Balancing Generative AI and Critical Thinking to Develop Written Communication Skills in Cybersecurity

Apostolos Charalambous
Faculty of Pure and Applied Sciences
Open University of Cyprus
Cyprus
apostolos.charalambous@st.ouc.ac.cy

Andriani Piki
School of Sciences
University of Central Lancashire Cyprus
Cyprus
apiki@uclan.ac.uk

Joakim Kävrestad
School of Engineering
Jönköping University
Sweeden
joakim.kavrestad@ju.se

Eliana Stavrou
Faculty of Pure and Applied Sciences
Open University of Cyprus
Cyprus
eliana.stavrou@ouc.ac.cy

***Abstract*—**As cybersecurity education continues to evolve, the need for curricula that effectively balance the capabilities of generative Artificial Intelligence (AI) tools with the development of critical thinking and active learning skills has become increasingly urgent. This study addresses this challenge by proposing a curriculum for postgraduate cybersecurity education that focuses on developing transferable skills, particularly critical thinking and written communication. These skills are essential for cybersecurity professionals to excel in both their technical and communication-oriented responsibilities, meeting the growing demand of the cybersecurity industry in the age of AI. The proposed curriculum emphasizes the integration of constructivist learning principles and Bloom's taxonomy, two widely applied pedagogical models, to enhance learners' critical thinking and written communication skills. Designed for a penetration testing module, the curriculum follows a structured, step-by-step approach to build the necessary competences and empower aspiring cybersecurity professionals to meet the expectations of the cybersecurity industry. Through targeted activities, learners develop foundational knowledge while refining advanced written communication skills, equipping them to produce professional-level documentation, such as penetration testing reports. Generative AI is incorporated in the curriculum, providing opportunities for learners to experiment with AI-generated content while fostering the cognitive skills needed to critically assess its accuracy, relevance, and alignment with professional standards. This study contributes to cybersecurity education by presenting a replicable curriculum model that equips learners with vital skills, preparing them to navigate the complexities of written communication responsibilities in cybersecurity roles and adapt to the evolving demands of the AI era.

Keywords—Cybersecurity, penetration testing report, generative AI, transferable skills, written communication skills, postgraduate education, curriculum design

I. Introduction

In the fast-evolving field of cybersecurity, technical proficiency alone is no longer sufficient [1][2] for navigating the complexities of technological advances such as generative Artificial Intelligence (genAI). This presents challenges for educational programmes which must remain resilient in the face of this evolution, by embracing innovative pedagogical approaches [3] and going beyond traditional teaching methods [4][5][6]. Furthermore, the interdisciplinary nature of this domain means that, alongside technical expertise, cybersecurity professionals must possess effective communication skills, particularly in written communication [7][8][9][10].

Transferable skills, such as written communication, are fundamental across various cybersecurity roles, whether documenting forensic evidence, reporting penetration testing results, or delivering comprehensive risk assessments. Written communication is vital for effectively presenting complex ideas across different contexts and audiences. The European Cybersecurity Skills Framework (ECSF) [11] highlights the importance of this skillset in ensuring that cybersecurity experts across several cybersecurity career roles can convey critical information effectively to a diverse range of stakeholders. However, mastering writing skills is not straightforward. It requires the combination of diverse knowledge areas and skills including domain expertise, topic comprehension, critical thinking, attention to detail, a clear understanding of the target audience, logical structuring, analysing and evaluating existing documentation and policies, and synthesising multiple resources to create new reports [12]. These abilities are essential for demonstrating writing proficiency and constitute a fundamental part of the cybersecurity profession [13].

Cultivating critical thinking and written communication skills is crucial, yet challenging, particularly in an era marked by rapid digital transformation and technological disruption. Specifically, in the field of education, the rise of genAI has intensified the efforts in cultivating these skills, presenting both opportunities and challenges [14] for the future of education. On one hand, genAI has the potential to enhance learning by enabling learners to quickly grasp complex ideas and refine their writing [15]. On the other hand, it introduces risks, such as over-dependence on AI-generated content and diminished creativity, undermining writing and critical thinking skills. Biases in AI algorithms [16] and reduced attention to detail further complicate its use in educational contexts. These challenges, if not addressed, can directly hinder the development of a skilful workforce, as graduates may struggle to demonstrate the proficiency needed to meet professional standards. In light of these challenges, the need for effective interventions to develop and sustain written communication skills has never been more pressing. Cybersecurity education, especially at the postgraduate level, must equip learners with strong critical thinking abilities while also presenting opportunities for embracing the genAI era professionally and ethically, ensuring they are prepared to balance the use of genAI tools with their continuous personal skill development [6][17].

This paper focuses on the importance of written communication skills within cybersecurity and proposes a new curriculum tailored to postgraduate cybersecurity education. The curriculum aims to enhance students' writing skills by leveraging the capabilities of genAI [17] while also

fostering their self-efficacy [18]. The curriculum further seeks to help students become self-aware of their strengths and weaknesses, promote continuous improvement of their communication and critical thinking skills, and maintain an ethical approach to using genAI tools. By blending these key components into cybersecurity education, we aim to bridge the current gap in writing proficiency and ensure that students are better prepared to excel in both their technical and communication-based responsibilities, meeting the expectations of the cybersecurity industry in the age of AI.

The paper is organized as follows: Section II discusses background and related research focusing on the importance of written communication skills; Section III presents the methodology implemented in this work; Section IV presents the proposed curriculum, followed by the discussion of empirical findings and evaluation of curriculum design in Section V. The last two sections critically discuss the key observations and provide study conclusions, respectively.

II. Related Work

A. Importance of Written Communication Skills in the genAI Era

Effective verbal and written communication skills are fundamental in social and professional contexts alike. Constructing and communicating new content entails demonstrating an array of skills such as critical evaluation and interpretation of existing knowledge, analytical thinking, the ability to apply prior knowledge in new situations, being able to explain and describe ideas to different audiences and demonstrate a holistic understanding (these are broadly captured by Bloom's Taxonomy of cognitive thinking skills).

Recently, equipping learners with critical thinking and effective written communication skills has attained greater impetus in view of the digitalisation and rising complexity of the information landscape [19]. Trends such as information overload, mis- and dis-information [14], the increasing distribution of fast, unfiltered and often biased content, alongside the growing promotion of unstructured, unformatted, or purpose-less social interaction styles, impede the cultivation of critical thinking and effective, professional written communication. Another worrying trend is the increasing misuse of genAI tools and the lack of critical evaluation of AI-generated content. The ease with which genAI tools can generate high-quality and believable content has led to over-reliance on these tools, reducing users' creative thinking skills [20] and their ability to methodically review and critique their own writing [14]. Many users, including students and professionals, use the generated content 'as is' without reflecting on, or questioning, its accuracy, logic, practical usefulness, completeness or ethical soundness [3][14]. Unquestionably, in the field of education, genAI tools such as ChatGPT have sparked both admiration and controversy [15].

