A Design Model for a Degree Programme in Cyber Security

Karo Saharinen
JAMK University of Applied Sciences
Piippukatu 2
40100 Jyväskylä
+358 50 410 4415
karo.saharinen@jamk.fi

Mika Karjalainen
JAMK University of Applied Sciences
Piippukatu 2
40100 Jyväskylä
+358 40 574 8012
mika.karjalainen@jamk.fi

Tero Kokkonen
JAMK University of Applied Sciences
Piippukatu 2
40100 Jyväskylä
+358 50 438 5317
tero.kokkonen@jamk.fi

ABSTRACT

The need for skillful cyber security workforce has increased dramatically during the last ten years. The contents of the degree programmmes have not been able to respond to this need adequately and the curriculum contents have not always met the industry's knowledge needs.

In this paper, we describe a model for designing a degree programme in Cyber Security. We establish the guiding frameworks and requirements within the European Union for a degree programme. Given the researched background, we propose a systematic way to implement knowledge, skill and competence objectives to a degree programme by using generally accepted frameworks. The framework targets engineering education in information technology, cyber security given on university level.

By having a well-established model for the degree programme, the private and public sector can flourish by having competent personnel at their use as employees.

CCS Concepts

• Social and professional topics → Professional topics → Computing education → Model Curricula

Keywords

Cyber Security, Education, Competence, Skill, Knowledge, European Qualifications Framework, Degree Programme

1. INTRODUCTION

Workforce need for Cyber Security professionals has grown in the field of information technology with a fast pace. ICASA White Paper on the State of Cyber Security 2019 reports that the need for technical cyber security personel is rising and enterprises are struggling to fill their open positions [1]. According to the research from $(ISC)^2$ Cybersecurity Workforce Study report, the worker gap is 142 000 in Europe, the Middle East and Africa [2].

The education sector is under pressure to fulfil the needs to train competent workforce for the needs of industry. According to Burley et al. [3], cyber security degree programs are seen to be undeveloped. It seems that there is a lack of university level education in the field of cyber security. Cohen et al. pointed out in their paper that it is essential to recognize the demanded skills needed in government, industry and company levels [4]. Ciampa et al. argued in their paper that keeping the curricula up to date in relation to industry needs is very challenging [5] due to the fast development of ICT technology. Hence, threat vectors in cyber security also develop and change very rapidly.

CSIS - Center for Strategic & International Studies - publication from January 2019 shows critique to the education system about how Cyber Security is organized in the Education systems: "Organizations are also frustrated by the current cyber security education ecosystem, which lacks common metrics or rankings to help employers understand what programs, certifications, and degrees are the most effective." [6]. Raj et al. argue in their paper that it is crucial to standardize the cyber security curricula and the expected board of skills needs to be defined based on cyber security domain needs [7]. It can be undeniably said that there is a need for clear frameworks that describe the competence needs of the substance. After describing the skill needs, the model can be modeled under the curriculum to be built, which will ensure that the curriculum responds to the industry's competence needs and focuses sufficiently on the intended area of expertise.

In this paper, we researched the frameworks within Cyber Security education sector and the general frameworks regulating and guiding academic education in the area of the European Union. These frameworks are presented in chapter 2. The proposed model for designing a degree programme is established in chapter 3, and examples are given in chapter 4. Finally, we conclude with remarks on future research that should be conducted in this area.

2. EDUCATIONAL FRAMEWORKS

2.1 Frameworks in the European Union

Within European Union the European Qualifications Framework (EQF) [8] EQF categorizes qualifications and competences into eight different levels, from EQF Level 1 to EQF Level 8. EQF also defines the characteristics of education to Knowledge, Skills and Competence, the explanations of which are given in table 1.

