basis of an Act;*
3) *Has acquired higher education required in his or her field of expertise in an institution of higher education of the Republic of Estonia or if the person's education corresponds to the said level;*
4) *If the person has acquired a foreign professional qualification, they may be employed as forensics' experts if their professional qualification is recognized by the Estonian Forensic Science Institute;*
5) *Has been employed in his or her field of expertise in forensics' or research institution or in another position for at least two years immediately prior to commencing employment as a forensics' expert (Forensic Examination Act, 2002).*

Restrictive circumstances, that do not allow person to be forensics' expert, are:

---

1) *Conviction of in intentionally committed criminal offence;*
2) *Punished under misdemeanor procedure for a violation of the Anti-corruption Act;*
3) *Has a close blood relationship (grandparent, parent, brother, sister, child or grandchild) or a relationship by marriage (spouse, spouse's parent, brother, sister or child) with the employee who has direct control over the corresponding position or with the immediate superior;*
4) *State of health prohibits him or her to work as a forensics' expert. Medical committee shall determine the person's state of health (Forensic Examination Act, 2002).*

The restrictions provided in the second clauses under "1) and 2) of this section do not extend to persons whose punishment data has been expunged from the punishment register pursuant to the Punishment Register Act" (Forensic Examination Act, 2002). As of the EFSI, EDF, EDL, RIA and PBGB peronnel have to go through a rigorous background check which all have to give their consent for. Under the virtue of office, the likelihood for an expert to obtain the right to gain access to state secrets or to classified information of foreign states is very probable. This means that a clean background and reputation comes a long way.

2.3.5 National legal constraints

According to G. Raudsepp Estonian legislation has not implemented any regulation for digital evidence in specific, which means, the use of digital evidence is regulated by the general provisions found in KrMS (Raudsepp, 2018). Under the Prosecutor's Office Act (ProkS) §

1 prosecutor's office is a government agency within the Ministry of Justice which is involved in planning the surveillance necessary to detect and prevent criminal offences, conducting pre-trial criminal procedures and ensuring the legality and effectiveness, representing the state prosecution and performing other duties assigned to the prosecutor's office by law (Prosecutor's Office Act, 1998). Referring to the obligation resulting from mentioned law suggests to KrMS § 211 which states that the objective of a pre-trial procedures is to collect evidentiary information, create other conditions necessary for court procedures and ascertain the facts and evidence vindicating or accusing the suspect or accused. The same act additionally inclines the Prosecutors office to involve supervising surveillance institutions and, if necessary, conducting procedural steps (Code of Criminal Procedure, 2004). G. Raudsepp stated, that there is no regulation in Estonia at the research institution level which focuses on specifically on digital evidence collection, investigation and the training DF workforce. (Raudsepp, 2018)

According to EDF LEGAD the evidence hence digital evidence can be viewed under KrMS § 124 to be any information or object which have been acknowledged by a competent investigation body. Problem which we noted is that under the KrMS § 31, the only competent investigative body in National Defence sector is military police (MP) (Code of Criminal Procedure, 2004). If MP conducts investigation which has digital evidence they don't have any legal authority signed and the same goes for EDF CIRC, although these units have capabilities to conduct investigative procedures over digital evidence. In criminal proceedings, court evidence is available that is collected in accordance with the provisions of the KrMS. Evidence in a civil matter are described and provided in Part 5 of the Code of Civil Procedure act (TsMS), however there are no specific requirements for the form or collection of evidence. Evidence to use in administrative proceedings, including disciplinary proceedings, is in accordance with the Administrative Procedure Act (HMS). In principle, there is no distinction in civil procedure. Although a disciplinary procedure is called a disciplinary offense, the requirements of an administrative procedure, and not the requirements of a criminal procedure apply. International co-operation is governed by EU regulations (see chapter International legal constraints). Most stringent rules are of criminal procedures, although in this case the proceedings (the investigator) the obligation to comply with the gathering of evidence and the proper formatting rules. According to EDF legal advisor (LEGAD) there is no need to use any regulation to interact with the authorities (Lehtla, 2018). All the institutions under the same legislative power forming a single country, among which there are shared different competences for effective functioning, like the different limbs of a person make up one body. One hand of man does not have to work with another hand to cooperate with one another to grab the object that is seen by the eyes. Currently, the legal service is in constant contact with the Estonian Internal Security Service (KAPO) in a criminal proceeding, and (Code of Criminal Procedure, 2004) responsible for issuing and formalizing evidence according to the investigator's inquiries.

Digital evidence handling, if an entity (in this case EDL CDU) receives the right of an investigative body, criminal training courses must be completed, in which both theoretical and practical collection of evidence is to be completed. If the research institution does not have a status, then internal procedure should be used for handling digital evidence. If the investigation touches upon state or foreign secrets, then guidelines for the protection of state secrets must be used. If the information has become evidence, in accordance with KrMS § 125 (3), the holder of the certificate ensures its inviolability and preservation. All processing requirements for specific information are valid. In the case of KrMS operations, competence must be monitored. For example, pursuit actions may only be carried out by an investigative body with the permission of the Prosecutor's Office or a preliminary investigating judge (KrMS

§ 126^2 and of the EDF Organisation Act § 41^2). Administrative procedure is initiated on the initiative of the administrative body, then from the notification of the person about the procedure (KrMS § 35 (1) 2) of the HMS. Civil procedure is in equal relationship between the two parties. The specificity of the administrative procedure is that in the administrative relationship the EDF is in the position of power and criminal proceeding is being stated as initiated by making the first procedural act (KrMS §193). It is possible to share one procedure between different authorities. Depending on the type of procedure, the procedure for formalization must be followed. One type of procedure does not go beyond the second. The administrative procedure starts in isolation, the criminal proceedings begin in their own right, and the beginning of civil proceedings may furthermore be earlier than a written agreement, perhaps already pre-contractual negotiations are civil relations, which may lead to rights and obligations (Lehtla, 2018).

2.3.6 International legal constraints

International legal constraints that deny or allow the acquisition of digital evidence are the same as for physical evidence. International agreements give the state the opportunity to fight crime in the best possible way. This meaning that its contractors additionally agree on effective cooperation mechanisms in the area of criminal justice that will allow fast delivery of the data they need. One of these mechanisms is the European Convention on Mutual Assistance in Criminal Matters. Under Article 1 the obligated parties shall provide each other with comprehensive mutual assistance in criminal matters in which the punishment falls within the competence of the judicial authorities of the requesting party at the time of application for assistance[16]. In addition, Estonia has transnational law cooperation agreements are divided into two separate groups by nature. Firstly there are national legal cooperation agreements in criminal matters, i.e. Estonia and Finland, and Estonia and the United States. And secondly there are legal aid agreements. These regulate international communication (Estonia – Ukraine[17], Estonia – Latvia and Lithuania[18]) in both criminal and civil law matters. (Luuk, 2017)

Cyberspace is by nature very difficult to pinpoint. Expert who is conducting the investigation and acquiring evidence, ask himself, whether the data is in regional state, allies, neutral for foes territory. If it falls out of national borders, then international element in criminal proceedings steps in. The need for international instruments of cooperation are needed. Investigation of cyber-attacks is not generally possible without international cooperation. Many countries have resolved the cross-border data retrieval issues differently. For example, the United States, Belgium and Portugal have taken steps to give them power, which gives them the right to issue searches and investigation on cases where the physical location of the computer is unknown. Most notable example is Portugal, who has taken the liberty to look at data from servers in other territories. And then there are countries where this area of jurisdictional expertise has been not regulated at all, only with the general clause, so that criminal proceedings will be enforced in their own national territory. As legal practice has shown, the reliability of a digital evidence is harder to prove in court due to its nature. The material is often technical and the investigator, prosecutor and furthermore the court needs some help examining digital evidence. This brings us back to training and educating every instance of personnel who deal with digital evidence.

[16] European Convention on Mutual Assistance in Criminal Matters; RT II 1997, 7, 36
[17] Agreement between the Republic of Estonia and Ukraine on Legal Assistance and Legal Relations in Civil and Criminal Matters. - RT II 1995, 13, 63
[18] Agreement on Legal Assistance and Legal Relations between the Republic of Estonia, the Republic of Lithuania and the Republic of Latvia. - RT II 1993, 6, 5

2.4 Chapter Summary

In this chapter we specified the reviewed state of the art for DF educational development. This needs to provide an answer to research question "What is the current emphasis and constraints of DF workforce development and training within the ranks of EDL CDU? (**SRQ1** in Section Research Questions). To answer this question, we broke it down into four sub-questions:

What are considered properties and emphasis for DF experts in Estonia? – Author reviewed the Forensic Examination Act and confirmed DF expert or any other person who has been appointed by bodies conducting the investigation and proceedings can be officially certified. One of such bodies is EFSI, which have stated criterias that must be fulfilled to be a DF expert. The person has to have active legal capacity; has to be proficient in Estonian; has acquired higher education or professional qualification required in his or her field of expertise, which has to be recognized by the Estonian Forensic Science Institute; and finally has to be employed in his or her field of expertise in a forensics' or research institution or in another position for at least two years immediately prior to commencing employment as a forensics' expert (Forensic Examination Act, 2002). The emphasis on core principle activities which each DF expert must know are Data Collection, Data Examination and Data Analyses.

Which standards are shaping the DF? – DF as expertise has been dictated by the Netherlands Advisory Committee of Standards (ACS) and the NRGD that DF would be divided into 6 subfields (Computer Forensics, Software Forensics, Database Forensics, Multimedia Forensics, Device Forensics and Network Forensics). By the NRGD, the DF is a discipline of forensic sciences and therefore should be reviewed under ISO standards. Author has mapped a list of ISO standards which are connected to DF in some form (overview can be see Annex Overview of standards regulating Digital Forensic community).

What are the DF constraints in the legal space in Estonia? – Mainly legal constraints can be divided into two sub-categories a) National and b) International constraints. Firstly, nationally the main working legal acts are Prosecutor's Office Act RT I 1998, 41, 625 and Code of Criminal Procedure (KrMS) RT I 2003, 27, 166, which states that objective of pretrial procedure is to collect evidentiary information can be done by competent investigative body, in which case problem arises in KrMS. Under KrMS act the only competent investigative body in National Defence sector is Military Police. Although EDL CDU can be called upon according to Code of Criminal Procedure (KrMS) § 109^1 as a qualified person in which case the specialist will be going through evaluation by the Prosecutor's Office.

3 Contribution

This chapter describes the contribution of this thesis and provides answers to the research question "How to develop and retain DF's workforce competency in EDL CDU?" (SRQ2 in Section Research Questions) and proposes a DF's workforce competency model(see Annex Proposal for Digital Forensic Competency Model Framework based DOL Competency Model), revised DF standard taxonomy (see Annex **Digital Forensic ontology on the example of EDL CDU**) with additions to sub-disciplines (new sub-discipline into DF taxonomy, see Annex Proposal for new Digital Forensic discipline – Unmanned Systems) and proposal for new structural layout for EDL CDU(see Annex EDL CDU structure plan after NICE Framework implementation to Digital Evidence Handling Group structure and Annex EDL CDU structure plan after implemented NICE Framework Component relationship).

How to enhance DF's education, training and workforce development in EDL CDU? The Institute of Information Security Professionals (IISP), the Joint Task Force on Cyber security (JTF), the National Initiative for Cyber security Education (NICE) and the National Cyber Security Centre (NCSC) – are frameworks that agree on an overall set of topics within the cyber security field, but they differ on the emphasis of the topics (Hallett, Larson, & Rashid, 2018). By mapping topics and knowledge units onto the Cyber security Body of Knowledge (CyBOK) guide, the four previously mentioned frameworks showed that although all four frameworks cover a range of social, technical and legal themes, they have different aims (Newhouse, Keith, Scribner, & Witte, 2017). For example the IISP Framework aims to define what knowledge experts need to work in cyber security, whilst the NCSC framework offers academic degree pathways for cyber security and DF to already on the field experts via a Certified Master's programs (NCSC, 2019). The NICE Framework aims to categorize and describe the tasks and skills needed to do cyber security, in our case DF jobs focusing on the training and competency progression which is making it the most suitable for EDL CDU workforce training and developing management. Although the JTF Curriculum is basically a combination of mixed curricular guidances for academic institutions, it aims to lead a resource of comprehensive cyber security curricular content for global academic institutions seeking to develop a broad range of cyber security offerings at the postsecondary level (Hallett, Larson, & Rashid, 2018). We welcome the NIST program by adapting NICE mission of "coordinating with government, academic, and industry partners to build on existing successful programs to increase the number of skilled cyber security professionals helping to keep our nation secure" (NICCS, 2016). NICE is committed to cultivating an integrated cyber security workforce that is globally competitive from hire to retire and prepared to protect organization or a nation from existing and emerging cyber security challenges (Newhouse, Keith, Scribner, & Witte, 2017).

3.1 Documenting the Current state of EDL CDU Digital Evidence Handling Group

In this section we will give an overview of the EDL CDU and ultimately answering the SRQ1 sub-questions:

1) How is the current EDL CDU shaped?

Firstly, to understand the current situation, we contacted the EDL CDU Digital Evidence Handling Group's chief of command – Hillar Põldmaa and to get an overview of the structure and level of training. The structural change of the EDL CDU took place in 2015, where the Tallinn 1-4 or "forensics" group was created. Since then there have been attempts to

work out its necessary level of knowledge, training plan and a recruitment policy though the results have not met the EDL CDU needs (Põldmaa, 2018). As the unit will be involved in ensuring the continuity of the information and communication technology infrastructure, in controlling and solving security incidents through active and passive measures, the skillset that the members must obtain may include security testing for information and communication technology solutions, monitoring and analysing digital information and analysing spyware, malware and computer viruses (Conditions and procedure for involvement of the Defence League in ensuring cyber security, 2014). The EDL CDU may be used for exercise purposes and in actual investigation proceedings, but it consists of volunteers who also have to fulfil their roles in their daily jobs. Consequently, there is a need for a DF's workforce competency development plan that supports continuous professional development and training in order to maintain the competence of professionals in finding and handling digital evidence, in order to support investigations and to provide valid evidence for the necessary partners.

EDL CDU itself is a voluntary organization unit aimed to protect Estonian cyberspace. Their main mission is to protect Estonia's information infrastructure and support broader national defence. By which EDL CDU has stated following objectives (The Estonian Defence League, 2018):

1) *Cooperation development among qualified volunteer IT specialists;*
2) *Raising the level of cyber security for critical information infrastructure through the dissemination of knowledge and training;*
3) *Creating a network which facilitates public private partnership and enhances preparedness in operating during a crisis situation;*
4) *Education and training in information security;*
5) *Participation in international cyber security training events (The Estonian Defence League, 2018).*

The EDL CDU consists of patriotic individuals with IT skills and experienced specialists in key nationally critical cyber security positions and in other fields concerning cyber security (The Estonian Defence League, 2018). In time technology continues to advance and majority of business and pleasure tends to move into cyber space, especially in Estonia as we have become world's most pre-eminent e-state:

> *"In just 20 years, Estonia has become one of the most wired and technologically advanced countries in the world – a true digital society. With internet access declared a human right, some of the fastest broadband speeds in the world widely available all across the country, and digital public services embedded into the daily lives of individuals and organisations, the country is now commonly called e-Estonia" (Tambur, 2018).*

That would naturally lead to massive increase in cyber-crimes such as hacking into business and private networks, credit card thefts and as past years have showed in both frequency and severity – ransomware attacks. WannaCry, NotPetya and Locky which cost international businesses billions – estimated damages were 325 million in 2015, 5 billion in 2017 and predicament of 11.5 billion dollars in 2019 (Morgan, 2018). From 2015 to 2017 the increase was 15 times, in which did ransomware also reach Estonia (Pau, 2017). Thus we added a whole new category in Software Forensics taxonomy under the Malware subdivi-

sion. The exponential growth of cyber-crimes leads to digital evidence in DF's investigations and for specialists to change and adapt with those changes, both training and practice in mind. Forensic' community has noted that in the coming years the "legal community must be prepared to deal with an increase of digital evidence in both volume and complexity" (Henseler & Loenhout, 2018).

3.1.1 Principle of operation in EDL CDU

Since the EDL CDU is involved in PBGB, RIA CERT, EDF and many others core roles, the functions of the members should be compared to ENISA CSIRT roles. Members of the team should be prepared to be regarded as expert witnesses or qualified personell in court hearings. CSIRT is known to have various abbreviations used for the same sort of teams (in Europe it is being used predominantly as the protected term CERT), furthermore known as:

- CERT or CERT/CC (Computer Emergency Response Team / Coordination Center)
- CSIRT (Computer Security Incident Response Team)
- IRT (Incident Response Team)
- CIRT (Computer Incident Response Team)
- SERT (Security Emergency Response Team)

As EDL CDU has been accepted in supporting these establishments, they must be able to fulfill their key functions, which are:

1) Mitigating and preventing major incidents and helping to protect' valuable assets of the organizations;
2) to have a centralized coordination for IT security issues within the organization (Point of Contact);
3) to have a centralized and specialized handling of and response to IT incidents;
4) to have the expertise at hand to support and assist the users to quickly recover from security incidents;
5) to help to deal with legal issues and preserving the evidence in the event of a lawsuit;
6) to keep track of developments in the security field;
7) stimulate cooperation within the constituency on IT security (Bronk, Thorbruegge, & Hakkaja, 2006).

We are using CSIRT roles as a prerequisite for EDL CDU members and have composed a comparable table with skills, tasks and possible training options brought out for better insight (Põldmaa, 2018). As mentioned before one of the main tasks of the EDL CDU is to share the knowledge and establish a supportive capacities for crisis situations, thus the EDL CDU considers its mission to share their competence and knowledge in the area of information security. Their training principle is that the members are not required to possess technical knowledge and skills although it is beneficial to have a baseline of knowledge in IT. Digital Evidence Handling Group members will be given the chance to participate in different courses to acquire necessary competencies. Although the EDL CDU uses 4 shared knowledge principals (knowledge transfer, exchange, collectivism and distribution) the correct workforce development or training plan has not yet been drawn up, making it a significant problem for developing DF's workforce inside the ranks.

3.1.2 Principals of development on current EDL CDU role structure

EDL CDU has been practicing member recruitment from the ranks EDF conscripts or from IT-based schools, universities or companies for years and they have developed the principle of development (see Figure 10), which by now is over 5 years old. As previously mentioned

the current training principle is based on shared knowledge principle basis (which we see should be continued even with using our proposed model). The four used principals are:

1) Knowledge transfer – This is traditional training at its purest form by using external means, courses, workshops and exercises to achieve the EDL CDU goal to educate and train their members in information security;
2) Knowledge exchange – According to EDL CDU objectives, EDL CDU wants to develop cooperation among qualified volunteer IT specialists. That is being done by organizing events among members and partner organizations i.e. get-together events, small seminars, brainstorming type of events and post exercise events;
3) Knowledge collectivism – This principle is used for building essential trust between the members and between partner organizations. This is used to achieve the EDL CDU goal to create a network which facilitates public-private partnership and enhances preparedness in operating during a crisis situation;
4) Knowledge distribution – One of the tasks which EDL CDU has been placed with is raising the level of cyber security for critical information infrastructures through the dissemination of knowledge and training (The Estonian Defence League, 2018).

The final goal of participating in international cyber security training events can be achieved by following all these 4 principals together (The Estonian Defence League, 2018). Unfortunately some of these international events have strict requirements to participants i.e. certificate for classified information of foreign states. We have brought out an overview of some of these events (see Annex Services - suggested courses and curriculums) and DF community requirements (see Annex Proposal for Digital Forensic Competency Model Framework based DOL Competency Model Tier 8) and standards (see Annex Proposal for Digital Forensic Competency Model Framework based DOL Competency Model Tier 9). Training is based around these principals and sketched out as following figure shows.

