Article

GPTs or Grim Position Threats? The Potential Impacts of Large Language Models on Non-Managerial Jobs and Certifications in Cybersecurity

Raza Nowrozy *

Posted Date: 24 April 2024

doi: 10.20944/preprints202404.1600.v1

Keywords: cybersecurity; skills; ChatGPT; workforce; large language model; generative AI

 doi:10.20944/preprints202404.1600.v1

Article

GPTs or Grim Position Threats? The Potential Impacts of Large Language Models on Non-Managerial Jobs and Certifications in Cybersecurity

Raza Nowrozy

Untapped Talent; raza.nowrozy@untapped-talent.com; Tel.: +61408 408 031

Abstract: ChatGPT, a *Large Language Model* (LLM) utilizing *Natural Language Processing* (NLP), has caused concerns about its impact on job sectors, including cybersecurity. In this study, we assessed ChatGPT's impacts in non-managerial cybersecurity roles using the NICE Framework and Technological Displacement theory. We also explored its potential in passing top cybersecurity certification exams. Findings revealed ChatGPT's promise in streamlining some jobs, especially those requiring memorization. Moreover, we highlighted ChatGPT's challenges and limitations, such as ethical implications, LLM limitations, and *Artificial Intelligence* (AI) security. The study suggests that LLMs like ChatGPT could transform the cybersecurity landscape, causing job losses, skill obsolescence, labor market shifts, and mixed socioeconomic impacts. We recommend a shift in focus from memorization to critical thinking, and collaboration between LLM developers and cybersecurity professionals.

Keywords: cybersecurity; skills; ChatGPT; workforce; large language model; generative AI

1. Introduction

Chat Generative Pre-trained Transformer (ChatGPT) is a *Large Language Model* (LLM) trained by OpenAI™, based on the GPT-4 architecture[1]. It is designed to understand and generate human-like text in response to natural language inputs [1]. LLMs are a specific type of generative *Artificial Intelligence* (AI) that focus on natural language understanding and generation[1]. With its ability to process a wide range of topics and styles, LLMs like ChatGPT have been used in various applications, including chatbots [2], content creation [3], and language translation [1]. Its capabilities are continuously expanding, with new features and improvements being added regularly. Other competitors of OpenAI have released similar LLM products, such as Bard by Google™, LLaMA by Meta™, and Wenxin Yiyan by Baidu™. However, as with any AI system, ethical considerations and potential biases must be taken into account[4]. Despite these challenges, ChatGPT has the potential to revolutionize the way the world interact with machines and each other, opening up new possibilities for communication, creativity, and innovation [1].

The rise of generative AI, including ChatGPT, has also raised concerns about the potential impact on human jobs, including in the field of cybersecurity[5]. Some experts argued that these generative AI technologies have the potential to automate a wide range of cybersecurity tasks, from threat detection and incident response to vulnerability scanning and penetration testing [5,6]. This could lead to significant job displacement and require cybersecurity professionals to acquire new skills to remain employable in the rapidly evolving job market. On the other hand, proponents of generative AI argued that these technologies could enhance human productivity and enable cybersecurity professionals to focus on higher-level tasks such as policy development and risk management [7]. Additionally, the use of generative AI in cybersecurity could help to scale up cybersecurity defenses, particularly in smaller organizations with limited human resources [8]. As an industry that heavily relies on and actively pursues the latest technology, the cybersecurity industry has vested interest in exploring the

[1] At the time of this article, the free version of ChatGPT uses GPT-3.5 architecture, whereas the paid version uses GPT-4 architecture. All experiments in this study were conducted using the paid version.

 doi:10.20944/preprints202404.1600.v1

potential impact of generative AI, especially LLM, on itself. In the absence of such a study focusing on the cybersecurity industry, we have decided to conduct such a study, to provide some results for discussions by the industry.

The key contributions of this study are as follows:

- We broadened the scope of *exposure* to ChatGPT, as previously defined in [1], to encompass several non-managerial cybersecurity industry positions and certifications.
- We employed the NICE Framework to assess the primary tasks of four distinct non-managerial cybersecurity roles and to empirically evaluate their potential exposure to ChatGPT's capabilities, before applying the *technological displacement* theory to interpret the results, and to investigate the long-term impact of ChatGPT on cybersecurity. We also studied the potential utilization of ChatGPT to pass cybersecurity certificate examination.
- We identified the challenges and limitations obtained from our study and suggested a shift from emphasizing memorization to fostering critical thinking skills for the industry, education, and certification institutions that might be exposed by ChatGPT.

