

# Empowering Professionals: A Generative AI Approach to Personalized Cybersecurity Learning

Christos Kallonas  
Faculty of Pure and Applied Sciences  
Open University of Cyprus  
Nicosia, Cyprus  
christos.kallonas@st.ouc.ac.cy

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

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

**Abstract**—We are navigating an era of ongoing technological transformations characterized by a growing need for developing digital skills, including cybersecurity and Artificial Intelligence (AI) literacy. The skills gap in cybersecurity has been acknowledged by the academic and business community at large, which faces an ongoing challenge in terms of finding and attaining talents. Even though different initiatives have been launched to upskill and reskill individuals, they are either ineffective in developing the required competencies or fail to motivate participants to learn and advance their competencies in relation to a cybersecurity job role. A key factor hindering these efforts is the adoption of a generic training approach rather than tailoring learning to the needs of individual learners. It is imperative to identify novel ways to motivate and engage learners, fostering a lifelong learning mindset that is essential for cybersecurity professional development and progression. This work aims to investigate how generative AI can be leveraged to empower professionals to take ownership of their learning by assisting them to create a personalized cybersecurity study plan. The objective is to inspire the design of innovative solutions focusing on accelerating skills development and contributing to increasing the supply of skilled cybersecurity professionals.

**Keywords**—*Cybersecurity learning, cybersecurity professional development, cybersecurity career, generative AI, personalized learning, ChatGPT, learning autonomy*

## I. INTRODUCTION

The ongoing challenge the cybersecurity domain is facing in terms of finding and attaining cybersecurity talent has become more pronounced in recent years [15]. The latest cybersecurity workforce reports [1] [2] [3] [4] indicate that the prevalent gap in cybersecurity skills will persist in the coming years, highlighting the genuine need for more skilled and competent cybersecurity professionals. In high-risk and ever-changing domains like cybersecurity, upskilling and reskilling are indispensable. Upskilling endeavours may transpire in professionals' working environment, due to emerging needs in their current job role, or may be pursued in the context of Continuous Professional Development (CPD). Although different initiatives have been developed to support upskilling and training efforts, in many cases these have been deemed ineffective. In fact, "one of the main factors cybersecurity training programs are often not very effective is the lack of engagement or motivation of participants. This is often the result of training not being tailored to the needs or preferences of participants." [16]. Therefore, there is an urgent need for more personalized and efficient ways to motivate and engage cybersecurity professionals to thrive in lifelong learning.

This paper aims to investigate how generative Artificial Intelligence (AI) [12] can be leveraged to create tailored

learning and training study plans that match a targeted professional profile or skillset. This paper implements an exploratory methodology [34] to support this research objective and to provide insights guiding individuals to specify their learning and training study plans based on personal preferences and professional needs. Although there is a wide range of interdisciplinary intersections between cyber security and AI [35] [36] [37][38], the use of generative AI tools for educational and upskilling purposes is still underexplored. The goal of our study is to explore if generative AI tools, such as ChatGPT, can help individuals plan their professional development in a structured and effective way, accelerating skills development and contributing to increasing the supply of skilled cybersecurity professionals. While the emphasis in this paper is on individuals who work in, or consider shifting into, the field of cybersecurity, it is envisioned that the investigations will inspire scholars to apply the proposed exploratory methodology in other interdisciplinary fields which require transferable skills development such as attention to detail, communication skills, critical thinking and problem solving, alongside domain-specific competencies.

The paper is organized as follows. In Section II we delve into background research and related developments. Section III presents the exploratory research methodology implemented in this work. Section IV discusses the key learning and training aspects drawing on learning theories and frameworks to inform this work's explorations. In Section V we present the empirical findings, critically analyse them, and evaluate the generative AI responses. The last two sections discuss the key observations and study conclusions, respectively.

## II. RELATED WORK

### A. Cybersecurity Skill Needs and Professional Development

The ongoing technological advances have made cybersecurity knowledge and skills indispensable across all domains. Both computing professionals and individuals in peripheral job roles need to remain up to date with the latest technological developments, cybersecurity threats, and policy changes. Recently, ENISA (European Union Agency for Cybersecurity) published the European Cybersecurity Skills Framework (ECSF) [5] which describes the profiles of key cybersecurity roles in the context of a typical management cycle (plan – implement – operate – improve). Likewise, the US National Institute of Standards and Technology (NIST) published the National Initiative for Cybersecurity Education (NICE) framework [6]. The latter has been developed to serve

as a reference taxonomy of the cybersecurity work that is carried out in specific cybersecurity roles, and describes the tasks, knowledge, and skills that are needed in each role. Through ECSF and NICE taxonomy, learners can explore different occupational profiles and engage in learning and practical activities to enhance their knowledge and skills. Nevertheless, this is not a straightforward task to perform. The scarcity of training guidelines and the variety of resources to utilize, may be overwhelming for professionals [7], especially for those entering the domain or early career staff lacking the experience to realize all the responsibilities a specific cybersecurity role may entail. Given the multidisciplinary nature of cybersecurity and the potential for professionals originating from different domains to enter the cybersecurity workforce [29], the challenge becomes greater. Hence, there is a genuine need for supporting aspiring cybersecurity professionals in designing effective and personalised learning and training study plans to build specific competencies within the context of their job roles and advance their career.

The need to adopt a tailored approach in professional development is discussed in a recent study [7] where the design of a new learning activity is presented, demonstrating how learners can be guided to identify their competencies and gaps and, subsequently, plan for their career development. Similarly, scholarly work focusing specifically on cybersecurity workforce and skills [8] highlights the challenge of identifying the cybersecurity qualifications or certifications that can assist in the development of a specific set of skills. It is also emphasised that professionals might pursue the wrong certification if they fail to establish the right match between the certification and their career goals and learning objectives. This challenge can be alleviated if appropriate guidance is provided to learners to identify roles of interest, their current skills, the skillsets and knowledge they lack, and identify an appropriate certification or training programme to pursue.

Recent research has also proposed mentoring as a highly impactful practice for strengthening cybersecurity education and professional advancement [9][10]. These initiatives are offering guidelines towards professional development and tailored learning and training goals, an approach that is essential to meet the distinct learning needs of each learner. Microsoft defense report 2023 [11] indicates the need to “conduct innovative experimentation with user engagement strategies” and recommends to “develop tailored and context-aware education models that treat users as distinct individuals and be implemented at scale”. This points to innovative directions towards investigating more actively how to empower professionals to analyze cybersecurity role profiles of interest and contextualize a profile into a learning and training study plan, considering personal traits, current competencies and learning preferences. This approach is expected to lead to focused and engaging learning experiences that can effectively lead to accelerated and more effective upskilling of individuals.