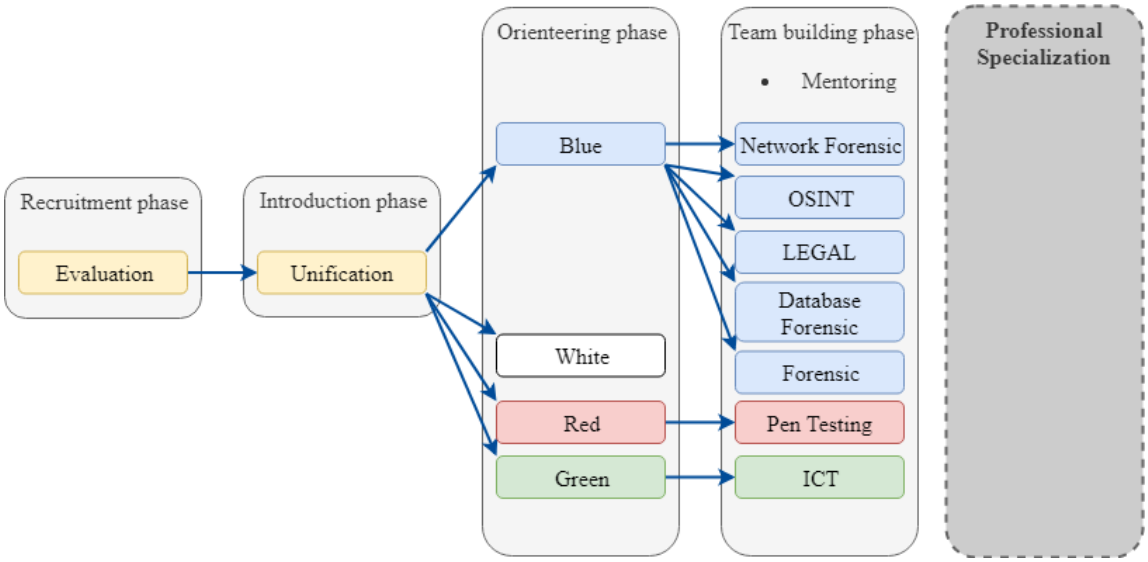

Figure 10 Recruitment and development plan for new EDL CDU members (Põldmaa, 2018)

As the given figure shows, new members have to first go through the evaluation process. The evaluation process is based on a CV and recruits have to fill in a form. After the information has been collected by the personnel specialist or team supervisor, the mapping of new recruits will be conducted. After this all newly added members will go through an unification course which, the goal of is to provide an overview of the unit's purpose, history, management, processes and activities. In the next phase, new members will be introduced

to and provided an overview of cyber threats and components of cyber defence this is called the orienteering phase. Here they will be given an overview and insight to new activities of different teams (the Red, Blue, White and Green teams). During this orienteering phase all new members who have filled in the forms and taken necessary tests, will be assigned to positions based on the test results and provided CVs. From this point forward integration of new members to EDL CDU activities will start. The assigned position is not fixed, changes might be made at any time on the request of the new member of by the unit commander, based on later studies and performance in different workshops, Tabletop Exercises (TTX), Functional Exercises (FE) and Full-Scale Exercises (FSE). EDL CDU has been trying to use this five year old plan and has noted that they need to re-evaluate this plan and need to develop specific learning paths for each of the branches. This thesis will be focusing on the Blue team that by 2018 has been divided into different sub-categories and proposing a new ontology within the ranks.

As stated in the previous chapter, EDL CDU has to be ready to fill in the role of RIA CERT, EDF CIRC or any other unit that is requiring EDL CDU assistant. The principal which the EDL CDU has been trying to achieve, is to work out the same unit structure and the roles as CSIRT teams. Given the small differences, that CSIRT team may consist of 19 different members who have specific roles, the EDL has tried to take the specific role and apply it to groups (e.g. First responder is not one member rather a separate First responder group consisting up to 10 EDL CDU members). The development of CDU internal structure is still going through changes, triggered by the need of expansion, which might suggest that there will not be just one group per role, but several. Their current development plan at this moment needs to be updated. The current structure has only managed to man 7 out of the 19 CSIRT roles (see Figure 11).

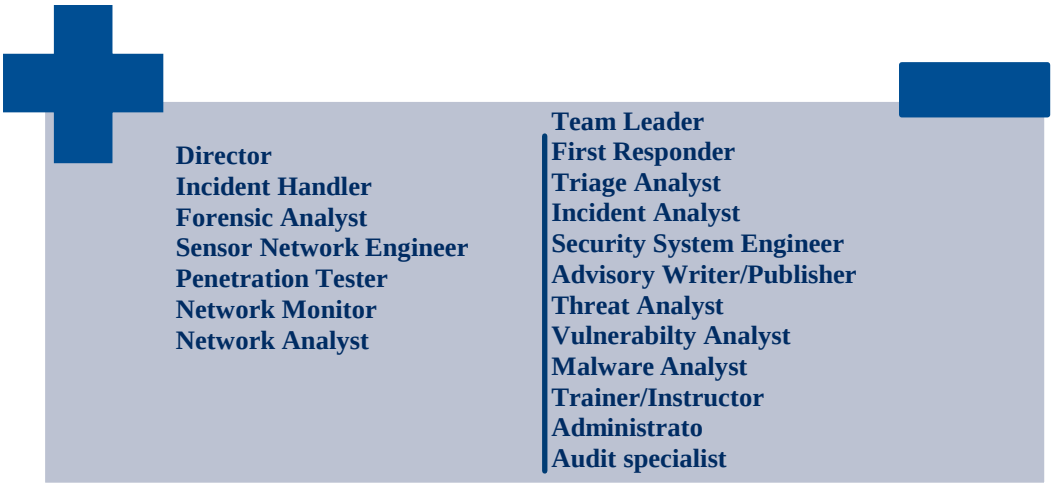

Figure 11 Key roles manned by EDL CDU and the missing roles (Põldmaa, 2018)

Although the EDL CDU has a Red (Penetration testing), White (no longer used, outdated position) and Green team (Communications and Information Technology Department), the focus will be on the Blue team (Forensic' branch). Next we will be proposing DF workforce competency model, bringing out the desired outcomes for DF and provide a proposal for the DF' structure changes for a better overview and management over specialists teams.

3.2 Proposal for DF workforce competency model

As stated in previous section the EDL CDU will have to do various tasks and be ready to assist different agencies/organizations related to cyber security. There is a wide range of tasks which DF experts must master. Here are some of those tasks:

- Conducting data breaches and security incident's investigations;
- Recover and examine data;
- Dismantle and rebuild damaged systems;
- Identify additional threats and compromises;
- Compile digital evidence;
- Establish and maintain a chain of custody;
- Write reports;
- Counsel law enforcement agencies and other entities about digital evidence;
- Advise investigators on the credibility of the collected data;
- Provide testimonies;
- Train other parties on digital evidence procedures.

In this list of tasks, the specialist has to come against data breaches and security incidents, which they need to conduct investigations in partnership with law enforcement agencies or other entities. These incidents can be high profile and highly damaging against a countries infrastructure or a company's value. Great deal of challenges arise here as the General Data Protection Regulation (GDPR) has made "digging" in the files and publishing finds complicated. This brings the need for specialists' legal training, as well as training in documenting findings, giving presentations, defending their findings and training their successors in line. Nevertheless foremost the expert has to be at the top of the field, must keep up to date with emerging technologies, software and methodologies and be proficient in forensics, response and reverse engineering skills. Not to mention the need for lots of practice.

Unfortunately only technical skills do not make a good DF's expert. Technical skills do not reflect other necessary qualities and knowledge of the experts. To be regarded as a good forensics' specialist, one needs to have certain personal characteristics and key attributes, for example:

1) Time-management skills;
2) Self-motivation;
3) Excellent communicator, fluent in occupational terminology and writing.

The need for communication skills is mainly necessary for experts who have to provide testimonies and give technical reports. Other technical qualities are the following: the knowledge about how to find and expose hidden, deleted, encrypted or obscured files, logs, browsing history and understand the types of legal evidence and legal rules regarding how evidence is collected, analysed, and reported. Also an expert should have the knowledge of security incidents, attack methodologies, incident response, access control mechanisms, including authentication and authorization, rights and privileges, accounts and controls, encryption/decryption, and how to attack and penetrate digital defences including technical attacks and social engineering (Tittel, 2017). We have mapped along with DOL competency model these competencies in our Proposal for Digital Forensic Competency Model Framework based DOL Competency Model. Due to all these requirements, it is very difficult to find good specialists and companies and institutions that have taken it upon themselves to train experts in their own institutions are at high risk, because experience in the workforce market shows that trained professionals are willing to move to another company or to another country as soon as they have achieved the necessary knowledge and degree. Other general skills should be project management, team building, intruder techniques, compliancy laws, privacy laws, ethics, GDPR, etc. (Carnegie Mellon University, 2017).

For this we have suggested an instructional strategy for DF's fully adapted revised Bloom's Taxonomy (see Annex Suggested Instructional Strategies for Digital Forensics Use With Each Level of revised Bloom's Taxonomy):

Knowledge – Demonstrate memory of previously learned skills by recalling facts, describing terms, identifying goals, naming methods, locating material and finding answers by all means necessary.

Understanding – Demonstrating your understanding of overall facts, ideas, methods by interpreting, summarizing, inferring, paraphrasing, classifying, comparing, explaining, exemplifying, giving descriptions and stating main ideas.

Applying – Characteristic words like implementing, carrying out, using, executing. Solving problems and incidents by applying acquired knowledge, facts, techniques and standards made available to you.

Analysing – Characteristic words like comparing, organizing, deconstructing, attributing, outlining, finding, structuring, integrating. Testing, breaking, finding evidences and examining information by identifying motives and causes. Finding support and evidence to your claims.

Evaluating – Characteristic words like checking, hypothesizing, critiquing, experimenting, judging, testing, detecting, monitoring. Presenting and defending opinions and findings by judging evaluations based on a set of standards and criteria.

Creating – Characteristic words like designing, compiling, constructing, planning, producing, inventing, devising, making. Proposing new or alternative solutions.

Proposed model is calculated to be with long lasting effects though it also has a long implementing phase. To have full effect on the organization, it is estimated to be as long as 5 years according to validators (described in Chapter Assessment of the Digital Forensic' workforce development plan for the EDL CDU). Implementing phases are divided into 5 groups (see Figure 12):

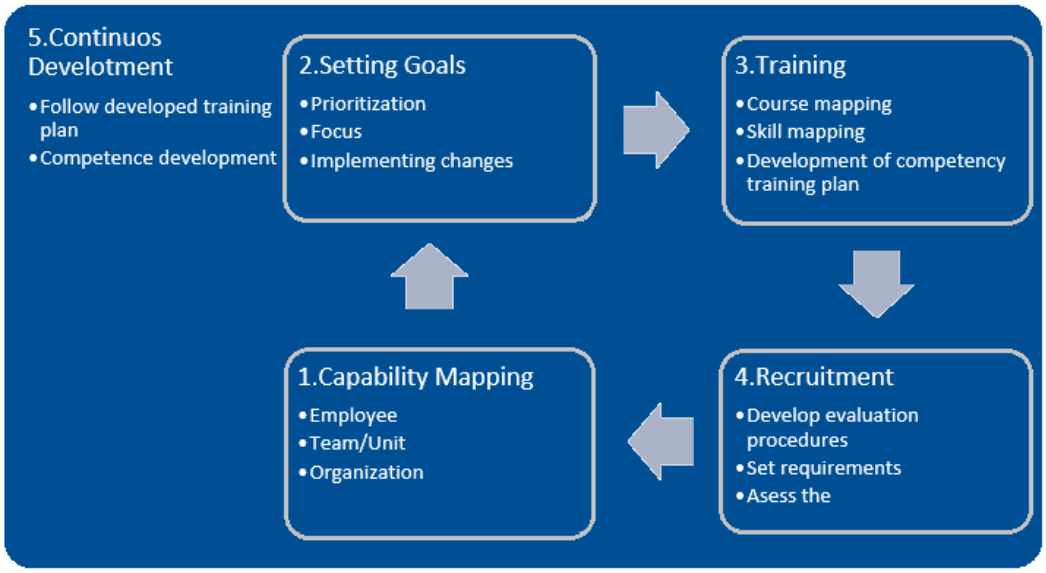

Figure 12 DF workforce competency development plan

In the first phase "Capability Mapping" we propose our DF's Competency model (see Annex Proposal for Digital Forensic Competency Model Framework based DOL Competency Model) which is the employee's and unit's capability mapping stage, as it fulfills the role of

mapping competencies with the proposed table of organization's team members by mapping the individual skills and knowledge (competencies) of your team members. After distinguishing each specialists' competencies the team leader/supervisor can draw the teams' overall competencies and limitations. As we suggest, the aim is to show the capability of the unit to partners and allies, within which competence your unit can assist;

The second phase "Setting Goals/Changes" we see it as organizational prioritizing and focus point's re-evaluation phase. Along with the capability mapping the goals and focus points might show shift in previously marked goals and this is a perfect opportunity to adapt these remarks accordingly – goals and lessons identified during the member/unit evaluation. If the unit is purely Network-oriented or First Responder-oriented and competence mapping shows that the required list of competencies is sufficient for the team (the level of competence meets 100% of the organization's/agencies goals), changes can be made to the table to simplify the subsequent recruitment process as well as to facilitate the training of new employees to the level of competence of the unit;

The third phase "Training" we see as an addition to mapping staff and unit competences and incorporating changes. This phase is necessary for mapping the courses/trainings, where the necessary skills and knowledge were addressed and created by the company training plan. By mapping these training sessions, staff training for the unit will be achieved quicker, having created a competence-based training plan for existing and future employees;

The fourth phase "Recruitment", we see the model as a tool for employees' recruitment as a basis for the skills base. Evaluating the level of correspondence with the needs of the unit through practical tasks or interviews and if there is a lack of competence, how much training is necessary to meet the required level of competence (priority is set in phases 1 to 3 to achieve the exact level of your specific role);

Final phase is the "Continuous development" which begins as soon as phases 1 – 4 have been put to use. We see it as stagnation prevention, competence development – we emphasize that the proposal is not intended to marginalize the level of expertise and knowledge of existing professionals (an employee who exactly meets the needs of his/her position e.g. Windows based specific analyst or Android based analyst), but to highlight the spectrum of competences in the field of digital expertise to encourage professionals and managers to develop their knowledge and to emphasize continuous training and development of DF's skills. With this we insist EDL CDU team leaders to see the danger in the following – routine and stagnation, which may lead to problems i.e. work errors, lack of motivation, leaving work for new knowledge and challenges.

3.2.1 Selected Competency levels

The difficulty in mapping the baseline competency skills needed in DF is connected to the organizations structure, which the team or department has put together. Do they have specific units for handling the digital evidence and specific people for writing the reports and presenting them or do they have rapid reaction teams (incident response teams) where there may be specialists with multiple skillsets although not as specific as let's say a Windows OS forensics expert. It is clear that to be an active, successful, DF's specialist, you need to have basic IT skills and sector-specific skills. Cyber security industry workforce competency has been separated into 3 major groups and 9 tiers (see Figure 13) by the DOL Competency Model Framework (Apollo Education Group Inc. and University of Phoenix, 2015) which we have made modifications for the purpose of developing DF workforce competency training and retaining model for the EDL CDU.

For our study we have selected DOL Competency Model Framework as a basis for developing the DF's competency model. The end result is DF oriented competency model which includes the revised Bloom's Taxonomy with additions to verbs and activities. We have implemented parts of DOL Competency Model (Tier system diagram and the baseline competencies from Tiers 1-4) and the National Initiative for Cyber Security Education Curricular Frameworks. The modified competency model can be found in Annex Proposal for Digital Forensic Competency Model Framework based DOL Competency Model.

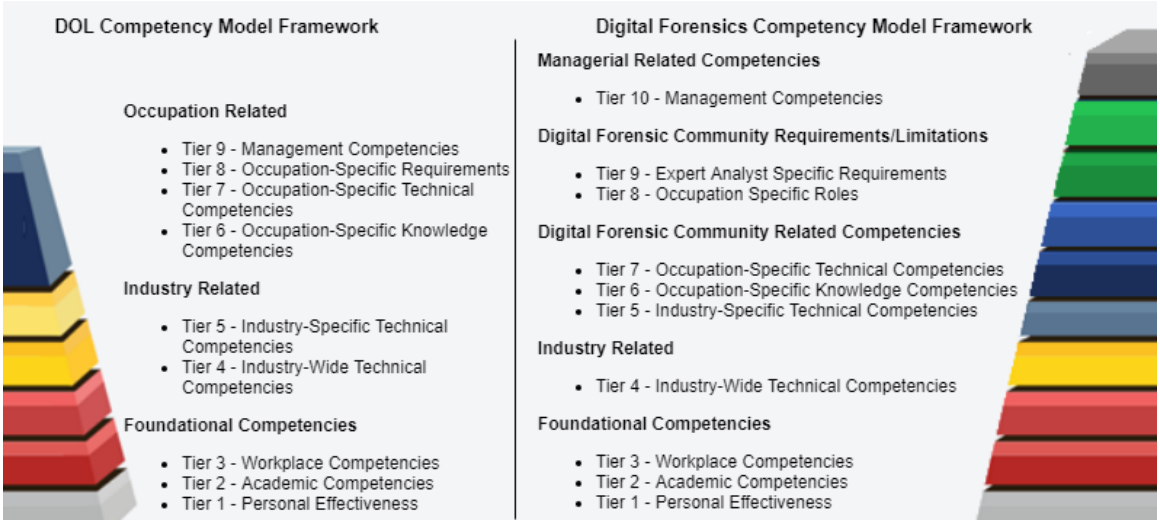

Figure 13 Left - DOL Competency Model Framework; Right - DF Competency Model Framework (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).

- **Foundational Competencies –** Tiers 1 - 3 are the baseline competencies "skills that are required of any individual in the workforce" (Apollo Education Group Inc. and University of Phoenix, 2015). These should be common across Cyber Security and DF industry and occupations.
- **Cyber Security Related Competencies –** Tiers 4 is specific to a Cyber Security work field or its subsector, however not specific to any occupation or role. Individuals who have these competencies can be move across roles and occupations within the Cyber Security field (Apollo Education Group Inc. and University of Phoenix, 2015).

Our focus would lay on Tiers 5 to 10 (see Figure 14), as DOL Competency Model does not pre-define these Tiers because of their specificity and uniqueness to the jobs (Apollo Education Group Inc. and University of Phoenix, 2015), we made these specifics according to EDL CDU needs. This was done by reviewing training service providers and topics covered in educational curriculums and mapping the key topics and competencies.

- **Digital Forensics Occupation Competencies –** Tiers 5 - 7 are highly specific to roles in the DF's work field. These can be used to define specific DF's job performance criteria, identify the requirements for a specific credential (e.g. professional license, degree or certification) and create continuous workforce development plan (Apollo Education Group Inc. and University of Phoenix, 2015). After collecting these competencies and compiling them into framework table we followed up with mini-Delphi Single round technique due to our time restrictions (Pan, Vega, Vella, Archer, & Parlett, 1996). Estimated competencies needed for DF workforce (focus

group on EDL CDU) were presented to evaluators from which we collected the feedback. For evaluation we focused on the EDL CDU partners which they are required to assist. Feedback was collected from 15 field specialists (5 team leaders and 10 specialists) from partner organizations. We encouraged constructive critique and we facilitated admission of errors. These remarks were put together in the final revised as which can be see Annex Proposal for Digital Forensic Competency Model Framework based DOL Competency Model (more of the evaluation process in section Assessment of the Digital Forensic' workforce development plan for the EDL CDU).

- **Digital Forensics Requirements/Limitations –** Tier 8 provides the key functional roles which in DOL Competency Model provided the whole cybersecurity functional role, we on the other hand list DF's field spectrum roles compiling the NRGD DF standard 1.1 and the roles from DOL Competency Model. Tier 9 contains restrictions and constraints as it provides restrictive circumstances if the EDL CDU wants to consider participate in investigations as DF's experts. These restrictions are the combined result of international Register of Court Experts in a Criminal Cases Decree (NRGD, 2018) and Forensic Examination Act (Forensic Examination Act, 2002).
- **Managerial Related Competencies –** Management and overseeing positions are often focused on directing the activities the division's and functions rather than workers. While there are overlapping or grey areas between managers and other roles, managers have a greater leadership role in an organization, have greater decision making powers and are held accountable for poorly made decisions and missteps. As a result the fourth major level with Tier 10 was added to our model.

