A comprehensive design framework for multi-disciplinary cyber security education

Gregor Langner[1][0000−0002−3271−5073], Steven Furnell[2][0000−0003−0984−7542], Gerald Quirchmayr[3], and Florian Skopik[1][0000−0002−1922−7892]

[1] AIT Austrian Insititute of Technology, Vienna, Austria
[2] University of Nottingham, Nottingham, UK
[3] University of Vienna, Vienna, Austria

Abstract. This paper presents an innovative approach to teaching soft skills in cyber security. It highlights the importance of integrating soft skills, such as critical thinking, problem solving, communication, and empathy, alongside technical skills. The COLTRANE framework is introduced as a tool for educators to enhance the teaching of soft skills. The framework involves several phases, including identifying relevant soft skills, establishing learning objectives, and designing conducive learning environments. By employing this framework, learners are exposed to real-life challenges that necessitate the integration of technical and soft skills. This approach ensures that learners not only gain technical knowledge but also develop the capacity to apply it in practical situations, fostering effective communication, collaboration, and empathy. By utilizing the COLTRANE framework, educators can better prepare their students for future careers in cyber security, where complex problem-solving and effective teamwork are essential.

Keywords: Cyber security education · Framwork · Soft Skills · Science education · Cyber Range · Collaborative learning space

1 Introduction

The digitalization of processes in organizations has brought about significant benefits, including increased efficiency, productivity, and innovation [1]. However, it has also created new challenges and threats that require specialized skills and knowledge to address [2]. Cyber security threats have continuously become more sophisticated and diverse, with cybercriminals exploiting vulnerabilities in software, hardware, and network infrastructures to gain unauthorized access to sensitive information, disrupt operations, and cause significant financial and reputational damage [3]. As a result, organizations are now looking to hire personnel with the necessary cyber security skills and competencies to identify and mitigate potential threats. However, there is a severe shortage of qualified individuals in this field, which can be attributed to various factors. One of the main challenges is the rapid pace of technological advancements, which means that cyber security threats evolve quickly, and higher education institutions often struggle to keep up with the latest developments [4].

This paper begins by examining the background to the topic, and highlighting the importance of both collaborative and multidisciplinary aspects in the delivery of cyber security education. From this foundation, Section 3 then proceeds to present the details of the COLTRANE Educational Design Framework (CEDF), which is the key focus of the paper. This includes the principles underpinning the framework and its use of scenario-based learning, leading into consideration of the process architecture for the practical implementation, including the configuration and delivery of module materials in a supporting technology environment. Section 4 then considers the practical implications of adopting the proposed framework and the benefits to be gained from doing so. The discussion conclusions with Section 5, which summarises the work presented and looks to the future potential of the COLTRANE work.

2 Background

Cyber security is a multidisciplinary field that requires expertise in several areas, including computer science, network security, cryptography, risk management and diverse, and ethical hacking, and are even more demanding, in additional areas such diverse as law, sociology, economics and business. It is therefore very challenging to find individuals with such a diverse skill set, and even if they exist, they often command high salaries, making it hard for organizations to attract and retain them [5]. In addition to hiring cyber security professionals, organizations must also ensure that all employees possess a basic level of cyber security knowledge and awareness. This is a central requirement, because cybercriminals often target individuals with limited cyber security knowledge, using them as a gateway to gain access to an organization's network or data [6]. Organizations must therefore invest in cyber security training and education for all employees, regardless of their job function or level of technical expertise. The current situation is best characterized as follows:

- The increasing speed of digitalization in organizations has consequently led to a high demand for cyber security professionals, but the supply of qualified individuals remains inadequate.
- Organizations must invest in cyber security training and education for all employees to ensure a basic level of cyber security knowledge and awareness.
- Higher education institutions (HEI) must adapt their curricula and their way of teaching to keep up with the latest developments in cyber security if they are to produce graduates with the necessary skills and competencies to address the evolving threat landscape.

The shortage of cyber security professionals remains a growing concern, as information technology becomes increasingly integrated into various industries and government infrastructures [7]. Addressing this shortage requires coordinated and comprehensive cooperation between higher education institutions, industry, and government agencies. These partnerships can provide students with hands-on experience in dealing with real-world cyber security cases and help them develop the necessary skills to succeed in the field. Industry also needs to play a crucial role in addressing the shortage of professionals by providing training and development opportunities for their employees.