### B. AI in Cybersecurity

The interplay between cybersecurity and AI is not something new [31][37]. Most of the applications of AI, however, focus on introducing AI techniques, such as machine learning and deep learning, to facilitate the prediction of future cyberattacks [37], to construct smart models for malware classification, intrusion detection and threats intelligence sensing [35], and for intelligent cybersecurity services and management [36]. While the application of AI in

cybersecurity helps prevent cyberattacks, AI technology has also resulted in unemployment in some cybersecurity posts it replaced, since it is incredibly efficient [37]. Therefore, the need for upskilling and reskilling becomes increasingly more prevalent. “Bringing humans into the loop” [31] constitutes one of the key challenges and research gaps in the horizon of AI and cybersecurity research. This calls for more research in the field as well as training practitioners [31]. While the latest advances present a greater challenge in the cybersecurity field, they also highlight the need for embracing AI for human empowerment. A key observation is that even though the intersection of AI and cybersecurity has been employed for the technical capabilities it can engender, the capabilities of employing generative AI tools for educational and upskilling purposes in cybersecurity is still underexplored. This defines the focus in the present study.

## III. RESEARCH METHODOLOGY

In this work we deployed an exploratory research methodology [34] to gather preliminary information on the capabilities of a generative AI tool (ChatGPT 3.5) to help aspiring professionals, especially early-career ones, to build a cybersecurity role-oriented study plan. Our research approach strives to discover new insights by working through a reflective exploration of emerging findings [34], with the aim to inform future research into the use of AI in cybersecurity education and training. Hence, the results of the exploratory research are discussed with the view to provide a route towards personalized cybersecurity learning by allowing learners to formulate effective prompts to optimize ChatGPT responses and inform their training study plan. It is envisioned that the findings can lead to effective learning experiences and enhance current efforts offering cybersecurity career training guidance. ChatGPT 3.5 community version was preferred over ChatGPT 4.0 since it is more widely accessible. Adopting an inclusive and accessible approach is important in all forward-looking educational initiatives.

We document below the steps we followed in the current study to promote replication of our approach by other scholars.

- **Cybersecurity profession in focus:** Initially, the key elements that should be taken into consideration when building a cybersecurity training study plan are specified. These elements can be considered for crafting opening prompts as well as for critically analysing subsequent ChatGPT responses.
- **Preliminary analysis:** In line with the studied literature and aligned with the research aim and objectives, specific codes (research constructs) are selected to facilitate subsequent qualitative analysis. The coding structure extracted during the preliminary analysis included the following codes, organized under four thematic categories: (i) ‘*learning and training study plan*’ (topics’ appropriateness, manageable learning sections, level of provided details, task completion time), (ii) ‘*resources*’ (diversity, specific examples, credibility), (iii) ‘*soft skills development*’ (learning topics, activities), (iv) ‘*advice for professional development*’ (networking, lifelong learning, certifications selection, ethics principles).

- **Colour coding:** A document is created to include the trail of prompts and ChatGPT responses. A colour-coding scheme is applied on the responses to facilitate the analysis.
- **Qualitative analysis:** A spreadsheet is created based on the codes to report prompts, responses, and relevant insights that could help amend subsequent prompts to receive more focused responses.
- **Contextualization and skills mapping:** A career role is selected from ECSF and the profile information is embedded into the initial ChatGPT thread.
- **Prompt engineering:** The prompts to input to ChatGPT are decided based on the learning and training aspects analyzed in the context of this study.
- **Exploration:** Following ChatGPT's responses, existing prompts are amended and/or new prompts are crafted to explore whether responses can be optimized, leading to more targeted professional learning and development advice.

#### IV. LEARNING AND TRAINING ASPECTS TO SUPPORT EXPLORATION

This section discusses the key learning and training aspects drawing on learning theories and frameworks that can inform the investigations performed in the study. The underlying learning principles can help in building more effective ChatGPT prompts toward investigating the potential of generative AI tools to assist learners formulating a personalized cybersecurity learning and training study plan.

##### A. Key learning and training aspects

Every venture which sets out to promote skills development needs to consider several pedagogical, technological, and practical aspects to be fully realized. Considering the increasing demand for cybersecurity expertise, scholars, practitioners, and organizations have strived to create training environments for professionals to have hands-on learning activities simulating various scenarios and cyber-attacks [14]. However, such efforts often focus on the features and technical characteristics of cyber-attacks and fail to provide a 'pedagogic point of view' [14]. As a result, many efforts do not reach the desirable outcomes and fail to assist professionals realize how to formulate their upskilling and/or reskilling plan. While training approaches and frameworks which provide hands-on learning activities can achieve good results, they face two common drawbacks. Firstly, such training is constrained to the known attacks at a particular point in time, and the database needs to be continuously upgraded to reflect newly surfaced incidents and attacks. Secondly, there is an emphasis on the technical aspects of the attacks and pedagogical aspects are often neglected [14]. While such training approaches may enhance technical skills in relation to specific types of cyber-attacks, failing to incorporate self-evaluation, self-reflection, human perspective [15] and soft skills, may be constraining for continuous professional development. Hence, it is essential to ensure that "the training offered must move beyond basic techniques and concepts to maintain a competent and robust workforce in the long term." [15]. Similarly, in the 2023 World Economic Forum 'Jobs of the Future' report [19], cognitive and self-efficacy skills, including lifelong learning, rank top among the core skills across all jobs, indicating that

there is a need for a more personalized approach for empowering professionals to develop their cybersecurity competencies and continue advancing within a cybersecurity role, as the one proposed in the paper.

1) *Pedagogical constructs and learning theories inspiring cybersecurity training.* It is widely established that successful learning and training methods are those which present learners with authentic activities [24], seamlessly simulating real-life environments [14] and allowing learners to explore and take ownership of their learning. Adult learning theory principles, such as self-direction, transformation, experience, mentorship, mental orientation, motivation and readiness to learn, could also provide insights and useful directions related to aspects of cybersecurity professional development. Self-determination, flow and task significance were also found to positively affect learning motivation in cybersecurity educational contexts [15]. Authentic activity theory [24], self-determination theory [15], constructivist learning, and experiential learning theory constitute pertinent theoretical frameworks for promoting these values [20]. However, translating core theories like constructivism and self-determination into instructional design [21] to formulate a personalized learning and training study plan, is not straightforward. This presents an opportunity to leverage generative AI tools.

2) *Types of interactions in distance education.* Various types of interactions take place in distance learning and web-based learning contexts [14], including learner-content, learner-instructor [22], and learner-interface interactions [23]. In this paper we argue that with the advent of generative AI tools, a novel type of interaction needs to be leveraged, namely 'learner-AI prompt' interaction. This goes beyond interacting with, and manipulating, the user interface of a web-based tool to accomplish a particular task [14] [23]. The 'learner-AI prompt' interaction entails a process of critical analysis and evaluation, which can contribute to formulating reflective professionals, a personal trait that is in demand by cybersecurity employers. Prompt engineering is well aligned with authentic learning practices [14], self-determination principles [15] and constructivist learning theories [20], as it provides the opportunity for learners to examine the task at hand from diverse or even conflicting perspectives and create unique scenarios through which to examine the task. Furthermore, this process provides the opportunity for reflection [14], which has a two-fold value. First, reflection is an important element in authentic online learning activities [24], and second, reflection is a cognitive skill in its own right which can trigger creativity and promote critical and analytical thinking. Along with technical skillsets, cognitive and self-efficacy skills are crucial for cybersecurity experts. While, "some aspects of cybersecurity require substantial effort and perseverance for conceptual understanding to be gained", encouraging individuals to pursue cybersecurity learning, can help to address "the critical shortage of cybersecurity talent" [15]. By pursuing cybersecurity learning enabled by generative AI prompt engineering, information security professionals can cultivate cybersecurity skills and deepen their conceptual understanding [15].

