Dynamic Cybersecurity Curriculum Optimization Method (DyCSCOM)

Marko Zivanovic
PhD Student, Faculty of Technical Science, Novi Sad, Serbia
zivanovic.m@gmail.com

Imre Lendák
Professor, Department of Power Engineering and Applied Software Engineering, Faculty of Technical Science, Novi Sad, Serbia; Professor, Data Science and Engineering Department, Faculty of Informatics, Eötvös Loránd University,
lendak@uns.ac.rs
lendak@staff.elte.hu

Ranko Popovic
Retired professor, Faculty of Technical Science, Novi Sad, Serbia
popranko78@gmail.com

ABSTRACT

Demand for cybersecurity experts is high, driven by the increasing digitization of society and increasing number of sophisticated, targeted cyber attacks. Despite this pressing need, a significant shortfall in the number of cybersecurity experts remains due to very diverse landscape of knowledge and complex curriculum accreditation process. In this paper, we present a new model for curriculum analysis and adjustment that addresses entire curricula or course material. It employs machine learning and text-mining techniques for keyword extraction and further comparison with reference skills frameworks. The analysis illustrates a new measurement that quantifies coverage of cybersecurity role and its importance within curriculum based on keyword matching. The case study was conducted with university curricula from Europe and North America. The results illustrate curriculum coverage according to the ENISA's European Cybersecurity Skills Framework (ECSF) roles and optimization progress after our method application.

CCS CONCEPTS

• **Social and professional topics**; • **Professional topics**; • **Computing education**; • **Model curricula**; • **Applied computing**; • **Education;**; • **Computing methodologies**; • **Machine learning.**;

KEYWORDS

Cybersecurity Education, Curriculum Optimization, Skills, Work Roles, Machine Learning

ACM Reference Format:
Marko Zivanovic, Imre Lendák, and Ranko Popovic. 2023. Dynamic Cybersecurity Curriculum Optimization Method (DyCSCOM). In *The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29–September 01, 2023, Benevento, Italy.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3600160.3605008

1 INTRODUCTION

The number of cyber attacks continues to grow and attacks are getting more sophisticated, targeted and successful. Check Point Corporation's Cyber Security Report for 2022 [1] presents a dramatic increase in ransomware, exploits, and attacks on critical infrastructure and research institutions. To defend themselves from such sophisticated attacks, cyber defenders need to extend dynamically and adjust their knowledge base according to ongoing dominant threats.

The latest available research done by the International Information System Security Certification Consortium (ISC)2 estimated a global shortfall of approximately 2.7 million cybersecurity experts [2]. Despite the pressing need, an academic institution needs to follow government and internal regulations regarding curriculum updates in their attempt to align their study programs with market needs. Unfortunately, in most European countries, the accreditation period for academic institutions is 4 to 7 years [3]. In such contexts it is quite difficult to maintain a curriculum up to date with the latest industry needs and relevant skills frameworks. The design of an appropriate curriculum is one of the most important issues in higher educational institutions, and there are many features to be considered. It is important to note that academic institutions need to keep their curricula up to date throughout their long accreditation period, thereby following the dynamic of changes in the related Knowledge Areas (KAs)

This paper defines a new model for curriculum analysis and adjustment with the main goal to optimize connections between academic institutions and industry demands. The model utilizes machine learning (ML) and data analytic algorithms with the idea to facilitate a dynamic adaptation to new requests (industry or academic) within existing study program accreditations. The focus of this novel model is on dynamic cyber security curriculum optimization. Curriculum coverage calculations and dynamic optimization includes data acquisition and processing. To automate those processes, a new software suite was developed. We provide details about the technical implementation of the tool and outline our novel curriculum optimization process. Case study results quantify importance of cybersecurity topics within curricula.

ARES 2023, August 29–September 01, 2023, Benevento, Italy

ACM ISBN 979-8-4007-0772-8/23/08…$15.00
https://doi.org/10.1145/3600160.3605008

The rest of this paper is organized as follows: Section 2 reviews related works of analysis on cybersecurity curricula. Proposed dynamic optimization method on curricula through text mining from course materials is in Section 3. Case study is conducted in Section 4 and our experimental results are presented in Section 5. The conclusion follows in Section 6.