The rest of the article is organized as follows: 2 introduces the related works. Section 3 introduces the factors that has motivated this study. Section 4 describes how this research has been conducted. Section 5 presents the alignment of ChatGPT abilities against several non-managerial cybersecurity industry jobs and some top cybersecurity certifications. Section 6 discusses the major themes identified during the study, and its potential implications on cybersecurity jobs, certifications and the educational sector teaching cybersecurity. Section Section 7 concludes this paper.

2. Related Works

Although there are limited publications on ChatGPT, there are plenty of studies on the NICE framework, which serves as a key reference for defining cybersecurity roles, responsibilities, and required skillsets [9,10]. Numerous studies have highlighted the framework's effectiveness in various contexts, including academic curricula development [9,11–15], workforce training programs [10,16–18], and organizational cybersecurity role mapping [19,20]. Researchers have also noted the NICE framework's flexibility in adapting to the dynamic cybersecurity landscape, while emphasizing the importance of continuous updates and revisions to maintain its relevance [14,21,22]. Moreover, the literature demonstrates how the NICE framework facilitates collaboration between various stakeholders, such as educational institutions, government agencies, and private sector organizations, promoting a unified approach to addressing the ever-growing demand for skilled cybersecurity professionals [14,23–25]. Overall, the literature underscores the significance of the NICE framework as a critical tool for building and sustaining a robust cybersecurity workforce capable of tackling the diverse challenges in this rapidly evolving field.

3. Research Motivation

In this section, we present the background information that has motivated our research.

3.1. Media Coverage of ChatGPT

As a generative AI language model, ChatGPT has gained significant attention from various media outlets around the world [26]. Its advanced language processing capabilities and ability to engage in human-like conversations have been the subject of numerous news articles and features in print, online, and broadcast media[27]. The technology behind ChatGPT has been extensively covered in tech and science publications, while its potential applications in industries such as customer service and healthcare have also garnered interest from business and trade media[27]. Additionally, ChatGPT's performance in *Natural Language Processing* (NLP) competitions and its ability to generate realistic and coherent text has been highlighted in numerous academic and research publications[1,26,27]. Despite its occasional unreliability[28], ChatGPT can efficiently handle repetitive tasks such as customer service inquiries or data entry, freeing up humans to focus on more complex and creative tasks [1]. The

 doi:10.20944/preprints202404.1600.v1

extensive media coverage of ChatGPT reflects the growing interest in generative AI, and its potential impact on various aspects of society.

3.2. Public Opinions of Generative AI in Cybersecurity

Generative AI, including ChatGPT, has sparked a lot of interest and debate in the cybersecurity industry. On one hand, some believe that the technology can be used to enhance security measures by automating tasks such as threat detection and response, freeing up human analysts to focus on more complex and strategic tasks[2]. However, others express concerns about the potential for generative AI to be used maliciously, such as in the creation of deepfake videos or social engineering attacks[3]. It appears that the public opinion of generative AI in the cybersecurity industry is nuanced, reflecting both excitement about its potential benefits and concerns about its potential risks. It is worth investigating further into the possible impact of generative AI on the cybersecurity workforce, to provide evidence for more balanced discussions on this matter.

3.3. Automation in Cybersecurity

Automation technologies, such as *Machine Learning* (ML) and data mining, have been rapidly transforming the cybersecurity industry, offering organizations new ways to defend against a growing array of cyber threats, by streamlining routine security tasks, speeding up threat detection and response, and augmenting the capabilities of human security professionals [29]. For example, Microsoft Sentinel™ is a *Security Information and Event Management* (SIEM) and *Extended Detection and Response* (XDR) security solution configured with ML and threat playbooks, which can leverage AI to perform attack pattern recognition on common attack types and to recommend remediation actions[4]. Nevertheless, concerns have been raised about the potential risks and limitations of automation in cybersecurity, including the potential for automation to create new vulnerabilities or false positives, as well as the need to balance automation with human expertise and oversight [30]. Generative AI solutions such as ChatGPT have great potentials in improving the accuracy and reliability of automation in cybersecurity defense, by utilizing its NLP capabilities to understand and interpret vast amounts of data related to cyber threats, and in analyzing the patterns and behaviors of cyber attackers and identify potential vulnerabilities in the system [1,26]. Therefore, it would be worthwhile to investigate how generative AI can enhance automation in cybersecurity, and help to create more resilient and dependable methods of mitigating the escalating cyber threats.

