Poster: The Need for a Collaborative Approach to Cyber Security Education

Gregor Langner
Center for Digital Safety & Security
AIT Austrian Institute of Technology
Vienna, Austria
gregor.langner@ait.ac.at

Jerry Andriessen
Wise & Munro Learning Research
Den Haag, Netherlands
jerry@wisemunro.eu

Gerald Quirchmayr
Research Group Multimedia Information Systems
University of Vienna
Vienna, Austria
gerald.quirchmayr@univie.ac.at

Steven Furnell
School of Computer Science
University of Nottingham
Nottingham, United Kingdom
Steven.Furnell@nottingham.ac.uk

Vittorio Scarano
Dipartimento di Informatica
Università degli Studi di Salerno
Salerno, Italy
vitsca@unisa.it

Teemu Johannes Tokola
Department of Electrical and Information Engineering
University of Oulu
Oulu, Finland
teemu.tokola@oulu.fi

2021 IEEE European Symposium on Security and Privacy (EuroS&P) | 978-1-6654-1491-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/EUROSP51992.2021.00058

***Abstract*—Traditional forms of cyber security education mainly focus on knowledge transmission, which means that knowledge is perceived as a tangible object being transferred from an expert (i.e., the teacher) to a beginner. When practiced well, the learner may acquire such knowledge, but not the resilience to apply it in various contexts [1], [2]. This is especially troubling for the cyber security domain, given the dynamic and constantly changing nature of the field and the environments in which it is required. We therefore need forms of education that aim at understanding the interdisciplinary nature of the field of cyber security as well as at the development of joint action in context: being able to quickly analyse and understand evolving and possibly previously unseen situations and take collaborative action to prevent, detect and recover from incidents.**

***Index Terms*—Computer science education, Cyber Security, Cyber Security Education, Security and Protection, Collaborative Learning**

1. Introduction

All facets of our work and life are permeated by digitalisation and interconnectivity which increasingly affects the critical assets of individuals and organisations. This results in virtually everyone becoming potentially targeted by a cyber-attack. Over the last years the number of incidents from the digital space has been multiplied. [3] Organisations had to realise that cybersecurity is not an agenda item limited to only the ICT staff. In reality, all employees need to be aware of cyber security threats and be equipped with competencies and capabilities in cyber security to recognise emerging attacks and apply appropriate measures to prevent or mitigate them. Higher education institutions have realised this shift of thinking and cybersecurity is a growing area of focus in university education. These institutions offer both undergraduate and postgraduate programmes with a specific focus on cybersecurity. While there is clearly a broad demand for such programmes, only a few other fields require such a holistic and multidisciplinary approach and perspective as cybersecurity. A challenge for both both, institutions and educators, is to create an effective curriculum while ensuring that learners feel that they are receiving an adequate experience. Against this background Collaborative Cybersecurity Awareness Learning (COLTRANE) aims to improve cybersecurity education by introducing innovative approaches in the context of collaborative awareness [4]. Conventional forms of education primarily focus purely on knowledge transfer, but in highly dynamic areas such as cybersecurity this approach does not lead to sufficient learning outcomes. So we need more innovative forms of education that contribute to the development of collaborative actions, i.e., learning how to act in different situations and knowing how to do it collaboratively.

2. Main Objectives of COLTRANE

To overcome existing deficiencies, COLTRANE aims at joining forces across Europe and creating a Cybersecurity Awareness Education Community, providing a collaborative environment with tools and methodologies, as well as developing a practice for sharing learning resources and good practices. COLTRANE is a strategic partnership under the ERASMUS+ programme with a group of 6 partners from Austria, Finland, Italy, the Netherlands, and the United Kingdom. The core objectives of the COLTRANE project therefore are:

1) To modernize and streamline cybersecurity Education across Europe by developing innovative educational concepts and teaching and learning methodologies.
2) To develop an educational concept for cybersecurity awareness that results in a paradigm shift from the current perception of cybersecurity (being an IT department problem), to cybersecurity as a collective societal and organisational problem where each employee and citizen has a role in improving the cybersecurity posture.
3) To foster collaboration among European cybersecurity educators for development and maintenance of education material. This action includes both the innovative use and development of technolog-

© 2021, Gregor Langner. Under license to IEEE.
DOI 10.1109/EuroSP51992.2021.00058

ical support (providing a collaboration environment), as well as providing technical support for transnational community management tailored to the cybersecurity education context.