Figure 14 Digital Forencis Specific Competencies (adabted from DOL Competency Model)

We propose that before calling a worker "Specialist", the recruit should be evaluated by the Competency Model Framework Tiers 1-3 (reminding that Tiers 1-4 have been mapped by US Department of Labor) and be graded according to the organizations' needs. Tier 1 shows Personal Effectiveness, e.g. displaying the skills to work effectively with others, displaying moral principals, demonstrating a commitment to self-development and improvement of knowledge and skills. Tier 2 gives an overview of if in the future a member of the organization is suitable for further testing or training within the ranks. Tiers 3 shows if the new member is a team player or likes to work alone and if they have the potential to run projects and make difficult decisions even under pressure. Tiers 1-3 will mainly give oversight in the candidate's knowledge about PCs, tablets, phones, networks, and Internet and commonly known problems, issues and some experience about security, safety, and preventative

maintenance of IT systems. These first three tiers we can acknowledge as "Junior Specialist/Analyst" level. These new recruits are the students who are performing common tasks, working and learning simultaneously. They will be new to an organizational working lifestyle. Students from the universities' freshmen year or from conscription – they work day-to-day, with a set of tasks given by supervisors and just beginning to investigate the professional options for their specialization field. They mostly have simpler skills, and tasks that are pre-requisites to a specialist being effective in this job role.

We suggest that on an "Specialist/Analyst" level is candidate who has acquired Tier 4 mid-level knowledge, skills, abilities and tasks. These specialists familiar in conceptualizing, designing, and building secure IT system's, providing the support and administration necessary to ensure effective IT systems performance and security (Apollo Education Group Inc. and University of Phoenix, 2015).

"Advanced Analyst" level specialist is someone who has mastered his or her DF's subdivision skills in the Tiers 5 and 6. It must be noted that a specialist can already be declared an advanced specialist even if he has mastered a portion of the competency listed in the model. Main focus here is that a specialist who has a higher level knowledge and skills in their work field and has proven to be very effective in this functional area. However we want to mention that some lower level, pre-requisite competencies may be left uncovered.

"Expert Analyst" level specialist is someone who has almost complete knowledge of their specific knowledge area. These experts can be enrolled in high value investigations, managing projects and assessing others' research and work. Tier 7 speaks about such specialists' competencies and is looked at as a highly focused area and assumes someone is already well trained and effective in this job role overall. Tier 7 expert focuses on expertise in a very specific, narrow area. Additionally if somebody wanted to be considered an expert in the eyes of Estonian judicial system, Tier 9 has to be followed.

Thus we have made a proposal for a Digital Expertise Competence Model (Annex Proposal for Digital Forensic Competency Model Framework based DOL Competency Model), which is based on the NICE and the DOL Competency model and we urge EDL CDU to adapt both this pre-defined model with DF's ontology (Annex Digital Forensic ontology on the example of EDL CDU). This tool does not aim to marginalize the expertise and knowledge of existing professionals. However also to create a competency stairway that corresponds to the needs and specifications which currently are offered by internationally renowned training and certification bodies - to train the DF's workforce in areas that internationally renowned top-level professionals find necessary. The goal is to provide the organization with a model of continuous development support that provides development opportunities for professionals at basic, intermediate, advanced and expert levels. With this, we try to create a situation where we avoid stagnation of specialists' skills and, consequently remove possibilities of resignation from the expert side. One way to solve this problem would be, in our opinion, a continuous development. In this case, the organization offers its specialists the opportunity to organize trainings, competitions and co-operation within the organization, for example, by applying the skills and knowledge of experienced professionals by training younger colleagues or allowing them to give lectures related to the profession. For our part, we propose a specialist's evaluation table (see Annex Proposal for Digital Forensic Competency Model Framework based DOL Competency Model) that lists the competencies. The assessment of the competency model has been carried out by experts in the field (e.g. Police and Border Guard Board, NCIRC, EDF), who are charged with electronic evidence at any level. A list of skills and knowledge is outlined using the revised Bloom taxonomy. In addition, we have identified key issues for evaluators to determine

whether the proposed model meets the needs of the digital expertise industry in improving the skills of the workforce and bringing in new specialists. Experts who will be trained by the model would increase the reliability of the unit or organization in managing and investigating incidents. Details on evaluations and results will be shown in Chapter 4 Assessment of the Digital Forensic' workforce development plan for the EDL CDU.

3.3 Proposal for new EDL CDU specialization structure layout

To follow up to Hallett, Larson and Rashid study we decided that the closest framework with most in common traits for EDL CDU DF's Evidence Handling Group was NICE. We took the NICE Framework as being the most favorable in training and career progression in mind for workforce development focusing on hire-to-retire principle. We suggest the EDL CDU to reformulate their structural components according the NICE Framework Components' relationships (see Figure 15). The color scheme is in relation to our view of EDL CDU proposal for DF's ontology in Annex **Digital Forensic ontology on the example of EDL CDU**.

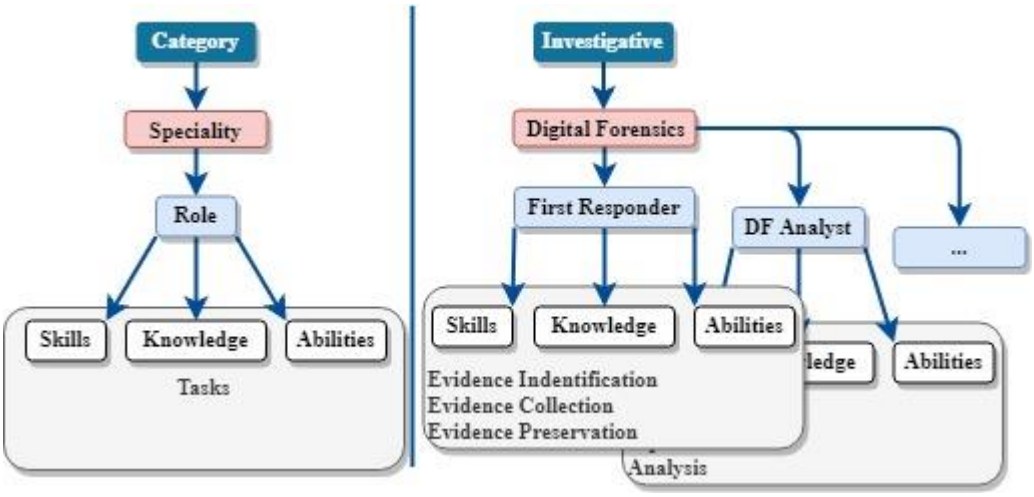

Figure 15 Left - Relationships among NICE Framework Components on the (Newhouse, Keith, Scribner, & Witte, 2017); Right - the example in correspondence with Digital Forensic ontology (see Annex **Digital Forensic ontology on the example of EDL CDU**)

After adapting the NICE Framework principals the new EDL CDU and EDL CDU DF's Evidence Handling Group workforce specialty component relationship diagram should be illustrated as shown on Annex EDL CDU structure plan after NICE Framework implementation to Digital Evidence Handling Group structure and Annex EDL CDU structure plan after implemented NICE Framework Component relationship and partially in Annex **Digital Forensic ontology on the example of EDL CDU**. The reason in behind the first two layouts is due to EDL CDU's demand, as the chief of EDL CDU has not been clear if they are planning to restructure the whole EDL CDU or their sub-branch Digital Evidence Handling Group. Eventually we should have managed to simplify grouping of DF's workforce topics and helped with the alignment in comparing with other frameworks. EDL CDU shall be divided into multiple specialty areas (e.g. in which case we have focused on DF's Evidence handling group. Specialty roles are composed of work roles. Each work role (e.g. First Responder, Team leader, DF Analyst, DF Expert - Network) in turn, includes Knowledge, Skills, Abilities (KSA) and Tasks (see Annex EDL CDU structure plan after NICE Framework implementation to Digital Evidence Handling Group structure and Annex EDL CDU structure plan after implemented NICE Framework Component relationship).

Furthermore recruitment, hiring, educating, training, retention and development of highly skilled workforce should be under constant evaluation, so all members should have clear career pathways described and promote progressive challenges for specialist evolvement. The usage of competencies and tasks in all these processes can help the existing staff to develop unit capabilities.

3.3.1 Proposal for a revised taxonomy of the DF standard

During the work regarding DF's taxonomy of NRGD, several instances came up which suggested the taxonomy should be revised the same way as ISO standards, in 5 years or even less. The taxonomy must be up-do-date as the workforce development needs to be reviewed and planned accordingly. Thus the following revisions should be taken into account.

Revised version of the Computer Forensics' taxonomy

First addition in DF's subdivision is single-board computers in the Computer forensic discipline (seen and on Annex **Digital Forensic ontology on the example of EDL CDU**). These small general-purpose computers (which are little bit slower that regular computers,) can be used for running desktop applications or anything you could do on an ordinary household computer. These mini computers share similarities with laptops and regular computers such as USB ports for keyboard, mouse and other USB devices, HDMI port for monitor, Audio headphone port, Ethernet port, WiFi, Bluetooth, SD Card slots for storage and run on operating system (e.g. Rasbian, Windows 10 IoT Core, Snappy Ubuntu Core, SUSE, Ubuntu Mate, Kali Linux, CentOS), thus in simplification the Single-board computers should be dealt with the same care as laptops, PC's and servers.

Revised version of Software Forensics' taxonomy

Next we added a whole family of Malware subdivision and divided Operating Systems subcategories into three separate groups distinctive by platform in Software Forensics. Malware Forensics is covering the complete process of responding to a malicious code incidents. Specialists have to examine a systems to collect and preserve critical live data, furthermore they must be able to perform live forensics and evidence collection procedures on different live systems in the context of identifying and capturing malicious codes and evidence effecting on the compromised system (Aquilina, 2008). The categorizing of OS via platform is needed for DF experts in order to facilitate the work and professional distribution of specialty. As tablets, smartphones and consoles go additionally under device forensics category they are in close relations with software forensics due to software running on them. This brings the need for a revised version for Software Forensics' taxonomy and introducing it for to simplify the development of the workforce development plan.

Why separate malware into different categories? When we talk about malware, we tend to talk about Trojan horses, viruses, and ransomware, which generally has a damaging effect against all electronic data. As all classes of malicious software own a payload and have different effects and targets, we would propose an addition to Software Forensics branch in Malware category by dividing it into 5 main groups: Trojan horses, worms and viruses, malware and Crimeware (see Annex **Digital Forensic ontology on the example of EDL CDU**).

Trojan horses often referred to as Trojans differ from other groups by not independently replicating themselves. Trojans disguise themselves as a program, of which particular function is desired by the user, hiding in themselves a payload. Methods of concealment are almost unlimited as they can hide in command lines for UNIX system administrators or turn up as Remote Access Trojans (known as RATs or simplified as backdoors) and they are sent

via email or ambush user in file sharing services or on websites. Their classification can be carried out based on their functions: Backdoors, Adware, Spyware, Scareware, Downloaders, Diallers, Keyloggers, and Rootkits (G DATA Software AG, 2018) (McAfee, LLC, 2019).

Viruses aim to multiply themselves and spread over the network. Commonly they attach themselves to other files or embed themselves in the boot sector of data carriers and are often smuggled onto the PCs undetected on USB sticks, via networks, by email or via the Internet. Because of the versatility viruses can range from being a nuisance to being extremely dangerous. They can be divided into the following categories: Boot sector viruses, File viruses, Multipartite viruses, Companion viruses, Macro viruses, Stealth viruses and rootkits, Polymorphic viruses, Intended Virus and lastly Email viruses (G DATA Software AG, 2018).

Worms are standalone software and do not require a host program or user to propagate. To spread, worms either exploit a vulnerability on the system or use some kind of social engineering to trick users into executing them. It spreads by transferring itself via networks or computer connections to other computers. Their classification can be carried out based on their transport channel: Network worms, Email worms, Peer-to-peer worms and Instant Messaging Worms (G DATA Software AG, 2018).

Crimeware is quite a new general term for software used to perpetrate crime, such as stealing personal identities, a computer user's financial and retail accounts, money or proprietary information. Crimeware uses viruses, Trojans, worms, spyware, or adware and other types of malware to get access to the victims devices. Their classification is done based on their function: Ransomware, Point-of-Sale malware, Cryptomining malware and wipers (G DATA Software AG, 2018).

Why distinguish OS via platform? What is the difference and why is it useful in the DF's field? As we have mentioned the Device Forensics' category before, the devices are divided into different branches and distinguishing Computer Forensic as a whole different forensic' group. By doing this we eventually formulate a more structured way to rank and recommend competency training. What is the difference between our proposed platform OSs? First of all the difference is in the fundamental environments for software applications. Main issue is that computer operating systems were not really designed for mobile use over wireless networks, as they were developed for wired systems, focused on technical specifics (multiple process handling, CPU operation, boot protocols). The computer forensic specialist must keep these facts in mind when choosing their training courses and keeping track of newly adaptable methods.

Mobile OS however is developed for being used across wireless environments, providing consistent ease of network access, responsive designs and user friendly software applications while on move. One hybrid phone which is looking closely similar to today's laptops and tablets alike is Samsung Galaxy Note 9 which is an Android tablet smartphone, which can be turned into small workstation via Samsung DeX docking station giving the user full personal computer capabilities (Kronfli, 2017).

Video game consoles are increasingly similar to personal computers as well as to mobile systems, catching up computers in performance and software vise. For example the early console systems ran on a simple code on ROM chip which ran the specific code on the cartridge. Older Sony consoles ran all software from the actual disk. Later on they ran a small proprietary piece of code on a kernel, which was a so called OS between the hardware and the software. Next version of the Sony console (PS3) had a custom version of FreeBSD

system. From this moment on the consoles acted like computers, it booted up from the consoles hard drive, one had UI and xcross media bar and one would install games on top of that. Furthermore one could change the OS system on these, for example run Linux OS on them. As we talk about the nowadays consoles, the similarities are on the hardware side. All of them have GPU's, HDD's, optical drives, network connectivity (wired and wireless), however they run on different platform bases (Performance Optimization with Enhanced RISC – Performance Computing). Furthermore these systems run virtualization environments, basically running different OS at the same time (OS for settings menu, OS for running games). Nintendo on the other hand held different versions of IOS on the HDD. The reason was that games that used lets say IOS version 13 just booted up Nintendo Wii IOS version 13 and when changing disks, the device would take information from the disk and jump to IOS version that is needed to run for this game. This same functional structure was used in Nintendo Cube, so you could basically take the Cube's games and play it on Wii U (Loveridge, 2016).

Because of these differences, the previously mentioned taxonomy, distinguishing devices on OS level, was proposed for a better device forensic' specialist competency training plan development.

Revised version of the Device Forensics' taxonomy

New additions were suggested for Device Forensics' taxonomies Small-scale devices. New category was added (Smart watches/activity trackers) and other categories were modified quite significantly (see Annex **Digital Forensic ontology on the example of EDL CDU**).

Firstly the embedded chip devices were distinguished into 6 categories by their purpose (Avionics, Controllers, Automotive, Medical, Personal home appliances, security and espionage). Though smart TV is not a small-scale device it can be categorized as an embedded chip device under the home appliance or moved to a large-scale devices as a new Smart-Devices. This distribution was seen to be most useful when explaining the field knowledge competency for newly appointed DF' specialists. Secondly new addition was proposed for mobile- and smartphones. Previous taxonomy only suggested distinguishing Phone memory cards and SIM cards although most new smartphones show the expansion of internal memory capacity, thus bringing into light a third category "Internal Memory" and changing Phone Memory Cards into External Memory. Thirdly we divided navigation systems by electronic methods (radio, radar and most satellite navigation). Furthermore it has to be mentioned that most of privately used ships navigation systems hold sonar capabilities. Fourthly a smart watch and an activity tracker category was introduced to this taxonomy with distinguishing devices via their operating systems (Android and Apple). And lastly we suggested a change in Personal Digital Assistants category to include E-readers.

Revised version of the Network Forensics' taxonomy

As wireless communication involves security systems, remote controls, Wi-Fi, Cell phones and the Near Field Communication, wireless power transfer, computer interface devices and various wireless communication based projects, the need to write down a more detailed taxonomy for wireless subdivision is necessary. In terms of wireless systems' and applications' security issues, it should be divided according to system types, as it helps to compare and evaluate DF's workforce competency. Within the Network Forensics we give a proposal distinguishing Wireless Forensics (see Annex **Digital Forensic ontology on the example of EDL CDU**).

An overall security issue that is continuing to exist is the possibility that an unauthorized entity can capture the wireless signals which spread through the air. It is important to improve securing measures for wireless networks and further develop and conduct counter intelligence in regards to seeing what can be recovered in different systems and by what means.

The additions that where done to these DF's taxonomy disciplines is our representation of giving a more detailed description and an overview to experts on the field, to better understand in which category do they belong to and which technologies fall under their responsibility. It is understood that digital and cyber is a fast growing and evolving field which can make a vast number or technologies obsolete or legacy technologies. It has to be noted, that it is better to have the knowledge and experience of old legacy systems, especially as they may be or are the technological solutions developed on the basis of these systems, thus we have left examples of legacy, such as in Software Forensics - FreeBSD or Network Forensics - Infrared connections into these taxonomies. In Annex Proposal for new Digital Forensic discipline – Unmanned SystemsVI we propose a whole new concept of digital forensic subdivision which introduces unmanned system forensics as a separate sub-discipline. In the next chapter we will focus on the DF's workforce competency model.

3.4 Chapter Summary

In this chapter we described the contribution of this thesis by providing an answer to the research question "How to develop and retain DF workforce competency in EDL CDU?" (SRQ2 in Section Research Questions) and propose a DF's workforce competency model(see Annex Proposal for Digital Forensic Competency Model Framework based DOL Competency Model), a revised DF's standard taxonomy (see Annex **Digital Forensic ontology on the example of EDL CDU**) with additions to sub-disciplines (new sub-discipline into DF taxonomy see Annex Proposal for new Digital Forensic discipline – Unmanned Systems) and a proposal for a new structural layout for EDL CDU (see Annex EDL CDU structure plan after NICE Framework implementation to Digital Evidence Handling Group structure and Annex EDL CDU structure plan after implemented NICE Framework Component relationship).

Before we can start developing and retaining the EDL CDU's DF's workforce competency, we first have to bring out the current stages.

How is the current EDL CDU shaped? – EDL CDU is an unit in a voluntary organization aimed at protecting the Estonian cyberspace. Emphasis on the voluntary part – members of the unit are Estonian patriots with IT skills, experienced specialists in key nationally critical infrastructural cyber security positions and in other fields concerning cyber security (The Estonian Defence League, 2018). Estonian Regulation No. 108, shows the EDL CDU's cooperation with PBGB, RIA CERT and EDF in their core roles in defending Estonia cyberspace. This means that the EDL CDU has to fulfill their key functions, which are:

1) Mitigating and preventing major incidents and helping to protect organizations valuable assets;
2) to have a centralized coordination for IT security issues within the organization (Point of Contact);
3) to have a centralized and specialized handling of and response to IT incidents;
4) to have the expertise at hand to support and assist the users with quickly recovering from security incidents;
5) to help with legal issues and preserving evidence in the event of a lawsuit.

For this purpose the EDL CDU has been using their own structural layout which mainly consists of Red, Blue, Green and previously White groups. The Blue further known as DF's group is divided into 5 sub-disciplines (see list below):

1) Network Forensic;
2) Database Forensic;
3) OSINT;
4) Legal Department;
5) Forensic.

As the EDL CDU has to be ready to fill in the CSIRT role for PBGB, RIA CERT, EDF CIRC or any other unit that requires EDL CDU's assistant, the unit' roles should match CSIRT team roles. Given the small difference, that a CSIRT team may consist of 19 different members who have specific roles, the EDL has gone with the role per group or team model (e.g. First responder is not a solely one member, but a separate First responder group consisting up to 10 EDL CDU members). As the unit is based on voluntary members, workforce recruitment and continuous training fare the troublesome points in the EDL CDU. For this the members of EDL CDU have to fulfill certain key requirements and guidelines set up for DF specialist roles. One of which is Netherlands Advisory Committee of Standards (ACS), ISO and the NRGD's DF standard's which distinguishes 6 subfields of DF (Computer Forensics, Software Forensics, Database Forensics, Multimedia Forensics, Device Forensics and Network Forensics). By the NRGD, the DF is a discipline of forensic sciences and therefore should be reviewed under ISO standards (overview can be see Annex Overview of standards regulating Digital Forensic community). As EDL CDU recruits and also is responsible for training their members, they have used 4 shared knowledge principals:

1) Knowledge transfer;
2) Knowledge exchange;
3) Knowledge collectivism;
4) Knowledge distribution.