4. Research Methods

In this section, we demonstrate how we evaluated the impact of ChatGPT on cybersecurity industry jobs and certifications, based on the *National Initiative for Cybersecurity Education* (NICE) Framework[5] by *National Institute of Standards and Technology* (NIST) [10,31].

4.1. The NICE Framework

NICE by NIST is a comprehensive guide that categorizes and describes cybersecurity work, aiming to improve the understanding of cybersecurity roles, responsibilities, and skill requirements, and to provide a common language for discussing cybersecurity work [10,31]. It is a structured approach widely used by organizations, educators and the cybersecurity workforce, to help them identify cybersecurity workforce needs and skill gaps, to develop consistent training and education programs, to create career paths and opportunities for cybersecurity professionals, and to improve

---

2 https://sekuro.io/blog/chatgpt-cybersecurity-benefits-and-risks/
3 https://www.businessinsider.com/how-to-detect-ai-generated-content-text-chatgpt-deepfake-videos-2023-3
4 https://www.microsoft.com/en-au/security/business/siem-and-xdr/microsoft-sentinel
5 https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

 doi:10.20944/preprints202404.1600.v1

recruitment, hiring, and retention efforts[31]. The main building blocks within NICE are the *Tasks, Knowledge and Skills* (TKS) statements, or can be expressed as:

$$Tasks = Knowledge \times Skills \tag{1}$$

According to [10,31], the application of NICE to cybersecurity jobs can be summarized into the following steps:

1. **Identify work roles and assess current workforce**: Review the NICE Framework to identify relevant work roles for an organization and map existing job titles and responsibilities to the framework.
2. **Evaluate job requirements and develop job descriptions**: Analyze the TKS and abilities associated with each work role to understand job requirements, and create comprehensive job descriptions accordingly.
3. **Align training, recruitment, and hiring**: Align training programs, recruitment and hiring strategies that target candidates with the required skills and knowledge.
4. **Monitor and adapt to the changes**: Regularly review the organization's use of the NICE Framework and update job roles, job descriptions, and training programs as needed to keep up with the evolving cybersecurity landscape.

This study is an empirical study, to focus on the second step by reviewing cybersecurity industry jobs, and the third step, by examining cybersecurity certifications.

4.2. Selection of Cybersecurity Industry Jobs

We decided to focus on some of the non-managerial jobs that are most in demand in the industry: *Governance, Risk, and Compliance* (GRC) consultants, *Security Operations Center* (SOC) Analysts, Network and Cloud Security Engineers, and Penetration Testers. We used LinkedIn (Australia) and Seek.com.au, the top websites used by Australians to perform job searches. For each role, we used the top 5 search results (sorted by relevance), extracted the commonality of their primary tasks that were not employer-specific, and ignored information that were not directly related to job tasks, knowledge or skills (*i.e.*, position locations, remuneration levels). Their brief job descriptions are listed as below:

- **GRC consultants** help organizations to manage risks and comply with regulations by developing and implementing security policies and procedures. They provide guidance on cybersecurity controls and work to ensure that an organization's operations are aligned with its security objectives.
- **SOC Analysts** monitor an organization's systems and networks for security incidents, analyze security logs, and respond to incidents as they occur. They use a variety of tools and techniques to detect and respond to security threats in real-time.
- **Network and Cloud Security Engineers** design and implement security solutions for an organization's systems and networks. They work to ensure that an organization's data and systems are secure by implementing security controls and monitoring for potential security threats.
- **Penetration Testers** simulate cyber attacks to identify vulnerabilities in an organization's systems and networks. They use various tools and techniques to identify potential vulnerabilities and provide recommendations for remediation.