The current dramatic situation of a significant global shortage of cyber security professionals is documented in various studies. According to the Cyber secuirty Jobs Report [8], there will be a shortfall of 3.5 million cyber security professionals by 2025. Another study by the Center for Strategic and International Studies found that nearly 60% of organizations report a shortage of cyber security professionals [9]. Additionally, it is often suggested that traditional teaching institutions struggle to produce graduates who meet the demands of the world of work, which is confirmed by various researchers and experts in the field of higher education. A study shows that 79% of CEOs worldwide have difficulty finding employees with the necessary skills to drive their company's digital transformation [10]. Another found that more than half of employers (56%) believe that graduates do not have the practical skills they need [11].

The challenge of creating a multidisciplinary environment in the classroom is seen by many experts as crucial to preparing graduates for the demands of the world of work. In terms of the difficulties of bringing practical examples into the classroom, there are several solutions. One possibility is to create a simulated real-life environment in which students can gain practical experience. Such an environment can be achieved, through the use of virtual laboratories or simulations (Cyber Range). An example of this is the NetLab and COLTRANE project, where students can gain hands-on experience in a virtual environment by configuring and managing real networks [12][13].

To ensure that learners acquire the skills they need to be successful in the field of cyber security, it is important that lessons include soft skills such as problem awareness and understanding, teamwork, problem solving, information sharing and communication. These soft skills are critical as they help learners overcome complex challenges and work effectively with other team members to keep companies and organisations safe. Yamin and Katt [14] found that integrating soft skills into the curriculum of cyber security programmes can help graduates be better prepared for their careers. The authors also emphasized the importance of realistic scenarios in the classroom to provide learners with an authentic learning experience. Such a model was presented by Langner et al. [15]. Another important element of the scenario-based teaching approach is the involvement of practitioners and experts from the industry. These experts can provide learners with valuable insights into cyber security practice and help them apply their skills and knowledge in real-life situations. Ruoslahti et al. [16] found that the involvement of practitioners and industry experts can help learners be better prepared for their careers.

By utilizing a cyber range and collaborative learning space, the COLTRANE project provides learners with a realistic and immersive learning environment that enables them to apply their knowledge and skills to real-world scenarios. The project also incorporates the expertise of practitioners and experts from the cyber security industry, who can provide valuable insights into the practical aspects of cyber security and help learners to apply their knowledge and skills in real-world situations. The project bridges the gap between the theoretical knowledge gained and the practical skills required in the field of cyber security.

3 COLTRANE Educational Design Framework CEDF

The **CEDF** is built on a divergent set of pillars. First, the origins of this project lay in the participation of some of its members in other European projects. These set the foundations, and some of the evidence, for our thinking and the types of solutions that we assume. The second source of information is evidence from the tasks and actions performed in COLTRANE. This work will give us input about the reasoning in EU polices about cyber security and related awareness, and about the current state of higher education concerning cyber security, and on the perceived needs of teachers and students. The third source of information are the consortium workshops, the discussions that we organized internally to arrive at shared thinking and joint ideas for the framework. This is done in multiple rounds, the first focused on the conceptual basis for Collaborative Cyber security Awareness Education, the second on the design and delivery approach underlying the framework, based on authentic examples of educational interventions.

3.1 COLTRANE design principles

Based on the principles identified in the project, we can now establish three conceptual modules (see Fig 1) that support each other, starting with a specification of the didactic goals, followed by construction and delivery, and evaluation and feedback.

Goals-oriented Didactics: it is important to ensure that the didactic goals are understood and agreed well before the content material is produced. At the core of the goal set we find the guiding principles for the special CEDF design aspects, such as Awareness Creation, Fostering Collaborative Problem Solving, Scenario- and Activity-Guidance.

Guided Construction and Delivery: this aspect is supported by a repository of examples, templates and teacher and learner guides to ensure that the CEDF principles are represented in the actual teaching materials and in their delivery.

Feedback-oriented Evaluation: to enable learners to reflect on how they handled the assigned exercises and to support the continuous improvement of the teaching materials and their delivery, evaluation needs to be Feedback-oriented. Such open-minded discussion rounds might not be easy in the first round of implementation, but they are absolutely necessary for establishing critical reflection on suggested solutions and on implemented processes. This step also enables learners to conduct a multidisciplinary and multi-perspective analysis, which in the case of cybersecurity is an essential prerequisite.