EDL CDU main goal is to get as much practice as possible in DF community and to participate in national and international cyber security training events which have set certain restrictions to training and recruitment policies. We have brought out overview of some of these events (see Annex Services - suggested courses and curriculums) and DF community requirements which EDL CDU might come up against (see Annex Proposal for Digital Forensic Competency Model Framework based DOL Competency Model Tier 9).

SRQ2 – How to develop and retain DF's workforce competency in the EDL CDU?

We shall answer this question with two parts, firstly "How to develop DF's workforce's competency?" and secondly "How to retain DF workforce's competency in EDL CDU?" For development of DF's competencies we have seen fitting to combine a NICE DOL Competency framework, DF's Standard 1.1, revised Bloom's Taxonomy with changes to DF's community(see Annex Suggested Instructional Strategies for Digital Forensics Use With Each Level of revised Bloom's Taxonomy), and DF ontology model(see Annex **Digital Forensic ontology on the example of EDL CDU**) to eventually create a task based competency model(see Annex Proposal for Digital Forensic Competency Model Framework based DOL Competency Model). Proposed model is calculated to be with long lasting effects though also has a long implementing phase. To have full effect on the EDL

CDU organization we could estimate maximum of 5 years (according to validators described in Section 4.1). Implementing phases are divided into 5 groups (see Figure 12):

1) Capability Mapping
2) Setting and re-evaluating Goals
3) Training
4) Recruitment
5) Continuous development (falls into second part of SRQ2 – Retaining DF competency in EDL CDU).

The model can be used in any time in these phases. Marking the evaluation by using the GAP analyses by "achieved" or "desired", marking the level of importance by "not applicable", "preferred" or "essential", using it as a recruitment baseline or for mapping and planning the course/training roadmap. As a result of these evaluations and from remarks by evaluators, we have compiled DF's workforce competency suggestions. Tiers which we focused on were Tiers 5-7.

In the second part of SRQ – "How to retain DF's workforce competency?" we suggest our proposed models' 5th phase "Continuous development" which is supported by Annex Services - suggested courses and curriculums. We provide an overview of courses, curriculums and exercises which support training in different levels – trainee/student, trainer/teacher, evaluator or planner/organizer. We see it as a preventive measure for workforce stagnation and as a possibility for a continuous development of competences. We emphasize that the proposed model (specially the evaluation of existing specialists) is not intended to marginalize the level of expertise and knowledge of existing professionals (an employee who exactly meets the needs of his/her position e.g. Windows based specific analyst or Android based analyst), but to highlight the spectrum of competences in the field of digital expertise to encourage professionals and managers to develop their knowledge and to emphasize continuous training and development of DF's skills. With this we insist that the EDL CDU's team leaders see danger in following – routine and stagnation, which may lead to problems i.e. work errors, lack of motivation, leaving work for new knowledge and challenges.

4 Evaluation of Digital Forensics' workforce development plan

In this chapter we show a series of results of the evaluation process and try to answer **SRQ3 – What are the means of validating of the workforce competency development model?** We will give the reader an overview of the evaluation of the proposed model and remarks given by the evaluators, who are leading experts of partner organizations from the DF's field of work.

Evaluation was done by identifying whether the intended competency model is usable in the DF's field for the purpose of the EDL CDU to assess the workforce and the overall unit through different key components and competency deficiencies, from an actual planning of learning opportunities and content will be specified. The assessment focuses on the utility of the thesis's proposals and the evaluation was judged by their usability. The primary intended users are DF's organizations, especially personnel managements. Primary uses are for recruitment, training and development of future DF's specialists for the job at hand and to be prepared to assist other agencies in their work. Three groups were monitored during the evaluation:

- Utility - Evaluation will show if this proposal serves the information needs of intended users (EDL CDU).
- Feasibility - Evaluation will show if this proposal is realistic, prudent and frugal.
- Accuracy - Evaluation will show if this proposal will reveal and convey technically adequate information about the features that determine the worth or merit of the evaluated program.

In the first part we looked over the assessment done by leading experts of the DF' workforce development plan for DF's specialists intended for EDL CDU. Evaluation letters were sent to TalTech[19], CERT, EDF, RIA, PBGB, Clarified Security[20], EKEI, Eesti Energia AS[21], The U.S. Military Academy at West Point, The U.S. Naval Academy, Canadian Armed Forces, NCIRC TC and stakeholder's assessment by chief of the EDL CDU Chief Andrus Padar[22]. The total of organizations/units contacted was fifteen, out of which seven responded in time, with answers to KEQs and specialist opinions. We gathered fifteen team leaders/specialists feedbacks which were compiled into our model (see Annex Proposal for Digital Forensic Competency Model Framework based DOL Competency Model) and calculated arithmetic mean for level of priority(e.g. 1-Not Applicable, 2-Preferred, 3-Essential) to each topic/task for our focus groups.

4.1 Assessment of the Digital Forensic' workforce development plan for the EDL CDU

Assessment of the proposal for DF's Competency Model's Framework was done by experts and professionals from different units, both national and international, to get the highest

[19] TalTech School of Information Technologies: Department of Software Sciences, Project Manager of Digital Forensics.
[20] Clarified Security is an Estonian information security company focused in delivering practical security services (manual WebApp pentesting) and deliver remote testing and on-site training services globally.
[21] Eesti Energia is a state-owned international energy company that operates in the electricity and gas markets of the Baltic countries and Poland, also in the international liquid fuels market. Eesti Energia is responsible of ensuring the security of electricity supply in Estonia.
[22] Chief of Estonian Defence League's Cyber Unit and co-writer of competency- based educational model for the criminal police. Development of the competence of the criminal police officer through practice and science.

variety of qualitative and authoritative feedback. A direct and explicit key evaluation questions – Key Evaluation Questions (KEQs) – were assigned with the aim to determine whether the proposed model fulfills the DF's industry needs in improving the workforce competency and continuation of comprehensive performance by DF's specialists. The purpose of this model is that it would ensure the units integrity and reliability in incident management and investigation.

Evaluations were conducted under the following categories:

1) Purpose: are all relevant competencies covered by this model;
2) Learning: does this model contribute to consistent improvement of the DF's workforce competence;
3) Comparison: does this model contribute to the current workforce development plan;
4) Applicability: would this model be more cost effective and less time consuming than the current personnel management development plan.

4.1.1 Key evaluation questions and supportive evaluation questions

1) **KEQ1 –** Does the proposed model support organization-wide goals?
   a) **SEQ1 –** Does this model support the unit's workforce development plan (e.g. method relevance, workplace compliance, and process efficiency)?
   b) **SEQ2** – What do you think of the overall structure? What alterations would you make?
2) **KEQ2 –** Could this model be most beneficial in terms of workforce performance improvement or continuation of good performance in areas of importance (i.e., speed of obtaining digital evidence)?
3) **KEQ3 –** What shall be the complexities and problems in terms of exchanging the current workforce development plan to the proposed model?
   a) **SEQ3 –** How does it compare (e.g. level, cost, time spent, unit's size redundancy / recruitment)?
   b) **SEQ4 –** What is the forecast for reaching the full extent of the previous work capacity and which of the results reflect the fulfillment of previous processes and work unit's standards to support organization-wide goals?

4.1.2 Evaluation of model's utility, feasibility and accuracy

During the evaluation process "5Ws" were used to prove the models applicability – Who, What, Where, When and Why. Evaluation will show if this proposal serves the information needs of the intended users (EDL CDU).

Who benefits from this? The key figures who will benefit from this model will be the commanders of the unit and the human resources department, who are responsible for hiring new members and developing the workforce training plan.

For whom is this model harmful for? It has to be noted that this model may be used in the wrong means, by this we mean showing the workers' lack of knowledge and using it to their disadvantage, which would result in pay cuts. As the purpose of this model is not to marginalize the specialists' competencies, it is used foremost to show the wide spectrum of competencies, which could be trained in the specialist.

Who shall be making decisions about the use and focus of this model? The key people in the first two stages (mapping the specialists and the whole units competencies, mapping the priorities and focus points of the unit) will be the specialists and group leaders, who will be

determining the baseline of the working unit and its basic needs. Additionally the decision making will go to the unit commanders and human recourses department who shall continue with mapping courses and start with recruitment and developing workforce training plan.

Who will be affected directly? The focus group is and will be the DF's specialist.

Who are affected by this problem – the lack of this development plan? Interviews showed that similar problems arose in every agency i.e. lack of existing specialists' development plan, lack of information from partner agencies about their competencies, lack of information about courses, which specialist could take.

Who will be the key people in this model? As previously mentioned in the decision making question, the key people shall be the DF's specialists, team leaders/commanders and human resources department's personnel, who are responsible of training and recruitment.

What are this models strengths? The biggest strength will be mapping the specialist's competencies and furthermore mapping the current competencies of the unit/agency/organization. This will be followed by simplifying the workforce training and recruitment phases and working on continues development.

What are this model's weaknesses? The two major weaknesses have been stated. First is the initial mapping of competencies which may take up to weeks or months, depending of the organization size and second is testing or proving of the competencies, which organization have to work out themselves or with partner agencies. After these tests have been developed, it would simplify the whole process.

What is another alternative to this model? Human resources department will continue their current recruitment and workforce development plan if the organization has one.

What is the best case scenario? In this case the best case scenario is that not only does the EDL CDU adapt the model as their official workforce development tool, but it will be adapted by the EDF and other agencies as well. Furthermore Estonia would adapt the NICE framework to start the development of a wholesome Cyber Security workforce.

What is the worst case scenario? The worst case scenario is that main focus group (EDL CDU Digital Evidence Handling Group) will not adapt the model and it will be deemed as unapplicable/usable by the stakeholders.

What is the most/least important focus point of this outcome? The most important outcome is the stakeholders' goodwill of reaching to the outcome which they have to fulfill – to assist partner agencies.

Where would we see this being used? In organizations who are in contact with digital evidence and DF in general – law enforcement, armed forces, CERT, organizations with internal capabilities of such competencies.

When will this model be used by the EDL CDU? EDL CDU Digital Evidence Group chief has notified me that this model will be put to use in April 2019 (Põldmaa, 2018). According to chief of EDL CDU the model has all the needs met for their

Why is it relevant to us? As the EDL CDU is a voluntary organization and a national defence organization, it is necessary to recruit and motivate members to give their contribution to national defence (Põldmaa, 2018). New members must be found for national defence from exercises and competitions and motivating them with continuous development possibilities is necessary. The possibility of recruiting MSc degree students or graduates are slim, thus motivating existing members and recruiting new highly motivated members is essential.

4.2 Answers to Key Evaluation Questions

In this chapter we show a series of evaluation results and answer research question **SRQ3 – What are the means of validating the workforce competency development model** by giving the reader overview of evaluation of the proposed model and remarks given by the evaluators from leading experts and partner organizations on the DF field of work.

For this we set up series of key evaluation questions (KEQ) and supportive evaluation questions. We are giving concluding answers with both positive and negative observations in mind. Answers were submitted in different forms i.e. interviews (personal meetings and via telephone), emails and official letters. No major conflicting opinions were observed, although all negative issues have been regarded in the answers and conclusions.

1) **KEQ1 –** Does the proposed model support organizational-wide goals?

After receiving the feedbacks from the evaluators the conclusive answer is – Yes it would support the organizational-wide goals. It is believed that this model links organizational objectives and a gives clear description of the 'problem' which is recruitment, development and retention issues linked to lack of appropriate plans and policies. Evaluators particularly liked the approach to providing clear responsibilities and a step by step list of competencies that would allow for career change/progression in an individual. This would assist in internal promotion and job satisfaction. There are feedbacks which show consistency of workforce commenting that the satisfaction in doing the job is an important part of their retention. Providing this framework must therefore be even more positive in a volunteer environment.

a) **SEQ1** – Does this model support the unit's workforce development plan (e.g. method relevance, workplace compliance, and process efficiency)?

The model focuses on skills on the other hand also contains much information that could be used to build RACI[23] models and even incident procedures. It is believed that it is through these steps suggested by thesis author both efficiency and trustworthiness could be improved through a more defined and transparent set of capabilities vs tasks. Consequently, this approach should lead to better effectiveness, and that can then be accredited and audited against the model. This should deliver assurance and supports the good governance of the organization. This must be a powerful benefit for such non-traditional approaches to cyber security as the EDL CDU.

b) **SEQ2** – What do you think of the overall structure? What alterations would you make?

Based on the evaluators' feedbacks the model would make Human Resources department work easier by making demands for recruiting new employees. Officially the model might need organizational or board approval, unofficially it could be used immediately. Although the model could unofficially be used promptly, there were suggestions for making more easy-to-use.

Firstly from the private sector the issue was moreover that a good specialist should not be a good communicator which this thesis suggests. In the feedback to suggestion was that mediators should be used. The problem lies in training timeframe, there is not enough time in one person's life to learn good personality qualities and at the same time to acquire vast amount of technological skills. Somewhere it would be necessary to draw a line that "this is

[23] RACI matrix is a visual representation of each individual's role within that process identifying those who are Responsible, Accountable, Consulted, and Informed (Jacka & Keller, 2012).

good enough". For example, we assume that the subordinate must have very good communication skills, however we do not expect the superior to have good technical skills to understand the subordinate. So there are problems here. The superior should have an understanding of the technical vocabulary to come halfway through the lack of communication with its subordinates. In the public/military sector the superior is mostly signed from the ranks of subordinates which makes them equally competent in related field.

Secondly the need for consolidation was mentioned, as this model on the basis of Tiers 6-10 have not been tested, it should be piloted and then consolidated with key competences for better specialization and easier handling.

Thirdly the issue of replication. Some of the competencies have been noted to be either replicated or near-replicated, which make the table long and a little cumbersome to use. Table should be reevaluated and listed.

Lastly the issue of presentation. Feedback and interviews conducted clearly showed that the model layout and perspectives should be redesigned somehow. Model should be presentable in Pivot table form or similar to allow concept to be viewed from differing perspectives.

These suggestions make primary suggestions for future work on the basis of model adjustment.

2) **KEQ2 –** Could this model be most beneficial in terms of workforce performance improvement or continuation of good performance in areas of importance (i.e., speed of obtaining digital evidence)?

The use of 10 Tiers works well, giving a clear structure and placing equal value on Managerial and Technical skills – this is better than the approach many organizations take, which lacks that transparency. It can be said that this model can absolutely be seen providing a structured approach to development that supports skillset development and individual advancement.

3) **KEQ3 –** What shall be the complexities and problems in terms of exchanging current workforce development plan to model being proposed?

Evaluators' feedback showed full support on the approach taken, though suspect that the size of the plan will hinder its implementation, especially wherever it is used by non-specialists (e.g. HR). Staff will be able to see what they need to learn to advance themselves – that is clear and motivational.

   a) **SEQ3 –** How does it compare (e.g. complexity level, cost, time spent, unit size redundancy / recruitment)?

Complexity is the biggest challenge in this plan, which is to be expected when synthesising concepts.

   b) **SEQ4 –** What is the prognoses of reaching the full extent of previous work capacity and to which your results reflect the fulfillment of your previous processes and work unit standards to support organizational-wide goals?

Feedback that the model would hold wholly positive effect for work capacity, as it will be believed that with the minor modification and following some pilot implementations, the model would be beneficial in both improving the skills of the workforce and recruiting new specialists. The full effect would be see 5-10 years after a quick evaluation, as the model contains a vast number of competencies that specialist today lack. The amount of training

needed cannot be completed in a short time. Additionally the resources for training are limited and need to be requested by the organization board. It seems that it is cheaper to hire new people, although already mentioned, it is almost impossible to find a specialist with all the required qualities and competencies.

In conclusion we can answer to SRQ3 - **What are the means of validating the workforce competency development model** by emphasizing that to improve and to validate EDL CDU's competency in DF community the main goal is to raise the volume of collaboration in investigations, participation in co-operated exercises and gaining more feedback from partner organizations about their results. This will ultimately raise their credibility and this in turn increases their involvement in protecting Estonia's information infrastructure and supporting broader objectives of national defence (The Estonian Defence League, 2018).

5 Concluding remarks

This thesis gives an overview and proposals for the DF workforce's competency based development and retaining plan. The model contributes to understanding the DF's competency-based training and its processes. In addition, there are suggestions for supplementing the DF's taxonomy model, changing the structure of the EDL CDU and distributing a new branch of DF's standards. The validation of the model took place through partner institutions, both national and international ones. The first level was the validation of competencies, where the competencies to be assessed were given to professionals to comment and prioritize. The second level of validation was based on the management level - evaluating the unit's growth of effectiveness, based on the organization's estimation assessment. Risks from feedbacks were studied and proposals for changes were implemented.

5.1 Answers to Research Questions

In this chapter we shall sum up all answers to main and supportive research questions.

MRQ – How to create effective Digital Forensic workforce competency based (competency structure) development and retaining a model for EDL CDU staff? This question was broken down into several sub-research-questions (**SRQ**):

SRQ1 – What is the current emphasis and constraints of DF's workforce development and training within the ranks of the EDL CDU? We investigated the existing EDL CDU's training program and decide which properties need to be considered for further development. Information was gathered and modeled using the GAP analyses method. In conclusion we can answer to **SRQ1** by pointing out that EDL CDU is a unit in a voluntary organization aimed at protecting Estonian cyberspace with its main mission to protect Estonia's information infrastructure and support broader objectives of national defence (The Estonian Defence League, 2018). EDL CDU can be called upon to service according to the Estonian Regulation No. 108, which mandates them to be used to fulfill the core roles in PBGB, RIA CERT and EDF in defending Estonia cyberspace. For this the members of EDL CDU have to fulfill certain key requirements and guidelines set up for DF specialist's roles. One of which is Netherlands Advisory Committee of Standards (ACS), ISO and the NRGD's DF standard's which distinguishes 6 subfields of DF(Computer Forensics, Software Forensics, Database Forensics, Multimedia Forensics, Device Forensics and Network Forensics). By the NRGD, the DF is a discipline of forensic sciences and therefore should be reviewed under ISO standards (overview can be see Annex Overview of standards regulating Digital Forensic community). As the EDL CDU recruits and is also responsible for training their members, they have used 4 shared knowledge principal:

1) Knowledge transfer;
2) Knowledge exchange;
3) Knowledge collectivism;
4) Knowledge distribution.

The main goal of the EDL CDU is to get as much practice as possible in the DF's community and to participate in national and international cyber security training events, which have set certain restrictions to training and recruitment policies (The Estonian Defence League, 2018). We have brought out an overview of some of these events (see Annex Services - suggested courses and curriculums) and DF's community requirements which the EDL CDU might come up against (see Annex Proposal for Digital Forensic Competency Model Framework based DOL Competency Model Tier 9).

SRQ2 – How to develop and retain DF workforce's competency in the EDL CDU? We answered this question in two parts, firstly "How to develop DF workforce's competency?" and secondly "How to retain DF workforce's competency in the EDL CDU?" For development of DF competencies we have seen fit to combine with the NICE DOL Competency framework, DF's Standard 1.1, revised Bloom's Taxonomy with changes to DF community(see Annex Suggested Instructional Strategies for Digital Forensics Use With Each Level of revised Bloom's Taxonomy), and DF ontology model(see Annex **Digital Forensic ontology on the example of EDL CDU**) to eventually create a task based competency model(see Annex Proposal for Digital Forensic Competency Model Framework based DOL Competency Model). The proposed model is calculated to be with long lasting effects though also having a long implementing phase. To have full effect on the EDL CDU, could be estimated to take maximum of 5 years (according to validators described in Section Assessment of the Digital Forensic' workforce development plan for the EDL CDU). Implementing phases are divided into 5 groups (see Figure 12):

1) Capability Mapping
2) Setting and re-evaluating Goals
3) Training
4) Recruitment
5) Continuous development (falls into second part of SRQ2 – Retaining DF competency in EDL CDU).