2 RELATED WORKS

The Joint Task Force on Computing Curricula Association for Computing Machinery (ACM) publish their joint computer science-related curricular guidelines. The latest computer science curriculum guideline was released on December 20, 2013 and named CS2013 [4]. It defines Knowledge Areas (KAs) for computer science curricula. Many of these KAs are derived directly from Curriculum Guidelines for Undergraduate Degree Programs in Computer Science CC2001 [5] and Computing Curricula Computer Science Volume CS2008 [6] but increased importance of computer and network security in the past decade led to the development of additional cyber security KA, the "Information Assurance and Security" (IAS). Many studies are based on text-mining and keyword extraction. Takayuki Sekiya, et al. further develop KAs definition from CS2013 with set of keywords for each KA [7]. Semi supervised Latent Dirichlet Allocation (ssLDA) is used to explicitly make each topic of ssLDA mapped to some KAs. Kornraphop Kawintiranon [8], et al., use Frequency–Inverse Document Frequency (TF-IDF) algorithm for keywords extraction and to quantify matching topics between a guideline and actual courses in order to indicate their association;

Referent curricula and certificates [9] are used as radix. The ACM cyber security curricula 2017 recommendations [10] were used in [11] to represent overall competencies that are to be considered central to a data science undergraduate curriculum. George Washington University published a model capable to describe and map cybersecurity positions to KAs in order to create better questionnaires for candidates and optimize search through available CVs [12]. Methods for creation of a certification-based security curriculum are presented in [13]. They closely follow the SSCP and CISSP certifications [9] to prepare students as Cybersecurity Trainees/Apprentices. Innovative approach of teaching cyber security across various computing curricula is described in [14]. In this approach fundamental programming concepts are taught from a security perspective, which builds a strong cyber security foundation for more specialized follow-up courses.

Cybersecurity skills frameworks facilitates curriculum design as well. SPARTA cybersecurity skills framework which includes tools for curriculum design based on mapping among work roles, knowledge, and tasks is provided in [15]. Brno University of Technology [15] utilizes SPARTA cybersecurity skills framework together with analytics of 89 curricula to propose an approach to reduce the gap between the supply of cybersecurity experts and the need of industries and society. The CONCORDIA pilot project [16] tries to establish an European Education Ecosystem for Cybersecurity and provides database of courses for cybersecurity professionals. Cyberseek framework [17] provides a great overview of cybersecurity roles and the skills needed to fulfil role task. This framework is mainly focus on USA region. The European agency for cybersecurity (ENISA) published European Cybersecurity Skills Framework (ECSF) [18]. ECSF describes 12 cybersecurity roles by providing mission, main tasks, key skills and key knowledge for each of them. This structure is suitable for curriculum design which will be shown in case study section.

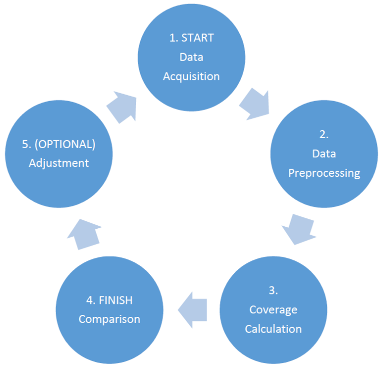

Figure 1: – Curriculum Optimization Method

Most of existing solutions are focused on initial curriculum creation at the beginning of the accreditation period. Novel solution tracks the complete curriculum life-cycle, including period between two accreditations. The new curriculum optimization method takes into count various factors during optimization process including amount of curriculum change allowed by existing accreditation.

3 THE DYNAMIC CYBERSECURITY CURRICULUM OPTIMIZATION METHOD (DYCSCOM)

We propose a novel Dynamic Cybersecurity Curriculum Optimization Model (DyCSCOM) which establishes a connection between academic institutions and industry through dynamic analysis and adjustments. Each curriculum can be treated as set of words written by humans. In every discussion, a human tends to express the importance of some topic by repeating words that are important according to the speaker. The proposed model (Figure 1) relies on this fact. For each curriculum and Knowledge Area (KA), we define a set of keywords. Key areas of the curriculum can be classified by keyword frequency in curriculum descriptions.

The curriculum classification in this paper is defined as the coverage ratio of a set of KAs and their corresponding keywords as defined in the example referent curriculum CS2013. Table 1 [7] lists the knowledge areas, their abbreviations and keywords. Optionally reference curricula might have a keyword importance factor (KIF) array associated to each KA keywords set which is used to emphasize keyword importance within the set.

The first step in Curriculum Optimization Model (Figure 1) is data acquisition in which curriculum description is read from various sources such as: university web pages, PDF documents, word documents or text files.

At this stage, the curriculum description is not ready for keyword extraction. Curriculum descriptions need to be pre-processed to