3) *Level of learning and training.* One potential pathway to addressing the shortage of cybersecurity talent is to retrain current non-cyber professionals so they develop the skills and competencies pertinent to cyber operations [15]. Another pathway is to upskill or retrain professionals who are already in cybersecurity roles. The level of learning and training will depend on their current level of expertise [30] or professional level based on the years of experience (basic, intermediate, advanced) [3]. Individuals at the basic level usually have less than 3 years of experience in a specific role, individuals at the intermediate level have 3-5 years of experience, while those considered at the advanced level have 6 or more years of experience. Given that cybersecurity is a domain where lifelong learning is critical, all three professional levels should pursue upskilling to stay up to date and be able to protect their organization from cyber threats. The level of learning and training will indicate the depth of knowledge that will be pursued by the individual.

4) *Learning style.* Individuals learn in different ways (visual, auditory, kinesthetic, reading/writing), and this aspect needs to be taken into consideration when recommending learning material. Different types of learning materials (e.g., video, podcasts, games, articles, blogs, etc.), can be utilized depending on the learners' preferred learning style(s).

5) *Availability.* Time to allocate to learning activities may vary depending on the learners' seniority and responsibilities. Some learners may prefer to pursue learning in a burst mode, while others may consider learning spanning across a longer timeframe.

6) *Learning plan duration.* There are individuals that perform well when they have short-term learning objectives. In this case, microlearning or pedagogies of microcredentials [32] should be pursued where learners cover small learning chunks. Once they achieve their learning objective they can move to their next objective. This approach also promotes the concept of micro-competencies where learners are expected to build specific competencies from a broader set of competencies included in a career role profile. On the other hand, there are learners that perform better when they have long-term learning objectives, in which case macro-learning can be pursued.

7) *Cybersecurity career role.* There are different career pathways in cybersecurity [5][6]. Each career role requires specific competencies that should be demonstrated by professionals that are interested in pursuing such a role. Specific knowledge, soft and domain-specific skills should be developed to support the responsibilities of a specific role. This means that different learning topics, learning activities and resources should be specified as part of a learning and training study plan to achieve the desired learning outcomes and build specific competencies.

8) *Lifelong learning and learning motivation.* The field of cybersecurity is multidisciplinary and ever-changing, hence lifelong learning is imperative. Cybersecurity requires professionals to be up to date with both the technological aspects (e.g., networking, Internet of Things (IoT), databases, software and hardware components), and the organizational and human aspects of security [15] [17] [18] (including

behavioral cybersecurity, security policies, risk governance, ethics, and legal dimensions, amongst others). Furthermore, it is not sufficient for cybersecurity professionals to be able to merely follow and maintain defensive cyber strategies and policies. Rather, a truly integrated cybersecurity workforce must be capable of designing, developing, and implementing such strategies [15]. This entails a long-term and lifelong learning endeavor. Therefore, cybersecurity professionals must be motivated to embrace the changes in the field and retrain to advance their skills sets.

Moreover, several studies have shown that participants' motivation and engagement in awareness-raising and training programs are of vital importance to increase behavioral changes [18] and the effectiveness of training [16] [25] [26] [27] [28]. Learning motivation and engagement can support learning persistence and help cultivate a pool of cybersecurity talent for addressing the critical workforce shortage [15] [16] which has been reported consistently in recent years [1] [2] [3] [4]. Nevertheless, current cybersecurity training appears to be inadequate or unable to change participants' behaviors, knowledge, and security attitudes, as it often lacks engagement or motivation of participants [16]. One approach which has attracted interest in both educational and professional contexts is to incorporate 'fun' into cybersecurity training programs [15]. This can be achieved with game-based learning (GBL) methods which aim to promote cybersecurity resilience through behavioral change [18] and skills development [16] [20]. Personalizing the learning has also proved to be an effective strategy for increasing engagement with cybersecurity training [16]. The advent of generative AI tools can be used for realizing such personalized learning strategies. Recently, the use of generative AI tools has emerged as a supplementary avenue for learning and training. In this paper we embrace the latter approach and explore how ChatGPT can empower cybersecurity professionals' lifelong learning through generating personalized learning and training study plans.

9) *Code of Ethics.* Cybersecurity professionals should operate within a legal context and be guided by ethical principles. This entails understanding the activities professionals could engage with, demonstrating the appropriate professional behavior, while realizing the ethical consequences of their actions on a personal, organizational, even on a national level.

## B. Cybersecurity career role selection

As previously mentioned, there are different skills frameworks that specify the competencies that need to be demonstrated under specific cybersecurity career roles. Examples of such frameworks are the ECSF [5] and NICE [6]. A learner can choose a career role based on his/her professional inspirations, personal interests, etc. For the purposes of this paper, we took into consideration the recent study performed in the context of the EU funded project REWIRE [33], that investigated the market needs and utilized ECSF to identify four career roles that are currently in demand: CISO (Chief Information Security Officer), Cyber Incident Responder, Cyber Threat Intelligence Specialist, and Penetration Tester. For our investigations, the career role of a cyber threat intelligence specialist is selected, assuming a learner that just starts in this role. Future work will extend the investigations to cover more career roles.

Once a career role is selected, appropriate context needs to be provided to the generative AI tool so that responses are given considering this context. For example, ECSF provides a summary of the key responsibilities of each role, its mission, the deliverables that professionals are expected to develop, alongside the main tasks, key skills and knowledge that need to be demonstrated.

### C. Cyber threat intelligence specialist role

As per the ECSF, a cyber threat intelligence specialist “manages cyber threat intelligence life cycle including cyber threat information collection, analysis and production of actionable intelligence and dissemination to security stakeholders and the CTI community, at a tactical, operational and strategic level. Identifies and monitors the Tactics, Techniques and Procedures (TTPs) used by cyber threat actors and their trends, track threat actors’ activities and observe how non-cyber events can influence cyber-related actions.”. Based on the mission of this role, ECSF elaborates on the main tasks undertaken and the key skills that a professional should develop. An education and training study plan should take into consideration the mission, main tasks and key skills listed in ECSF to identify appropriate learning topics and resources to include in the study plan. Moreover, appropriate certifications could be considered to inform the development of a personalized training study plan. For example, entry-level certifications syllabus such as EC-Council Certified Threat Intelligence Analyst (CTIA) and CREST Practitioner Threat Intelligence Analyst (CPTIA), consider the threat intelligence lifecycle and elaborate relevant learning topics under the key functional areas [13]: planning and direction, collection, processing and exploitation, analysis and production, dissemination, and integration. Overall, developing a personalized training study plan could be a challenging task to achieve, especially for professionals just starting into this role without any prior experience.