Table 1. EQF terminology [8]

Skills	means the ability to apply knowledge and use know-how to complete tasks and solve problems. In the context of the EQF, skills are described as cognitive (involving the use of logical, intuitive and creative thinking) or practical (involving manual dexterity and the use of methods, materials, tools and instruments)
Knowledge	means the outcome of the assimilation of information through learning. Knowledge is the body of facts, principles, theories and practices that is related to a field of work or study. In the context of the EQF, knowledge is described as theoretical and/or factual
Competence	means the proven ability to use knowledge, skills and personal, social and/or methodological abilities, in work or study situations and in professional and personal development

To harmonize, increase quality and enable student possibilities for multinational education within the EU, the member states are required to publish National Qualifications Frameworks [9]. These NQFs describe how current degree programmes within a member state map to the level requirements of the EQF.

ECTS User's Guide [10] describes and gives recommendations how degree programme supporting documents should be written.

This is to promote transparency and transferability of studies within the European Higher Education Area (EHEA).

European Network for Accreditation of Engineering Education (ENAEE) gives out a framework for engineering education that ensures quality in all branches of engineering education [11]. EUR-ACE® label is awarded to degree programmes as a sign of quality of the degree programme. EUR-ACE categorizes the Programme Outcomes into eight learning areas, which are same for both the Master's Degree and the Bachelor's Degree:

- Knowledge and Understanding - KU
- Engineering Analysis - EA
- Engineering Design - ED
- Investigations - IN
- Engineering Practice - EP
- Making Judgements - MJ
- Communication and Team-working - CT
- Lifelong Learning – LL

Additionally, in the home country of the writers, the Finnish Cyber Security strategy insists that cyber security skills should be a part of all education levels of the Finnish education system [12].

2.2 Education Frameworks within the Cyber Security

Cybersecurity education Joint Task Force (JTF) has launched curriculum guidelines for post-secondary degree programs in cybersecurity [3] where the Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS) and Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC) combined their views on curriculum development. The report also takes into account the different knowledge areas of cyber security. The report also presents well the wide range of knowledge's and the complexity of cyber security as it also has to take into account the relation to the IT environment where the needed cyber security skills are applied. Thus, in curriculum development one needs to accurately select the skills and abilities that one is aiming to educate. The overall picture of cyber security is too wide to be covered by one curriculum.

Internationally recognized accreditation body for engineering programs (ABET) has proposed the accreditation criteria for cybersecurity [13].

In Comprehensive National Cybersecurity Initiative [14] US President Barack Obama recognized cybersecurity as a critical challenge of economic and national security. By that recognition National Initiative for Cybersecurity Education (NICE) was initiated with the idea that an important resource in cyber resilience are the people with appropriate skills [15].

NICE framework is published by The National Institute of Science and Technology (NIST) [16]. Fundamentally NICE originates and focuses on the US; however the global nature of cyberspace is noticed there by partnering and global communities [15].

NICE framework describes and categorizes the work in cybersecurity into Work Roles and tasks assigned to those Work Roles. Those tasks require certain Knowledge, Skills and Abilities shortened as KSAs. With the mapping of KSAs to work roles, Educators can have awareness of how to map them into current course curricula. As stated in [15] "*Educators and trainers can use the framework to help answer these critical questions: What am I preparing my students for? What knowledge and skills do they need? What should I be teaching?".* In this study, that mapping is carried out as the design approach for a Degree Programme in Cyber Security.

The National Security Agency in the United States recognises two types of Centers of Academic Excellence (CAE): one in Cyber Defence (CAE-CD) and one in Cyber Operations (CAE-CO). NSA lists these degree programmes on their webpages, acknowledging the degree programme's quality, however, NSA does not directly fund the degree programmes. [17]

Cyber Defence (CAE-CD) consists of Knowledge Units. These Knowledge Units have been assigned to fit into NICE Framework Categories [18]. The Knowledge Units are for example:

- Cybersecurity Principles - SPY
- Basic Cryptography - BCY
- Security Program Management - SPM
- Basic Cyber Operations - BCO

Cyber Operations has only the criteria for measurement according to NSA [19] [20] but no valid Knowledge Units could be found during the writing of this paper. National Cyberwatch Center of the United States hands out a guide for mapping degree programme courses to the Knowledge Units of CAE-CD [21]. Based on the presentation "What They Are Teaching Kids These Days - Comparing Security Curricula and Accreditations to Industry Needs" at Black Hat 2017 [22], the degree field of the United States is in discussion how to implement Cyber Security in to their degree programs.