The model can be used at any time in these phases. Marking evaluations using the GAP analyses by "achieved" or "desired", marking the level of importance by "not applicable", "preferred" or "essential", used as in recruitment baseline or mapping and planning the course/training roadmap. As result of evaluations and remarks by evaluators we have compiled a DF workforce's competency suggestions. Tiers which we focused on were Tiers 5-7.

In the second part of SRQ2 – "How to retain DF workforce's competency?" we suggest our proposed model's 5th phase "Continuous development", which is supported by the Annex Services - suggested courses and curriculums. We provide an overview of the courses, curriculums and exercises which support training in different levels – trainee/student, trainer/teacher, evaluator or planner/organizer. We see it as a preventive measure for workforce stagnation and as a possibility for competency's continuous development. We emphasize that the proposed model (especially evaluation of existing specialists) is not intended to marginalize the level of expertise and knowledge of existing professionals (an employee who exactly meets the needs of his/her position i.e. Windows based specific analyst or Android based analyst), but to highlight the spectrum of competencies in the field of digital expertise to encourage professionals and managers to develop their knowledge and to emphasize continuous training and development of DF's skills. With this we insist the EDL CDU's team leaders to see the danger in the following – routine and stagnation, which may lead to problems i.e. work errors, lack of motivation, leaving work for new knowledge and challenges.

SRQ3 – What are the means of validating the workforce development roadmap? We focused on validating the proposed workforce's training and development roadmap accuracy by assessment from Estonia's leading experts in the field. In conclusion we can answer by emphasizing that to improve and validate the EDL CDU's competency in the DF's community the main goal is to raise the volume of collaboration in investigations, participation in co-operated exercises and gaining more feedback from partner organizations about their results. This will ultimately raise their credibility and in turn increases their involvement in

protecting Estonia's information infrastructure and supporting broader objectives of national defence (The Estonian Defence League, 2018).

In conclusion to answer our **MRQ - How to create an effective Digital Forensic workforce's competency based (competency structure) development and retainment model for the EDL CDU's staff**, we must first assess our current situation for the DF community (standards, requirements, etc.) and our target audience (to analyze what tasks are involved, what activities they are involved with and under what conditions, perform GAP analyses). From there, we can start comparing which existing models of competency development are best suited to our ability to provide workforce training. If the suitable model is chosen it needs to be tailored to the needs of the organization and reviewed to support collaboration with partners and workforce's continuous development. All of this, however, must be based on the DF community's supportive certifiable competencies.

5.2 Threats to Validity

As discussed in this paper, certain situations may endanger the validity of this model's evaluation results.

Risks to the internal and external validity of the research plan can mean that factors outside the EDL CDU's partner institutions may evaluate the results of the assessment. By ensuring internal validity, we want to make sure that our proposed model has the desired effect on the EDL CDU, whether our experimental model makes a difference and there is sufficient evidence to support the claim.

History – specific events that occur between measurements. For example, while awaiting for the results of the evaluation, there was a change in the internal staff policy and development plan of the partner organization, the results of which were not reflected by the evaluators, as the changes were not implemented 100% and there was no experience that could be reflected in the assessment. Additionally, these changes would be welcomed in terms of updating the model and updating the requirements and recommendations for the development of the workforce in the light of technological developments and the introduction of new solutions in cyber crime.

Maturation – Due to this model's long process, i.e. measuring competence, introduction of the changes and overall adaptability of the organization to use this model can last up to five years. Some employees, partner institutions can change their positions and priorities in terms of competences.

Testing – The effect of conducting a second experiment may already indicate changes in the organization's focus and priorities. This, in turn, would allow the model to be improved within the organization (goal setting) and within the framework (upgrading the list of competences).

Instrumentation – Changes in the observers and assessors of the EDL CDU and their affiliated partner organizations may differ in time due to the changes to the organization's internal structural changes, personnel policies, and focus. In addition, a change in the result may also be considered as adding competencies to this model over time.

Statistical regression – This risk is due to the choice of topics, taking into account the personal assessment of the supervisors and specialists, based on their view of the organizations' priorities. Differences may occur if assessment is done by groups of newly appointed vs experienced specialists/experts and supervisors.

Selection of subjects – As we mentioned, we chose a specific group of people and an organization to conduct our evaluation and we suggest avoiding randomization of the group chosen for the assessment as these may show differences between our findings and later testing.

Attrition – Professionals involved in the first assessment may see the full deployment and ability of this model, although we are not sure whether these specialists will remain working in their organization throughout the model, due to job changes within the company, as well as the possibility of an external career change. Those who remain in the organization until the model has reached the final fifth level may be more motivated to participate in the training and reach the level of experts.

We marked four contextual factors that may jeopardize the validity of our model.

First threat is, the fact that all the evaluators thought this whole spectrum of competencies is required from one person, and left out the chance of evaluating the whole unit. Thus their point of view, finding a person who has all the competencies, is almost impossible to achieve. Not to mention, training traits and values in Tier 1 i.e. compassion is something that is obtained in early childhood and later it may be through a psychotherapist. What this table is good for is being a good guide to all the skills and requirements that one person could look for.

Second threat is proving the effectiveness of low time and resource costs in developing a fully trained specialist. The model should provide certain areas to be more distinguishable - what are the key skills of a position and what are the skills that support key skills. For example, network forensics skills are supported by network knowledge. At the moment it only reads that this skill is necessary when the relationship is incomprehensible. Relationships would help a lot in "tuning" a person's skills.

Thirdly it was noted that the model might not be used for internal performance management and reporting because these assessment systems are often highly divisive and can harm morale to the detriment of overall organizational performance, unless managed very well. The size and complexity of the model would make it hard to apply to such performance management systems.

Lastly we are accepting the fact that having one profile of a forensics' analyst is not realistic. Especially in the context of EDL CDU, where there are volunteers, not necessarily being forensics professionals in their daily jobs. Through evaluators' recruitment experience it can be shown that is very difficult to identify professionals (so called versatilists), who have the skillset and knowledge wide and deep enough to fit in any possible digital forensics' scenario.

5.3 Conclusion

This is a primary theoretical assessment that has not been hardened in real life. Certainly the need for functions could be improved if EDL CDU could act as an active unit with this competency model for 1-2 years. It is important to keep in mind that the EDL CDU is a quite mobile and versatile unit and that the newly formulized team model consists of a static (management) and dynamic (team experts) part. The team must have enough hardware, software and skills to independently deliver the criminality in the cyber area with all the principals and practices of forensic field in order to use the data collected later by the prosecutor's office It should be taken into account that the team has communication with the main center, but must be prepared for the loss of the communication and the team itself has to deal with

the skills acquired and what they have. At expert level, there should be a very comprehensive digital forensic capability with legislation, document management systems, psychological and, in addition, physical properties above average.

EDL CDU Digital Evidence Handling team is taking more of RRT role and therefore taking into account evaluation suggestions – 5 different profiles of a forensics professionals have been mapped. The competency requirements will depend on the profile (suggestions are brought out in Annex VIII):

1) First line forensics professional – responsible for data acquisition and basic analysis (based on step by step procedures and available tools)
2) Digital forensics analyst – he is a second line analyst with wide overall knowledge and skills, being able to use more sophisticated forensics tools and have understanding of forensics aspects related to widely used IT products, such as Windows, Linux, android operating systems and their file systems, being able to perform not overly complex malware analysis, memory analysis, etc.
3) Digital forensics expert – is an expert in particular field of IT, e.g. expert in static malware analysis, Windows internals, Lotus notes mail server, Oracle e-business software, proprietary, non-standard database, a PLC, particular router etc. The idea is to identify as much as possible of different niche, specialist profiles, map some names to the profiles (people coming from industry, academia, partner organizations or nations) and call them only in cases when their particular knowledge is needed.
4) Incident handler – is responsible for overview of nontechnical forensics activity and has a coordination responsibility
5) Team manager – technical lead of a team of forensic analysts, in situation of bigger cyber unit or RRT team with a team of forensics professionals

Although these roles have been regarded as separate level of expertise, all members must be able to do everything – quickly adapt into new roles and situations if needed. This also means that the team leader / assistant / manager has to understand what the team is doing, this perception only occurs when the processes themselves have been passed and knowledge exists. We suggest EDL CDU to have big number of first line analysts, smaller amount of second line analysts (more expert professionals), and a number of deep specialists/experts, each in his/her own field and develop relations with partner organizations for more training possibilities.

5.4 Future Work

For further work, we have identified the proposed validation of a structural change through real-time use (training / exercises) and recording corrections. Secondly, we see testing the competency model in a real-life situation, using the team provided by the EDL CDU. Third, as a continuous work – upgrading the competency list of model and preparing tests for measuring competencies. A later goal would be to find a cost-effective action plan for the EDL CDU. The EDL CDU sees the opportunity to develop a similar competency-based model for other roles. In the long run, we will see that the next step should be to combine competency-based models between the EDL CDU and partner organizations to achieve a better domestic cyber security community as a whole.

6 References

Altawy, R., & Youssef, A. M. (2016). Security, Privacy, and Safety Aspects of Civilian Drones: A Survey. *ACM Transactions on Cyber-Physical Systems*, Concordia University. Retrieved from Concordia Institute for Information Systems.

Apollo Education Group Inc. and University of Phoenix. (2015). *Competency Models for Enterprise Security and Cybersecurity.* Apollo Education Group. Retrieved 01 07, 2019, from Apollo.

Aquilina, J. M. (2008). *Malware Forensics: Investigating and Analyzing Malicious Code.* Elsevier Inc.

Bogost, I. (2018, March 20). Can You Sue a Robocar? Retrieved from The Atlantic.

Brandom, R. (2018, July 3). Self-driving cars are headed toward an AI roadblock. Retrieved from The Verge.

Brinson, A., Robinson, A., & Rogers, M. (2006). A cyber forensics ontology: Creating a new approach to study cyber forensics. *Digital Investigation*, 37-43.

Bronk, H., Thorbruegge, M., & Hakkaja, M. (2006, December 22). *A step-by-step approach on how to set up CSIRT.* Retrieved from ENISA Publications.

Carnegie Mellon University. (2017). *What skills are needed when staffing your CSIRT?* Retrieved from Software Engineering Institute.

CCDCOE. (2019). *Training*. Retrieved from The NATO Cooperative Cyber Defence Centre of Excellence.

Central Intelligence Agency. (2018, July). *World Factbook 2017.* Central Intelligence Agency. Retrieved from CIA.

Charette, R. N. (2012, June 25). *Commercial Drones and GPS Spoofers a Bad Mix*. Retrieved from IEEE Spectrum.

Code of Criminal Procedure, RT I 2003, 27, 166 (August 1, 2004). Retrieved from Riigi teataja.

Columbus, L. (2016, November). *Roundup Of Internet Of Things Forecasts And Market Estimates, 2016.* Retrieved from Forbes.

CompTIA Certifications. (2018). Retrieved from CompTIA.

Conditions and procedure for involvement of the Defence League in ensuring cyber security, RT I, 10.07.2014, 3 nr 108 (August 3, 2014). Retrieved April 4, 2018, from Riigi Teataja.

Crisp, J., Pelletier, D., Duffield, C. F., Adams, A. A., & Nagy, S. (1997). Delphi method? *Nursing research*, 93-113.

Data Recovery Services Ltd. (2018). *What is volatile data?* (Data Recovery Services Ltd) Retrieved July 18, 2018, from Xcina Computer Forensics Specialists.

Davis, A. (2016, October 26). *UBER's self-driving truck makes its first delivery: 50,000 beers*. Retrieved from WIRED.

Dirik, A. E., & Karaküçük, A. (2014). *Forensic use of photo response non-uniformity of imaging sensors and a counter method*. Retrieved from Stemmer Imaging.

Ducharme, J. (2014). *Drone Journalism Code of Conduct*. Retrieved from College of the North Atlantic.

EASS. (2018). *EASS Specialties.* Retrieved February 19, 2019, from Estonian Academy of Security Sciences.

ENFSI. (2015, November). *Best Practice Manual for the Forensic Examination of Digital Technology*. Retrieved July 15, 2018, from European Network of Forensic Science Institutes.

ENISA. (2019). *Technical Training material*. Retrieved May 16, 2018, from European Union Agency for Network and Information Security.
Ford, R. (2018, August 31). Drone gang delivered drugs to prison windows. The Times. Retrieved from The Times.
Forensic Examination Act, RT I 2001, 53, 309 (January 1, 2002). Retrieved from Riigi Teataja.
G DATA Software AG. (2018). Malware Categories. Retrieved from Malware Categories.
Gettinger, D. (2018). *Public Safety Drones: An Update.* Center for the Study of the Drone. Bard College.
Hallett, J., Larson, R., & Rashid, A. (2018). *Mirror, Mirror, On the Wall: What are we Teaching Them All? Characterising the Focus of Cybersecurity Curricular Frameworks.* Baltimore: University of Bristol.
Harris, M. (2015, September 4). *Researcher Hacks Self-driving Car Sensors*. Retrieved from IEEE Spectrum.
Hederson, W. (2009). *New Federal Investigative Standards*.
Henseler, H., & Loenhout, S. v. (2018). Educating judges, prosecutors and lawyers in the use of digita lforensic experts. *Proceedings of the Fifth Annual DFRWS Europe, 24*, 76-82.
Hjelmvik, E. (n.d.). *Passive Network Security Analysis with NetworkMiner*. Retrieved from Forensic Focus.
Institute of the Estonian Language. (2018). *IT Terminology Dictionary*. (Institute of the Estonian Language) Retrieved July 19, 2018, from Institute of the Estonian Language.
International Organization for Standardization. (2018). *ISO OBP*. Retrieved from ISO Online Browsing Platform.
Jacka, M. J., & Keller, P. J. (2012, January 2). *Business Process Mapping: Improving Customer Satisfaction, Second Edition.* John Wiley & Sons, Inc. Retrieved from Wiley Online Library.
Jeffers, J. (2018). *What is Big Data?* Retrieved from InfoSec Institute.
Kaplan, A., & Haenlein, M. (2019, Januar). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, 15-25. Retrieved from ScienceDirect.
Karie, N. M., & Venter, H. S. (2014). Towards a General Ontology for Digital Forensic Disciplines. *Journal of Forensic Sciences*.
Keller, J. (2016, May 3). Iran–U.S. RQ-170 incident has defense industry saying 'never again' to unmanned vehicle hacking. Endeavor Business Media, LLC. Retrieved from Military & Aerospace Electronics.
Kemp, S. (2018). Digital report 2018. Hootsuite & WeAreSocial.
Keysight Technologies. (2018, July 28). *How 5G Will Influence Autonomous Driving Systems.* Retrieved February 27, 2019, from Keysight Technologies.
Kiper, J. R. (2017, January 30). *Forensication Education: Towards a Digital Forensics Intructional Framework.* Retrieved from SANS.
Kronfli, B. (2017, May). *Samsung DeX review*. Retrieved from The Inquirer.
Kukk, K. (2017). *Mapping the best practices for designing multi-level cyber security exercises in Estonia.* Tallinn: Tallinn University of Technology.
Lamus-Tšistotin, S. (2018). *Kaitseliit 100 juubeliüritused koguvad hoogu*. Retrieved from Kuulutaja.
Lee, T. B. (2018, December 30). *The hype around driverless cars came crashing down in 2018*. Retrieved from ARS Technica.
Lehtla, K. (2018, March 29). EDF LEGAD.

Loveridge, S. (2016, March). *Videogames*. Retrieved from Digital Spy.
Luuk, M. (2017). *Digitaalsete Tõendite Kasutamise Erisused.* Tartu: University of Tartu.
McAfee, LLC. (2019). *What is the Difference Between Malware and a Virus?* Retrieved from McAfee.
Metcalfe, T. (2018, August 20). *Pseudo-Satellite Drone Flies for 25 Days Straight, Sets Endurance Record*. Retrieved from Live Science.
Michigan Legal Publishing Ltd. (2017, December 1). *Rule 902 – Evidence That Is Self-Authenticating*, 2018 Edition. Retrieved from Federal Rules of Evidence.
Mile2. (2018). *Cyber Security Certification Roadmap*. (Mile2 Cyber Security Certifications) Retrieved May 16, 2018, from Mile2.
Morgan, S. (2018, June 28). *Global Ransomware Damage Costs Predicted To Exceed $8 Billion In 2018*. Retrieved from Cybersecurity Ventures.
NCSC. (2019). *NCSC-certified degrees*. Retrieved from National Cyber Security Centre.
Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* Gaithersburg: National Institute of Standards and Technology.
NICCS. (2016, March 15). *NICE Cybersecurity Workforce Framework*. Retrieved from Department of Homeland Security.
Noroff Education AS. (2019). *Bachelor in Digital Forensics*. Retrieved from Noroff - School of technology and digital media.
Noyes, D. (2019). *The Top 20 Valuable Facebook Statistics*. Retrieved from Zephoria Inc.
NRGD. (2018, June 5). *Standards: Digital Forensics (008.1 - 008.6),* 1.1. Retrieved July 1, 2018, from Netherlands Register of Court Experts.
Nääs, O. (2018, September 19). *Ringvaade - Nääs:"massiline pealtkuulamine surub ka seaduskuulekat inimest alla"*. Retrieved from Eesti Rahvus Ringhääling.
Owano, N. (2011, December 17). *RQ-170 drone's ambush facts spilled by Iranian engineer*. Retrieved from Phys.org.
Pan, S., Vega, M., Vella, A. J., Archer, B. H., & Parlett, G. R. (1996). Mini-Delphi Approach: An Improvement on Single Round Techniques. *Progress in Tourism and Hospitality Research*, 27-39.
Parate, S., & Nirkhi, S. M. (2012, December 6). A Review of Network Forensics Techniques for the Analysis of Web Based Attack. *International Journal of Advanced Computer Research*, 114-119. Retrieved from SemanticScholar.
Pau, A. (2017, May 17). *WannaCry reaches computers in Estonia*. Retrieved from Postimees Online.
Poikonen, J., Hyvönen, M., Kulo, A., Jokela, T., Tissari, J., & Paasio, A. (2016). *Remote and Autonomous Ships - The next steps.* London: Rolls-Royce. Retrieved from Media.
Postscapes. (2018). *Agriculture Drone Companies*. Retrieved from PostScapes.
Prosecutor's Office Act, RT I 1998, 41, 625 (May 20, 1998). Retrieved from Riigi Teataja.
Põldmaa, H. (2018, June 28). Director of EDL Cyber Defence Unit's Digital Forensic Group.
Raudsepp, G. (2018). *Perspective of Acquiring and Using Digital Evidence in Criminal Proceedings.* Tartu: University of Tartu. Retrieved from University of Tartu.
Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN/2017/0450 final (September 13, 2017).
Risk Placement Services, Inc. (2018). *Data Breach QuickView Report.* Illinois: Risk Placement Services, Inc.
Rollins, T. (2018, April 20). *MD5 Hashing: The Foundation of a Defensible E-Discovery Process*. Retrieved from exterro - E-Discovery and Legal Software.

SANS Institute. (2018). *Curricula*. (SANS Institute) Retrieved from SANS.
SANS Technology Institute. (2018). *Master of Science in Information Security Engineering*. Retrieved from SANS Technology Institute.
Security and Safeguarding Liberties - Prevention of and Fight against Crime, (2007/125/JHA) (2013). Retrieved from European Commision.
Skulmoski, G. J., Hartman, F., & Krahn, J. (2007). The Delphi Method for Graduate Research. *Journal of Information Technology Education:Research*, 1-21.
TalTech. (2019). *Curriculums*. Retrieved from Õppeinfosüsteem.
Tambur, S. (2018). Digital Economy Estonia: From IT tiger to the World's Most Pre-eminent e-state. Retrieved from New European Economy.
The Estonian Defence League. (2018). *The Estonian Defence League's Cyber Unit*. Retrieved April 3, 2018, from The Estonian Defence League Web site.
Tittel, E. (2017, October 12). How to become digital forensics expert.
University of Turku. (2019). *Cyber Security*. Retrieved from University of Turku.
Yan, W. Q. (2017). *Introduction to Intelligent Surveillance: Surveillance Data Capture, Transmission and Analytics.* Auckland: Springer.