In response to these trends, academics, instructional designers and professional trainers have recognized the importance of leveraging the capabilities of genAI tools in education [15][17]. As AI-enabled applications increasingly permeate various aspects of our social and professional lives, the need for critical thinking skills and the ability to produce thoughtful, inquiry-based, well-structured, and purposive content has never been more crucial [3]. However, developing written communication skills requires leveraging genAI effectively and purposefully [19], while at the same time balancing the use of these tools with the cultivation of critical thinking skills. When embedded in purposefully designed curricula [19] which emphasize the balance between self-efficacy [18], informed engagement [15], robust critical thinking skills [3], and appropriate prompt engineering techniques [17], genAI can help streamline various aspects of the writing process and help enhance learners' competence in written communication. The curriculum proposed in this study is a step towards this direction.

B. Written Communication Skills in Cybersecurity

Transferable skills, also known as soft skills, cognitive skills, or complementary skills, encompass a set of personality traits, competencies, or behaviors that professionals display in various situations [21] and which extend beyond technical or domain expertise. Transferable skills can be developed through experience over time [21]. Cultivating these skills enables cybersecurity professionals to effectively address and mitigate cyber threats, protect assets, and strengthen organizational resilience against cyberattacks. In cybersecurity, essential transferable skills include communication, problem-solving, teamwork, analytical thinking, and writing skills [22] – skills which are considered critical for professionals to perform their roles successfully.

Among the essential transferable skills, effective communication, particularly written communication, is a key prerequisite for success in many areas of life and is essential for career advancement [23]. The ability to interpret complex situations and convey insights clearly and concisely to support informed decision-making is highly valued by employers. The ISC2 Cybersecurity Workforce report [22] highlights the importance of effective communication among cybersecurity professionals, senior management, and board members, emphasizing the need to present facts in accessible language when interacting with diverse audiences [24]. Beyond verbal communication, it is equally essential to emphasize the development of strong writing skills.

Written communication is a key function in business environments, taking various forms ranging from emails and technical reports to memos and press releases. Hence, it plays a crucial role in ensuring clarity and professionalism during internal and external communications. In complex fields such as cybersecurity where clarity, accuracy, accountability, and professionalism are imperative, written communication skills are vital for promoting effective information sharing, risk mitigation, and operational consistency [25]. Cybersecurity professionals must articulate and describe complex technical findings to both technical and non-technical audiences, ensuring that vulnerabilities, risks, and mitigation strategies are accurately understood and appropriately acted upon. Clear and concise cybersecurity technical documentation standardizes protocols across the organization, enabling all employees to follow procedures that protect sensitive information and systems. Additionally, well-structured reports – such as vulnerability assessments and penetration testing reports – serve as formal records, helping organizations assess their security posture over time and comply with regulatory requirements. Well-structured security policies and plans play a crucial role in incident response, providing a clear reference during security events and reducing response time by guiding teams through established protocols. Accessible documentation also supports collaboration between technical teams and other stakeholders, promoting a culture of security awareness and facilitating faster, more coordinated responses

to security incidents, ultimately enhancing operational efficiency. In a field where miscommunication can lead to significant security lapses, strong writing skills are invaluable for articulating detailed insights, fostering trust with stakeholders, and enhancing organizational resilience against cyber threats.

C. ENISA ECSF Communication Skill Needs

The ECSF, developed by the European agency for cybersecurity (ENISA), aims to define the skills relevant for various cybersecurity roles. ECSF defines 12 cybersecurity roles and lists communication as a key competence for all of them (Table I), showcasing its importance for cybersecurity experts [11]. The communication skills needed differ between roles but typically include both the ability to write technical reports and communicating technical concepts to non-technical audiences such as stakeholder boards. While technical skills are important for the cyber workforce, they are often overemphasized and the ability to communicate with different stakeholders is often overlooked [2]. When participants at Black Hat 2016 and DEF CON 24 were asked about the most important skills for their job, communication was rated as a core skill, but also one that was rarely included in education programs [26]. Although the need for communication skills in the cybersecurity field has been advocated for years, it is still largely considered a service-oriented field, suggesting that more emphasis should be placed on discipline diversity [24]. Cybersecurity professionals must be able to advocate for security at different levels of the organization, from the board of managers down to each employee. Considering that the human aspects in cybersecurity are increasingly emphasized, the focus on cultivating transferable skills in a systematic way should be elevated.

TABLE I. COMMUNICATION SKILLS IN ECSF

ECSF Profile	Communication Skills	Deliverables
#1 CISO	Communicate, coordinate and cooperate with internal and external stakeholder, Develop, champion and lead the execution of a cybersecurity strategy	Cybersecurity strategy, cybersecurity policy
#2 Cyber incident responder	Communicate, present and report to relevant stakeholders	Incident response plan, cyber incident report
#3 Cyber legal, policy & compliance officer	Explain and communicate data protection and privacy topics to stakeholders and users	Compliance manual, compliance report
#4 Cyber threat intelligence specialist	Conduct technical analysis and reporting, Communicate, coordinate and cooperate with internal and external stakeholders, Communicate, present and report to relevant stakeholders	Cyber threat intelligence manual, cyber threat report
#5 Cybersecurity architect	Communicate, present and report to relevant stakeholders, Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles	Cybersecurity architecture diagram, cybersecurity requirements report
#6 Cybersecurity auditor	Communicate, explain and adapt legal and regulatory requirements and business needs	Cybersecurity audit plan/report
#7 Cybersecurity educator	Develop evaluation programs for the awareness, training and education activities, Communicate, present and report to relevant stakeholders	Cybersecurity awareness program, cybersecurity training material
#8 Cybersecurity implementer	Communicate, present and report to relevant stakeholders	Cybersecurity solutions
#9 Cybersecurity researcher	Communicate, present and report to relevant stakeholders	Publication in cybersecurity
#10 Cybersecurity risk manager	Communicate, present and report to relevant stakeholders	Cybersecurity risk assesment report / risk remediation action plan
#11 Digital forensics investigator	Explain and present digital evidence in a simple, straightforward and easy to understand way, Develop and communicate, detailed and reasoned investigation reports	Digital forensics analysis results, electronic evidence
#12 Penetration tester	Communicate, present and report to relevant stakeholders, Conduct technical analysis and reporting	Vulnerability assessment results report, penetration testing Report