4) To provide a toolkit for innovative evaluation and validation of learning outcomes (grading) to allow for the assessment of the collaborative and hands-on context of the project material in European HEI environments. Furthermore, the toolkit will provide guidelines for institutional implementation of the novel COLTRANE learning and validation approach.

3. Educational content analyses

There are reference frameworks, such as the European Qualifications Framework (EQF), for the general comparability of education and training, but these only show the general skills and competences learners are required to have after finishing their education in order to achieve the respective stage. However, they do not indicate which knowledge, competences and capabilities learners have to achieve in specific knowledge domains. Learners in cybersecurity have to cover a broad range of domains and disciplines in order to gain the knowledge, skills and competences which are necessary to be able to respond adequately to current and future challenges. Alongside the classic technical areas, teaching programs also have to include human, organisational and regulatory aspects to provide a comprehensive understanding of cybersecurity. Therefore, it can be concluded that learners need to be prepared in the following areas:

1) **Technological:** System security, Network Security, Component Security, Data Security, Software security
2) **Legal:** Law, ethics, policy privacy, cybercrime disciplines
3) **Business:** Organization, Risk management, business, compliance disciplines
4) **Internship:** a period of training spent e.g. in companies, research labs, or governmental agencies.

Based on these knowledge areas, we were able to analyse the cybersecurity education programmes offered at different European universities. These universities are located within the countries represented in the project, so we were able to include curricula in the analysis that were not accessible in other languages. As the second important source of information for the analysis, we used the Higher Education Database [5] from ENISA. This made it possible for us to include the mentioned domains and corresponding ECTS. These data are used to establish a correlation between the Master's programmes and the above knowledge areas in cybersecurity by using the GINI index [7]. The figure 1 reveals that the universities are implementing cybersecurity in different depths, the heterogeneity and multidisciplinarity of the programmes varies throughout. Although the topics are somehow standardised in European bodies (e.g. ENISA), the number of credits for each category varies considerably. Here, the coefficient ranges from 0 to 1, where 0 stands for perfect equality and 1 for perfect inequality.
Only one university (Bocconi and PoliMI) covers all fields (perhaps due to the joint programme between a traditional business school (Bocconi) and a traditional technology-oriented school (Politecnico di Milano)), and many have little practical experience embedded in the programme (e.g. internships). On the other hand, all but three universities (Twente, Turku and Milan) cover all but one field. So heterogeneity is at least addressed, although not in a consistent and coherent way. There is also a significant variation within the categories, with Technological going from a minimum positive value of 21 to a maximum of 90, Legal from 0 to 25, Business 0 to 34, Internship from 0 to 20 and Other topics from 0 to 90 ECTS.
The teaching concept for cyber security must overcome several current challenges to education. Closing the qualification gap to increase the number of cyber security professionals is one of them, and so is the type of knowledge which needs to be applied in a resilient and dynamic way. This means that education not only needs to provide an understanding of the theory and facts, but also an in-depth understanding of how threats arise from different perspectives and countermeasures can be elaborated on different bases. For this purpose, the COLTRANE project integrates interdisciplinary and multidisciplinary aspects into the methodology for teaching and solves challenges that may arise with a collaborative and integrative approach. A practice-based approach is integrated that can include complex and interconnected variables alongside the core knowledge. Enhanced use of advanced technology in teaching such as cyber-ranges and sophisticated interactive learning spaces is also included to facilitate a broad diversity in all disciplines.

4. COLTRANE methodology

The COLTRANE methodology aims to develop interdisciplinary and collaborative learning scenarios that aim for increasing students awareness of cyber security, especially in professional contexts. The scenarios describe the elements that a COLTRANE teaching module should contain, fostering a consistent view on cyber security awareness. These modules are designed in cooperation with the educators, to be able to meet their particular requirements, but also to increase their awareness about the approach. The teaching modules will be further designed to enable the use of new technologies as well as interactive platforms for example Cyber Range [8] and interactive learning spaces.
Two elements of the learning scenarios especially foster the view of cyber security as a collective rather than as an individual problem. The first is their collaborative nature: the learning tasks require students to engage into a confrontation with real-world and practice-relevant cyber security challenges, planning exercises, incident handling and forensic analysis. The problems faced are such, that they cannot be resolved by an individual, but require learners to share information, make joint decisions, and engage in argumentative discussions. Moreover, the collaborative nature allows for different roles, including interdisciplinary specialisation. The problems they confront sometimes have a clear resolution, but often, many solutions are possible, and even valid, just like in real life. By being specific about the learning goals to be achieved, in terms of curriculum content, professional context, as