Teaching units designed in this way are directly aimed at delivering content in a way that allows learners to develop the much-needed soft skills through applying the acquired theoretical knowledge to real-world cases in a practice-oriented

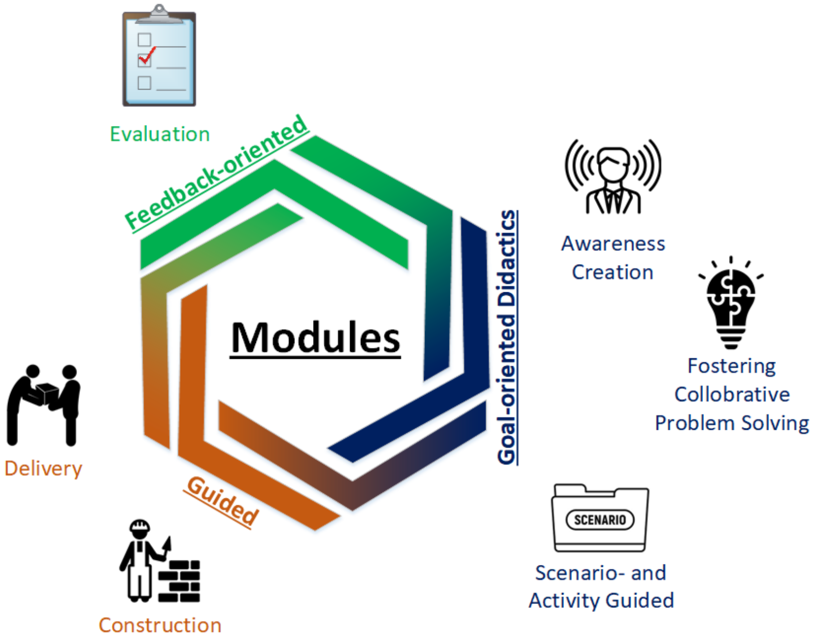

Fig. 1. Conceptual modules

way. This is also in line with ample analyses of teaching styles that clearly see a three-level model, the lectures laying the foundations, exercises helping learners to understand the content, and small projects enabling learners to apply what they have been taught in lectures and have developed an understanding of in exercises. It is this last step where, the principles-based CEDF delivers best, being guided by the COLTRANE principles and three conceptual modules described above. With the COLTRANE repository providing a good starting point for educators, it becomes feasible to integrate this new way of teaching cybersecurity into existing curricula.

3.2 Core COLTRANE Process Architecture

The proposed process architecture is intended to cover the entire teaching cycle, which in our approach is structured into three main phases (see Fig. 2): Requirements elicitation, course/module configuration and course/module delivery. The requirements elicitation phase involves gathering information and feedback from various sources to understand the needs and requirements of learners, teachers and the market. In this phase, potential difficulties and needs can be identified to ensure that the course content is relevant, up-to-date and effective. The course/module configuration phase involves the development of courses and modules based on the gathered requirements. In this phase, the curriculum is developed and the course content is elaborated, including learning objectives, teaching materials, examinations and evaluations. This phase also enables the course structure to be defined to ensure that the content is presented effectively and the learning objectives are achieved. The course/module delivery phase involves the implementation of the developed course and module. In this phase, the teaching and learning activities are carried out and the evaluation results are collected to ensure that the course content and teaching methods are effective and that the learners can achieve their learning objectives.