Table 1: Keywords per Knowledge Area

Area of interest		Keywords
Algorithms and Complexity	AL	algorithm, graph, tree, complexity, automatum, solve, implement, algorithmic, class, strategy
Architecture and Organization	AR	instruction, memory, architecture, familiarity, assembly, level, organization, processor, representation, machine
Computational Science	CN	simulation, modeling, science, information, including, datum, model, algorithm, computational, processing
Discrete Structures	DS	proof, probability, induction, propositional, relation, predicate, usage, bayes, counting, theorem
Graphics and Visualization	GV	rendering, visualization, graphic, surface, image, representation, animation, rasterization, light, color
Human-Computer Interaction	HCI	user, interface, interaction, design, motivation, HCI, evaluation, technology, quantitative, report
Information Assurance and Security	IAS	security, attack, secure, forensic, cryptographic, threat, cryptography, familiarity, policy, SE
Information Management	IM	query, relational, database, information, index, datum, schema, transaction, file, mining
Intelligent Systems	IS	search, agent, reasoning, planning, classification, robot, representation, learning, implement, algorithm
Networking and Communication	NC	network, platform, social, layer, familiarity, application, allocation, industrial, IP, describe
Operating Systems	OS	system, operating, memory, device, access, SF, virtual, OS, file, management
Platform-Based Development	PD	parallel, parallelism, distributed, shared, message, versus, race, algorithm, synchronization, SF
Parallel and Distributed Computing	PBD	function, programming, web, mobile, operation, class, constraint, variant, language, event
Programming Languages	PL	type, program, language, code, static, analysis, semantic, syntax, memory, optimization
Social Issues and Professional Practice	SP	social, professional, privacy, computing, ethical, computer, intellectual, policy, HCI, environmental
Software Development Fundamentals	SDF	design, program, software, component, principle, coding, programming, error, code, structure
Software Engineering	SE	software, requirement, team, risk, project, process, specification, testing, development, validation
Systems Fundamentals	SF	performance, logic, scheduling, memory, machine, error, program, simple, resource, figure

remove HTML tags and stop words. Furthermore, each course syllabus is organized as separate document inside curriculum dataset. Another goal of the pre-processing step is to identify keywords in the text and quantify their importance. In our software tool, we use the porter stemmer [19] and term frequency–inverse document frequency (TF-IDF) with Non-Negative Matrix Factorization (NMF) an unsupervised ML algorithm. Final output of this step is set of key value pairs where words from curriculum are keys and numeric quantifications of words importance are values.

Coverage calculation step aims to quantify amount of KA topic covered by observed curriculum and KA importance within curriculum. For that purposes we used TDF-IDF and NMF output where each curriculum word has associated weight. KA coverage is defined with the following formula:

$$C\left(ka\right) = \sum_{kw\ \in CR} NMF\left(kw\right) * KIF\left(kw\right)$$

Curriculum coverage (C(ka)) equal sum of present KA keyword (Table 1) weight deducted by NMF algorithm multiplied by KIF. Each KA keyword from Table 1 does not need to have same importance and KIF illustrates that feature. The calculation can be done with identical importance of all KA keywords if KIF(kw) = 1 always. This curriculum coverage quantifies the difference between the reference curriculum CS2013 and other curricula which were identified as part of this research. The output of the first iteration through the iterative model shown in Figure 1 is the initial curriculum coverage array.

In most European countries the accreditation period for academic institutions is 4 to 7 years [3]. The key goal of our novel COM is to maintain a curriculum up to date with the latest technologies and within existing regulatory study program accreditation limits. We define curriculum adjustments as updates to the course syllabi constituting study program descriptions. Such updates can be driven by the cyber security academic community (provided in [20]), the latest Cyber Threat Report [1] or any other source treated as relevant by curriculum authors. The novel COM facilitates quantification of overall curriculum change and KA direction in which curriculum adjustment leads.

The final step is comparing initial curriculum coverage results with coverage calculation results after curriculum adjustment. The overall curriculum change is defined with following formula:

$$overallcurriculumchange = \sum \Delta \left(C \left(ka \right) \right)$$

It equals sum of all changes in the KA coverage before and after adjustments. The key goal is to keep overall change within pre-defined values (regulated by local accreditation rules) and to adjust curriculum according to the latest demands. An example of calculation is provided in next section.

4 CASE STUDY

The proposed curriculum optimization method relies on keyword extraction and text mining. Therefore, the first experiment was conducted on curricula ([22, 23, 24, 25, 26, 27, 28]) and the ACM Computer Science Curricula 2013 as the reference curriculum. In the next experiment the CS2013 was replaced with the European Cybersecurity Skills Framework (ECSF) to quantify association with cybersecurity roles and illustrate the utility of cybersecurity skills frameworks in curricula design.

4.1 Experiment with CS2013 reference curriculum

In focus of experiment are curricula of several academic courses from ENISA cyber security academic programs database [21], namely programs offered by the Catholic University of Leuven [22], the University of Agder [23], Masaryk University in Brno [24], KTH Royal Institute of Technology [25] and St. Pölten University of Applied Sciences [26]; all from the European Union. We also included one curriculum from the University of California, Berkeley (USA) [27] and from the Faculty of Technical Sciences, University of Novi Sad, Serbia [28].

Massachusetts Institute of Technology (MIT) [20] provides good overview of keywords used in cybersecurity. We mapped cyber security industry requirements via an array of keywords defined in [20]. Cyber security industry is introduced to this experiment as additional KA named “CS Industry” (CSI). New KA is associated with a set of keyword (attack infrastructure cloud-computing information risk stuxnet security malware ids cyber) defined in [20] and added to set of KAs in CS2013 which was the reference curriculum in this experiment. This approach enables quantification of newly created CSI KA importance within curriculum.