4.3. Selection of Cybersecurity Certifications

We decided to focus on some of the most pursued cybersecurity certifications in the industry, based on their popularity in the Australian job market: *Certified Information Systems Security Professional* (CISSP) by $(ISC)^2$, *Certified Ethical Hacker* (CEH) by E-Council, *Certified Information Systems Auditor* (CISA) and *Certified Information Security Manager* (CISM) both by ISACA, and *Offensive Security Certified Professional* (OSCP) by Offensive Security. Their vendors, abbreviations, full names, minimum work experienced required, and popularity on LinkedIn (Australia) and Seek.com.au have been summarized in Table 1.

 doi:10.20944/preprints202404.1600.v1

Table 1. A list of cybersecurity certifications examined and their popularity in Australian job market in March 2023

Vendor	Abbr.	Full name	Min work experience	Popularity	
				LinkedIn	Seek
$(ISC)^2$	CISSP	Certified Information Systems Security Professional	5 years	9,282	1,133
ISACA	CISA	Certified Information Systems Auditor	5 years	1,359	696
EC-Council	CEH	Certified Ethical Hacker	2 years	445	320
ISACA	CISM	Certified Information Security Manager	5 years	308	511
Offensive Security	OSCP	Offensive Security Certified Professional	N/A	370	486

4.4. Defining Exposure to ChatGPT

In [1], *exposure* was defined as a metric that determined if accessing a ChatGPT or GPT-powered system would result in at least a 50% decrease in the time required for a human to accomplish a particular *Detailed Work Activities* (DWA) or task. [1] defined 3 levels of *exposure* to LLM:

- **No exposure (E0)** if using the LLM reduces the quality of work, or does not save time while maintaining quality of work.
- **Direct exposure (E1)** if the described LLM reduces DWA/task time by at least 50%.
- **LLM+ Exposed (E2)** if the LLM itself alone does not reduce task time by 50%, but additional software built on LLM can achieve this goal while maintaining quality of work, *e.g.*, using WebChatGPT, a ChatGPT plugin with Internet access to access latest information beyond 2021. To date, OpenAI has approved 3 categories of extensions for ChatGPT: web browsing, Python code interpreter, and semantic search.

In this study, we inherit and expand their definition of *exposure* for cybersecurity jobs, and redefined it in Table 2. We arbitrarily assign values to them: 0 for no exposure, 0.5 for LLM+ exposure, and 1 for direct exposure. For certifications, if copying and pasting the certification exam questions into the LLM can generate the correct answers to pass the exam, the certification is considered to have direct exposure to LLM. For a particular job task (t), the estimated exposure of the task is T. Each task can be mapped to several knowledge points (k) and skills (s).

If the exposure of the i^{th} knowledge point is k_i, the overall exposure of the body of knowledge, K is given by

$$K = \frac{1}{m}\sum_{i=1}^{m} k_i. \tag{2}$$

Using equation (2), we obtain human-specific knowledge,

$$K_h = \frac{1}{m_1}\sum_{i=1}^{m_1} k_i \tag{3}$$

where $m_1 \in 1, 2, 3, \ldots, N_1$.

Similarly, using equation (2), we obtain LLM-assisted knowledge,

$$K_{LLM} = \frac{1}{m_2}\sum_{i=1}^{m_2} k_i \tag{4}$$

where $m_2 \in 1, 2, 3, \ldots, N_2$.

If the exposure of the i^{th} skill is s_i, the overall exposure of skillset, S is given by

$$S = \frac{1}{n}\sum_{i=1}^{n} s_i \tag{5}$$

where $n \in 1, 2, 3, \ldots, M$.

 doi:10.20944/preprints202404.1600.v1

Table 2. Redefinition of exposure against job tasks and certifications

Exposure	Job task		Certifications
	Skill	Knowledge	
No exposure (0)	LLM does not reduce the time to perform the skill.	LLM does not help with knowledge presentation.	LLM cannot be used to pass the exam.
LLM+ exposure (0.5)	LLM combined with additional software can partially ($\gtrsim$ 50%) perform the skill.	LLM combined with additional software can partially ($\gtrsim$ 50%) present the knowledge.	LLM combined with additional software can be used to pass the exam.
Direct exposure (1)	LLM alone can partially ($\gtrsim$ 50%) perform the skill.	LLM alone can partially ($\gtrsim$ 50%) or fully present knowledge.	LLM alone can pass the exam.