License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Marek Matsalu**,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright, "The Development of Digital Forensics Workforce Competency on the Example of Estonian Defence League", supervised by Raimundas Matulevičius and Hillar Põldmaa.

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.
3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.
4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Marek Matsalu

Tartu, **16.05.2019**

7 Annex

I. Digital Forensic ontology on the example of EDL CDU

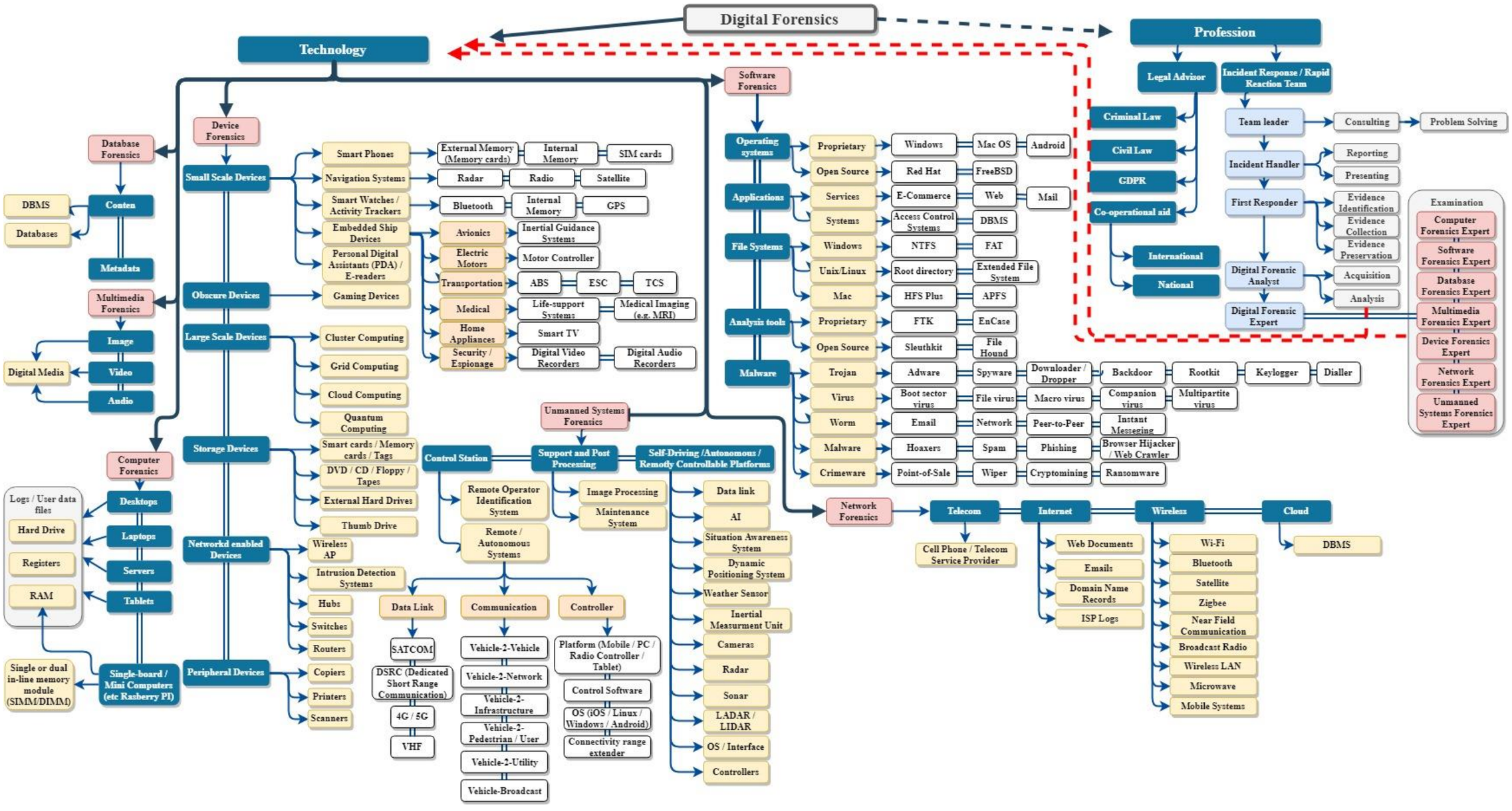

Figure 16 Proposal for complete Digital Forensic ontology for EDL CDU

II. Overview of standards regulating Digital Forensic community

Applicability of standards to investigation process classes and activities can be seen Figure 18, overview of these standards associated with DF's are:

ISO/IEC 15489-1:2016 – Defines the basic concepts and principals for creating, collecting and managing records regardless of structure or form, in all types of business and technological environments (International Organization for Standardization).

ISO/IEC 17025:2017 – Specifies the general requirements for the competence, impartiality and consistent operation of laboratories (International Organization for Standardization).

ISO/IEC 21043:2018 – Defines different components of the forensic process from scene to courtroom in Forensic sciences such as the detection and collection of physical evidence, the subsequent analysis and interpretation of the evidence, and the reporting of results and findings (as illustrated in Figure 17) (International Organization for Standardization).

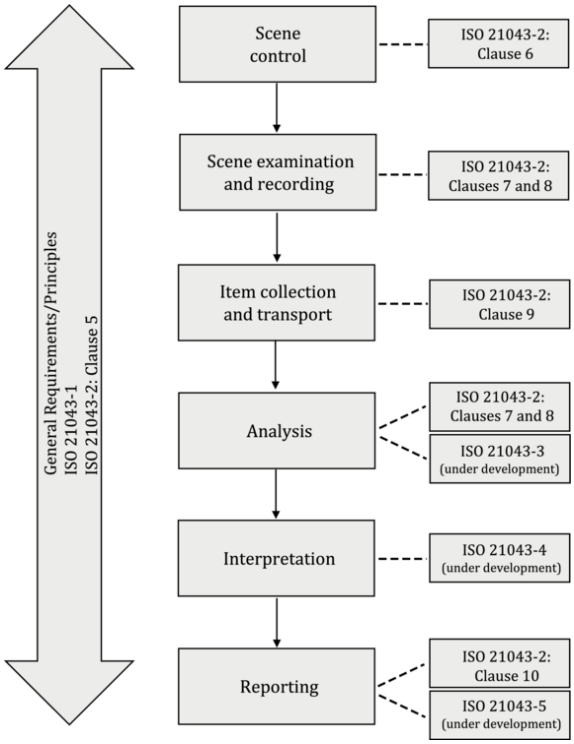

Figure 17 Relationship between the various components in the forensic process and the clauses within the ISO 21043 series (International Organization for Standardization).

ISO/IEC 23081-1 and 2:2009 – Defines the generic metadata types both for records entities as well as other entities that need to be managed in order to document and understand the context of records and also identifies, for key entities, a minimum number of fixed aggregation layers that are required for interoperability purposes (International Organization for Standardization).

ISO/IEC 27001:2013 – "Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization" (International Organization for Standardization).

ISO/IEC 27032:2012 – Provides guidance for improving the state of Cyber security, drawing out the unique aspects of that activity and its dependencies on other security domains (International Organization for Standardization).

ISO/IEC 27035-1 and 2:2016 – Part 1 outlines the basic concepts and steps for managing information security incidents and how to manage incident management by combining these concepts with principals with a structured approach to detect, report, evaluate and responding to incidents, and apply lessons learnt. Part 2 addresses the development of guidelines to increase the confidence of an organization's actual readiness to respond to an information security incident. This is achieved through the management of case management policies and plans, as well as on the creation of team response times and the results achieved over time, by taking lessons learnt and evaluating them (International Organization for Standardization).

ISO/IEC 27037:2012 – Provides detailed guidance on the identification, collection and/or acquisition, marking, storage, transport and preservation of electronic evidence, particularly to maintain its integrity (International Organization for Standardization). Devices that are affected by this ISO are storage media, mobile phones, cameras, computers e.g.

ISO/IEC 27038:2014 – Specifies the features of digital editing techniques for digital documents and also specifies the requirements for software editing tools and test methods for ensuring that digital editing is securely completed (International Organization for Standardization).

ISO/IEC 27040:2015 – Provides overview of concepts for data storage security in an organization and contains references to other international standards and technical reports on existing practices and techniques that can be applied to secure data storage (International Organization for Standardization).

ISO/IEC 27041:2015 – Provides guidance on mechanisms for ensuring that methods and processes used in the investigation of information security incidents are "fit for purpose", by ensuring that the appropriate methods and tools are used properly. "It should be applied prior to any investigation, in the context of principals and processes (defined in ISO/IEC 27043:2015) and sound preparation and planning (defined in ISO/IEC 27035-2) to ensure the suitability of methods to be applied in the investigative processes described in ISO/IEC 27037:2012 and ISO/IEC 27042:2015" (International Organization for Standardization).

ISO/IEC 27042:2015 – Provides guidance on the analysis and interpretation of digital evidence in a manner which addresses issues of continuity, validity, reproducibility, and repeatability. It covers what happens after digital evidence has been collected i.e. its analysis and interpretation (International Organization for Standardization).

ISO/IEC 27043:2015 – Provides guidelines based on idealized models for common incident investigation processes across various incident investigation scenarios involving digital evidence. Conclusively covers the broader incident investigation activities, within which forensics usually occur (International Organization for Standardization).

ISO/IEC 27050 (in 4 parts) concerns electronic discovery. Part 1 (2016) is giving overview of eDiscovery, defining terms, concepts, processes etc. Part 2 (2018) describes how technical and non-technical personnel at management can identify and take ownership of risks related to electronic discovery. Part 3 (2017) basically generic how-to-do-it guide laying out the key elements that shall form the basis of many DF manuals in future. Also this document offers guidance on the seven main steps of eDiscovery noted above (ESI identification, preservation, collection, processing, review, analysis and production). Part 4 which is under development, will be providing guidance on the ways an organization can plan and prepare for electronic discovery from the perspective of both technology and processes (International Organization for Standardization).

ISO/IEC 29100:2011 – This standard is intended for information and communication technology (ICT) systems for the protection of personally identifiable information (PII) also knows as personal data). The connection is through some privacy limitations on the use of custodian data in eDiscovery. In particular, there might be some restrictions on personally identifiable information (PII). This applies to natural persons and organizations involved in the identification, procurement, architecture, design, development, testing, maintenance, management, and management of information and communication technology systems or services for which identification information is required to control the processing of PII (International Organization for Standardization).

ISO/IEC 30121:2015 – This standard provides a framework for organizations to prepare them for a digital investigation before they occur and it applies to the organizations the development of strategic processes relating to the disclosure, maintenance, availability and cost-effectiveness of digital evidence (International Organization for Standardization).

BS 10008:2014 – This standard outlines best practice for transferring electronic information between systems and migrating paper records to digital files and furthermore it gives guidelines for managing the availability and accessibility of any records that could be required as evidence (International Organization for Standardization).

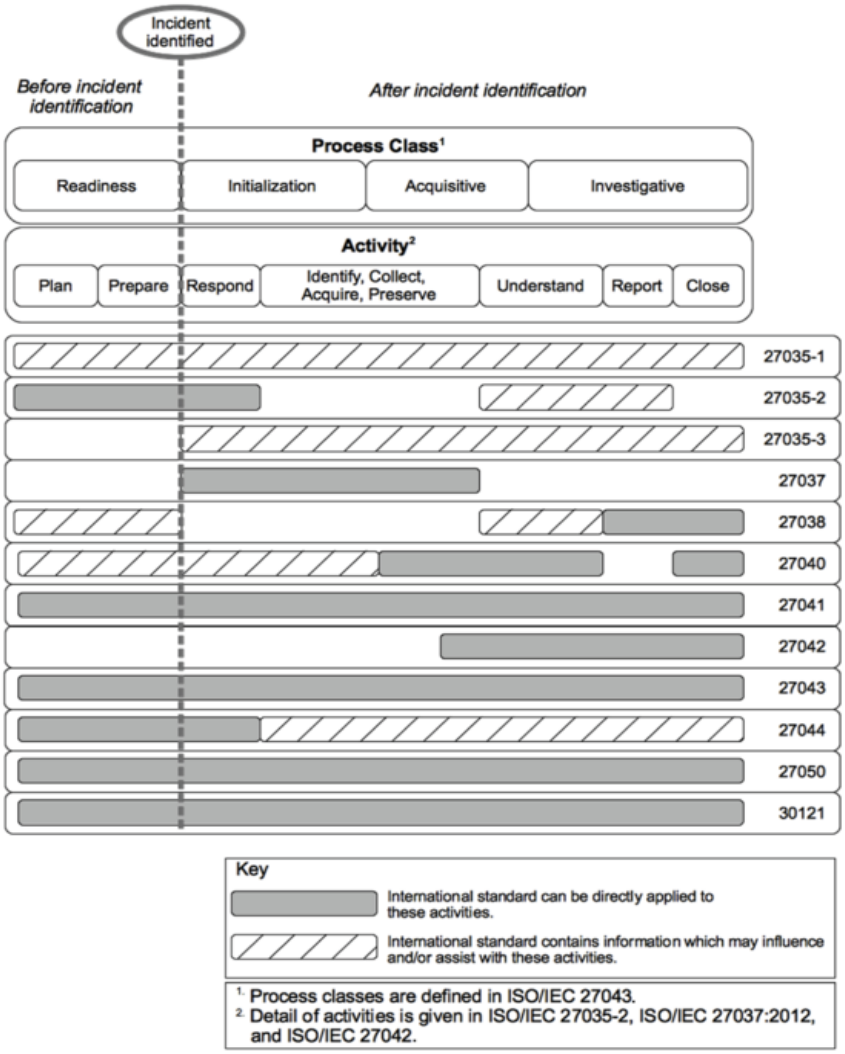

Figure 18 Applicability of standards to investigation process classes and activities (International Organization for Standardization).