## V. INVESTIGATIONS AND ANALYSIS OF GENERATIVE AI RESPONSES

This section presents the exploration and evaluation performed to investigate the potential of a generative AI tool (ChatGPT) to assist learners in the development of a personalised cybersecurity education and training study plan.

Initially, this work considered the ECSF profile and the skills listed in the cyber threat intelligence specialist role. Overall, ChatGPT responses with regards to suggested learning topics were evaluated considering the ECSF profile, the CTIA and CPTIA certifications’ syllabus, to conclude whether the learning topics are appropriate to inform a personalized training study plan.

The learning and training aspects discussed earlier informed the development of the prompts that were utilized in ChatGPT and supported the objective of this work. In the following paragraphs ChatGPT responses are critically analysed, evaluated, and discussed in relation to seven thematic areas: (a) appropriateness of learning topics, (b) soft skills development, (c) manageable learning content sections, (d) level of provided details, (e) diversity and credibility of proposed learning resources, (f) realistic task completion time, and (g) providing professional development advice.

### A. Appropriateness of learning topics

Cyber threat intelligence is a field that requires knowledge and skills across the threat intelligence lifecycle. An early

career professional entering this field is first expected to develop fundamental knowledge and skills. In addition to learning ‘on the job’, it is essential to follow a targeted learning study plan and progressively develop competencies covering more advanced topics in cyber threat intelligence. During this progression path, it is imperative for suggested learning materials to be appropriate for the chosen role and fit the competencies and level of expertise that is pursued by a learner. To investigate this aspect, we utilized a top to bottom approach, starting with high level prompts and elaborating them accordingly based on the tool’s responses.

Initially, the tool was instructed (prompt #1) to “*propose a training study plan to build the following skills as part of my role as cyber threat intelligence specialist:*”

- *Collaborate with other team members and colleagues*
- *Collect, analyse and correlate cyber threat information originating from multiple sources*
- *Identify threat actors TTPs and campaigns*
- *Automate threat intelligence management procedures*
- *Conduct technical analysis and reporting*
- *Identify non-cyber events with implications on cyber-related activities*
- *Model threats, actors and TTPs*
- *Communicate, coordinate and cooperate with internal and external stakeholders*
- *Communicate, present and report to relevant stakeholders*
- *Use and apply CTI platforms and tools”*

The tool considered competencies of varying levels, and this is demonstrated by the provided training study plan that listed guidelines under eight categories: basic training, specialized training, hands-on experience, continuous learning, soft skills development, certification, mentoring and collaboration, model threats and actors. The guidelines provided under each category addressed topics in a broad manner. For example, as part of specialized training, the tool suggested to “*enroll in courses like the SANS Institute’s FOR578: Cyber Threat Intelligence or similar programs to learn about collecting, analyzing, and correlating threat information from various sources*”. The subsequent prompts aimed to investigate if the tool can provide deeper information to guide the learner to inform his/her study plan. Specifically, prompt #2 instructed the tool to “*create a monthly study plan to learn threat intelligence fundamentals*”. This prompt resulted into a list of weekly learning topics considering the cyber threat intelligence lifecycle (Week 1: Understanding Threat Intelligence Basics; Week 2: Intelligence Lifecycle and Data Collection; Week 3: Threat Analysis and Correlation; Week 4: Threat Intelligence Platforms and Reporting) and touching upon some basic concepts that should be covered in each case. For example, under week 3, the tool suggested covering threat analysis techniques and correlating threat data. Prompt #4 instructed ChatGPT to provide a three-month training study plan, giving space to the tool to expand on the topics and guide the learners further on the learning topics that could be covered. For example, under month 2 “Threat analysis and correlation” (in prompt #2 this was listed as week 3), the tool suggested two extra learning topics, indicator-based analysis, and behavioral analysis. Prompt #5 investigated the case where the learner has some experience in the role and would like to advance this experience. The tool provided a study plan with topics that delve into more advanced aspects. For example, month 1 covered advanced threat intelligence analysis topics: Threat Actor Attribution, Threat Actor TTPs

(Tactics, Techniques, and Procedures), Advanced Threat Analysis Techniques, Threat Hunting and Advanced Detection Methods. A variety of other prompts were also developed to instruct the tool to suggest education and training online resources. This aspect is analysed in detail in a subsequent dedicated section. Overall, it is notable to comment that the tool provided a variety of resources, promoting a superior learning experience that could effectively engage the learners with the learning process. Furthermore, ChatGPT suggested learning topics that are covered in industry accepted resources such as the ECSF, CTIA and CPTIA certifications (the suggested topics were listed at least in one of these resources). Another prompt was built to investigate whether the tool can suggest real-world examples under the topic of Threat Actor TTPs (prompt #9 – “*propose a real case study*”). ChatGPT elaborated on a real case of an Advanced Persistent Threat group (APT29, called Cozy Bear), analyzing the key TTPs that the group is observed to be utilizing. Moreover, the tool advised that one should “*use this case study to analyze their tactics, gather additional information, and practice identifying patterns and trends in threat actor behavior*”. Overall, the learning topics proposed by ChatGPT were appropriate for the selected cybersecurity role and the level of experience pursued. This means that learners can utilize the proposed learning topics with confidence to inform and expand their training study plan.

#### B. Soft skills development

Soft (or transferable) skills, such as communication, teamwork, analytical thinking, and problem solving, are recognised as essential competencies to be demonstrated by cybersecurity professionals. In the cybersecurity industry soft skills are as important as domain-specific skills [3]. However, in terms of training resources, the focus is placed more on developing domain-specific skills. This is demonstrated by the syllabi of various cybersecurity certifications. Although soft skills can be cultivated through the development of domain-specific skills, the fact that this aspect is not strongly highlighted, it can prohibit learners from seeking learning resources to develop specific soft skills. ChatGPT seems to be a valuable assistant in terms of guiding learners to develop soft skills. Investigations focused on asking the tool to elaborate and provide guidance on one of the soft skills listed under the ECSF Cyber Threat Intelligence specialist profile, that is to “Communicate, coordinate and cooperate with internal and external stakeholders” (prompt #10 – “*provide a plan for one month to build soft skills related to Communicate, coordinate and cooperate with internal and external stakeholders*”). ChatGPT response elaborated on valuable aspects that are not usually covered in cybersecurity training and certification programs. For example, the following learning topics and activities were proposed:

- **Effective communication.** The tool provided directions towards building skills and demonstrating active listening, conveying complex technical information in a clear and concise manner, and showing confidence and empathy through nonverbal communication.
- **Interpersonal skills.** ChatGPT highlighted the importance of conflict resolution, networking and building rapport skills and trust with stakeholders.
- **Coordination and cooperation.** The skillset that was suggested by ChatGPT under this topic included

fundamental principles such as teamwork, understanding the dynamics of working with different teams within the organization, apply strategies to engage external stakeholders such as government agencies, industry partners, or law enforcement.