Using equations (3), (4), and (5), the overall exposure of the task with $m_1 + m_2$ number of knowledge points and n number of skills can be expressed as:

$$T = KS = \left(\frac{1}{m_1} \sum_{i=1}^{m_1} k_i + \frac{1}{m_2} \sum_{i=1}^{m_2} k_i \right) \frac{1}{n} \sum_{i=1}^{n} s_i \tag{6}$$

where $K = K_h + K_{LLM}$.

4.5. Knowledge Optimization

Instead of focusing on a person's capacity to acquire and retain material with a large language model like ChatGPT, human-specific knowledge is used in tests to evaluate a person's genuine understanding and comprehension of a topic. This promotes critical thinking and problem-solving skills, which are necessary for the completion in various real-world situations. Moreover, discouraging LLM-assisted knowledge in exams contributes to upholding the fairness and integrity of the grading process.

We propose a solution to optimize human-specific knowledge and minimize LLM-assisted ability. A list of symbols used in the proposed model can be found in Table 3.

$$\max_{\psi \in X} \ (1 - \beta) K_h(\psi) - \beta K_{LLM}(\psi). \tag{7}$$

We ensure that both $K_h(\psi) > 0$ and $K_{LLM}(\psi) > 0, \forall t$, are positive for each exam, using the assessments $X = \psi_1, \psi_2, \ldots, \psi_\psi$ and weight factor, $\beta \in [0, 1]$.

Our objective is to develop assessments to maximize the utilization of human-specific knowledge, $K_h(\psi)$, while reducing the dependence on LLM-assisted information, $K_{LLM}(\psi)$.

Table 3. List of symbols used in the proposed model

Symbol	Description
T	Tasks
K	Number of knowledge points
S	Knowledge
K_h	Human specific knowledge
K_{LLM}	LLM assisted knowledge
N_1	Number of human-specific knowledge available, where $m_1 \in 1, 2, 3, \ldots, N_1$
N_2	Number of LLM-assisted knowledge available, where $m_2 \in 1, 2, 3, \ldots, N_2$
M	Number of skills available, where $n \in 1, 2, 3, \ldots, M$
β	Weight factor
ψ	Assessments, where $X = \psi_1, \psi_2, \ldots, \psi_\psi$

 doi:10.20944/preprints202404.1600.v1

4.6. The Technology Displacement Theory

The *Technological Displacement* theory refers to the idea that advancements in technology can sometimes lead to the replacement of human labor in specific job roles or industries [32–35]. In this study, we will interpret the results by examining the following aspects in the context of cybersecurity:

- **Job Loss**: We hope to explore the degree to which the introduction of ChatGPT could result in job losses within the cybersecurity field, with a focus on roles that may be more susceptible to this change.
- **Skill Obsolescence**: We aim to investigate the speed at which the skills of impacted professionals may become outdated, as well as the potential need for reskilling or upskilling.
- **Labor Market Shifts**: We attempt estimate the possible effects on the cybersecurity labor market, including changed demands for various cybersecurity skill sets, the emergence of new job roles, and shifts in employment sectors.
- **Socioeconomic Impact**: We will explore the wider socioeconomic ramifications of technological displacement in cybersecurity, such as its influence on productivity, wages, and income inequality.

By utilizing this theory as a framework, we aim to gain a deeper understanding of ChatGPT's potential to replace certain cybersecurity jobs and place our empirical findings within the larger conversation surrounding technology-driven changes in the labor market.

5. Alignment of Cybersecurity Jobs and Certifications against GPT Capabilities

In this section, we align the cybersecurity jobs and certifications against GPT capabilities.

5.1. Industry Jobs

In this subsection, we aim to evaluate the main job tasks associated with various cybersecurity roles by breaking them down into skills and knowledge requirements. Our objective is to determine the extent to which these roles may be exposed to, or even potentially augmented by, the capabilities of ChatGPT. By analyzing the degree to which LLM may influence or impact these professions, we can better understand the future landscape of the cybersecurity industry.

5.1.1. GRC Consultants

The primary task expected to be performed by GRC consultants is to help organizations **establish and maintain effective GRC frameworks**. Among its body of knowledge, the cybersecurity fundamentals, compliance and regulations, and legal knowledge and ethics can be directly obtained by ChatGPT, whereas the knowledge of the client can be extracted and summarized using LLM from records of client interviews. Among the skillset expected on GRC consultants, the risk management and project management can be LLM+ exposed to ChatGPT via bridging software to perform data collection, cleansing and transformation. Therefore, we believe its overall exposure of body of knowledge is estimated to be 1, its exposure of skillset is estimated to be 0.67, and the overall task exposure of is estimated to be 0.67 (Table 4).