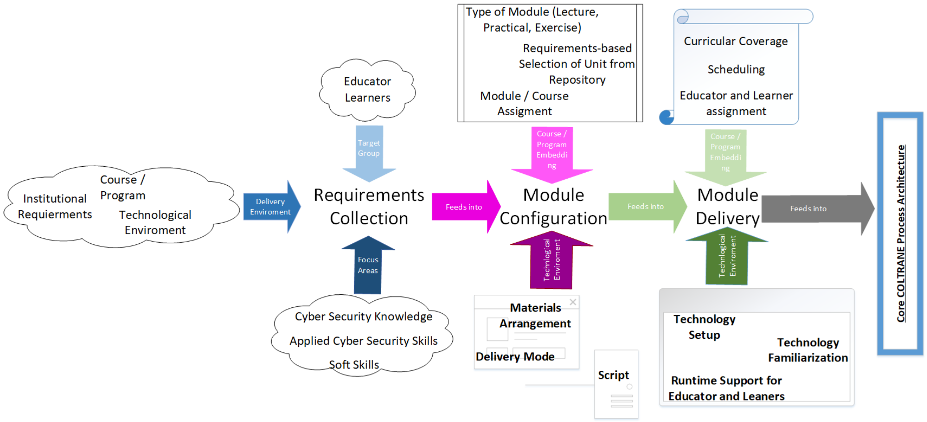
Institutional Requierments
Course / Program
Technological Enviroment
Delivery Enviroment
Educator Learners
Target Group
Requirements Collection
Focus Areas
Cyber Security Knowledge
Applied Cyber Security Skills
Soft Skills
Feeds into
Type of Module (Lecture, Practical, Exercise)
Requirements-based Selection of Unit from Repository
Module / Course Assigment
Course / Program Embedding
Module Configuration
Technlogical Enviroment
Materials Arrangement
Delivery Mode
Script
Feeds into
Curricular Coverage
Scheduling
Educator and Learner assignment
Course / Program Embedding
Module Delivery
Technlogical Enviroment
Technology Setup
Technology Familiarization
Runtime Support for Educator and Leaners
Feeds into
Core COLTRANE Process Architecture

Fig. 2. Core Architecture Phases

These phases form a logical sequence with possible feedback loops from course/module configuration and course/module delivery to requirements elicitation and from course/module delivery to course/module configuration. As this feedback can be either on the content developed or on the process phase, we follow Argyris' proven double learning loop approach. [17] This feedback mechanism is the central basis for maintaining and adapting process and content materials, which is essential in a field that is changing as fast as cyber security.

3.3 Requirements Collection

The requirements gathering needs to be done by the core stakeholders:

- Actor Requirements: the actors concerned are the target audience, comprising the job market, educational institutions, and planners, and at the core of the framework learners and educators
- Focus Area: in addition to the usually well-covered domain knowledge this includes soft skills and application skills.
- Delivery Environment: the setting of educational programs and course, institutional requirements and technological infrastructure need to be considered realistically to make the implementation of a developed teaching unit work.

Depending on the target group, it was necessary to conduct a requirements elicitation workshop with representatives of the stakeholder groups of each HEI. Priority was given to institutions that intend to use the COLTRANE methodology and infrastructure. This ensured that the focus areas were balanced according to local needs and that the teaching model and technical infrastructure could be implemented appropriately. The workshops were led and evaluated by pedagogical technology experts. They had to be able to carry out the process of requirements elicitation and identify the needs and requirements of the different stakeholder groups and present them in an abstract form and compare them with international standards and results. Participants included representatives from different sectors of the higher education community, including students, teachers, administrators and IT experts. The results of these workshops form the basis for the requirements elicitation and curriculum design. The focus and topic areas may vary depending on the target group. For students pursuing a career in cyber security, for example, the focus may be on the latest technologies, attack methods and defence strategies. For IT administrators, the focus may be on managing networks, databases and security measures. The results of the requirements survey were then used to design the course/module configuration phase. Here, the learning objectives and materials necessary to meet the needs of the target group were developed.

Overall, requirements elicitation has been an essential part of COLTRANE approach, ensuring that the curriculum is relevant and up-to-date. By involving the target groups and conducting different workshops, the COLTRANE approach can be adapted to the needs of each university and target group as circumstances arise, ensuring that learners acquire the skills and knowledge they will need in the future to succeed in the rapidly evolving world of cyber security. The requirements elicitation needs to be solicited from the core stakeholders.

3.4 Module Configuration

Embedding this in the COLTRANE repository is a crucial step in the development of the framework. In this process, repository elements were assigned based on the module type and requirements gathered in the first phase. Matching the module type and content with the focus areas also decides the teaching approach, with the problem-based paradigm predominating in the case of practical exercises. This approach enables the teaching of applied as well as social skills and makes the learning process more effective and practice-oriented. To realize the full potential of the COLTRANE framework, it is important to create a suitable technical environment and facility. With these technologies, it is expected that teachers will be enabled to develop collaborative tasks.

In addition to providing students with practical experience, the use of the framework also offers the opportunity to invite industry and government to cooperate with universities in developing practice-oriented teaching content. This will not only increase the employability of graduates, but also provide employers with graduates who know how to apply acquired knowledge and skills. The ability to link the teaching content directly to curricular elements to established process models, such as the NIST/CSF cycle, and to standards, such as the ISO 27000 series, is an advantage of the COLTRANE framework. Thus, it provides a solid foundation for developing a comprehensive and coherent cyber security curriculum that is aligned with industry standards and practices.