The data acquisition step was concluded by downloading the syllabi of the above-listed study programs. After that each course description was pre-processed: HTML tag and frequently used English words (stop words) were removed. TF-IDF and NMF were applied on the stemmed [19] text to produce set of key value pairs where words from curricula descriptions were keys while numeric quantifications of words' importance were the values. The data pre-processing step of novel curriculum optimization method was concluded with KIF array definition in which we defined the importance of each keyword within the KA keyword set. In our experiment we defined that first keyword has double importance comparing to last word by applying following KIF array "2.0 1.7 1.5 1.3 1.2 1.15 1.1 1.05 1.0 1.0". First element of array corresponds to importance of first keyword in set of KA keywords etc. Values of KIF are chosen based on NMF quantification.

Calculation step utilize inputs from previous step and curriculum coverage calculation formula (C(ka)) defined in section 4. The bar chart in Figure 2 illustrates KA comparison among KAs in reference curriculum while the radar char in Figure 3 emphasizes the dominant KAs. All curricula have KA “Information Assurance and Security” among top rated.

Berkeley and KU Leuven have similar curriculum structures. “Information Assurance and Security” is top rated followed by industry topics and fundamental KAs such as “Software Development Fundamentals”, “Software Engineering”, “Networking and Communication” and “Algorithms and Complexity”. KTH Royal Institute of Technology Stockholm top 3 KAs are “Information Assurance and Security”, “Networking and Communication” and CS Industry. We conclude that based on this list of dominant KAs further development and the inclusion of networking security topics is expected.

The University of Agder follows similar pattern. Their dominant KAs are “Information Assurance and Security”, “CS Industry” and “Computational Science”. These three KAs are quite dominant comparing to other KAs from the reference curriculum which makes this curriculum highly specialized.

Masaryk University in Brno has excellent reference curriculum coverage as every KA is covered. “Information Assurance and Security” and “Software Development Fundamentals” are among the top rated, but fundamental KAs are also covered. This coverage provides a solid baseline for further curriculum optimization.

The Faculty of Technical Sciences, University of Novi Sad (FTN) is only curriculum in this experiment which has CS Industry KA as top rated. “Software Engineering”, “Information Assurance and Security” and foundation KAs such as “Programming Languages” and “Computational Science” are among top 5 rated.

Majority of curricula is focused on the “Information Assurance and Security” KA and one of fundamental KAs which could be a good base for further cybersecurity industry specialization.

4.1.1 *Curriculum optimization.*

In the (optional) curriculum adjustment step we experimented with hypothetical introduction of new content into existing curricula descriptions guided by keywords defined for “CS Industry” KA [20], namely the following keywords: attack, infrastructure, cloud-computing, information risk, Stuxnet, security, malware, ids, cyber. Our main goal was to increase the coverage for the “CS Industry” KA, but keep overall curriculum change level within acceptable accreditation update levels [3]. For this experiment we choose to use the “Becoming a Cybersecurity Consultant” course [29] from Concordia course database for cyber security professionals [16]. The syllabus of this course [29] was added to each curriculum from our dataset and the data pre-processing step was re-applied. Table 2 illustrates comparison between overall curriculum change and “CS Industry” KA coverage change.

As expected, after the above adjustment the “CS Industry” KAs coverage increased in each curriculum as illustrated in Figure 4 and Table 2.