We believe GRC consultants could greatly benefit from ChatGPT in a variety of ways. ChatGPT can quickly provide information, generate reports, and answer queries, which can save time and increase the efficiency of GRC consultants. It can help them access relevant information from a vast knowledge base, making research and staying up-to-date with new developments more manageable. It can process and analyze large volumes of text data, which can be helpful in tasks like sentiment analysis, topic modeling, or extracting insights from unstructured data sources. It can assist them in drafting or editing various documents, such as policies, procedures, audit reports, and risk assessments, improving the overall quality and consistency of the content. It can also help ensure that responses and recommendations are consistent and based on established best practices, reducing the potential for human bias or errors. However, its knowledge is restricted to the training data it was fed, and it may not be aware of the latest trends, threats, or regulatory changes that occur after its knowledge cut-off date, unless it uses a plugin to read from the Internet unverified and potentially unreliable data. It may

 doi:10.20944/preprints202404.1600.v1

not fully understand the context or specific requirements of a given organization, which could lead to recommendations that are not applicable or suitable for the organization's unique circumstances. It can occasionally generate incorrect or misleading information, making it essential for GRC consultants to verify the accuracy of any outputs before relying on them. The use of ChatGPT can also raise concerns related to privacy, security, and fairness, which GRC consultants need to consider when integrating it into their workflow.

Table 4. Evaluation of the TKS exposure of *GRC Consultants* to ChatGPT

Task list		**Body of knowledge**		**Skillsets**	
Task	**Exposure**	**Knowledge**	**Exposure**	**Skill**	**Exposure**
Establish and maintain effective GRC frameworks	0.67	Cybersecurity fudnamentals	Direct (1)	Risk management	LLM+ exposed (0.5)
		Compliance and regulations	Direct (1)	Problem solving and time management	No exposure (0)
		Legal knowledge and ethics	Direct (1)	Governance and policy development	Direct (1)
				Auditing and assessment	Direct (1)
		Knowledge of the client, their environment and preferences	Direct (1)	Communication, presentation and media literacy	Direct (1)
				Project management	LLM+ exposed (0.5)

5.1.2. SOC Analysts

The primary task expected to be performed by SOC analysts is to **monitor and analyze security events and incidents** that occur within an organization's network or systems. Among its body of knowledge, ChatGPT can have direct exposure to advanced cybersecurity knowledge, can obtain threat intelligence via data collection software from the Internet, and can summarize client baseline norms from security log data. Among its skills, ChatGPT can generate scripting for automation, and help to improve communication and presentation, but needs additional software to be able to use SIEM tools, perform automated incident detection and response (as already implemented in Microsoft Sentinel), and perform basic forensic analysis. Therefore, we believe the exposure of its body of knowledge is estimated to be 0.67, the exposure of skills is estimated to be 0.58, and the overall task exposure of monitoring and analyzing security events and incidents is estimated to be 0.39 (Table 5).

SOC analysts can have their work experience enhanced by adopting LLMs like ChatGPT. ChatGPT can quickly provide information, answer queries, and generate reports, saving time and increasing the efficiency of SOC analysts. It can access relevant information from a vast knowledge base, making research and staying up-to-date with new developments more manageable. It can process and analyze large volumes of text data, helpful in tasks like log analysis, pattern recognition, or extracting insights from unstructured data sources. It can provide guidance on automation tasks and scripting, to streamline SOC analysts' workflow and improve their efficiency in incident detection and response. It can also serve as a knowledge repository, helping SOC analysts learn from each other's experiences, best practices, and solutions to common problems. However, it can suffer the similar drawbacks: It has limited knowledge beyond its knowledge cut-off date. It may not fully understand the context or specific requirements of a given organization, which could lead to recommendations that are not applicable or suitable for the organization's unique circumstances. It can occasionally generate incorrect or misleading information, making it essential for SOC analysts to verify the accuracy of any outputs before relying on them. It can raise concerns related to privacy, security, and fairness, which SOC analysts need to consider when integrating ChatGPT into their workflow.