D. AI in Cybersecurity

AI has become deeply integrated into the field of cybersecurity [6], with AI applications typically centered on enhancing technical capabilities such as predicting future cyberattacks [27], constructing intelligent models for malware analysis and classification, real-time intrusion detection [6], and threat intelligence sensing [28], and supporting smart cybersecurity services and management [29]. While these applications strengthen defenses against cyber threats, they also highlight a growing need for upskilling, as the efficiency of AI-driven tools emphasizes the importance of advancing human capabilities to effectively manage and mitigate evolving risks arising from AI itself [27]. Thus, the focus on human empowerment and upskilling has become crucial in AI-cybersecurity research, emphasizing the importance of "bringing humans into the loop" [30]. Despite AI's extensive use in technical applications, and studies highlighting the importance of incorporating AI into network security curricula at the undergraduate level [6], genAI's potential for enhancing cybersecurity education and upskilling in the context of postgraduate education remains largely unexplored, highlighting an area well-suited for further research. This study is motivated by these gaps, aiming to investigate the application of genAI to support skills development in cybersecurity.

III. METHODOLOGY

This research addresses the challenges of an evolving cybersecurity landscape and the emerging role of genAI in education, by proposing a postgraduate cybersecurity curriculum that balances genAI and critical thinking to develop learners' written communication skills and foster a mindset focused on reflection and critical analysis. The goal is to develop a more informed and critically engaged cybersecurity workforce. Specifically, the proposed curriculum focuses on developing written communication competencies in the context of penetration testing.

To address the research objectives, background research was initially conducted, to explore alternative pedagogical

frameworks and written communication needs in cybersecurity and guide the design of the curriculum. Background research informed curriculum development, guiding the selection of key learning topics to address critical aspects of written communication essential for penetration testers. The curriculum was designed following constructivist learning principles and Bloom's taxonomy, gradually introducing learners to both theoretical and practical components to foster skill development. The curriculum was implemented with a cohort of 60 learners enrolled in a distance learning program as part of a postgraduate cybersecurity course focusing on penetration testing. Following the implementation of the curriculum, an anonymous evaluation questionnaire was administered to assess the curriculum's effectiveness and usefulness in developing written communication skills relevant to penetration testing. In addition to quantitative data highlighting the students' assessment of different aspects of their learning, qualitative insights were captured through an open-ended question. In the analysis below verbatim quotes are used to enrich the discussion of the findings. The combination of different types of data provided a comprehensive understanding of students' learning experiences. Overall, the gathered feedback provided valuable insights for refining the curriculum and motivating future research in this area.

IV. Curriculum Design

This section discusses the scope of the curriculum and the target audience, the pedagogical philosophy and the learning objectives that informed the curriculum design. Finally, the curriculum thematic areas are presented.

A. Audience and Scope

The proposed curriculum focuses on postgraduate cybersecurity education delivered through distance learning. Postgraduate programmes in cybersecurity often include individuals who have completed a computing-related Bachelor's degree, professionals that pursue a career change and originate from different backgrounds or cybersecurity professionals interested in advancing their career. This means that programmes include cohorts with varying degrees of knowledge and skills, and this should be considered when designing curricula for postgraduate cybersecurity education, so all learners stay engaged and motivated independent of their expertise [31]. Specifically, the learning content should be structured and developed in a way that will empower all learners to master their written communication competences to a professional level.

B. Penetration tester career role

Penetration testers, also known as ethical hackers, play a key role in cybersecurity. Their mission is to simulate cyberattacks to identify potential vulnerabilities in an organization's systems, networks, and applications, utilizing a range of tools and techniques [32]. Their primary goal is to uncover security weaknesses before malicious actors can exploit them, while also assessing the potential severity of any vulnerabilities that could be exploited [11]. Upon completing a penetration test, penetration testers provide a vulnerability assessment report and a penetration testing report.

To be effective in their roles, penetration testers require a range of transferable skills, including analytical thinking, attention to detail, and the ability to collaborate effectively with others [11]. Among the most essential skills are communication abilities, particularly in written communication. Clear and effective communication enables penetration testers to present their findings in a way that ensures vulnerabilities are fully understood and addressed appropriately by organizations [33]. Written communication is especially crucial for preparing and presenting detailed reports of the penetration test findings. These reports must be clear, precise, and actionable so that the organization can take the necessary steps to remediate identified vulnerabilities and strengthen its security posture.

C. Curriculum pedagogical philosophy

Cultivating written communication skills in cybersecurity, especially in the context of penetration testing, can be challenging as an individual needs to have a clear view of different aspects that need to be synthesized to produce a professional-level report. In the genAI era, this challenge can become even greater if the learners are not mindful of inherent biases, ethical considerations [16] and the risks that emerge when over-relying on the capabilities of genAI, without exercising their critical thinking in the process. New curricula should focus on empowering learners to navigate these risks by becoming knowledgeable of the written communication aspects that can lead to a professional-level report and by developing a high-degree of cognitive skills when utilizing genAI.

Given the potential of genAI tools as well as the importance of critical thinking, the authors suggest that purposefully balancing these elements can contribute to achieving the required learning outcomes. The proposed curriculum draws threads from constructivist learning and Bloom's Taxonomy of cognitive thinking skills with the aim to create engaging cybersecurity learning experiences. On one hand, constructivism is based on the tenet that learners construct knowledge based on their experiences. According to Piaget [34], constructivism theoretically captures how individuals build, acquire, or construct their knowledge through their real-world experiences and interactions. Hence the learners, rather than the educators, are the centre of constructivist pedagogies. Learning environments based on constructivist philosophy present genuine opportunities for learners to generate their own meaning and encourage them to establish connections between new knowledge and prior experiences. This emphasises the role of active student engagement, critical thinking, reflective reasoning, and self-directed learning, rather than passively consuming information as traditionally done in many classrooms [35]. We believe this fits well specifically in postgraduate education. On the other hand, Bloom's Taxonomy defines six cognitive levels of learning, starting with remembering basic knowledge to combining new and prior knowledge to form new concepts or create new artefacts [36]. The emphasis of both models on creation and construction is well-aligned with the learning objectives of a curriculum on penetration testing which emphasises written communication skills, as explored in this study. By combining constructivist learning and Bloom's taxonomy, the proposed curriculum aims to create a dynamic and effective cybersecurity education experience that equips learners not only with the knowledge but also with the written communication skills they need for performing their versatile roles.