- **Presentation and reporting skills.** Suggestions included studying techniques to deliver impactful presentations, developing report-writing skills while focusing on clarity and professionalism, and providing feedback to stakeholders regarding an incident.

#### C. Manageable learning content sections

Creating a structured learning environment could foster an engaging and effective learning experience. Such a structured learning environment could be established through the provision of manageable learning content that can benefit learners by helping them set realistic learning goals, effectively acquire knowledge, and develop their skills. This approach can prove extremely beneficial in complicated domains like cyber threat intelligence. Organising the material into digestible learning chunks can present various benefits to learners. First, it encourages a methodical and structured approach for learning, avoiding cognitive overload and guaranteeing a distinct course for advancement. Learners can concentrate on learning a specific subject and developing relevant skills before moving on to more complex concepts. Moreover, having manageable sections could help learners organize their time more effectively, enabling them to allocate certain periods of time for studying. Having dedicated study times can contribute towards a sustainable learning routine, which is appropriate for professionals with strong cybersecurity capabilities. By decomposing the learning material, learners could also monitor their progress and adjust their learning accordingly to achieve their learning goals. ChatGPT demonstrated the capacity to create a structured and manageable training study plan.

When the tool was prompted to “*create a monthly study plan to learn threat intelligence fundamentals*” (prompt #2), the suggested plan was broken down into four weekly topics, each subdivided into two study subjects and allocated study time as “days 1-3” and “days 4-7” respectively. As discussed in section “A. Appropriateness of learning topics”, each week was dedicated to a specific aspect of the cyber threat intelligence lifecycle. The tool suggested topics, starting from fundamental concepts and then moving to more advanced topics. This approach decomposed the complexity of threat intelligence which could assist the learners to build a foundation and progressively develop their knowledge and skills.

The tool was also instructed “*for week 2 create a more detailed study plan for 5 days to study 2 hours per day*” (prompt #8) to further investigate ChatGPT’s ability to suggest manageable study sections. The topic suggested in week 2 focused on “Threat Actor TTPs (Tactics, Techniques, and Procedures)”. The suggested study plan included a reasonable breakdown of topics and activities: day 1 - Understanding Threat Actor TTPs, day 2 - Advanced Threat Actor TTP Analysis, day 3 - Identifying TTP Patterns, day 4 - TTP Simulation and Hands-On Practice, day 5 Threat Actor TTP Research and Presentation. The hourly subdivision of topics could also be helpful to learners, guiding them where to focus their learning. For example, for the first study hour in

day 1, the tool suggested reading articles explaining the concept of threat actors TTPs, focusing on understanding what TTPs are and why they are important in threat intelligence. For the second study hour, ChatGPT suggested reviewing a real-world example of a threat actor TTPs and analyze the incident to understand the TTPs utilized.

#### D. Level of provided details

The monthly and weekly plans, in addition to the recommended resources, offered sufficient details to help learners create a structured and effective learning study plan for threat intelligence. ChatGPT provided valuable guidelines, covering different aspects of an effective training study plan. Specifically, the tool provided details highlighting potential learning topics to include, where to find learning resources, what type of resources to search for, and specified relevant learning objectives. By providing a wealth of information, progressively structuring the learning material from fundamental to advance concepts and providing a balanced mix of theory and practical application, various level of expertise can be catered. This approach is valuable and can benefit learners with varying expertise, who can investigate further aspects that are of interest and create their personal study plan based on the depth of knowledge they wish to acquire.

#### E. Diversity and credibility of proposed learning resources

Identifying learning resources is an essential task when developing a training study plan to build specific cybersecurity competencies. These learning resources should be considered reputable and widely recognized by the cybersecurity community, leading to high quality and credible learning in the field. Moreover, identifying diverse learning resources can enhance learners' experience, engage them with the learning material, and lead to better learning outcomes. ChatGPT suggestions included a variety of diverse and credible resources where learners could obtain more information, read articles and blogs, listen to podcasts, view videos, participate in communities, practice with specific tools, etc. Table I presents the diverse list of learning resources and relevant examples as suggested by the tool. The suggested resources (reference prompts #3,#6,#7 from Table I) are widely recognized in the field of cybersecurity as they have established credibility based on factors such as authors' expertise, national authorities' endorsement, track record of accurate reporting, contributions to the industry, affiliations with respected cybersecurity organizations, etc. Given that people learn in different ways, the tool was prompted to "suggest resources for a visual learner" (prompt #12) to investigate its ability to provide tailored content based on the learners' preferences. The tool suggested a broad list of potential visual-based learning resources, e.g., video tutorials, infographics, diagrams, webinars, interactive cyber labs, cheat sheets, documentaries, etc. Prompt #13 instructed the tool to "propose an online community that shares visual resources", suggesting some of the popular and well-established venues where someone can find visual resources related to cybersecurity and threat intelligence, e.g., Reddit, Cybrary forums, etc.

Notable to report is the observation that when the tool was prompted to "Suggest three LinkedIn groups to stay up to date" (Table I, Prompt #11), it supplied unreliable information. The suggested groups (Threat Intelligence and Cybersecurity Group, Cybersecurity & Information Security Community, Information Security and Threat Intelligence)

were examined, and we found out that they were invalid, irrelevant or did not exist. Overall, the generated responses provided credible suggestions regarding learning resources, however, it seems that information regarding social media groups shall not be trusted and should be considered with a critical eye.