3. PROPOSED MODEL FOR DESIGNING A DEGREE PROGRAMME IN CYBER SECURITY

Given the developments of different frameworks into the field of Cyber Security, we propose the following model for Educational Organizations given in figure 1.

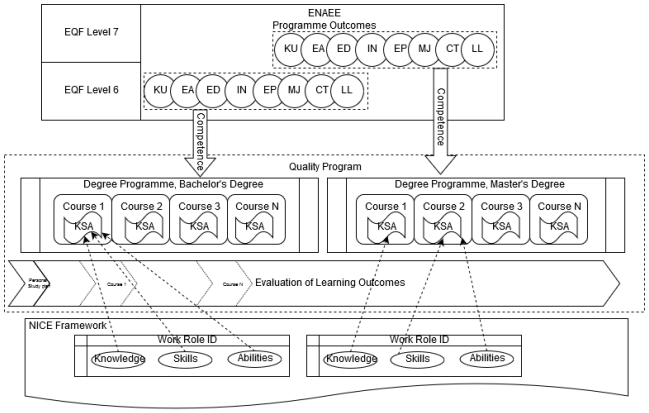

Figure 1. Model for Cyber Security Education Framework

The Programme Outcomes of ENAEE are described as competences of the degree programme. In order to achieve these

ICETC, 11th International Conference on Education Technology and Computers, October 28-31, 2019, Amsterdam, Netherlands.

DOI: http://dx.doi.org/10.1145/12345.67890

outcomes the courses are mapped to develop these competences accordingly to their degree level. Degree levels are mapped to the European Qualifications Framework according to National Qualifications Framework.

NICE Framework gives strict Work Role ID's that demand the development of certain Knowledge, Skills and Abilities to perform in given tasks assigned to the Work Role ID. These KSAs should be distributed as learning outcomes for the courses within the degree programme. These outcomes are also mapped to competences.

The development of the learning situations, laboratory exercises and types of assessment is left for the given course lecturer to choose the pedagogical solutions, which might include e.g. personal or group assignments, presentations, essays and exams.

Nonetheless the assignments should always develop the learning outcomes of the course. In addition, whatever evaluation method is used, it should assess the students' capability in the given NICE Knowledge, Skill or Ability.

4. RESULTS

4.1 Competences

Competences should be mapped to different courses as described earlier in chapter 2. The ECTS User's Guide also promotes that these should be recorded as the learning outcomes of the programme. In our course descriptions these are seen as the competences -field.

In table 2, we present our mapping of the ENAEE competence model and how it is brought down to our Master's Degree courses in our degree programme at JAMK University of Applied Sciences [23].

Table 2. Competence Mapping to Courses

Cyber Security, Master's Degree	ECTS	KN	EA	ED	IV	ER	CT	LL
Security Management in Cyber Domain	5	X	X					
Cyber Security Implementation in Practice	5		X	X				
Auditing and Testing Technical Security	5				X	X		
Cyber Security Exercise	5						X	X

In our model the last course, Cyber Security Exercise, summarizes the degree programme and promotes life-long learning competence. The student, under the guidance of an educator, can evaluate all the earlier competences in the exercise, run in a safe learning environment.

Given table 2, the following chapters give examples as a case study for the Cyber Security Implementation in Practice course [24].

4.2 Learning Objectives

The learning objectives in our model are a double-edged sword. In the ENAEE competence model, we have generalized competences that every engineer should possess. In NICE framework, we have very specific tasks that competent personnel should handle in the field of Cyber Security. The Learning Objectives in the course description should have the best of both worlds.