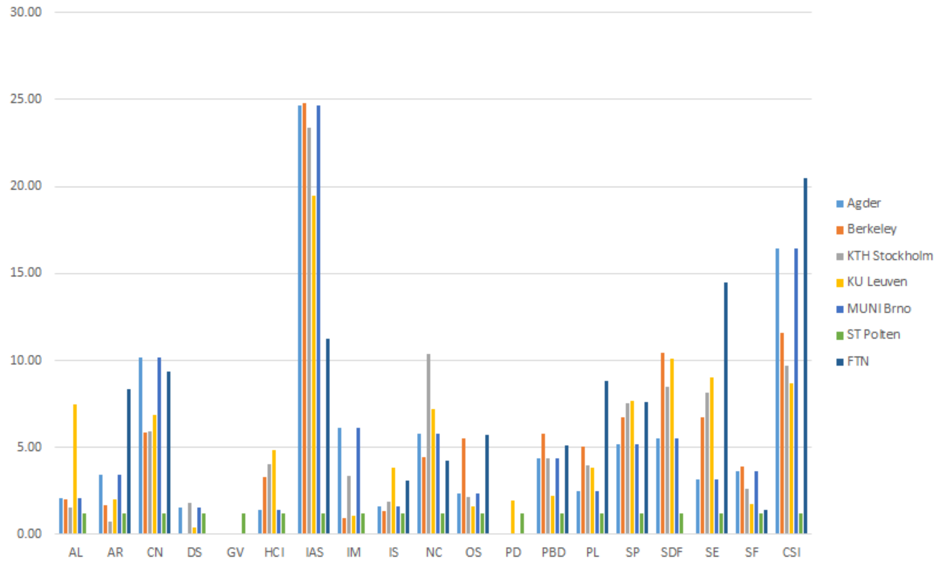

Figure 2: Initial CS2013KA coverage calculation results

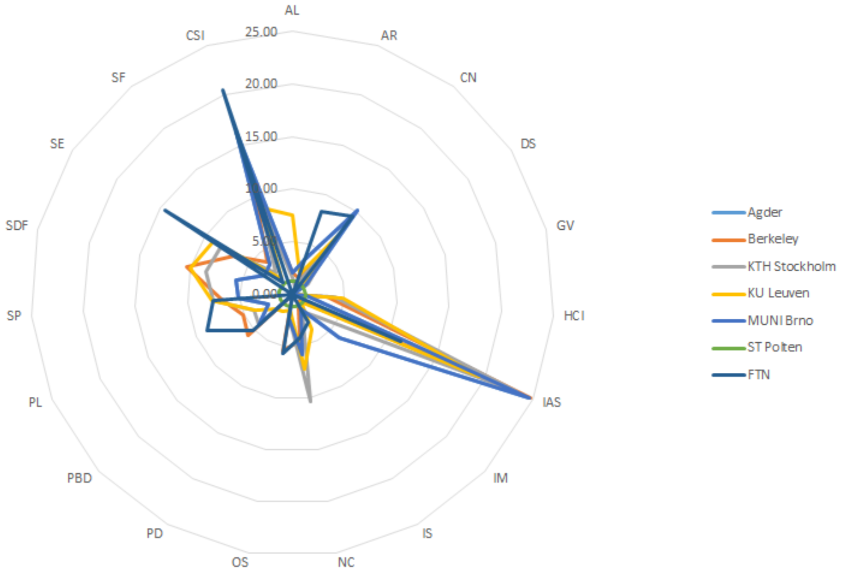

Figure 3: - Initial CS2013 KA coverage calculation results

4.2 Experiment with ENISA's European Cybersecurity Skills Framework (ECSF)

The European Union Agency for Cybersecurity (ENISA) published European Cybersecurity Skills Framework (ECSF) in September 2022. It defines 12 key cybersecurity roles described through their (1) mission, (2) deliverables, (3) main tasks, (4) key skills and (5) key knowledge. For the purpose of this study keywords were extracted from the description of each role in a process similar to the one applied in our curricula keyword extraction. The final output of this step was a set of key value pairs with where words from the descriptions were the keys and the numeric quantifications of words' importance were the values. The final keywords were extracted by sorting the set of key value pairs as illustrated in Table 3.

Table 3 provides a similar reference source as Table 1 used in our first experiment with the CS2013 reference curriculum. Similarly to our previous experiment we again applied a hypothetical adjustment of the baseline curriculum analysis of the above-identified

Table 2: - Comparison between overall curriculum change and CSI KA change

University	Curriculum Δ%	CSI Δ %
Agder	9.52	1.46
Berkeley	8.45	20.36
KTH Stockholm	5.27	9.30
KU Leuven	7.47	16.00
MUNI Brno	5.72	16.64
ST Polten	16.44	29.88
FTN	19.37	5.41