TABLE I. CHATGPT PROMPTS RELATED TO LEARNING RESOURCES

ChatGPT prompts	Examples provided by the tool
Prompt #3: Can you provide some links to study introduction to threat intelligence	SANS Reading Room ( <a href="https://www.sans.org/reading-room/">https://www.sans.org/reading-room/</a> ), Recorded Future Blog ( <a href="https://www.recordedfuture.com/blog/">https://www.recordedfuture.com/blog/</a> ), CISA Cybersecurity Resources ( <a href="https://www.cisa.gov/cybersecurity-resources">https://www.cisa.gov/cybersecurity-resources</a> ), KrebsOnSecurity Blog ( <a href="https://krebsonsecurity.com/">https://krebsonsecurity.com/</a> ), youtube, LinkedIn Learning (formerly Lynda.com), Coursera and edX
Prompt #6: What kind of resources should I look for month 1	Research papers and case studies, real-world examples, online courses, webinars, forums, communities, specialized courses, training programs, In-depth threat intelligence reports and articles, Online platforms and sandboxes, Advanced cybersecurity courses, books, Capture the Flag (CTF) competitions, tools, documentation, guides, practical exercises, conferences, webinars, YARA, Sigma, and Elasticsearch
Prompt #7: Propose blogs on threat intelligence	Recorded Future Blog ( <a href="https://www.recordedfuture.com/blog/">https://www.recordedfuture.com/blog/</a> ), SANS ISC Diary ( <a href="https://isc.sans.edu/">https://isc.sans.edu/</a> ), Threatpost ( <a href="https://threatpost.com/">https://threatpost.com/</a> ), FireEye Threat Research Blog <a href="https://www.fireeye.com/blog/threat-research.html">https://www.fireeye.com/blog/threat-research.html</a> , Trend Micro Blog <a href="https://www.trendmicro.com/vinfo/us/security/news">https://www.trendmicro.com/vinfo/us/security/news</a> , Kaspersky Threat Intelligence Blog <a href="https://www.kaspersky.com/blog/">https://www.kaspersky.com/blog/</a> , CrowdStrike Blog <a href="https://www.crowdstrike.com/blog/">https://www.crowdstrike.com/blog/</a> , DarkReading Threat Intelligence Section ( <a href="https://www.darkreading.com/threat-intelligence.asp">https://www.darkreading.com/threat-intelligence.asp</a> ), AlienVault OTX Blog ( <a href="https://www.alienvault.com/blogs/open-threat-exchange">https://www.alienvault.com/blogs/open-threat-exchange</a> )
Prompt #11: Suggest 3 linkedin groups to stay up to date	Threat Intelligence and Cybersecurity Group <a href="https://www.linkedin.com/groups/1866005/">https://www.linkedin.com/groups/1866005/</a> , Cybersecurity & Information Security Community <a href="https://www.linkedin.com/groups/3377232/">https://www.linkedin.com/groups/3377232/</a> , Information Security and Threat Intelligence <a href="https://www.linkedin.com/groups/8432872/">https://www.linkedin.com/groups/8432872/</a>
Prompt #12: Suggest resources for a visual learner	Video Tutorials and Courses, Infographics and Diagrams, Webinars and Virtual Workshops, Cybersecurity Conferences, online labs and simulators, Mind Maps and Visual Note-Taking, online forums and communities, Interactive Threat Intelligence Platforms, visual documentation and cheat sheets
Prompt #13: Propose an online community that shares visual resources	<a href="https://www.reddit.com/r/cybersecurity/">https://www.reddit.com/r/cybersecurity/</a> , "KrebsOnSecurity" and "Recorded Future's" blog <a href="https://www.cybrary.it/forums">https://www.cybrary.it/forums</a>

Given that the credibility of resources may change over time, learners should stay informed about the latest developments in cybersecurity to be able to verify the accuracy and reliability of the obtained information. This is an aspect that is highlighted by ChatGPT itself, which provides a good ground for staying vigilant and informed (ChatGPT response: "Keep in mind that the threat landscape is constantly changing, so staying up-to-date with these sources is crucial for a threat intelligence specialist").

#### F. Realistic task completion time

Developing a realistic training study plan means allocating enough study time to cover the material and complete the learning activities. Various factors can impact the actual study time needed to achieve the desired learning objectives; some key factors include the complexity of the learning material, the learners' prior experience and the depth of learning pursued. For example, the time to complete practical exercises could vary depending on the learners' familiarity with the cybersecurity tools. Having the above in mind, the completion time of the tasks proposed by ChatGPT seems moderately realistic. If we consider the case of a learner with no prior experience in threat intelligence, there are topics that can be covered in a reasonable amount of time. For example, when providing a monthly study plan (prompt #2), the tool allocates three days in week 2 to read about the intelligence lifecycle and understand the process which includes stages like collection, analysis, dissemination, and feedback. It then suggests allocating 4 days to explore materials (such as videos and blogs) about different data collection methods, e.g., OSINT, HUMINT, etc. The tool did not indicate the number of hours allocated per day but allocating approximately 2 hours of study per day seems reasonable and sufficient time to cover fundamental aspects. However, in terms of more advanced topics, additional time would be needed to acquire the necessary knowledge and build the relevant skills. For example, in week 4 the learners are guided to allocate three days researching and comparing threat intelligence platforms such as ThreatConnect, MISP, and Anomali. This task would probably require more than two hours per day to be completed, especially if we consider that the learner would need to utilize these platforms to critically compare their functionality. ChatGPT's deficiency to allocate appropriate study time to practical tasks compared to tasks covering theoretical concepts (e.g. reading, watching a video, etc.) become more evident with prompt #8 that prompted the tool to create a five-day plan considering two hours study time per day. Specifically, the tool assumed one hour to practice using threat intelligence platforms or sandboxes, simulating and analyzing TTPs. This timeframe can be considered insufficient for a learner that has no prior experience.

To some extent, it should be expected that generative AI tools could indicate a study timeframe but cannot entirely predict the study time needed to build skills on specific learning concepts. This is due to the various factors discussed earlier and concern each individual learner. ChatGPT recognized that aspect and provided appropriate guidelines highlighting the need to build some flexibility in a study plan (ChatGPT response: "*Be sure to adjust the pace based on your personal learning style and the depth of knowledge you wish to acquire*").

#### G. Providing professional development advice

Professional development and progression in cybersecurity is a challenging task. There are many aspects to be considered which are not always evident to a novice entering this domain. Although there is a lot of information about cybersecurity careers and cybersecurity education, the scarcity of resources hinders their visibility and may overwhelm or disorient learners regarding where to start and how to progress through their learning journey.

The overall career advice generated by ChatGPT, appears to be effective in terms of guiding learners where to place their efforts in terms of their professional development such as how

to build their network (ChatGPT response: "*...joining cybersecurity communities and forums to network*", "*...subreddits, or LinkedIn groups*", "*...seek mentorship*", "*Building a strong professional network can provide valuable insights and opportunities for collaboration*"), what kind of learning topics and resources to search for (ChatGPT response: "*When exploring these resources, look for articles and materials that cover topics like Introduction to Threat Intelligence and Understanding the Intelligence Cycle.*", "*Remember to combine visual resources with practical exercises ... to reinforce your learning*"), how to build practical skills (ChatGPT response: "*...build a personal threat intelligence lab*"), and what certifications are relevant (ChatGPT response: "*The CTIA certification is a solid starting point for those looking to enter the field of threat intel and gain a foundational understanding of the discipline*").

Also, in most of its answers, the tool provides advice focusing on the need for and importance of lifelong learning. ChatGPT's advice with regards to this aspect is an essential reminder and re-enforcement of continuous learning; cybersecurity is a dynamic and constantly evolving domain that requires keeping up with all modern technologies and the dynamics of the threat landscape (ChatGPT responses: "*Remember that cybersecurity is a constantly evolving field, so ongoing learning and adaptation are essential*", "*Keep up with the latest industry trends and adapt your training study plan as needed to stay at the forefront of cyber threat intelligence*"). The tool also highlights a significant element of effective lifelong learning that involves the personal reflection that learners should demonstrate in terms of their development versus their learning objectives (ChatGPT response: "*Reflect on your progress and continue practicing and refining these soft skills over time*"). Another factor for effective lifelong learning is the necessity to seek for the most up-to-date resources which is recognized by the tool, providing relevant advice (ChatGPT response: "*These blogs and websites offer a wealth of information and insights into the ever-evolving field of threat intelligence. Keep in mind that the threat landscape is constantly changing, so staying up-to-date with these sources is crucial for a threat intelligence specialist*"). Overall, the AI generated responses highlight the necessity for continuous learning on this subject in the context of creating personalized learning study plans.