Cyber Security Implementation in Practice course [24] has had cryptography as a field of implementation: How are mathematical algorithms are written in different computer languages and how cryptographic material is stored and used in computer systems? This learning objective is tied to two different work roles (as an example) in NICE:

- Cyber Defense Analyst (PR-CDA-001)
  - Knowledge of cryptography and cryptographic key management concepts, K0019
- Communications Security (COMSEC) Manager (OV-MGT-002)
  - Knowledge of encryption algorithms, K0018
  - Skill in using Public-Key Infrastructire (PKI) encryption and digital signature capabilities into applications (e.g. S/MIME email, SSL traffic), S0138
  - Ability to manage Communications Security (COMSEC) material accounting, control and use procedure, A0165

In the ENAEE competence model, these tie to Engineering Analysis: how do the algorithms work and are written? The understanding of what different dependencies computer systems have in the written cryptographic libraries. They are also bound to Engineering Design competence on how to manage the cryptographic material in different computer systems and how it is created, distributed and used within the organization. This is summarized by the Learning Objective of Cryptography in Computer Systems.

Thus, the KSAs that NICE framework presents are mapped to learning objectives that are presented in the curriculum's course description in the learning outcomes -field.

4.3 Learning Situations & Assessment

Given student assignments should reflect the learning objectives. In the Cyber Security Implementation in Practice -course, the cryptography topic is further delved into with having lectures on the subject, classroom implementations as step-by-step guides followed by a research/implementation paper written on the chosen topic by the student. The written paper is then peer-reviewed and graded in the course by a fellow student. The lecturer grades the paper, multiple peer reviewers grade the paper, and the grade is then given for the whole assignment using a mathematical equation agreed at the start of the course.

Lectures increase knowledge, but also by writing and peer reviewing the student's understanding is further enhanced. Step-by-step classroom implementation enhances the theory into implementation skills, and the given implementation or research project enhances the ability to take this knowledge and skills into use. Understanding of the phenomenon further enhances as the students peer review each other's work.

As stated earlier, the learning situations can be from lectures to increase Knowledge and Understanding, to Investigations on researching and writing research/implementation papers, however, to enhance Communications and Team-working, full cyber security exercises could be run by the degree programme.

The assessment should concentrate on the KSAs assigned for the course and also be visible to the students in the course description. Different taxonomies such as Bloom's [25] or Solo's [26] Taxonomy could be used for assessing the levels of learning.

Technical competences were highly demanded in the background literature [1] [2] [4]. Based on our experience, a technical cyber range should be implemented to fully grasp the concepts of Cyber Security. Individual laboratory exercises can, in our opinion, develop the understanding and skills of some technical detail; however, cyber security often covers the interdependency of multiple technical details. Such interdependency, and resilience to withstand problems facing that interdependency, can only be taught in a realistic cyber environment, often called a cyber range.

At JAMK University of Applied Sciences in the Master's Degree programme [23], the competences are developed and can be

publicly viewed. In addition, different courses can be further examined on what NICE KSAs they develop [27] [24] [28] [29].

Quality of the Degree programme should be monitored by the Quality Program within the Education Organization. In the European Union we recommend official accreditation programs such as ENAEE EUR-ACE® -label.

5. DISCUSSION

As the need for cyber security expertise grows in the industry, the need for an up-to-date degree program also increases. It is vital that when building the curriculum, the degree program should use some existing generally accepted framework researched from the industry. As the field of cyber security is broad, these frameworks help to focus on the learning objectives in the curriculum.

By providing good education on a well-established model, we can provide students a with a well-organized study path and the industry with clear visibility on the developed competences of the student. Increasing the performance of both the student and the industry.

Thus, we have mapped the EQF framework into our curricula and accredited one of the curricula by ENAEE, EUR-ACE –label. In this research paper, we mapped the curriculum courses to NICE framework to ensure that our degree programme is up-to-date and the education meet the needs of the industry. NICE framework is an extensive and multidimensional frame that can be used as a guideline for scoping the degree program and to ensure that the learning outcomes meet the industry demands.

Given the wide variety of different frameworks, some more specified to cyber security than others, the terminology within the frameworks overlaps, has different meanings and the interpretation is left to the reader. One example is Knowledge from the EQF which translates in ENAEE as Knowledge and Understanding. Another is Abilities in the NICE Framework, while EQF only recognizes Knowledge, Skills and Competence.

One inconsistency of the NICE Framework is that one singular knowledge is too specific and another one is too broad. As an example of this, the Knowledge of computer algorithms (K0015) is very abstract. However, encryption algorithms do not count as computer algorithms as they are categorized as a different Knowledge's (K0018)?