III. EDL CDU structure plan after NICE Framework implementation to Digital Evidence Handling Group structure

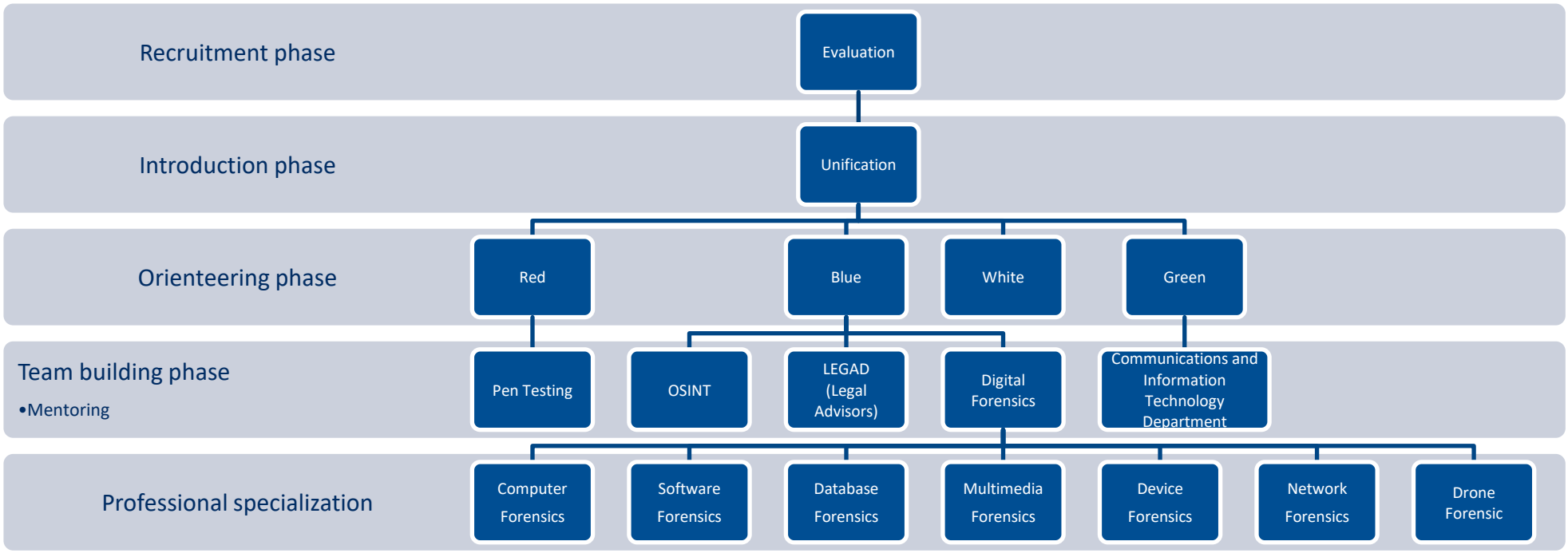

Figure 19 New EDL CU structure plan

IV. EDL CDU structure plan after implemented NICE Framework Component relationship

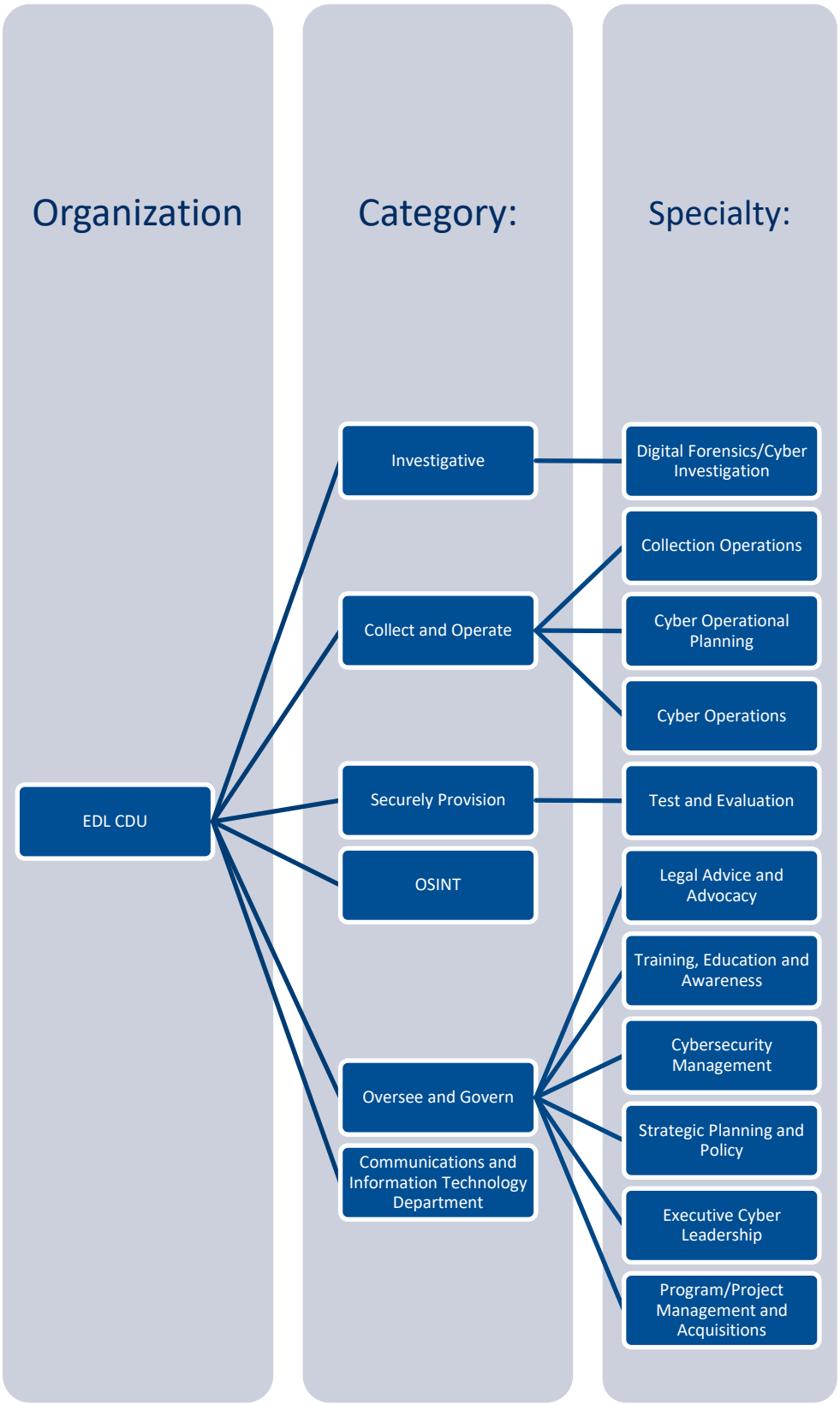

Figure 20 EDL CDU after implemented NICE Framework Component relationship

V. Suggested Instructional Strategies for Digital Forensics Use With Each Level of revised Bloom's Taxonomy

Activities					
		Workshops			Research projects
		Training			Problem statements
Facts		Practice			Case studies
Study		Exercises		Case studies	Creative Exercises
Lectures		Demonstrations		Research projects	Development Plans
Visual Aides		Projects	Problems	Exercises	Constructs
Audio and Video	Mentoring	Visualizations	Full-Scale Exercise (FSE)	Critiques	Simulations management
Narrative Examples	Online self-study	Simulations	Case Studies	Simulations	Exercise management
Illustrations	Questions	Role Play	Critical Incidents	Appraisals	Evaluation forms
Analogies	Discussion	Presentations	Discussion	Validate training	Workflow management
Conferences	Reviews	Functional Exercise (FE)	Questions	Evaluate equipment	Team management
Tutorials	Objective Tests	Full-Scale Exercise (FSE)	Tests	Evaluate techniques	Promote awareness
Tabletop Exercise (TTX)	Assessments	Operations-based Exercise	Exams	Evaluate processes	Develop competence
Drills	Reports	Examinations	Identify gaps	Evaluate plans	**CREATING**
Seminars	Tutoring	Practise interoperability	Explore issues	**EVALUATING**	Adapt
Games	Presentations	Demonstrate capabilities	**ANALYSING**	Agree	Arrange
Standards	Writing Assignments	**APPLYING**	Advertize	Anticipate	Build
Concepts	**UNDERSTANDING**	Act	Analyze	Appraise	Change
KNOWLEDGE	Associate	Administer	Appraise	Argue	Choose
Ask	Cite	Apply	Assume	Assess	Collect
Choose	Classify	Aqcuire	Break down	Award	Combine
Copy	Compare	Attack	Calculate	Choose	Compile
Count	Contrast	Build	Categorize	Compare	Compose
Define	Demonstrate	Capture	Classify	Conclude	Construct
Discover	Describe	Change	Compare	Confirm	Create
Enumerate	Discover	Contain	Conclusion	Consider	Delete
Find	Discuss	Conduct	Connect	Criteria	Design
How	Distinguish	Construct	Contrast	Criticize	Develop
Label	Estimate	Coordinate	Correlate	Decide	Discuss
List	Explain	Defend	Criticize	Deduct	Elaborate
Listen	Express	Demonstrate	Debate	Defend	Estimate
Match	Extend	Develop	Deduce	Determine	Formulate
Memorize	Generalize	Detect	Devise	Disprove	Happen
Name	Give examples	Experiment with	Detect	Estimate	Imagine
Observe	Identify	Identify	Differentiate	Evaluate	Improve
Omit	Illustrate	Illustrate	Discover	Explain	Intervene
Recall	Infer	Inform	Dissect	Find errors	Invent
Recite	Interpret	Interpret	Distinguish	Grade	Make
Recognize	Outline	Interrupt	Divide	Importance	Make up
Record	Relate	Interview	Examine	Influence	Manage
Relate	Rephrase	Make use of	Experiment	Interpret	Maximize
Repeat	Represent	Hunt down	Explain	Judge	Minimize
Reproduce	Research	Model	Function	Justify	Modify
Retell	Restate	Modify	Group	Mark	Organize
Select	Review	Operate	Inference	Measure	Original
Show	Rewrite	Organize	Inspect	Opinion	Originate
Spell	Show	Pen test	Inventory	Perceive	Plan
State	Sort	Perform	List	Persuade	Predict
Tabualte	Summarize	Plan	Motive	Prioritize	Prepare
Tell	Translate	Practice	Observe	Prove	Propose
What		Predict	Order	Rank	Promote
When		Produce	Outline	Rate	Schematize
Where		Report	Point out	Recommend	Set up
Which		Resolve	Prioritize	Reframe	Solution
Who		Schedule	Process	Revise	Solve
Why		Select	Question	Rule on	Structure

Visualize	Simulate	Relationships	Score	Suppose
	Sketch	Select	Select	Test
	Solve	Simplify	Summerize	Theory
	Teach	Subdivide	Support	Validate
	Transfer	Survey	Value	
	Track	Take part in		
	Utilize	Test for		
	Recover	Theme		
	Write			
Action Verbs				

Tabel 1 Suggested Instructional Strategies for Digital Forensics Use with Each Level of revised Bloom's Taxonomy

VI. Proposal for new Digital Forensic discipline – Unmanned Systems

As unmanned aerial vehicles (UAV's) have become more affordable, Smart Vehicles, Self-driving cars, Autonomous trucks (Davis, 2016) already hitting, the remote-controlled cargo ships are not far left behind. The threats for criminal misuses of these multi-complex systems is looking to be increasingly troublesome for both the users and the investigators. The interest in unmanned systems (UMS) by the general public has made car manufacturers (Lee, 2018) and UAV companies doing extensive research and investment in these recent years (Metcalfe, 2018) making it more likely to see these autonomous systems doing the biddings of average Joe, by the end of next decade (Brandom, 2018). While self-driving cars are thing of the future, UAV's are already present practice. Whilst common practice with these UAV's remain for the hobbyist and enthusiast, they are already fully used in many areas e.g. law enforcement (Gettinger, 2018), agricultural (Postscapes, 2018), sports, media and journalism (Ducharme, 2014). The need for forensical expertise arises when despite legitimate uses, the UAV's is being used for misconduct and or hijacked or tampered by third-party for criminal indent e.g. flying drugs in prisons (Ford, 2018). Cases where there is a need for forensic analysis of these devices in order to establish the chain of events. Forensic specialists must conduct acquisition and analysis of the device's internal storage, on-board flight data, captured media and operating system as well as the device can be controlled via Android and iOS devices. The proposed UMS taxonomy (see Figure 21 UMV Forensic taxonomy) will try to cover the aspects of all forensical field categories which the specialist should be familiarize himself. As far as the self-driving car forensic goes, the investigations is being done internally by the companies themselves as they try to limit the possibilities of commercial espionage. Although recent accidents which had lethal results, had to regard law enforcement as well still to what extent. The judistical system is not ready for autonomous cars as the first lethal cases have showed, as investigators try to decide who is to blame in these kinds of accidents (Bogost, 2018). On the other hand we can relate more freely with terms of UAV's. They are operated either by remote control or autonomously using onboard computers. The physical elements onboard a drone employ a network of sensors and actuators same as self-driving cars, that communicate with the ground control system via a wireless link. This meaning the UAV as well as any UMS system is vulnerable to attacks that target either the cyber and/or physical elements of these systems (e.g. the interface or software, data link). Perfect example of these elements being used against UAV's was in 2011 December, when U.S. Lockheed Martin RQ-170 Sentinel stealth drone was hijacked by Iranian cyber warriors in mid-flight (Keller, 2016). It is thought that mix of cyber-attacks were behind of capturing the U.S UAV. The weakest point was said to be the drones GPS which the Iranian engineers made spoofing attack to calibrate it to land on the "safe" base on Iranian soil. All communications were jammed (satellite and ground control) (Owano, 2011) (Altawy & Youssef, 2016). This said, it has to be noted that almost any UAV or other UMS manufacturer involved in command and control, streaming sensor downlinks or any other wireless connections (shown in taxonomy as Data link and Communication type) could be targeted and any system can be hijacked and hacked. These flaws still exist and although the manufacturers have made patches to fix them, they cannot foresee solutions for every kind of attack vector. Depending of the size or platform of the UMS's, they will have number of different systems on board to operate. Thus we have proposed for the new sub-divison of UMS forensics to be introduces as a separate sub-discipline in DF Standard. The cameras, radar, LIDAR, vehicle state monitoring, environmental mapping and obstacle detection, collision avoidance systems are just some examples which are present in autonomous vehicles (equally present at marine, aerial and ground vehicles).

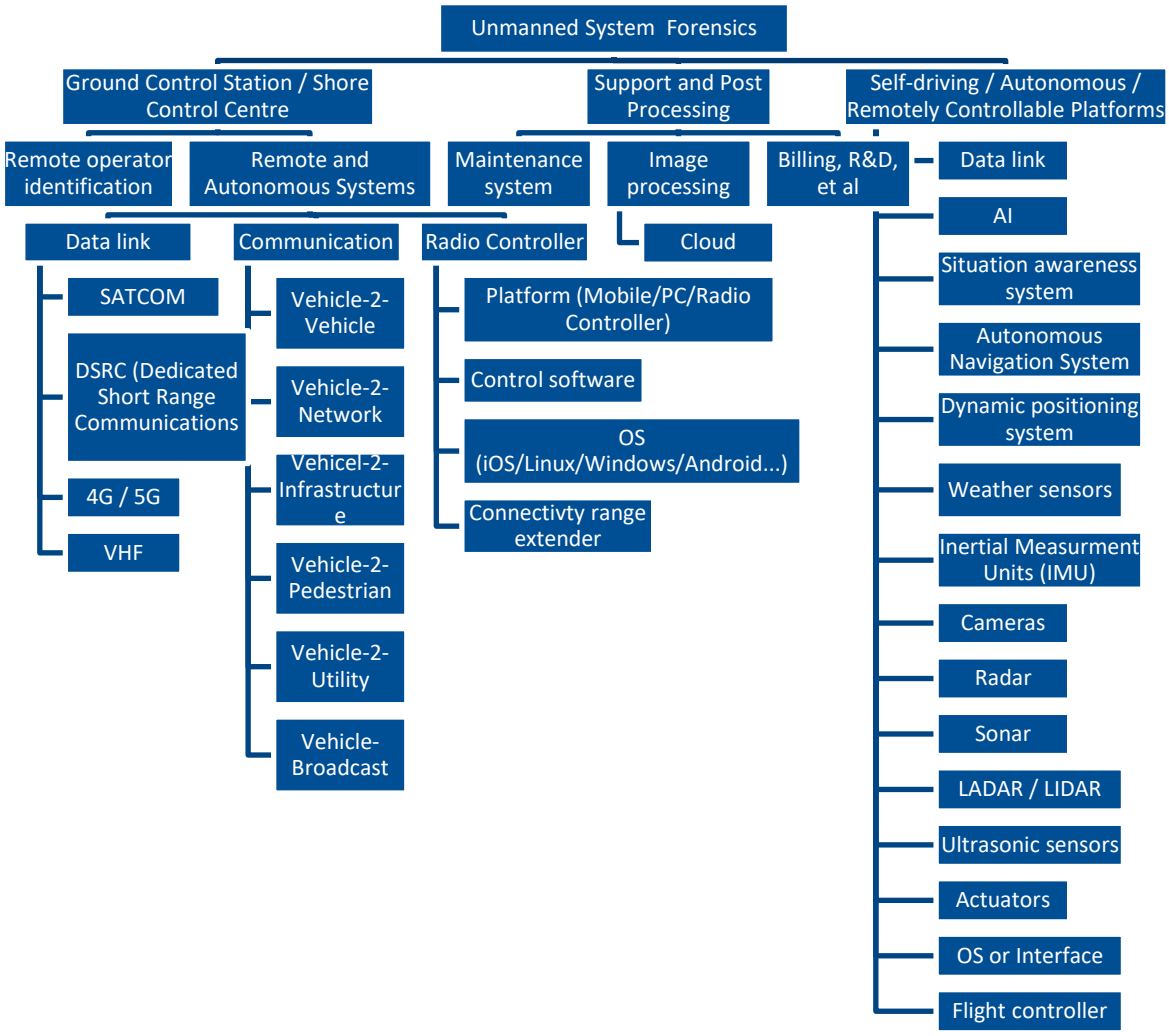

Figure 21 UMV Forensic taxonomy

All these systems are prone to flaws, malfunctions and attacks. Although these capabilities will be fusion together to perform as one navigation system, combining multiple sensor information and thus eliminating individual system or sensor error (Poikonen, et al., 2016). All platforms have GPS systems onboard and as previously mentioned, these are being seen one weakest points. Route planning via predefined waypoints may be recalculated by outside "force" and send vehicle to its new home base or even worse make cargo ships, drone or cars crash regardless if passengers are on board or not (Charette, 2012). Leaving GPS tampering aside, there shall be still possibility of spoofing attack against LIDAR[24], radar[25] or weather monitoring systems to make vehicle immobile of force them to return to base or harbor. A multi-thousand dollar system (LIDAR) was proven to be vulnerable by a $60 dollar setup (Raspberry Pi or an Arduino) (Harris, 2015), by putting fake objects anywhere near the vehicle, making it do perform sudden actions. Upcoming 5G promises to bring autonomous vehicles to all new level of safety and convenience. Advanced Driver Assistance Systems (ADAS) introduces new automotive ecosystem where sensor fusions with, previously mentioned RADAR, LIDAR and camera combination will be combine with

[24] Light Detection and Ranging system – scanning laser sensor technology for distance measurement.
[25] Radio Detection and Ranging system - to determine the range, angle, or velocity of objects.

Ethernet networking, high definition mapping with high precision navigation, and artificial intelligence. We use the "AI" definition by Kaplan and Haenlein – "a system's ability to correctly interpret external data, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation" (Kaplan & Haenlein, 2019) e.g. route planning and collision avoidance. This meaning there will be new possible attack vectors against remote or automotive systems. 5G coming also means developing and adapting wireless communication technologies like vehicle-2-vehicle (V2V), vehicle-2-network (V2N), vehicle-2-infrastructure (V2I), vehicle-2-pedestrian (V2P), vehicle-2-utility (V2U), and vehicle-2-everything or vehicle broadcasting (V2X). Vehicles will be "talking" to each other (real-time road conditions, pre- and post-collision warning, blind spot awareness), sharing real-time traffic information, SOS calls, reading roadside signs and sharing the changes found. Vehicles will additionally be able to interact with pedestrians (connecting to pedestrians smart device to inform them in case they might not see the vehicle approach) and refueling stations or power grid (hybrid or electrical vehicles contact charging stations) (Keysight Technologies, 2018).

This taxonomy highlights the future subdivision of prospective expertise, according to which a prospective specialist can plan the application of his/her competence. This list is not to regarded as a complete, as the UMS, driverless cars or autonomous vehicles have not yet been fully developed and proved to be failsafe and completely secure (from both self-inflicted mistakes and outside cyber-attacks).

VII. Services - suggested courses and curriculums

This Annex will give a brief overview of our suggested courses and curriculums which will provide some of the necessary training topics for our proposed competency model listing. Disclaimer - This is not complete list of possible courses, however it gives to the DF workforce development (in this case mostly for the EDL CDU) the selection courses which will be useful in fulfilling necessary competency level. We will give our suggestions for DF specialist competency roadmap specific courses and training possibilities which should fulfill EDL CDU needs as they may be called for upon Regulation No. 108. Course list consist training and course providers such as CCDCOE, SANS, CompTIA, Mile^2, TalTech, UT, ENISA and many more. Additionally we will list the FBI's Tier 1-3 Cyber backgrounds chart what are the preferred degrees and certificates.

CCDCOE's mission is to enhance the capability, cooperation and information sharing among NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation (CCDCOE, 2019). On the research part CCDCOE is well known to be authors of the "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" and previous "Tallinn Manual on the International Law Applicable to Cyber Warfare" which are influential resources for legal advisers dealing with cyber issues. CCDCOE offers a list of cyber-related courses to share the knowledge in the field of cyber security:

Introductory/Apprentice level courses

This paragraph gives our suggestion for mandatory courses for newly appointed DF specialist who are being introduced to DF tasks and to consolidate their already obtained knowledge and skills.

1. CCDCOE Introduction to Digital Forensics Course and Digital Forensics and Digital Evidence course

Introductory courses on DF and addressed for new specialist on forensic analysis field. Aim is to introduce new specialists with DF terminology, methodologies, chain of custody and principals of investigation authority. It cares to mention that this course focuses on Windows hosts and uses open source software as introductory course to in-depth forensics and reverse engineering training. Digital Forensics and Digital Evidence course is mostly a supporting course for the introductory course (CCDCOE).

2. CCDCOE Smartphone Security and Forensics Course

Perfect introduction to intermediate course for Device Forensics specialist who will be conducting digital evidence collecting and acquisitions. Although this course mainly focuses on Android and iOS mobile devices, it is perfect course for practicing same techniques on similar smaller devices as the course provides technical challenges and respective solutions in order to tackle threats form small-devices (e.g. smartphones, e-readers, personal assistant managers) (CCDCOE).

3. SANS SEC 301 Introduction to Cyber Security

Perfect for people who are new to information security and in need of an introduction to the fundamentals of security and also professionals with basic computer and technical knowledge in all disciplines who need to be conversant in basic security concepts, principals, and terms Introduces core security terms and principals e.g. principal of least privilege and the Confidentiality, Integrity, and Availability (CIA) triad, fundamentals of risk management, security policy, accountability and computer functions and networking (SANS

Institute, 2018). This course also provides an Introduction to cryptography and cyber security technologies (e.g. network and device security, malware and anti-malware).

4. SANS SEC 301 Introduction to Cyber Security

Perfect for people who are new to information security and in need of an introduction to the fundamentals of security and also professionals with basic computer and technical knowledge in all disciplines who need to be conversant in basic security concepts, principals, and terms Introduces core security terms and principals e.g. principle of least privilege and the Confidentiality, Integrity, and Availability (CIA) triad, fundamentals of risk management, security policy, authentication/authorization/accountability and computer functions and networking. This course also provides an Introduction to cryptography and cyber security technologies (e.g. network and device security, malware and anti-malware) (SANS Institute).

5. Mile^2 SP

This is mandatory course for all Cyber Security IT professionals, and should be regarded as a stepping-stone course for all DF specialist (especially Network, Device and Computer Forensics specialists). Topics which are provided are risk management, cryptography, identity and access management, data and network security, mobile device and application security amongst many others. The focus is to fully understanding of risk management and IT security in real-world point of view (Mile2, 2018).

6. Mile^2 IHE

This is apprentice to intermediate level course for First Responders and RRT members who have to prevent, detect and respond to cyber-attacks and start the digital evidence handling process and procedures (Mile2, 2018).

7. CompTIA Network+

This is a mandatory for course for apprentice Network Forensics specialist who has had some networking experience. This basic course covers networking concepts and their implementation, infrastructure, network physical security and common attack vectors and network management[26].

8. ENISA Digital forensics

Mandatory training material by ENISA for all DF specialist that introduces the principals of DF and digital evidence gathering and Chain of custody (ENISA).

9. ENISA Forensic analysis: Local Incident Response

This is a follow-up training material for ENISA Digital Forensics which practices incident response and investigation processes. Practical value in incident management by systematic approach (ENISA).

10. ENISA Introduction to network forensics

This online training material has all new version 1.0 released in January 2019 and it focuses exclusively in Network Forensics and best practices. Covers topics like, network-based evidence (difference and collection), logging and monitoring, timeline analysis, intrusion detection, SCADA, SSL traffic inspection, possibilities of VPN compromise and chain of custody amongst many others. Material is free of charge for all ENISA courses and they provide virtual images for these courses (ENISA).

[26] https://certification.comptia.org/training/certmaster/learn-network

11. ENISA Identification and handling of electronic evidence

This training material will be covering the basic principals of evidence gathering (e.g. image clone, live data capture) and verifying the applicability of gathered digital evidence (ENISA).

12. ENISA Building artefact handling and analysis environment

Apprentice to intermediate training material which is focused on building and practicing safe and secure conditions for operating important digital evidence or some form of malware (ENISA).

13. ENISA Processing and storing artefacts

This Software Forensics (Malware Forensics) apprentice to intermediate training focuses on different methods of collecting, sorting and storing artifacts. Specialists will be introduced to tools such as Shiva and Viper (ENISA).

14. ENISA Artefact analysis fundamentals

This training is the follow-up for previous Malware Forensics course. Topics that will be covered are static analysis techniques (string analysis, portable header analysis, import address table analysis i.e.), network analysis, behavioral analysis and will be conducting automatic analysis using the Cuckoo Sandbox tool (ENISA).

15. ENISA Forensic analysis: Network Incident Response

Practical training material for Network Forensic specialists covering network forensics techniques(collecting and analysing network traffic logs) (ENISA).