Another noteworthy observation was the response generated for the prompt #15 "*What are the ethical issues that a threat intelligence professional should be aware of*". The AI-generated response included a comprehensive list of various ethical issues that must be considered by a cyber threat intelligence professional, including data privacy and protection, dissemination of sensitive information, attribution accuracy, neutrality and non-discrimination, and ethical reporting and disclosure. Each point was well-justified, discussing the reasons why it is essential to be considered. These ethical principles might not be evident for individuals in early career stages in the threat intelligence domain. Therefore, it is important that the tool highlighted that professionals working in threat intelligence must be guided by ethical principles to demonstrate responsible and professional behavior (ChatGPT response: "*Threat intelligence professionals should be guided by ethical principles and exercise good judgment in their work. Ethical conduct is essential for maintaining trust, credibility, and the responsible use of threat intelligence data and tools*").



## VI. DISCUSSION

This work deployed an exploratory research methodology to investigate if generative AI could be utilized to assist developing professionals working in cybersecurity building their training study plan by providing tailored learning resources and activities based on learners' career goals. ChatGPT 3.5 was utilized to facilitate the investigations and provide insights regarding the capabilities of a generative AI tool to advise on training study plan development, considering developing competencies relevant to a cybersecurity role. Overall, fifteen prompts have been developed to investigate ChatGPT's capabilities to suggest learning topics and relevant resources to include in a study plan. Based on the prompts, the tool suggested a structured monthly plan broken down into digestible weekly subjects to develop fundamental skills and knowledge related to ECSF cyber threat intelligence specialist role profile. Every weekly topic was carefully crafted to address different aspects of threat intelligence, progressively moving from basic to more advanced topics, enabling learners to manage their learning and thoroughly explore key concepts. The recommended learning resources provided a well-rounded approach to learning, considering a variety of learning styles. The tool incorporated resources such as practical case studies, visual-based resources, interactive laboratories, webinars, forums, blogs, etc., accommodating diverse learning styles and fostering a superior learning experience. The learning process was further enhanced by expanding on soft skills development and ethical considerations. The comprehensive study plan and resources offered a well-balanced blend of theory and practical application. The balanced approach alongside the valuable professional development advice offered by the tool provided a flexible learning environment for the learners to personalize their study plan according to their current knowledge, skillset, and career aspirations. Moreover, the proposed learning subjects were aligned with resources utilized in the industry, demonstrating the appropriateness of the suggested content. The degree of specificity provided by the tool was appropriate to provide guidelines to the learners to inform their study plan and further investigate areas of interest. Caution should be placed to confirm the credibility of proposed online resources as it was found that the suggested LinkedIn resources were not valid, they were either fabricated or inaccurate. This is an aspect already identified as a shortcoming of generative AI tools. Therefore, learners should be educated about the capabilities and deficiencies of generative AI tools, critically reflecting upon the responses received and utilizing them accordingly so they would use content that have verified as being credible. Another aspect that is notable to highlight when utilizing a generative AI tool to inform a training study plan, is that task completion time can vary depending on factors such as learners' expertise, prior familiarity with suggested tools, and the complexity of the suggested learning activities. Overall, ChatGPT demonstrated that it can suggest learning activities within a reasonable completion timeframe. It seems that suggested learning activities that concern activities such as reading articles, watching videos, etc., can be completed within the provided timeframes, while more practical tasks and hands-on activities would probably require more time to complete than the suggested, depending on the aforementioned factors. This should be considered by learners so they could allocate realistic task completion to activities they include in their training study plan.

The investigations performed in this work confirmed that generative AI tools could be very useful at the hands of cybersecurity professionals. Especially in the case of newcomers, these tools can assist learners develop a training study plan in cybersecurity, organize their study time, promote focused learning and effective competencies development.

## VII. CONCLUSIONS

In an era where the cybersecurity community is focusing its efforts to attract more talented people to work in cybersecurity and bridge the skills gap, it is crucial to identify ways to accelerate skills development. Although there is a wealth of information related to cybersecurity professional development, this is not adequate. The scarcity and variety of resources may be overwhelming, and learners may struggle to structure the available content in a way that can benefit them and help them develop their competencies. This challenge becomes greater when entering a new cybersecurity role which requires building fundamental knowledge and skills and advancing progressively into the role. Without prior experience, newcomers would need to invest a lot of time researching and trying to navigate the complexity of the cybersecurity domain to identify where to start and what to include in a tailored training study plan to build specific competencies relevant to a career role. This may lead to lack of engagement or motivation [16].

AI tools showcased their potential in different areas of cybersecurity [31][35][36][37]. Nevertheless, their role in creating training study plans to develop competencies relevant to a cybersecurity role has not been actively investigated to date. This work demonstrated the potential of generative AI tools in the context of cybersecurity competencies development using ChatGPT as a case study. Generative AI tools can empower the workforce to direct their learning according to a job role of interest, create a personalised study plan based on their long-term career goals, and methodologically progress their cybersecurity competencies development informed by the tools' responses.

The exploratory research performed in this paper demonstrated the potential of generative AI tools to act as advisors to learners to aid their learning and development. Several observations endorse this potential such as the ability of generative AI tools to: suggest key learning topics relevant to the tasks and competencies of a cybersecurity role, break down the study plan in manageable sections, provide credible resources to search for learning material, cater for different learning needs by suggesting different types of learning resources, promote responsible professional behavior by providing guidance considering ethical principles, offer advice to learners with regards to their professional development, and motivate the learners to invest in lifelong learning in cybersecurity.

Explorations also provided valuable insights regarding the aspects that were not handled sufficiently by the tool. Although the suggested learning material was broken down into manageable sections, some of the tasks would probably need more time for a learner to complete them. Of course, this is an aspect that is affected by different factors such as the familiarity of the learners with the overall topic, their expertise and learning pace, and should be further investigated. This research was performed in the context of a specific cybersecurity role to study whether there is potential to use generative AI tools to assist in the development of a training

study plan. The full potential of generative AI tools should be further investigated and validated by performing extensive explorations across different cybersecurity roles and relevant competencies. Future work will expand upon the investigations, designing an appropriate generative AI prompt-powered framework that could be utilized by learners to create a personalized training study plan in cybersecurity, considering a variety of learning and training aspects identified by the current investigations.

#### ACKNOWLEDGMENT

This paper has received funding from the Digital Europe Programme under grant agreement project no. 101128049. The work reflects only the authors' view, and the Agency is not responsible for any use that may be made of the information it contains.