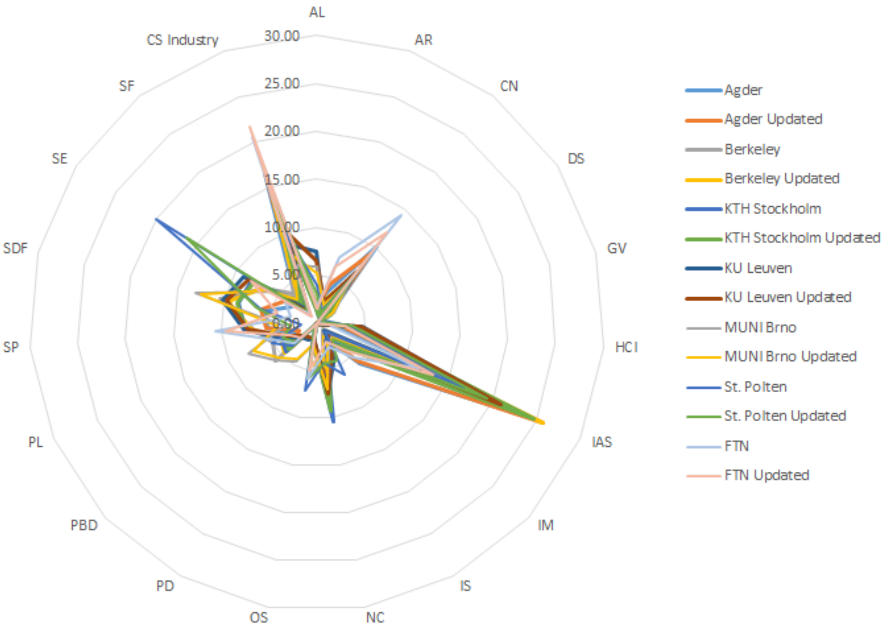

Figure 4: - Results after curriculum update

study programs. Course “Becoming a Cybersecurity Consultant” [29] used in previous experiment provides general cybersecurity knowledge which is suitable for supporting complete KA of CS2013 but not for ECSF role. In this experiment we added the SANS’ “Enterprise Penetration Testing” [30] course as adjustment. This course supports “penetration tester” role very well and it is expected that coverage of that role is increased after applying adjustment. Table 4 illustrates comparison between overall curriculum change and “Penetration Tester” role coverage change

After adjustment applied coverage of penetration tester role is increased for every curriculum in test dataset as it is presented in Figure 5.

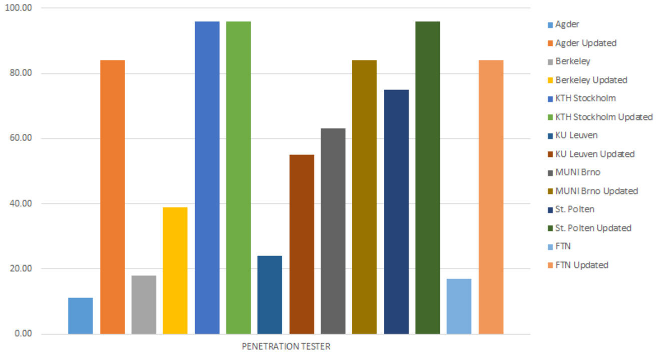

Figure 5: - Results after curriculum update

5 DISCUSSION

The conducted case study showed successful application of the Dynamic Cybersecurity Curriculum Optimization Method (DyCSCOM). In first iteration we mapped curriculum to KAs defined in the CS2013 reference curriculum. We experimented with hypothetical study program adjustment by extending them with external courses whose syllabi were available online and quantified the extent of changes. Figure 6 illustrates comparison between amount of curriculum changes (Curriculum Δ) and progress towards a higher

Table 3: - ECSF keywords per role

Roles	keywords
Chief Information Security Officer	cybersecurity management senior related organisation risks policies organisations develop ensure
Cyber Incident Responder	incident handling procedures cybersecurity response develop analysis results related actions
Cyber Legal Policy & Compliance Officer	data protection privacy compliance cybersecurity organisations legal ensure standards communicate
Cyber Threat Intelligence Specialist	threat intelligence cyber actors procedures threats identify ttps information data
Cybersecurity Architect	cybersecurity architecture security organisations related design requirements solutions evaluate privacy
Cybersecurity Auditor	standards auditing frameworks methodologies cybersecurity audit develop conformity procedures related
Cybersecurity Educator	cybersecurity training related awareness education develop deliver data protection methodologies
Cybersecurity Implementer	cybersecurity related solutions controls integrate performance security implement organisations products
Cybersecurity Researcher	cybersecurity related solutions development technologies identify research innovation topics ideas
Cybersecurity Risk Manager	cybersecurity risk controls management related organisations risks effectiveness practices strategy
Digital Forensics Investigator	digital forensics evidence procedures analysis present investigation document testing develop
Penetration Tester	testing penetration tools procedures test standards develop stakeholders report analysis

Table 4: - Comparison between overall curriculum change and penetration tester role coverage change

University	InitialCoverage %	UpdatedCoverage %	Penetration Tester Δ	Curriculum Δ %	Penetration Tester Δ %
Agder	11.00	84.00	73.00	28.07	324.04
Berkeley	18.00	39.00	21.00	9.28	135.31
KTH Stockholm	96.00	96.00	0.00	5.39	45.45
KU Leuven	24.00	55.00	31.00	11.46	123.29
MUNI Brno	63.00	84.00	21.00	6.31	20.32
ST Polten	75.00	96.00	21.00	10.18	39.77
FTN	17.00	84.00	67.00	21.11	75.94

coverage of topics necessitated by the industry (CS Industry Δ). If curriculum is initially well aligned with optimization target (cyber security industry in our case study) bigger curriculum changes are needed to reach significant optimization progress (Agder and Berkeley). Universities in Brno and Leuven have curricula which were initially not well-aligned with cyber security industry topics therefore optimization progress follows overall curriculum change. For already aligned curricula such as the FTN optimization progess is less than overall curriculum change.