 doi:10.20944/preprints202404.1600.v1

Table 5. Evaluation of the TKS exposure of *SOC Analysts* to ChatGPT

Task list		Body of knowledge		Skillsets	
Task	**Exposure**	**Knowledge**	**Exposure**	**Skill**	**Exposure**
Monitor and analyze security events and incidents	0.39	Advanced cybersecurity	Direct (1)	Using SIEM tools	LLM+ exposed (0.5)
				Incident detection and response	LLM+ exposed (0.5)
		Threat intelligence	LLM+ exposed (0.5)	Basic forensic analysis	LLM+ exposed (0.5)
				Scripting and automation	Direct (1)
		Knowledge of the client and their baseline norms	LLM+ exposed (0.5)	Communication skills	Direct (1)
				Problem solving and time management	No exposure (0)

5.1.3. Network and Cloud Security Engineers

The primary task expected to be performed by Network and Cloud Security Engineers is to **design, implement and maintain secure network and cloud infrastructures** for organizations. Among its body of knowledge, all of them were found to be directly exposed by ChatGPT. Of the skills, ChatGPT can generate scripting for automation, and help to improve communication and presentation, perform automated incident detection and response, and perform basic network or cloud diagnoses. Many cloud providers offer AI-based automated detection playbooks (*e.g.*, Amazon GuardDuty, Azure Sentinel) and troubleshooting utilities (*e.g.*, AWS Trusted Advisor, Azure Advisor) as part of their service offerings to help customers diagnose and resolve issues with their cloud resources. Therefore, we believe its overall exposure of body of knowledge is 1, its overall exposure of skills is 0.8, and the overall task exposure of designing, implementing and maintaining secure network and cloud infrastructures is 0.8 (Table 6).

Table 6. Evaluation of the TKS exposure of *Network and cloud security engineers* to ChatGPT

Task list		Body of knowledge		Skillsets	
Task	**Exposure**	**Knowledge**	**Exposure**	**Skill**	**Exposure**
Design, implement and maintain secure network and cloud infrastructures	0.8	Advanced cybersecurity	Direct (1)	Incident detection	Direct (1)
		Network and cloud technologies and best practice	Direct (1)	Network or cloud diagnoses	Direct (1)
		Identity and asset management	Direct (1)	Scripting and automation	Direct (1)
		Data protection	Direct (1)	Communication skills	Direct (1)
		Legal and regulatory compliance	Direct (1)	Problem solving and time management	No exposure (0)

Network and cloud cybersecurity engineers can benefit from using LLMs like ChatGPT to support their work. ChatGPT can quickly provide information, answer queries, and generate documentation. It can access relevant information from a vast knowledge base, making research and staying up-to-date with new developments more manageable. It can provide suggestions or potential solutions to network or cloud problems, offer guidance on scripting and automation tasks, or serve as a knowledge repository to help engineers learn from each other's experiences, best practices, and solutions to common problems. However, it also suffers its usual issues of limited information

 doi:10.20944/preprints202404.1600.v1

beyond its knowledge cut-off date, lack of full understanding of the context, occasional generation of wrong results, and ethical concerns related to privacy, security, and fairness when using AI to process information.

5.1.4. Penetration Testers

The primary task expected to be performed by penetration testers is **pentesting and reporting**, which is to execute Red Team and penetration testing assessments, and to develop high-quality reports detailing identified attack paths, vulnerabilities, and pragmatic recommendations for remediation, written for both management and technical audiences. Among its body of knowledge, the cybersecurity knowledge and the legal knowledge and ethics are directly exposed to ChatGPT via simple queries. The knowledge of the client via reconnaissance and *Open Source Intelligence* (OSINT) cannot be directly obtained by ChatGPT, because it does not have access to classified information or sensitive data. Among the skillset expected on pentesting and reporting, ChatGPT is unable to directly operate forensic software, nor to directly perform problem solving or time management. However, it could use data cleansing plugins to perform timeline analysis and artifact correlation, or perform basic level of analytics. It is highly capable of generating a professional report and presenting it to the public with high level of media literacy. Therefore, we believe the overall exposure of body of knowledge is estimated to be 0.67, the exposure of skills is estimated to be 0.4, and the overall task exposure of pentesting and reporting is estimated to be 0.27 (Table 7).