In our opinion, the knowledges expand from EQF level to another, further deepening the students' grasp of the concept. Thus, even though it isn't a part of the learning outcomes of a course, or an item of assessment, it should not be completely discarded from the course. This gives many interpretation problems for the teacher of the course and might be seen as an inconsistency of the degree programme.

In addition, some courses (e.g. the Cyber Security Exercise [27]) in the degree program, are so vast that they develop multitude of different knowledge, skills and abilities. These cannot be all evaluated within the course but are known to develop during the course. These cases are problematic to describe in the course description.

6. FUTURE WORK

Cyber Security is taught in the area of the EU; however future research should be made to study different competence models and course descriptions within those educational organizations. We know that in the area of ICT the labor force can move globally; hence, the research should also compare degree programs between the EU and for example USA or Asia.

One aspect for the future research is also to study how the students achieve the NICE KSA skills, brought down to the degree programme by this model, by conducting a survey study with the students attending the programme. In the survey, the student experience of the learning outcomes could be measured to reflect the NICE KSAs given for the course.

In addition, the workforce needs change based on the physical locations of the education organization, thus maybe the frameworks of describing cyber security workforce should differentiate between the locations. Further market inquiries could be made on how to match the industry needs of a location.

7. REFERENCES

[1] State of Cybersecurity 2019: Current Trends in Workforce Development. 2019. White Paper. ICASA.

[2] $(ISC)^2$ Cybersecurity Workforce Study. 2018. $(ISC)^2$.

[3] Burley, D., Bishop, M., Buck, S., Ekstrom, J., Gibson, D., Hawthorne, E., Kaza, S., Yair, L., Mattord, H. and Parrish A. Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. 2015. DOI: http://doi.acm.org/10.1145/3184594

[4] Cohen, B., Albert, M.G. and McDaniel, E.A., 2018. The Need for Higher Education in Cyber Supply Chain Security and Hardware Assurance. International Journal of Systems and Software Security and Protection (IJSSSP), 9(2), pp.14-27.

[5] Ciampa, M. and Blankenship, R., 2019. Do Students and Instructors See Cybersecurity the Same? A Comparison of Perceptions About Selected Cybersecurity Topics. International Journal for Innovation Education and Research, 7(1), pp.121-135.

[6] The Cybersecurity Workforce Gap. 2019. CSIS.

[7] Raj, R.K. and Parrish, A., 2018. Toward Standards in Undergraduate Cybersecurity Education in 2018. Computer, 51(2), pp.72-75.

[8] COUNCIL RECOMMENDATION of 22 May 2017 on the European Qualifications Framework for lifelong learning. 2017. Retrieved March 20, 2019 from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017H0615(01)&qid=1552997420044&from=EN

[9] Government Decree on the National Framework for Qualifications and Other Competence Modules. 2017. Finland. Retrieved April 2, 2019 from https://www.oph.fi/download/182107_Government_Decree_120-2017_27.2.2017_.pdf

[10] ECTS Users' Guide. Publicatins Office of the European Union. DOI: 10.2766/87192

[11] EUR-ACE® Framework Standards and Guidelines. 2015. ENAEE. Retrieved April 1, 2019 from https://www.enaee.eu/wp-assets-enaee/uploads/2017/11/EAFSG-Doc-Full-status-8-Sept-15-on-web-fm.pdf

[12] Finland's Cyber security Strategy. 2013. Ministry of Defence. Retrieved March 21, 2019 from https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

[13] Proposed Accreditation Criteria for Cybersecurity Academic Programs, ABET, Inc., Nov. 2017, [online] Available:

www.abet.org/blog/news/abet-seeks-feedback-on-proposed-accreditation-criteria-for-cybersecurity-academic-programs

[14] United States. White House Office, Comprehensive National Cybersecurity Initiative, Apr 2010.