D. Learning Objectives

The proposed curriculum (Table II) follows the guidelines provided in [37] to formulate its learning objectives. Emphasis

was placed on ensuring that learners develop a holistic understanding of the penetration testing reporting process. Each objective is designed to help learners grasp core aspects of the reporting process, from understanding the scope and reporting requirements to applying best practices in written communication. Additionally, with the growing role of genAI in education and industry, specific objectives target the responsible use of AI tools, encouraging learners to critically evaluate AI-generated content and integrate it effectively into their work.

The learning objectives are structured using constructivism principles and Bloom's taxonomy to progressively develop cognitive skills. To achieve this, the curriculum begins by focusing on the lower cognitive layers of Bloom's taxonomy, to build a strong foundation regarding written communication aspects in penetration testing. As learners advance, the curriculum shifts to higher-order thinking skills, including analysis, evaluation, and creation, enabling them to apply their knowledge critically, synthesize information, and produce professional-level penetration test reports (often called pentest reports). This scaffolded approach ensures a gradual, yet comprehensive mastery of the diverse skills required for effective written communication, ultimately preparing learners to meet the specific communication demands of the penetration tester career role.

TABLE II. LEARNING OBJECTIVES

ID	Learning Objective	Bloom's taxonomy
LO1	Recognize the scope and professional obligations involved in conducting and reporting a pentest	Remember
LO2	Explain how the scope of the pentest informs the reporting requirements, ensuring alignment between the test's objectives and the content of the final report	Understand
LO3	Distinguish between the expectations of senior management and the technical team to ensure the report content is tailored to meet the specific needs of each audience	Understand
LO4	Summarize the core qualities of effective written communication in a pentest report	Understand
LO5	Explain the risks associated with using genAI in written communication and the importance of developing cognitive skills to critically evaluate AI-generated content	Understand
LO6	Apply the appropriate structure and content to a pentest report, based on audience expectations	Apply
L07	Use a report template to create a well-structured and professional-level pentest report	Apply
L08	Experiment with genAI to enhance the executive summary of a pentest report	Apply
L09	Analyze written communication practices in existing pentest reports to identify good and bad practices that influence the overal quality of a report	Analyze
L010	Analyze the expectations of different audiences to determine and align content appropriately for the executive summary and technical sections of a pentest report	Analyze
LO11	Critically evaluate the quality of a pentest report and recommend improvements	Evaluate
LO12	Judge the effectiveness of genAI-enhanced content and determine where human revision is necessary	Evaluate
LO13	Create a comprehensive and professional pentest report by synthesizing information from an OSINT investigation and applying effective written communication practices	Create
LO14	Formulate effective prompt engineering techniques to enhance the quality of a pentest report	Create

E. Curriculum Content Structure

The curriculum was structured considering four thematic areas as presented below.

1) Scope and professional obligations

Initially, the curriculum placed emphasis on the importance of the penetration testing scope and how it should be considered when documenting the test findings. This direction was considered critical for the learners to understand that they need to demonstrate a professional stand in terms of how they handle the overall testing and then how they report the findings. The scope of the penetration test is an important component that drives the activities to be performed, and which needs to be given the appropriate attention, both during the initial stages when the scope needs to be defined and subsequently when the testing team needs to document the findings.

The outcome of the scope definition phase is the Rules of Engagement (RoE), which outlines essential guidelines that direct the activities of penetration testers. These include the objective of the penetration test, the systems to be tested, those explicitly excluded, involved parties, the testing timeframe, and the permissible extent of exploitation. The curriculum covers these elements, along with penetration testing types that vary based on the information provided to the test team prior to testing. Accordingly, black, white, and gray box approaches were introduced, emphasizing the importance of clearly indicating in the report which information was provided in advance and what was gathered during the test. Overall, the content covered was carefully selected to help learners understand how the planning phase is closely linked to the report-writing process in penetration testing.

Additional professional and ethical considerations were emphasized in the curriculum. Learners were guided to understand that the report contains confidential information and must be handled with diligence, implementing all necessary measures to protect its integrity and confidentiality. Understanding professional obligations is crucial, as it ensures that learners recognize their responsibility to uphold ethical standards and protect sensitive information. This awareness not only safeguards client trust but also reinforces their credibility and integrity within the cybersecurity field.

2) Audience expectations and knowledge areas

The key objective of this thematic area was to enable the learners to structure their report based on the audience's expectations. The curriculum delivered content to highlight that the report is read by the senior management and by the technical team of the organization. The expectations of each audience are different regarding the information documented in the report. Considering the audience's expectations, the learners should demonstrate different competences to effectively document their findings and meet expectations.

Specifically, the senior management is interested in the overall security posture of the organization, and the impact that the organization will face due to exploitation that might happen of vulnerabilities that have been identified during the test. Typically, this audience does not have technical knowledge, thus technical jargon should be avoided. Moreover, it is expected that high-level recommendations will

be provided, considering the severity of the identified vulnerabilities. The senior management expectations call for specific competences that the learners should possess. It should not be taken for granted that the learners have a clear view of the knowledge areas and skills they should cultivate. These competences were identified from background research and discussed in the curriculum. Specifically, learners should be knowledgeable regarding the organization's business context. Even though they might have technical expertise, at the same time they need to identify the valuable assets of the organization and the impact that might occur if an asset is affected. This knowledge is essential so they can discuss this aspect in their report and convey the situation to the senior management. Another knowledge area that is essential for the purpose of report writing is risk assessment, as the learners need to be able to prioritize the risk and provide appropriate recommendations. This means that they need to be able to evaluate the severity of the vulnerabilities and to do so, they need to specify the relevant severity scale that should be utilized. This is a core aspect in risk assessment.

The expectations of the organization's technical team are very different compared to those of the senior management. The technical team is interested in all the technical details that led to the identification and exploitation of the listed vulnerabilities. They need to be able to reproduce the steps taken during the penetration testing. This means that an appropriate level of detail should be provided, with clear and accurate information about the methodology that was followed and the tools that have been utilized. The analysis of the findings should be accompanied by appropriate screenshots taken during the testing process as proof of evidence of the vulnerabilities. Learners should realize that the screenshots serve as secondary sources of information, and that the primary source is the analysis they perform and document appropriately in the report. All screenshots should be accompanied by an appropriate caption and referenced directly in the report. Directions towards resolving the vulnerabilities should also be provided. Given the information that the technical team expects the report to contain, the penetration testers must demonstrate proficiency across several knowledge areas. These include identifying various types of vulnerabilities, evaluating them based on severity and impact, and prioritizing them effectively. Additionally, the penetration testers must be able to provide recommendations to address specific vulnerabilities. To maintain proficiency in a constantly shifting cyber threat landscape, it is also essential to locate and utilize diverse information sources, ensuring they remain current with emerging threats and best practices.