However, the success of the COLTRANE Framework ultimately depends on its ability to meet the needs of the target audience. As listed above, these stakeholders include universities, students, employers and policy makers. It was therefore important to involve representatives of these groups in the development and support them in the implementation of the framework to ensure that their needs and expectations are met and that a smooth adaptation process is carried out.

For individual implementation, we recommend conducting workshops with the target group and initiating requirements gathering with representatives of the groups of individual HEI's planning to use the COLTRANE methodology and infrastructure. This ensures that the focus areas are balanced according to local needs and that the teaching model and technical infrastructure can be implemented appropriately. The feedback mechanism provided for in the framework is central to maintaining and adapting process and content materials, which is essential in a field that changes as rapidly as cyber security. The incorporation of this feedback mechanism allows to add possible loops from the course/module material configuration enabling educators to adapt and reflect on the material and therefore be able to make quick adjustments.

3.5 Module Delivery

It is important to ensure that learners can apply the knowledge and skills taught in practical situations. To achieve this, educational institutions are increasingly using technology to enhance the learning environment. One promising technology is becoming more prevalent in the education sector is the integration of a technological environment that combines collaboration and analysis tools with a cyber-range environment. The use of this technology can enhance the development of practical problem-solving and knowledge application skills in learners.

The cyber-range environment is a virtual platform that provides learners with a realistic simulation of real-world scenarios. This environment is particularly useful in areas that require hands-on experience, where learners can practice defending against cyber-attacks in a safe and controlled environment. Using a cyber-range environment in combination with collaboration and analysis tools can provide learners with a powerful learning experience that can significantly improve their understanding and skills. The Collaborative Training and Experimentation Infrastructure is an example of a platform that combines collaboration and analysis tools with a cyber-range environment. One of the main advantages of the platform used in COLTRANE is its ability to facilitate collaboration between learners. Collaboration is an essential part of the learning process as it allows learners to share ideas and knowledge and work together to solve complex problems. In addition to collaboration tools, the COLTRANE platform also provides analytics tools that enable learners to analyse data and make informed decisions - a critical skill in many fields.

However, the use of technology in education is not without its problems. One of the biggest challenges is the need for adequate infrastructure and support. Educational institutions need to invest in the necessary hardware, software and staff to ensure that the technology is properly maintained and supported. In addition, learners need to have access to a reliable internet connection and appropriate devices to make full use of the technology. Another challenge is the need for adequate training and support for teachers. Teachers need to be skilled in the use of technology to ensure that learners can take full advantage of the learning environment.

4 Practical implications of the CEDF

The escalating demand for cyber security graduates in the industry, both in terms of quantity and applicable qualifications, imposes significant pressure on HEIs to enhance their output and equip graduates with specialized skills beyond conventional teachings. The COLTRANE approach aims to expose students to relevant content by exposing them to realistic, multidisciplinary scenarios, is therefore an essential contribution to the training of labour market-ready graduates. The integration of soft skills like teamwork, communication, and problem-solving within practical exercises brings about notable changes to the affected programs and courses, particularly in their delivery methods.

Environments that necessitate self-paced, self-directed, and goal- oriented teamwork compel students to comprehend the problem at hand and its ramifications. Consequently, this creates an optimal setting for cultivating a broader awareness and fostering critical thinking skills. Working in multidisciplinary teams, particularly, affords students the opportunity to analyze problems and potential solutions from diverse perspectives. Since the CEDF is collaboratively designed by partners from various European countries and disciplines, its outcomes will empower educators to better prepare graduates for the multifaceted, multicultural, and multinational challenges they will encounter in the cyber security field. Holistic approaches are imperative in producing the required solutions.

The finalized CEDF framework is accompanied by guides, templates, and readily applicable teaching units, primarily consisting of scenario-based exercises and cases. As a result, it can be directly employed to enhance the practical relevance of existing courses with reasonable effort. To implement this approach effectively, educators need to transition from a lecture-based style to a more coaching-oriented and discussion / reflection-oriented style, if they have not done so already. Although this transition initially demands significant effort, it yields benefits by fostering a more active learning environment. The CEDF, along with its supporting materials, helps alleviate this barrier in some cases and generally reduces it to a manageable level.