[15] C. Paulsen, E. McDuffie, W. Newhouse and P. Toth, "NICE: Creating a Cybersecurity Workforce and Aware Public," in *IEEE Security & Privacy*, vol. 10, no. 3, pp. 76-79, May-June 2012. DOI: 10.1109/MSP.2012.73

[16] National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. 2017. NIST. DOI: https://doi.org/10.6028/NIST.SP.800-181

[17] Centers of Academic Excellence in Cybersecurity. Retrieved April 2, 2019 from https://www.caecommunity.org/content/what-is-a-cae

[18] Centers of Academic Excellence Cyber Defence Knowledge Units. Retrieved March 27, 2019 from https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf

[19] Criteria for Measurement for CAE in Cyber Operations Fundamental. NSA. Retrieved March 27,2019 from https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-fundamental/

[20] Criteria for Measurement for CAE in Cyber Operations Advanced. NSA. Retrieved March 27, 2019 from https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-advanced/

[21] A Guide for Mapping Courses to Knowledge Units. National Cyber Watch. Retrieved March 27, 2019 from https://www.nationalcyberwatch.org/ncw-content/uploads/2017/12/NCC_Resource_Guide_A_Guide_for_Mapping_Courses_to_Knowledge_Units_v2.pdf

[22] Olson, R. and Sanders, C. What They're Teaching Kids These Days. 2017. Retrieved March 27, 2019 from https://www.blackhat.com/docs/us-17/wednesday/us-17-Sanders-What-Theyre-Teaching-Kids-These-Days-Comparing-Security-Curricula-And-Accreditations-To-Industry-Needs.pdf

[23] Master's Degree Programme in Information Technology, Cyber Security. 2019. JAMK University of Applied Sciences. Retrieved April 18, 2019 from https://asio.jamk.fi/pls/asio/asio_rakenne_julkaisu.rakenne_komp_osaamisalue?ckohj=YTC&csuunt=99999&cvuosi=9S&caste=J&cark=2019-2020&lan=e

[24] Cyber Security Implementation in Practice. Course Information. JAMK University of Applied Sciences. Retrieved April 12, 2019 from https://asio.jamk.fi/pls/asio/asio_ectskuv1.kurssin_ks?ktun=YTCP0200&knro=&ark=&lan=e

[25] Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H. and Krathwohl, D. R. (1956) *Taxonomy of educational objectives Handbook 1: cognitive domain*. London, Longman Group Ltd.

[26] Biggs, J. and Collis, K. 1982. Evaluating the Quality of Learning The SOLO Taxonomy (Structure of Observed Learning Outcome). Academic Press.

[27] Security Management in Cyber Domain. Course Information. JAMK University of Applied Sciences. Retrieved April 18, 2019 from https://asio.jamk.fi/pls/asio/asio_ectskuv1.kurssin_ks?ktun=YTCP0100&knro=&lan=e&ark=

[28] Auditing and Testing Technical Security. Course Information. JAMK University of Applied Sciences. Retrieved April 18, 2019 from https://asio.jamk.fi/pls/asio/asio_ectskuv1.kurssin_ks?ktun=YTCP0300&knro=&lan=e&ark=

[29] Cyber Security Exercise. Course Information. JAMK University of Applied Sciences. Retrieved April 12, 2019 from https://asio.jamk.fi/pls/asio/asio_ectskuv1.kurssin_ks?ktun=YTCP0400&knro=&ark=&lan=e

Columns on Last Page Should Be Made As Close As Possible to Equal Length

Authors' background

Your Name	Title*	Research Field	Personal website
Karo Saharinen	Phd candidate, Senior Lecturer	Software Defined Networks, Automatization and DevSecOps, Cyber Security Training and Education.	https://www.linkedin.com/in/karo-saharinen

Mika Karjalainen	Phd candidate, Director Institute of Information Technology	Cyber Security Training and Education.	
Dr Tero Kokkonen	PhD, R&D-manager / Senior Lecturer	Data Analytics and Anomaly Detection in Cyber Security, Cyber Security Exercises, Training and Education	

***This form helps us to understand your paper better, the form itself will not be published.**

***Title can be chosen from: master student, Phd candidate, assistant professor, lecture, senior lecture, associate professor, full professor**