In this thematic area, activities were designed to help learners identify poor writing practices specific to the executive summary and technical analysis sections. By recognizing these ineffective practices in contrast to professional standards, the target was for learners to gain a clearer understanding of how a poorly written report that fails to meet expectations can leave potential clients dissatisfied and damage their reputation.

3) Report structure and content

A penetration testing report should be structured into two parts, the executive summary and the technical analysis. Considering the information that needs to be reported under each part, structuring the report in a logical way is essential to effectively present the findings to the intended audience. In terms of the report's structure, the target should be to achieve a logical flow of information, providing a clear walk-through of the steps that have been taken. This can promote reproducibility of tasks. Organizing the presentation of findings in a consistent approach is also necessary, producing a professionally looking report. Results that can be grouped together, for example port scanning results for several hosts, should be presented in a similar way. This means that relevant sections and subsections should all have the same structure. Sectioning should be visible, thus numbering sections is advisable. Furthermore, various elements, such as tables and graphs, can be used to effectively present the findings, enhancing the report's readability and supporting decision-making at both business and technical levels. This approach helps convey critical information clearly, enabling the organization to address findings efficiently and improve its security posture. Additionally, the table of contents, list of figures, and list of tables should accurately reflect the report's structure and content, free from indexing errors.

Organizing penetration testing notes is crucial to be able to handle report writing and structure it in an effective and efficient manner. Different tools have been presented, discussing how they can assist in the development of structured notes. The value of creating a template for note taking and for the overall report has also been highlighted. Understanding that a proactive, repeatable note-taking process can help standardize sections of the report and save time during the writing phase is key to producing consistent, high-quality documentation. This approach not only streamlines the report-writing process but also ensures accuracy and clarity, enabling the final report to meet professional standards effectively.

Overall, the curriculum gave emphasis on discussing the core written communication qualities needed to report the findings effectively, conveying the key details of the test that are of interest to the senior management and the technical teams, demonstrating a professional approach. Specifically, core qualities of written communication that have been covered in the curriculum include: 1) Appropriate – making sure that it has the right tone and the necessary level of formality, 2) Comprehensive – it includes the expected details, 3) Presentation – it is consistent in terms of formatting aspects and has correct spelling and grammar, 4) Accurate and Clear – it includes correct information, and it is understandable.

The curriculum covered all aspects that might be ignored during report writing, and which can affect the report's readability and value, even though the actual testing was performed with accuracy. The quote "If you do not document it, it did not happen", reflects how important it is to handle all aspects of the reporting phase with attention and professionalism.

A practical activity was conducted in which learners performed an OSINT investigation and documented their findings in a penetration testing report. They applied a report template to structure the content, addressing the needs of two distinct audiences: senior management and the organization's technical team. After creating the report, learners engaged in a quality control process, evaluating the report's clarity, accuracy, and alignment with professional standards.

4) GenAI competences

The final thematic area of the curriculum focused on genAI to familiarize learners with its capabilities and applications in professional report writing. Learners were

introduced to prompt engineering within the context of report writing in cybersecurity, exploring how genAI can enhance key elements such as structure, language, syntax, and summary quality to produce a professional-level report. Additionally, the curriculum addressed the risks associated with genAI, including over-reliance on AI-generated content and potential impacts on writing and critical thinking skills. Emphasis was placed on the importance of cultivating cognitive skills—such as critical thinking, attention to detail, and analytical abilities—which genAI can support but should not replace. Learners were cautioned that lack of foundational skills may lead to an overdependence on genAI, ultimately undermining proficiency and professionalism in the long run.

An activity was conducted to explore how generative AI can be leveraged to enhance the executive summary of a report. Learners were asked to reflect on the changes made, identifying specific aspects of the original report that were improved, such as clarity, conciseness, and overall readability. A key point of their reflection focused on determining where human revision is necessary to ensure accuracy, maintain the intended tone, and address specific areas that AI may overlook. This exercise aimed to assist learners critically assess the balance between AI-generated content and human oversight in producing a professional-level report.

TABLE III. LEARNING CONTENT AND PEDAGOGY

#	Learning Content (LC)	Pedagogy
1	Penetration testing scope and professional obligations	L/CD
2	Audience expectations	L/SGA
3	Report structure and content	L/CSA/CD
4	GenAI competences	L/D/PA
L= Lecture, CD=Critical Discussion, CSA= Case Study Analysis, D=Demonstration, SGA=Small Group Activity, PA= Practical Activity		

V. EVALUATION

The proposed curriculum was evaluated using a questionnaire that included a set of multiple-choice questions and an open-ended question. The questionnaire was completed by 60 learners. The purpose of the questionnaire was to evaluate the delivered content and its effectiveness to enhance the learners' written communication skills. Responses were submitted anonymously, and no sensitive information was recorded as part of the responders' feedback.

Initially, it was important to acquire a clear view of whether the participants had prior experience with writing a penetration testing report and the context in which they developed the report (Fig.1). The results indicate that the majority of participants (74%) had not previously created a penetration testing report before engaging in the course unit. Among those with prior experience, most had developed penetration testing reports in an academic setting, with 4% doing so at the undergraduate level and 10% at the postgraduate level. Interestingly, only a small percentage (3%) had created a report independently or for certification purposes.

A core aspect of the evaluation was to assess the usefulness of the curriculum content to assist learners realizing good and bad documentation practices and writing a penetration testing report that meet professional standards. Five topical areas have been included in the evaluation scope (Fig.2) which are mapped to key topics covered by the curriculum:

- Presentation elements (cover page, graphics, text consistency, tables, etc.)
- Report information (title, version, author, reviewed/approved by, classification, version control, etc.)
- Executive summary structure (information to include, practices to avoid)
- Methodology (reference to widely recognized standards/guidelines, stages, vulnerability severity scale, tools, etc.)
- Technical analysis structure (documentation of vulnerabilities, recommendations, screenshots, appendices, etc.)

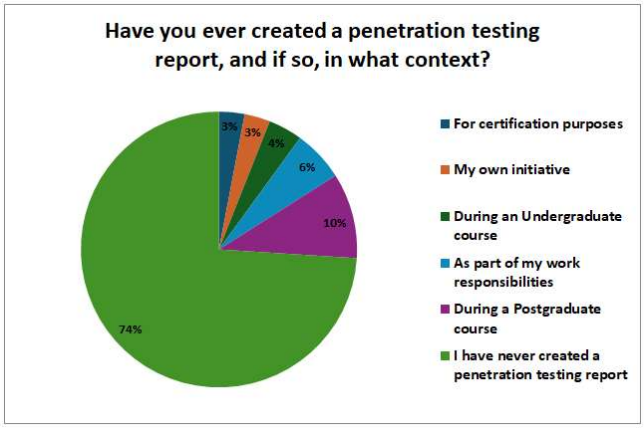

Fig. 1. Creation of a penetration testing report.