University	Gini Index
FH Joanneum	0.73
(IT & MS) FH Oberösterreich	0.43
(SIS) FH Oberösterreich	0.56
(IS) FH St. Pölten	0.58
(CS and R) FH St. Pölten	0.36
Alpen-Adria Univ. Klagenfurt	0.83
TU Wien	0.75
Rome	0.68
Pisa	0.74
Padova	0.63
Bari	0.66
Udine	0.61
Molise	0.61
Cagliari	0.70
Milan	0.58
Bocconi - Politecnico	0.18
Turku	0.77
Jyväskylä	0.57
Jyväskylä (JAMK)	0.83
Amsterdam	0.65
TU Delft	0.81
Eindhoven	0.67

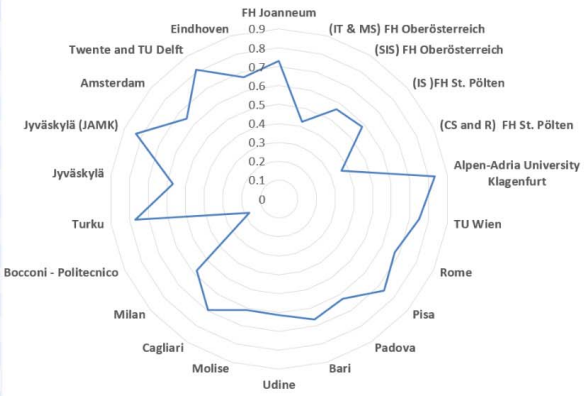

Figure 1. Correlation between the sample European universities and Gini coefficient

well as particular learning processes (e.g. argumentation, problem-solving), our scenarios and modules can be easily adapted to existing curricula. In addition, we will specify criteria for evaluation that educators can use for their certification needs. The second element of our learning scenarios that serves increased awareness of the collective nature of cyber security is joint reflection. Being engaged into a group working on some cyber security problem can be an engaging experience, also because there often are time constraints caused by propagation of a cyber threat, or for practical necessity of a group dealing with complex information within the time frame of an exercise. A phase where participants can reflect on this experience, and this reflection is (in part) aiming for a focus on the task goals and on how the students worked together, can greatly contribute to their awareness.

5. Conclusion and Future Work

Digitalisation is a challenge that can only be overcome by acting together as a community. This is why it is essential that all individuals gain an awareness of the risks associated with digitalisation and how they can deal with them. The target here should be to establish a basic understanding but also a basic security in handling the digital space. To achieve this, all areas of education, from primary school to adult education, must to some extent modify the curriculum and recognise cyber security as an essential part of it. Only with a target group-oriented, interdisciplinary and multi-perspective education and training can all framework conditions be included in order to be able to react adequately to security threats. Educators however cannot carry out this step alone. Besides the human resources they so need tools and learning content to support them in transferring knowledge, capabilities and competences. The approaches and content developed in the project are a first step and form the basis for this education. National and international authorities however must cooperate and provide both resources and training courses in this area for educators. Learners from across the disciplines need to develop an interest, understanding and awareness of cyber security so that they do not become targets themselves and when they do they also know how to address it. Developments made as part of COLTRANE need to be reviewed by the end of the project in order to ensure that the best possible range of tools are available to educators.

6. Acknowledgement & Disclaimer

The authors would like to thank the ERASMUS+ Project COLTRANE (2020-1-AT01-KA203-078070) for supporting the research presented in this work.
The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

References

[1] Bereiter, Carl. “Liberal education in a knowledge society.” Barry Smith. Open. 2002.

[2] Resnick, Lauren B. “The 1987 presidential address learning in school and out.” Educational researcher 16.9 (1987): 13-54.

[3] Lourenço,Marco Barros, Marinos,Louis. “The year in review ENISA Threat Landscape” 2020.

[4] Coltrane Homepage. https://coltrane.ait.ac.at . last accessed 2021/05/13.

[5] Cybersecurity Higher Education Database. https://www.enisa.europa.eu/topics/cybersecurity-education/education-map . last accessed 2021/02/06.

[6] Knowledgebase. https://www.cybok.org/knowledgebase/. last accessed 2021/02/06.

[7] Ceriani, Lidia, and Paolo Verme. “The origins of the Gini index: extracts from Variabilità e Mutabilità (1912) by Corrado Gini.” The Journal of Economic Inequality 10.3 (2012): 421-443.

[8] Leitner, Maria, et al. ”AIT Cyber Range: Flexible Cyber Security Environment for Exercises, Training and Research.”. Proceedings of the European Interdisciplinary Cybersecurity Conference. 2020.