#### REFERENCES

- [1] "Cybersecurity workforce study 2023," *ISC<sup>2</sup>*. [Online]. Available: <https://www.isc2.org/research>.
- [2] "State of Cybersecurity 2023," *ISACA*. [Online]. Available: <https://www.isaca.org/resources/reports/state-of-cybersecurity-2023>.
- [3] S. Coutinho et al., Cyber security skills in the UK labour market 2023. Ipsos & Department for Science, Innovation and Technology (DSIT). 2023. [Online]. Available: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1173325/Cyber\\_security\\_skills\\_in\\_the\\_UK\\_labour\\_market\\_2023.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1173325/Cyber_security_skills_in_the_UK_labour_market_2023.pdf).
- [4] Chartered Institute of Information Security - The Security Profession 2022/23. [Online]. Available: [https://mcusercontent.com/2b790e748aed4c8b80df0d9f6/files/4f7f3305-250c-628a-eba8-1b73fedf05ec/SOTP\\_SURVEY\\_V1.pdf](https://mcusercontent.com/2b790e748aed4c8b80df0d9f6/files/4f7f3305-250c-628a-eba8-1b73fedf05ec/SOTP_SURVEY_V1.pdf).
- [5] "European cybersecurity skills framework (ECSF)," *ENISA*, 2018. [Online]. Available: <https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework>.
- [6] R. Petersen, D. Santos, M. C. Smith, K. A. Wetzel, and G. Witte, "Workforce Framework for cybersecurity (NICE Framework SP 800-181 rev1)," National Institute of Standards and Technology (NIST), 2020.
- [7] 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.
- [8] S. Furnell, "The cybersecurity workforce and skills," *Computers & Security*, vol. 100, no. 102080, p. 102080, 2021. <https://doi.org/10.1016/j.cose.2020.102080>.
- [9] B. Payne, L. Mayes, T. Paredes, E. Smith, H. Wu, and C. Xin, "Applying High Impact Practices in an Interdisciplinary Cybersecurity Program," in *Journal of Cybersecurity Education, Research and Practice*, Kennesaw State University Institute for cybersecurity workforce development, 2020.
- [10] J. Pinchot, D. Cellante, S. Mishra, and K. Pullet, "Student Perceptions of Challenges and Role of Mentorship in Cybersecurity Careers: Addressing the Gender Gap," *Information Systems Education Journal*, 2020.
- [11] "Microsoft Digital Defense Report 2023," *Microsoft*. 2023. [Online]. Available: <https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023>.
- [12] F. Fui-Hoon Nah, R. Zheng, J. Cai, K. Siau, and L. Chen, "Generative AI and ChatGPT: Applications, challenges, and AI-human collaboration," *Journal of Information Technology Case and Application Research*, vol. 25, no. 3, pp. 277–304, 2023. <https://doi.org/10.1080/15228053.2023.2233814>.
- [13] "Exploring the opportunities and limitations of current Threat Intelligence Platforms," *ENISA*, 2018. [Online]. Available: <https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms>.
- [14] D. Tang, C. Pham, K.-I. Chinen, and R. Beuran, "Interactive cybersecurity defense training inspired by web-based learning theory," in *2017 IEEE 9th International Conference on Engineering Education (ICEED)*, pp. 90–95, 2017.
- [15] 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.
- [16] N. Chowdhury and V. Gkioulos, "A personalized learning theory-based cyber-security training exercise," *International Journal of Information Security*, vol. 22, no. 6, pp. 1531–1546, 2023.
- [17] L. González-Manzano, "Design recommendations for online cybersecurity courses Comput," *Computers & Security*, 2019.
- [18] R. A. Maalem Lahcen, B. Caulkins, R. Mohapatra, and M. Kumar, "Review and insight on the behavioral aspects of cybersecurity," *Cybersecurity*, vol. 3, no. 1, 2020.
- [19] "The future of Jobs Report 2023," *World Economic Forum (WEF)*, 30-Apr 2023. [Online]. Available: <https://www.weforum.org/reports/the-future-of-jobs-report-2023/>.
- [20] A. Piki, E. Stavrou, A. Procopiou, and A. Demosthenous, "Fostering Cybersecurity Awareness and Skills Development Through Digital Game-Based Learning," in *10th IEEE International Conference on Behavioural and Social Computing (BESC 2023)*, Lamaca, Cyprus, 2023.
- [21] Y. Karagiorgi and L. Symeou, "Translating constructivism into instructional design: Potential and limitations," *Journal of Educational Technology & Society*, vol. 8, no. 1, pp. 17–27, 2005.
- [22] M. G. Moore, "Editorial: Three types of interaction," *American Journal of Distance Education*, vol. 3, no. 2, pp. 1–7, 1989.
- [23] D. C. A. Hillman, D. J. Willis, and C. N. Gunawardena, "Learner - interface interaction in distance education: An extension of contemporary models and strategies for practitioners," *Am. J. Distance Educ.*, vol. 8, no. 2, pp. 30–42, 1994.
- [24] T. C. Reeves, J. Herrington and R. Oliver, "Authentic activities and online learning", *Quality conversations: Research and development in higher education*, vol. 25, pp. 562–567, 2004.
- [25] R. Beuran, "Integrated framework for hands-on cybersecurity training: cyTrONE, Comput," *Comput. Secur.*, 2018.
- [26] M. Bada, A. M. Sasse, and J. R. C. Nurse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?," *arXiv*, 2019.
- [27] A. Gross, "Effective security training requires change in employee behavior." *Health IT Answers*, 2018.
- [28] D. Kostadinov, "The components of a successful security awareness program." *InfoSec Institute*, 2018.
- [29] D. Hulatt and E. Stavrou, "The Development of a Multidisciplinary Cybersecurity Workforce: An Investigation", *Human Aspects of Information Security and Assurance. Proceedings 15th IFIP WG 11.12 International Symposium, HAISA 2021, Virtual Event*, vol. 15, July 7–9, 2021.
- [30] E. Stavrou and I. Polycapou, "Cybersecurity-related curriculum for diverse postgraduate cohorts: A case study," *18th International Conference on Education and Information Systems, Technologies and Applications (EISTA 2020)*, 2020.
- [31] "Artificial Intelligence and Cybersecurity Research", *ENISA*, 2023. [Online]. Available: <https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research>.
- [32] Kukulska-Hulme, A., Bossu, C., Charitonos, K., Coughlan, T., Ferguson, R., FitzGerald, E., Gaved, M., Guitert, M., Herodotou, C., Maina, M. and Prieto-Blázquez, J., "Innovating pedagogy 2022: exploring new forms of teaching, learning and assessment, to guide educators and policy makers." *Open University Innovation Report 10*. Milton Keynes: The Open University, 2022.
- [33] REWIRE Vocational Open Online Courses. [Online]. Available: <https://vle.rewireproject.eu/>.
- [34] R. Swedberg, "Exploratory research. The production of knowledge: Enhancing progress in social science," pp. 17–41, 2020.
- [35] J.-H. Li, "Cyber security meets artificial intelligence: a survey," *Front. Inf. Technol. Electron. Eng.*, vol. 19, no. 12, pp. 1462–1474, 2018.
- [36] 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.
- [37] 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.