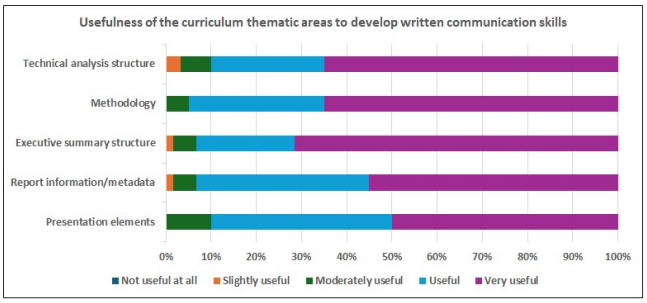

Fig. 2. Usefulness of the curriculum thematic areas.

Results reveal that, across all categories, a significant majority of respondents found the provided material and discussion to be either "Useful" or "Very Useful" in developing their understanding of effective documentation and presentation practices in penetration testing (Fig.2). The highest rating for "Very Useful" responses were found in Executive Summary Structure (71.7%), indicating that this is an area that is particularly impactful for learners aiming to master professional reporting standards. The inclusion of Methodology and Technical Analysis Structure, also scored highly, with 65% rating these areas as "Very Useful." Although the Presentation Elements category was rated "Very Useful" by 50% of the respondents, this percentage was lower compared to previous categories, with 40% rating it as "Useful" and 10% as "Moderately Useful." Report Information had a similar percentage of "Very Useful" ratings (55%). Interestingly, a very small percentage that ranged between 1.7-10%, rated some of the categories as "Slightly Useful" and/or "Moderately Useful," with Report Information

and Executive Summary Structure areas receiving minimal "Slightly Useful" feedback (1.7%).

Learners also responded to how useful the learning material and activities were to develop their skills and knowledge in written communication and to effectively present results from a penetration test (Fig. 3). The feedback indicates a strong positive response to the material and activities provided, with a substantial majority of participants (91%) agreeing or strongly agreeing that these resources were useful in enhancing their skills and knowledge in documentation and professional report writing for OSINT-based findings. With 53% "Strongly Agreeing" and another 38% "Agreeing," it is a good indication that the curriculum's approach effectively supported learners in achieving a high standard of professional documentation skills in the context of penetration testing.

This positive outcome suggests that the curriculum's content, focused activities, and hands-on approach were well-aligned with the learners' needs for professional development. The small percentage of "Slightly Disagree" (2%) and "Neutral" (7%) responses may indicate minor gaps or individual variations in learning preferences or prior knowledge levels. Such feedback can inform potential adjustments, such as incorporating even more diverse instructional methods or tailored support, to ensure all learners fully benefit from the curriculum.

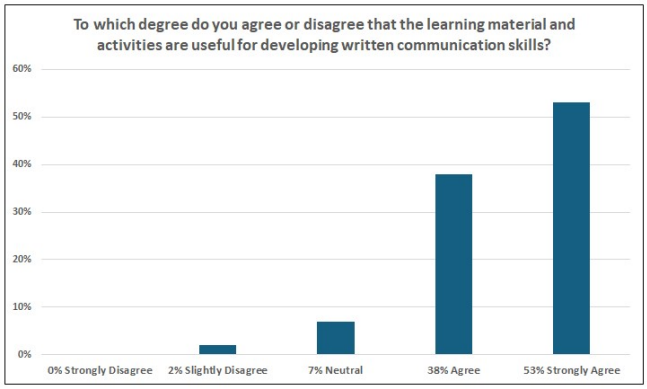

Fig. 3. Curriculum effectiveness.

The questionnaire also included an open-ended question inviting learners to share additional feedback. Some representative comments extracted from the responses include: "*sufficient material to bring us as close as possible to a professional level*", "*the material provided and taught in the course serves as a very good guide for creating a penetration testing report*", "*..it was very interesting... we gained considerable knowledge, especially on how to structure a proper and well-documented investigation*", "*helped us understand poor practices that may exist*", "*the coverage of topics aligns perfectly with the focus on creating a detailed and effective report*". Overall, the results validate the effectiveness of the curriculum in meeting professional documentation and reporting expectations within the context of penetration testing, demonstrating that most learners felt equipped to produce reports that meet industry standards.

VI. Discussion

A. *Balancing genAI and Critical Thinking for Developing Written Communication Skills*

Going beyond traditional teaching methods contributes to ensuring educational programmes remain resilient in the face of evolving challenges [4] by emphasising upskilling and reskilling [5][18]. In the evolving field of cybersecurity education, the integration of genAI alongside critical thinking is emerging as a powerful approach to developing key written communication skills among other competencies. The writing assistance features of genAI tools, when purposefully embedded in the learning process, can enhance learners' understanding of their capabilities, limitations and autoregressive nature [15], hence becoming more critical of their own writing skills. As genAI continues to influence various domains, its potential to enhance educational experiences, particularly in postgraduate settings, is under active exploration. In the context of teaching how to produce effective cybersecurity documentation, genAI can provide substantial support in structuring and refining complex content, while critical thinking remains essential for learners to evaluate and ensure accuracy, clarity, and appropriateness. Combining genAI with a focus on critical analysis and theoretical exploration [6] equips learners with the ability to leverage technology responsibly and effectively, promoting both skill development and a deeper understanding of professional standards in cybersecurity communication. To be effective, this approach should be implemented in a systematic and structured manner.

Given the diversity of experience levels common in postgraduate education, cybersecurity cohorts often include recent bachelor's graduates continuing with postgraduate studies, professionals pursuing career changes, and those already working in the field who wish to advance their competencies. This range of experience must be carefully considered to create a curriculum that caters to the diverse needs of learners. Evaluation results indicated that most learners entered the module with limited practical experience in professional documentation specific to penetration testing. This finding highlights the importance of incorporating foundational elements of report writing into a curriculum focused on developing written communication skills, especially for learners unfamiliar with industry-standard cybersecurity reporting practices.

Additionally, findings suggest that while some learners acquired relevant experience through informal education, this is less common, with academic and workplace settings remaining the primary avenues for developing transferable skills. These results highlight the need to design curricula that emphasize professional writing standards and systematically build relevant written communication skills within higher education. For learners with limited experience in penetration testing report creation, a course should prioritize documentation, structure, and content requirements to build foundational competencies. For those with prior experience, the curriculum can serve to refine and elevate existing skills, ensuring that all learners meet a consistent professional standard in reporting practices.