16. ENISA Mobile threats incident handling Part 1

Mandatory course material for Device Forensics specialist which will introduce concepts, tools, and techniques used for mobile devices (e.g. mobile phones, GPS, tablets, personal assistants, smartphones). Course material touches also network topics and operating systems which the DF specialist must familiarize themselves to perform essential device forensics processes (ENISA).

Intermediate level courses

1. CCDCOE IT Systems Attack and Defence

This is must-have course for any DF specialist in any sub-discipline field as this will give the experts perfect opportunity to think and see as the attacker. During this course, the specialists will conduct different so-called Capture the Flag competition type attacks on virtual machines and learn different penetration testing methods (e.g. Scanning and Enumeration, Privilege Escalation) (CCDCOE, 2019).

2. SANS FOR498 Battlefield Forensics & Data Acquisition

This a mandatory introductory/intermediate course for recognizing digital evidence (e.g. USB drives, smartphones, digital acquisition from different devices), and the various ways to collect them by rapid reaction team members, first responders and law enforcement officers. This course focuses on digital evidence identification, collection and preserving the chain of custody (SANS Institute).

3. SANS SEC 401 Security Essentials Bootcamp Style

Perfect for managerial board who want to understand information security beyond simple terminology and concepts although need an understanding of security to be effective, network administrators responsible for maintaining systems that are being targeted by attackers and forensic specialists and penetration testers who need a solid foundation of security principals to be as effective as possible at their tasks (SANS Institute). Few of these topics that will be covered are defensible network architecture, virtualization and cloud security, network device security, networking and protocols, securing wireless networks, securing web communications, security policies, critical controls, malicious code and exploit mitigations, Linux security, automation, auditing and forensics and many more.

4. SANS SEC 504 Hacker Tools, Techniques, Exploits, and Incident Handling

Core course for incident handling teams, system administrators, rapid reaction teams and other security personnel first responders. This course covers incident handling and computer crime investigation. Incident handling is introduced on a Step-by-Step method by introduction to the incident handling process, using the six steps (preparation, identification, containment, eradication, recovery, and lessons learned) which are necessary to prepare for and deal with a computer incident. Course also covers the details associated with reconnaissance, scanning, gaining access, buffer overflow and format string attack techniques and much more. (SANS Institute)

5. SANS MGMT 512 Security Leadership Essentials For Managers

Mandatory course for newly-appointed Information or Communication Security personnel who have been given leadership responsibilities (team leaders). This course covers what a security manager must know to function in today's environment (e.g. safety, physical security, how network protocols work, security, vulnerability) (SANS Institute). Specialists, team and project leaders will learn more about budget awareness and project management, network infrastructure, computer and network addressing, IP terminology and concepts, vulnerability management, managing physical safety and security.

6. SANS MGTM 525 and 535 - IT Project Management, Effective Communication and Incident Response Team Management

Mandatory for rapid reaction team and incident response team leaders to navigate in difficult and highly structured units/organizations and to analyze the data and information provided by technical staff, and translate this information into business relevant information that will be representable for superiors (SANS Institute).

7. SANS FOR 500 Windows Forensic Analysis

This course is essential for any DF specialist. It covers Windows OS components, core forensic principals, live response and triage-based acquisition techniques, acquisition review with write blocker, advanced acquisition challenges, windows image mounting and examination, file system overviews, document and file metadata, file carving, custom carving signatures, memory and unallocated space analysis, all which are core competencies what every DF expert must be familiar if not perfectly obtained (SANS Institute).

8. Mile^2 DFE

Regarded as essential course for digital evidence handling specialists and first responders who are responsible for evaluate, collect and document the digital evidence in focus of following the correct chain-of-custody and write detailed reports, skills needed for most forensic specialists disregarded from their sub-discipline field of expertize (Mile2, 2018).

9. CompTIA Security+

Targeted to networking and administrative personnel. Gives overview of security fundamentals, threats and vulnerabilities, application and host security an implementing network security (CompTIA Certifications, 2018).

10. ENISA Introduction to advanced artefact analysis

Introductory training material for Computer and Software Forensics specialist giving practical examples of dynamic and static analysis with OllyDbg debugger and IDA Pro (ENISA)

a. ENISA Advanced artefact handling – follow-up course.

11. ENISA Advanced artefact analysis

Mandatory training material is for Computer and Software Forensics specialist however suggested for all DF specialist who's task involve acquiring and analysing memory images from Windows and Linux operating systems. This course should be followed-up by Dynamic analysis of artefacts training material and Static analysis of artefacts material (ENISA).

12. ENISA Mobile Threats Incident Handling (Pt II)

This is mandatory training material Device Forensic specialists which covers mobile, network and malware forensic topics (ENISA).

Advanced level courses

1. CCDCOE Industrial Control Systems Security Course

This course explains security issues of ICS/SCADA environments, and to provide technical IT-staff who are fulfilling roles such as administrators and auditor whose daily duties do not necessarily include IC/SCADA-security, with the knowledge necessary to protect Programmable Logic Controllers (PLC) and industrial field devices. It offers hands-on exercises for training as well as taught content (CCDCOE).

2. CCDCOE Cyber Defence Monitoring Course

This course is perfect for Network Forensics specialist and who also are participating in Locked Shields exercise as a Blue Team member. It provides large-scale packet capture analysis with Moloch and gives practical experience in network traffic analysis (CCDCOE).

3. CCDCOE Malware and Exploit Essentials

As the name suggests it is essential course for specialist who will be training the Software Forensics sub-discipline field as their main specialty. Although this course is far from introductory course, because specialist who will be attending must already proven himself/herself with good or excellent skills in Linux and Windows environments (command line) and programming experience in assembler. This course will give you core principals of malware and exploit vulnerabilities and insight into intruder techniques. As this is highly technical course, it is highly recommended to view this course as Expert level training (e.g. specialist has previously gained the knowledge of Tier 6 and 7 in focus of assembler and higher programming languages and has proofed programming experience in assembler, C(++) or Python (CCDCOE).

4. CCDCOE Web Applications Attack and Defence

This course is both useful for Network and Software Forensics sub-discipline specialists. This course provides basic principals in web application security. Some of the topics covered are web app firewalls, web app pen-testing, web app vulnerabilities (CCDCOE, 2019).

5. SANS FOR 508 Advanced Incident Response, Threat Hunting, and Digital Forensics

It is intended for experienced DF specialists who want to improve their knowledge of intrusion investigation, incident response and expand their understanding of memory and schedule forensic. Course will be covering topics such as real incident response tactics, malware persistence identification, memory forensics analysis, event log analysis, advanced evidence of execution detection, timeline analysis, malware and anti-forensic detection and containment and threat intelligence gathering. Course can be summed up with three key activities: Detect, identify and perform damage assessment (SANS Institute).

6. SANS FOR 518 Mac and iOS Forensic Analysis and Incident Response

This is mandatory advanced course for Ideal for experienced Software, Computer and Device Forensics specialist who have to master Mac and iOS investigative skills. Course teaches Mac and iOS essentials and acquisition, thorough understanding of HFS+ file system, Mac and iOS triage, log parsing and analysis, Apple applications and password cracking and encrypted containers (SANS Institute).

7. SANS FOR 572 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

This advanced Network Forensics specialist hands-on course with Linux SIFT and other forensic tools (e.g. tcpdump and Wireshark). Course cover topics like core protocols, log aggregation, NetFlow and File Access protocols, wireless network forensics, full-packet hunting, Man in the Middle, Network protocol reverse engineering and investigation operation security and threat intel (SANS Institute).

8. SANS FOR 578 Cyber Threat Intelligence

This is a structured cyber threat analysis course for all sub-disciplines of DF specialists, especially for Software Forensics specialists (e.g. malware) who want to widen the skillset in filesystem forensics, investigations of technically advanced adversaries, incident response tactics, and advanced intrusion investigations (SANS Institute).

9. SANS FOR 585 Smartphone Forensic Analysis In-Depth

We suggest this as a mandatory course for Device Forensic specialists who are responsible in smartphones forensics. Course includes most commonly used smartphone devices with OS's such as Android, iOS, BlackBerry, Windows Phone and Chinese counterparts. Course covers different acquisition methods, analysis methods, files of interest, smartphone malware detection techniques and locating the infection vector (SANS Institute).

10. SANS FOR 526 Advanced Memory Forensics & Threat Detection

This advanced level memory forensics course crucial for Computer, Sofware and Device Forensic specialists to successfully perform live system memory triage and analyze captured memory images. Example of topics covered: List walking and scanning, pool memory, process relationships, kernel objects, DLL's virtual machine descriptors, detection of injected codes, user artifacts in memory, Linux/Mac/Windows memory acquisition and analysis (SANS Institute).

11. SANS FOR 610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques

As the name already suggest it is meant for Software (Malware) Forensics specialists. This advanced level purely technical course looks into real-world malware analysis and how to bypass them using a disassembler and a debugger (SANS Institute).

12. Mile^2 VFE

Course which is for performing virtualization forensic examinations. Target group is forensic investigators and virtual infrastructure specialists (Mile2, 2018).

13. Mile^2 NFE

Network forensic course that covers investigation and recovery of data in a network, Physical Interception, Traffic Acquisition, Analysis, Wireless Attacks, and SNORT. "The course focuses on the centralizing and investigating of logging systems as well as network devices" (Mile2, 2018).

Curriculums

The United Kingdom's has taken education and skills training seriously by adapting industry, government and academia to support the next generation of experts. Teachers, researchers, students and cyber security professionals all have been included National Cyber Security Centre (NCSC) workforce development model by providing support on Cyber School hubs to address the knowledge and skill gap in cyber security and also provide certified curriculums in Bachelor's, Integrated Master's and Master's degrees all over the UK. One examples is Edinburgh Napier University, which supports international studies and courses include software development, introduction to human-computer interaction, programming fundamentals, database systems, scripting for cyber security and forensics, digital forensics, web technologies, data analytics, networked services, network security and cryptography, OS forensics, security systems for lot, security testing and advanced network forensics, secure software development and many more (NCSC, 2019). This is perfect example of government involvement enhancing Cyber Security awareness and improving the possibilities of recruiting new specialist.

Moving closer to Estonia, the Norway provides three bachelor programmes (Cyber Security, Digital Forensics and Applied Data Science) which international students can also participate. Suggested DF curriculum gives an overall knowledge about the protection and research of digital systems and covers core theories, which are combined with practice. Amongst of these courses are Problem Based Learning and Research Methodologies, Introduction to Information Security, Professional Aspects of Computing, Introduction to Programming, Network Principals, Programming and Databases, Digital Forensics Practice and Procedure, Operating File Systems, File System Analysis, Network Security, Wireless and Mobile Devices and Digital Investigation (Noroff Education AS).

Furthermore University of Turku (UTU) in Finland and their Master's programme in Information Security, Cryptography and Security of Networked Systems covers System and Application Security, Network Infrastructure Technologies and Security, Human Element in Information Security, Management of Information System Security and IT Service Continuity, Cryptography, Protocol Processing and Security, Secure Sensor Network Systems, Software Development and Software Security amongst many other courses which can be studied on campus or via online studies (University of Turku).

Estonian own educational system provides both Bachelor's and Master's programmes. Bachelor Curriculum by Estonian Information Technology College, provides a higher education in broad domain of Cyber Security, integrating Software Development and IT Systems Administration. Curriculum includes topics like Malware, Network Security, social

Engineering, Digital Forensics (disk, network, host), Incident Handling, Intrusion Detection amongst other IT System Administration and Development courses (TalTech). Furthermore TalTech and UT united Master's programme, provides three main specializations (Cyber Security, Digital Forensics and Cryptography) in depth. This is perfect follow-up to Bachelor studies at Estonian Information Technology College. It provides students with core skills in the security of information systems and specialized skills in the chosen specialization. Student have chance to study under law enforcement, CERT, NATO CCDCOE specialists and other industries and institutions (TalTech). Courses topics include Computer Network Security, Malware, Data Mining, Cryptology, Secure Programming Techniques, System Forensics, Cyber Security Management, Network Forensics amongst many other specialized courses.

On the other hand SANS Technology Institute (additionally to single course provider) has developed a Masters is Information Security Engineering which is a non-thesis program that consist of series of technical, management, and communications SANS courses which are focusing on Cyber Defence Operations, Incident Response, Industrial Control Systems, Penetration Testing and Security Management amongst other courses e.g. FOR508, FOR572, FOR610 and SEC504 (SANS Technology Institute).

These are just a few of possible Bachelor's and Master's degree courses which can be suggested for DF specialist in EDL CDU as these can done via online studies and by graduating a student will be able to achieve the level of competence required in DF core activities in the industry.

Exercises / Competitions / Workshops

1. CyberCracker

Exercise type: Awareness study

Goal: Introduce 10-18-year-old students to digital safety in a olympic like competition manner (Kukk, 2017).

2. KüberNaaskel (CyberSpike)

Exercise type: National technical level

Goal: Promote Estonian Cyber Defence Talent Championship for 14-24 year olds, who will be participating at competition held at the Defence Forces Cyber Range. A miniature competition for young people who have not participated in major cyber competitions at primary school, upper secondary school, 14-25 years old (Kukk, 2017).

3. KüberSiil (Cyber Hedhog)

Exercise type: National operational and strategic level

Goal: Rehearse the applicability of national comprehensive cyber incident's resolution plan. The exercise included emergency response at operational and strategic level, involving partners. The aim was to assess the authorities' responsibilities, rights, readiness and procedures for communication (Kukk, 2017).

4. Crossed Swords

Exercise type: International technical level

Goal: To developing technical capabilities in a responsive way. Focuses on penetration testing in a simulated environment where participants are solving various complex tasks e.g. such as evidence collection, gathered data analyzation, identification of malicious actions (Kukk, 2017).

5. Locked Shields

Exercise type: International technical level

Goal: Practice the entire chain of command in solving a large-scale a cyber incidents using media and legal injections giving training possibilities for legal teams and threat analytics not only concentrating to forensic and technical network complexities. Locked Shields is known as the largest technical cyber defence exercise, which is held annually since 2010 and its target group is national security specialists whose profession is to defend IT systems in their organizations. Locked Shields is conducted in real-time and using real-life technologies and networks (Kukk, 2017).

6. Cyber Coalition

Exercise type: International technical, operational or strategic level

Goal: Rehearse existing processes and collaboration between national specialists handling different scenarios. Exercise is being held in a simulated environment and all participants are solving scenarios, which involved various tasks e.g. malware forensics, device forensics and hacking of prescribed networks (Kukk, 2017).

For comparing purposes we have also listed the FBI's Cyber backgrounds list of preferred Tier 1 – 3 degrees and certificates provided by Mile2 (Mile2, 2018). Tier 1 (Table 1)– low-risk positions, non-sensitive positions, and positions involving physical and/or logical access to government facilities and computer systems, Tier 2 (Table 2)– moderate-risk positions, non-critical sensitive positions, and positions requiring access to Confidential, Secret level information and Tier 3 (Table 3)– high-risk positions, critical sensitive positions, special sensitive positions, and positions requiring access to Top Secret and Sensitive Compartmented Information (Hederson, 2009).

1. C)IHE – Mile 2 Certified Incident Handling Engineer
2. C)NFE – Mile 2 Certified Network Forensics Examiner
3. C)NPTE – Mile2 Certified Penetration Testing Engineer
4. C)PTC – Mile2 Certified Penetration Testing Consultant
5. C)SWAE – Mile2 Certified Secure Web Applications Engineer
6. C)VA – Mile2 Certified Vulnerability Assessor
7. C)WSE – Mile2 Certified Wireless Security Engineer
8. CCDE – Cisco Certified Design Expert
9. CCE – ISFCE Certified Computer Examiner
10. CEH – EC–Council Certified Ethical Hacker
11. CEPT – Certified Expert Penetration Tester
12. CFCE – IACIS Certified Forensic Computer Examiner
13. CHFI – EC Council Computer Hacking Forensic Investigator
14. CISSP – (ISC)2 Certified Information Systems Security Professional
15. CNDA – EC Council Certified network Defence Architect
16. CPT – IACRB Certified Penetration Tester
17. CREA – IACRB Certified Reverse Engineering Analyst
18. CSSA – IACRB Certified SCADA Security Architect
19. CWAPT – IACRB Certified Web Application Penetration Tester
20. GAWN – GIAC Assessing and Auditing Wireless Networks
21. GCFA – GIAC Certified Forensic Analyst
22. GCFE – GIAC Certified Forensic Examiner
23. GCIA – GIAC Certified Intrusion Analyst
24. GCIH – GIAC Certified Incident Handler
25. GCUX – GIAC Certified UNIX Security Administrator
26. GICSP – GIAC Global Industrial Cyber Security Professional
27. GMOB – GIAC Mobile Device Security Analyst
28. GPEN – GIAC Certified Penetration Tester
29. GPPA – GIAC Certified Perimeter Protection Analyst
30. GREM – GIAC Reverse Engineering Malware
31. GSE – GIAC Security Engineer
32. GWAPT – GIAC Web Application Penetration Tester
33. GXPN – GIAC Exploit Research and Advanced Penetration Tester
34. MCSD – Microsoft Certified Solutions Developer
35. MCSE – Microsoft Certified Solutions Expert
36. SNFA – GIAC Network Forensic Analyst
37. SSCP – (ISC)2 Systems Security

Table 1 FBI's Cyber backgrounds list of preferred Tier 1 degrees and certificates Mile2 (Mile2, 2018)

1. ACE – AccessData Certified Examiner
2. C)DFE – Mile2 Certified Digital Forensics Examiner
3. CASS – Certified Application Security Specialist
4. CCCI – HTCN Certified Computer Crime Investigator
5. CCDA – CISCO Certified Design Associate
6. CCDP – Cisco Certified Design Professional
7. CCFE – IACRB Certified Computer Forensics Examiner
8. CCFP – (ISC)2 Certified Cyber Forensics Professional
9. CCIE – Cisco Certified Internetwork Expert
10. CCNA – Cisco Certified Network Associate
11. CCNP – Cisco Certified Network Professional
12. CCWS – IACRB Certified Windows Security Specialist

13. CISA – ISACA Certified Information Systems Auditor
14. CWNE – Certified Wireless Network Engineer
15. CWNP – Certified Wireless Network Professional
16. EnCE – Encase Certified Examiner
17. GCED – GIAC Certified Enterprise Defender
18. GCWN – GIAC Certified Windows Security Administrator
19. GSEC – GIAC Security Essentials
20. LPIC – 2 – Linux Professional Institute – Advanced Level
21. LPT – EC Council Licensed Penetration Tester
22. MCSA – Microsoft Certified Solutions Associate
23. Net+ – CompTIA Network+
24. Sec+ – CompTIA Security+
25. Server+ – CompTIA Server+
26. SSCP – (ISC)2 Systems Security Certified Professional

Table 2 FBI's Cyber backgrounds list of preferred Tier 2 degrees and certificates Mile2 (Mile2, 2018)

1. A+ – CompTIA A+
2. ACSP – Apple Certified Support Professional
3. ACTC – Apple Certified Technical Coordinator
4. C)ISSO – Mile2 Certified Information Systems Security Officer
5. C)SLE – Mile2 Certified Secure Linux Engineer
6. C)SS – Mile2 Certified Security Sentinel
7. CCENT – Cisco Certified Entry Networking Technician
8. CCT – Cisco Certified Technician
9. GISF – GIAC Information Security Fundamentals
10. IAM – INFOSEC Assessment Methodology
11. IEM – INFOSEC Evaluation Methodology
12. Linux+ – CompTIA Linux+
13. LPIC–1 – Linux Professional Institute Certification – Junior Level
14. TICSA – TrueSecure ICAS Certified Security
15. VMware – Vmware Certified Professional (vSphere)

Table 3 FBI's Cyber backgrounds list of preferred Tier 3 degrees and certificates Mile2 (Mile2, 2018)

These are one of many possible courses and trainings which provide excellent competency development environments for DF specialist. We urge the EDL CDU and other entities who are developing DF workforce competency roadmap to include this model and wide arrange of courses to be mandatory part in personnel management.

VIII. Proposal for Digital Forensic Competency Model Framework based DOL Competency Model

*Model table will be separate attachment