The pilot implementations conducted by participating universities in the project serve as exemplary instances of the transformative potential of the CEDF. These initiatives have the capacity to revolutionize the field by aligning with the core principles driving the framework.

5 Conclusions

Government agencies can help address the cyber security skills shortage by providing funding and support for cyber security education and training programmes. Raising public awareness of the importance of cyber security and promoting education and training initiatives can also help attract more people to cyber security careers. Collaboration between educational institutions, industry partners and government agencies is essential to ensure that the cyber security workforce is adequately prepared to meet the challenges of an digital world.

The paper discusses the importance of practical application of knowledge in the educational process and the use of technology to enhance the learning environment. One promising technology is the use of a cyber-range environment that provides learners with a realistic simulation of real-world scenarios. The Collaborative Training and Experimentation Infrastructure is an example of a platform that combines collaboration and analysis tools with a cyber-range environment to provide learners with a powerful learning experience. The success of the platform depends on proper set-up, familiarisation with the technology and support for teachers and learners during its lifetime. One of the main benefits of the platform is the ability to facilitate collaboration between learners through chat rooms, forums and shared documents. Analytical tools such as data visualisation and machine learning algorithms can enhance learners' ability to analyze and interpret complex data. In addition, the COLTRANE framework encourages collaboration and sharing of knowledge and experiences among its users, which further increases its efficiency and adaptability.

Overall, the COLTRANE framework provides a comprehensive and practical approach to cyber security education that is aligned with industry standards and practices and provides students with valuable real-world experience. By involving stakeholders in its development and implementation and providing a feedback mechanism for continuous improvement, the framework can evolve to meet the needs of its users.

Acknowledgements Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

References

1. Parviainen, Päivi and Tihinen, Maarit and Kääriäinen, Jukka and Teppola, Susanna: Tackling the digitalization challenge: how to benefit from digitalization in practice, Int'l journal of inf. systems and project management, pp. 63–77
2. Dawson, Jessica and Thomson, Robert: The future cybersecurity workforce: going beyond technical skills for successful cyber performance, Frontiers in psychology, pp. 774

3. ENISA Threat Landscape 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.
4. Hina, Sadaf and Selvam, Dhanapal Durai Dominic Panneer and Lowry, Paul Benjamin: Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world: Computers & Security
5. Furnell, Steven and Langner, Gregor and Tokola, Teemu and Andriessen, Jerry and Quirchmayr, Gerald and Luciano, Carmela: Collaborative Cybersecurity Learning: Establishing Educator and Learner Expectations and Requirements: Information Security Education-Adapting to the Fourth Industrial Revolution: 15th IFIP WG 11.8 World Conference, WISE 2022, pp.46–59
6. Park, Sungha, Jungbin Lim, and Dongkyu Kim. "The Human Factor Of Cybersecurity And The Prevention And Counter Measures Against Cybercrime In South Korea." Webology (ISSN: 1735-188X) 19.2 (2022).
7. Crumpler, William and Lewis, James A: The cybersecurity workforce gap: JSTOR
8. Cybersecurity Jobs Report: 3.5 Million Unfilled Positions In 2025 https://cybersecurityventures.com/jobs, Cybercrime Magazine
9. 2019 Cybersecurity Workforce Study https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study
10. Perspectives in higher education https://www.pwc.com/us/en/industries/health-industries/library/higher-education-perspectives.html
11. How HR Can Prepare for the Future of Work https://www.knowledgecity.com/blog/future-of-work Apr 2023
12. Haag, Jens, Harald Vranken, and Marko van Eekelen. "A virtual classroom for cybersecurity education." Transactions on Edutainment XV (2019): 173-208.
13. Coltrane https://coltrane.ait.ac.at
14. Yamin, Muhammad Mudassar, and Basel Katt. "Cyber security skill set analysis for common curricula development." Proceedings of the 14th International Conference on Availability, Reliability and Security. 2019.
15. Langner, G., Skopik, F., Furnell, S., & Quirchmayr, G. (2022). A Tailored Model for Cyber Security Education Utilizing a Cyber Range. In ICISSP (pp. 365-377).
16. Ruoslahti, Harri, et al. "Cyber Skills Gaps–A Systematic Review of the Academic Literature." (2022).
17. Argyris, C. (1977). Double loop learning in organizations. Harvard business review, 55(5), 115-125.