This structured approach can effectively balance the benefits of genAI with the essential skill of critical thinking to develop effective written communication skills that meet professional standards. By integrating genAI, learners can

access tools that help them structure reports and enhance their language precision. The emphasis on critical thinking encourages learners to evaluate AI-generated content, identifying areas where human insight is crucial to meet industry-specific requirements. This dual focus prepares learners not only to utilize AI responsibly but also to refine their skills independently, resulting in a curriculum that addresses the diverse competencies within the cohort and aligns with cybersecurity professional standards.

B. Learning Topics

Findings indicate that high value is placed on Executive Summary Structure, which may reflect its importance in aligning report content with the expectations of different audiences, particularly in distinguishing between content suitable for senior management versus technical stakeholders. Similarly, the emphasis on Technical Analysis Structure suggests that learners recognize the value of documenting vulnerabilities, recommendations, and supplemental details like screenshots, which are crucial for a comprehensive and professional penetration testing report. Based on learners' perception, Methodology scores second in terms of usefulness, alongside Technical Analysis Structure. This highlights the importance of emphasizing widely accepted standards and guidelines in the curriculum, to ensure consistency and credibility in reporting. Less emphasis was given to Presentation Aspects and Report Information. This may indicate that while presentation is essential, learners may view it as secondary to content-specific components, such as the executive summary and technical analysis. Similarly, given that Report Information received a lower percentage of being useful compared to all the other categories, this might suggest that while it is essential for professionalism, report metadata is considered less impactful on the overall quality of the report's substantive content. A few learners perceived some of the categories as slightly useful or moderately useful. This could reflect diverse learning needs or existing knowledge among learners. Authors will investigate this aspect further as part of their future work.

Overall, the results suggest that the curriculum effectively targets the critical areas learners perceive as most valuable for professional-level reporting, particularly in structuring and presenting both technical findings and executive summaries. Although all categories scored high, it is important to recognize that secondary elements, such as presentation aspects, play a significant role in establishing effective written communication. These elements contribute to the clarity, professionalism, and overall readability of the report, enhancing the impact of the technical content and ensuring that the report meets professional standards.

C. Limitations

One limitation of this work is the small cohort size, which affects the generalizability of the findings. With a limited sample it is challenging to fully understand how different experience levels might shape learners' understanding and expectations of professional written communication standards. Further research with a larger and more diverse cohort would provide valuable insights into how prior experience influences learners' perceptions and competencies, allowing for a more tailored approach in curriculum design to meet the needs of learners with varying levels of experience.

D. Future directions

The approach utilized in this study provides a solid foundation for identifying essential focus areas to effectively support the development of written communication skills in cybersecurity. The proposed approach can inform the creation of targeted learning activities that address both foundational and advanced competencies, ensuring a comprehensive skill-building experience. Future interventions should focus on creating adaptive and resilient curricula that accommodate the diverse experience levels of learners. Integrating real-world scenarios, such as case studies and simulated reporting tasks, can help bridge the gap between academic learning and industry expectations. Additionally, expanding the use of genAI tools in a controlled environment can support learners in refining their writing skills while fostering critical thinking about AI-generated content. Innovative cybersecurity programmes that emphasize personalized cybersecurity learning [17], design AI-augmented hands-on learning activities [6], foster intensive training and reskilling of cybersecurity professionals [5], and seamlessly integrate academic pursuits with real-world industry skill needs [4], present learners with unique opportunities to learn about cybersecurity while benefiting companies in terms of future talent recruitment [4]. Thus, they contribute to efforts towards addressing the skills gaps in the field of cybersecurity [22] and the broader cybersecurity talent shortage [5][6][37][38].

VII. Conclusions

Written communication skills are crucial for current and future generations of cybersecurity professionals. Even if there are diverse roles in the cybersecurity industry, a consistent task is to deliver written information to different stakeholders. This task encompasses a range of skills that cybersecurity professionals are expected to cultivate through formal or informal education, and through working experience. Current cybersecurity education programmes often overlook the importance of written communications skills and, as a result, they may fail to equip learners with this competence. Acquiring written communication skills in a consistent manner through working experience is also challenging if proper mentoring is not offered, especially for junior employees. In this paper, we are addressing the challenges of developing written communication skills for cybersecurity professionals and the challenges of utilizing generative AI. We do so by developing a curriculum where learners enhance their critical thinking skills while exploring the use of generative AI as a tool to help improve written communication in the context of penetration testing reports.

Our evaluation shows that by combining constructivist learning principles and Bloom's levels of cognitive learning, we can create a dynamic and effective cybersecurity education experience that equips learners with the knowledge and skillset they need to excel in their versatile roles. The evaluation also shows that balancing genAI-infused curricula with activities that trigger critical thinking can help postgraduate students enrich the written communication competencies needed to thrive in the everchanging cybersecurity jobs landscape. We envision that the proposed curriculum can inspire educators across the world and provide guidance on how to integrate communication skills into existing education plans in a novel way. As part of our future work, we plan to contact studies with a larger sample size and employ mixed methods to assess the long-term impact of the

curriculum on learners' written communication skills and professional competency in cybersecurity.

REFERENCES

[1] J. L. Hall and A. Rao, "Non-Technical skills needed by cyber security graduates," in 2020 IEEE Global Engineering Education Conference (EDUCON), 2020.

[2] J. Dawson and R. Thomson, "The future cybersecurity workforce: Going beyond technical skills for successful cyber performance," Front. Psychol., vol. 9, p. 744, 2018.

[3] C. Bhuman, C. Khawar, "Fostering Critical Thinking in the AI Era: Innovative Educational Approaches for a Data-Driven Society," 2024.

[4] J. Rajamäki, P. Rathod and P. Kämppi, "Integrating International Research-Innovation Projects and Working Life Partners into Cybersecurity Degree Programme," *2024 IEEE Global Engineering Education Conference (EDUCON)*, Kos Island, Greece, 2024, pp. 1-9, doi: 10.1109/EDUCON60312.2024.10578728.

[5] G. Karlsson, "From Campus to Boot Camp — Lessons from Extramural Teaching in Cybersecurity," *2024 IEEE Global Engineering Education Conference (EDUCON)*, Kos Island, Greece, 2024, pp. 1-8, doi: 10.1109/EDUCON60312.2024.10578866.

[6] B. Alomar, Z. Trabelsi, T. Qayyum and M. M. Ambali Parambil, "AI and Network Security Curricula: Minding the Gap," *2024 IEEE Global Engineering Education Conference (EDUCON)*, Kos Island, Greece, 2024, pp. 1-7, doi: 10.1109/EDUCON60312.2024.10578588.