Apart from a quantifiable progress towards the CS2013 reference curriculum, we also experimented with measurable incremental curriculum changes were towards a higher coverage of skills and knowledge defined in the cybersecurity roles of the ECSF. Figure 7 illustrates the comparison between the amount of curriculum changes (Curriculum Δ%) and optimization progress (Penetration Tester Δ = Penetration Tester updated - Penetration Tester initial). Again, initially less aligned curricula (Agder, Muni Brno, FTN and Berkeley) show higher levels of progress and sensitivity to change towards the setpoint defined in the ECSF. For example, KTH Stockholm curriculum which is initially very well aligned, shows very limited optimization progress.

6 CONCLUSION

This paper presents a novel Dynamic Cybersecurity Curriculum Optimization Method (DyCSCOM), for higher education curriculum analysis and dynamic optimization within regulatory bounds. This method solves a real challenge as although there is a significant market need for significant numbers of additional cybersecurity experts, academic institutions are often slow to respond with study program updates. Their nimbleness is further hampered by complex accreditation procedures and regulatory burdens as in most European countries the accreditation period for academic institutions is 4 to 7 with very limited annual program changes allowed. Our proposed model addresses this problem by allowing higher education institutions to easily quantify curriculum changes and

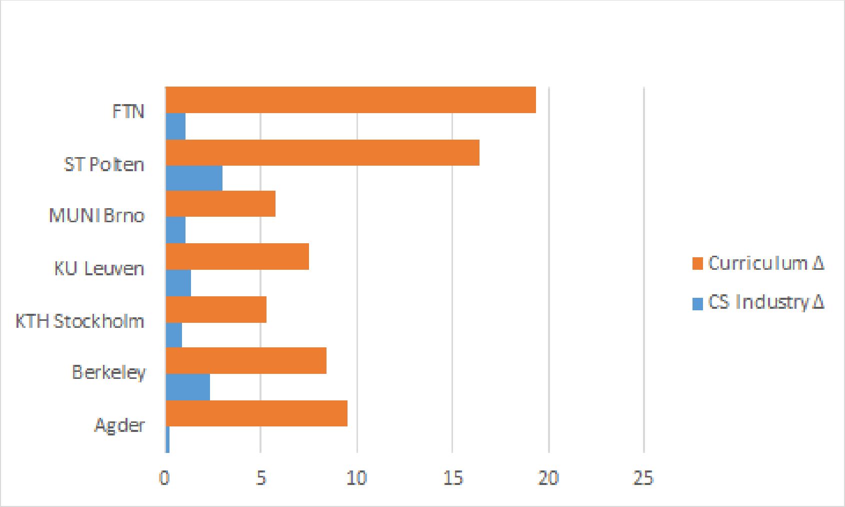

Figure 6: – Comparison between overall curriculum change and cs industry topic coverage increase in percentage

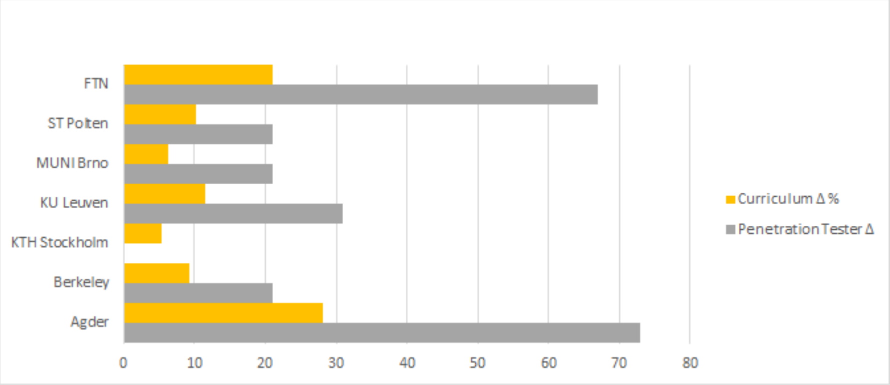

Figure 7: - Comparison between overall curriculum change and penetration tester role coverage increase in percentage

measure their progress towards industry-grade setpoints defined in reference curricula and skills frameworks.

The DyCSCOM consists of the following stages: data acquisition, preprocessing, coverage calculation and optimization. The coverage calculus relies on text mining, more specifically keyword extraction with Term Frequency–Inverse Document Frequency (TF-IDF) and Non-Negative Matrix Factorization algorithms.

The effectiveness of the method and our approach was assessed via two case studies. With small update, curricula from various countries were optimized toward targeted cybersecurity topics or the job roles defined in ENISA's European Cybersecurity Skills Framework (ECSF).

Our future work will be focused on automation of five new cybersecurity curriculum optimization method steps and the inclusion of the curricula of other cybersecurity study programs.

ACKNOWLEDGMENTS

The following funding source is gratefully acknowledged by the authors: the ERASMUS+ Erasmus Mundus Design Measures (EMDM) programme of the European Union (grant 1701-EPP-1-2020-1-LT-EPPKA2-SSA-B 'DJM-CYBER'), the ERASMUS+ Sector Skills Alliance (SSA) programme of the European Union (grant 621701-EPP-1-2020-1-LT-EPPKA2-SSA-B 'REWIRE') and Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund (grant TKP2021-NVA, TKP2021-NVA-29).