[7] C. Maurer, M. Sumner, D. Mazzola, K. Pearlson, and T. Jacks, "The Cybersecurity Skills Survey: Response to the 2020 SIM IT Trends Study", In *Proceedings of the 2021 on Computers and People Research Conference,* pp. 35-37, 2021.

[8] O. Ozyurt, A. Ayaz, "Identifying cyber security competencies and skills from online job advertisements through topic modelling", *Security Journal*, pp.1-21, 2024.

[9] C.M. Graham, Y. Lu, "Skills expectations in cybersecurity: semantic network analysis of job advertisements", *Journal of Computer Information Systems*, *63*(4), pp.937-949, 2023.

[10] C. Somers, E. Byrne, "Cyber Security Skills Report 2021 National Survey", *Cyber Ireland*, 2021. [Online]. Available: https://www.cyberireland.ie/wp-content/uploads/2021/02/Cyber-Ireland-Skills-Report-2021.pdf

[11] ENISA, "European Cybersecurity Skills Framework Role Profiles", 2022. [Online]. Available: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

[12] N. Mcnulty, Bloom's Taxonomy Reimagined: Digital Strategies for Today's Teachers. 2020.

[13] G. White, "Higher education model for security literacy using bloom's revised taxonomy," *Cybersecurity Pedagogy and Practice Journal*, pp. 27–36, 2024.

[14] M. M. Thiga, "Generative AI and the Development of Critical Thinking Skills," Iconic Research and Engineering (IRE) Journals, vol. 7, no. 9, pp. 83–90, 2024.

[15] S. Hammer, S. Ottinger, B. Zönnchen, M. Hohendanner, M. Hobelsberger and V. Thurner, "ChatGPT in Higher Education: Perceptions of Computer Science-Related Students," *2024 IEEE Global Engineering Education Conference (EDUCON)*, Kos Island, Greece, 2024, pp. 01-08.

[16] J. Otterbacher and Y. Manolopoulos, "Machine Ethics Research: Promises and Potential Pitfalls," *IEEE Intelligent Systems*, vol. 38, no. 4, pp. 62–68, 2023.

[17] C. Kallonas, A. Piki, E. Stavrou, "Empowering Professionals: A Generative AI Approach to Personalized Cybersecurity Learning", *IEEE Global Engineering Education Conference (EDUCON)*, pp. 1-10, Kos Island, Greece, 2024.

[18] E. Stavrou and A. Piki, "Cultivating self-efficacy to empower professionals' re-up skilling in cybersecurity," *Inf. Comput. Secur.*, vol. 32, no. 4, pp. 523–541, 2024.

[19] S. S. Lim, T. Makany, "Deploying chatbots to build students' critical thinking skills: Leveraging generative AI effectively and purposefully in higher education," in *Encyclopedia of Educational Innovation*, M. A. Peters and R. Heraud, Eds. Springer, 2023.

[20] H. B. Essel, D. Vlachopoulos, A. B. Essuman, and J. O. Amankwa, "ChatGPT effects on cognitive skills of undergraduate students: Receiving instant responses from AI-based conversational large language models (LLMs)," Computers and Education: Artificial Intelligence, vol. 6, 2024.

[21] B. Tulgan, "Bridging the Soft Skills Gap: How to Teach the Missing Basics to Todays Young Talent," John Wiley & Sons, 2015.

[22] ISC2, *Cybersecurity Workforce Study*, Report, www.isc2.org/research, 2023.

[23] J.R. Sparks, Y. Song, W. Brantley, O. L. Liu, "Assessing Written Communication in Higher Education: Review and Recommendations for Next-Generation Assessment," *ETS Research Report Series*, no.2, pp.1–52, 2014.

[24] J. M. Haney, W.G. Lutters, "Skills and Characteristics of Successful Cybersecurity Advocates," *In SOUPS*, 2017.

[25] R. Augusto, *The Role of Technical Writing in Cybersecurity*. *Doakio*. https://doakio.com/blog/the-role-of-technical-writing-in-cybersecurity/, 2023

[26] K. S. Jones., A. S. Namin, M. E. Armstrong, "The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals," *ACM Transactions on Computing Education (TOCE)* 18, no.3, pp.1-12, 2018.

[27] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, "The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review," *International Journal of Advanced Research in Computer and Communication Engineering*, 2022.

[28] J.-H. Li, "Cyber security meets artificial intelligence: a survey," *Front. Inf. Technol. Electron. Eng.*, vol. 19, no. 12, pp. 1462–1474, 2018.

[29] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-driven cybersecurity: An overview, security intelligence modeling and research directions," *SN Comput. Sci.*, vol. 2, no. 3, 2021.

[30] "Artificial Intelligence and Cybersecurity Research", ENISA, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/artificial-intelligence-and cybersecurity-research.

[31] T. Crick, J.H. Davenport, P. Hanna, A.Irons, T. Prickett, "Overcoming the Challenges of Teaching Cybersecurity in UK Computer Science Degree Programmes", *2020 IEEE Frontiers in Education Conference (FIE)*, pp. 1-9, 2020.

[32] M. Alhamed, and M.M.H. Rahman. "A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions" *Applied Sciences*, 13, no. 12: 6986, 2023.

[33] D. J. Beukes, "Evaluating the Cyber Security Skills Gap relating to Penetration Testing", Master Thesis, Rhodes University, 2021.

[34] J. Piaget, "The Theory of Stages in Cognitive Development," in *Measurement and Piaget*, D. Green, M. P. Ford, and G. B. Flamer, Eds. New York, NY: McGraw-Hill, 1971, pp. 1–11.

[35] H. V. Le and L. Q. Nguyen, "Promoting L2 Learners' Critical Thinking Skills: The Role of Social Constructivism in Reading Class," *Frontiers in Education*, vol. 9, 2024.

[36] L. W. Anderson and D. R. Krathwohl, *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives*. New York: Addison Wesley Longman, Inc, 2001.

[37] E. Stavrou, "Planning for Professional Development in Cybersecurity: A New Curriculum Design," in *Human Aspects of Information Security and Assurance. HAISA 2023. IFIP Advances in Information and Communication Technology*, vol. 674, S. Furnell and N. Clarke, Eds. Cham: Springer, 2023.

[38] H.-J. Kam, P. Menard, D. Ormond, and R. E. Crossler, "Cultivating cybersecurity learning: An integration of self-determination and flow," Computers & Security, vol. 96, no. 101875, p. 101875, 2020.