REFERENCES

[1] CheckPoint Corporation, https://resources.checkpoint.com/cyber-security-resources/2022-cyber-security-report(accessed 04.05.2023)
[2] (ISC)2. 2021. (ISC)2 Cybersecurity Workforce Study, https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx (accessed 04.05.2023)
[3] Europe council decision 765/2008, setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93

[4] Computer Science Curricula 2013, Association for Computing Machinery (ACM) IEEE Computer Society https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf (accessed 04.05.2023)

[5] ACM Curriculum Guidelines for Undergraduate Degree Programs in Computer Science CC2001 https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2001.pdf (accessed 04.05.2023)

[6] ACM Computing Curricula Computer Science Volume CS2008 https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2001.pdf (accessed 04.05.2023)

[7] Yoshitatsu Matsuda, 2018, "Curriculum Analysis of Computer Science Departments by Simplified, Supervised LDA", Journal of information processing

[8] Kornraphop Kawintiranon, Peerapon Vateekul and Proadpran Punyabukkana, 2016, "Understanding knowledge areas in curriculum through text mining from course materials", TALE

[9] Cyber security certification, https://www.cybersecurityeducation.org/certifications/ (accessed 17.04.2023)

[10] ACM cyber security curricula 2017, https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf (accessed 04.05.2023)

[11] Andrea Danyluk and Scott Buck, 2019, "Artificial Intelligence Competencies for Data Science Undergraduate Curricula", The Ninth AAAI Symposium on Educational Advances in Artificial Intelligence (EAAI-19)

[12] Diana Burley and Alfred H. Lewis Jr, 2019, "Cybersecurity Curricula 2017 and Boeing: Linking Curricular Guidance to Professional Practice", IEEE

[13] Gary L. Wallace, 2021, "The Need for Certification-Based Security Curriculum: A Matter of National Security", IEEE

[14] Akhtar Lodgher, Jeong Yang and Ummugul Bulut, 2018, "An Innovative Modular Approach of Teaching CyberSecurity across Computing Curricula", IEEE

[15] Jan Hajny, Sara Ricci, Edmundas Piesarskas, Olivier Levillain, Letterio Galletta and Rocco De Nicola, 2021, "Framework, Tools and Good Practices for Cybersecurity Curricula", IEEE

[16] Concordia courses database for cyber security professionals https://www.concordia-h2020.eu/map-courses-cyber-professionals/ (accessed 04.05.2023)

[17] Cyberseek framework, https://www.cyberseek.org/pathway.html (accessed 04.05.2023)

[18] ENISA European Cybersecurity Skills Framework2022, https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles/download/fullReport, (accessed 04.05.2023)

[19] Tomáš Brychcín and Miloslav Konopík, 2015, "HPS: High precision stemmer", Information Processing & Management

[20] Robert Ramirez and Nazli Choucri, 2016, "Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review", IEEE

[21] Cyber security academic programs database https://www.enisa.europa.eu/topics/education/cyberhead #

[22] KU Leuven Cyber Security curriculum https://wms.cs.kuleuven.be/cs/studeren/master-of-cybersecurity/cybersecurity-programme (accessed 04.05.2023)

[23] University of Agder Cyber Security curriculum https://www.uia.no/en/studieplaner/programme/M-SEC (accessed 04.05.2023)

[24] Masaryk University Brno Cyber Security curriculum, https://www.fi.muni.cz/catalogue-current/?program$=$nmgr_pskb_en (accessed 04.05.2023)

[25] KTH Royal Institute of Technology Cyber Security curriculum https://www.kth.se/en/studies/master/cybersecurity/courses-cybersecurity-1.1076018 (accessed 04.05.2023)

[26] St. Pölten University of Applied Sciences Cyber Security curriculum https://www.fhstp.ac.at/en/academic-studies-continuing-education/computer-science-security/cyber-security-and-resilience/course-contents#/ (accessed 04.05.2023)

[27] Berkeley School of Information Cyber Security curriculum https://ischoolonline.berkeley.edu/cybersecurity/curriculum/ (accessed 04.05.2023)

[28] Faculty of technical sciences, University of Novi Sad(FTN) Cyber Security curriculum http://www.ftn.uns.ac.rs/1149659633/informaciona-bezbednost (accessed 04.05.2023)

[29] Concordia "Becoming a Cybersecurity Consultant" course https://www.concordia-h2020.eu/becoming-a-cybersecurity-consultant (accessed 04.05.2023)

[30] SANS Institute "Enterprise Penetration Testing" course https://www.sans.org/cyber-security-courses/enterprise-penetration-testing (accessed 04.05.2023)