Table 7. Evaluation of the TKS exposure of *Penetration Testers* to ChatGPT

Task list		**Body of knowledge**		**Skillsets**	
Task	**Exposure**	**Knowledge**	**Exposure**	**Skill**	**Exposure**
Pentesting and reporting	0.27	Advanced cybersecurity	Direct (1)	Using forensic tools and software	No exposure (0)
				Problem solving and time management	No exposure (0)
		Legal knowledge and ethics	Direct (1)	Timeline analysis and artifact correlation	LLM+ exposed (0.5)
		Knowledge of the client via reconnaissance and OSINT	No exposure (0)	Analytical skills	LLM+ exposed (0.5)
				Communication skills and storytelling, presentation and media literacy	Direct (1)

We believe penetration testers could use ChatGPT to simulate social engineering attacks with increased speed, efficiency and creativity, to generate well-constructed custom security testing reports, and to identify potential vulnerabilities through NLP. However, ChatGPT is unlikely to understand the full context of the client being pentested on, given its reliance on existing data and its inability to collect or extract sensitive or classified data from the public. While ChatGPT can be a useful tool for pentesting, it should be used alongside other methods and with caution to avoid unintended consequences.

5.2. Certifications

In this subsection, we conduct a series of tests and evaluations to determine whether ChatGPT possesses the necessary knowledge and skills required to pass the cybersecurity certification exams. We cannot use the exact questions from the certification exams, as this would compromise the integrity of the exam and violate the exam security policies. Instead, we will use existing official sample questions, if readily provided by the vendors, which are similar in nature and difficulty to those found in the actual certification exams. We were unable to find the official sample test questions of OSCP by

 doi:10.20944/preprints202404.1600.v1

Offensive Security, but according to the OSCP exam guide[6], it only contains lab-based challenge tasks, without MCQs. Therefore, it is reasonable to assume that the current version of ChatGPT will fail this lab-based exam. Other official sample questions used were listed as follows:

- **CISSP**: The free CISSP practice quiz[7] is publicly available on the (ISC)^2 website, and is made up of 10 questions.
- **CISA**: The free CISA practice quiz[8] consisted of 10 questions, and ISACA explicitly claimed that they were at the same difficulty level of the actual exams.
- **CEH**: The free CEH practice quiz[9] included 5 questions.
- **CISM**: The free CISM practice quiz[10] consisted of 10 questions, and ISACA also explicitly claimed that they were at the same difficulty level of the actual exams.

Table 8. Certification exam details and the results by ChatGPT on their practice questions

Vendor	Abbr.	Exam format	Exam marking				ChatGPT attempts with practice questions		
			Lowest	Highest	Passing	Scaled	Exposure	Score	Result
(ISC)2	CISSP	MCQ	0	1000	700	✓	Direct	9/10	pass
ISACA	CISA	MCQ	200	800	450	✓	Direct	10/10	pass
ISACA	CISM	MCQ	200	800	450	✓	Direct	7/10	pass
EC-Council	CEH	MCQ	0	1000	700	✓	Direct	4/5	pass
Offensive Security	OSCP	Lab-based	0	100	70	×	No exposure	N/A	fail

6. Discussion

Based on our analysis in section 5, we have made the following observations and summarize them as follows.

6.1. Major Themes Identified

6.1.1. ChatGPT Excels in Tasks Related to NLP, but Not in Critical Thinking

ChatGPT tends to excel in tasks related to NLP, such as presenting cybersecurity factual knowledge, analyzing system logs, detecting system or data access patterns, or extracting information from unstructured data such as system logs, which can be helpful in tasks like automating threat intelligence gathering, or analyzing organizational policy documents for potential cybersecurity risks. However, it does not perform well in critical thinking tasks that require deep understanding, evaluation, and decision-making based on real-world experience and abstract concepts. For example, it may struggle to assess the true impact of a cybersecurity vulnerability, prioritize risk mitigation strategies, or make decisions on which mitigation strategy is the most optimal in a given scenario. These tasks often require human expertise, situational awareness, and the ability to think critically to evaluate potential outcomes and consequences. ChatGPT has limitations when it comes to critical thinking, as it lacks the human ability to reason, evaluate, and make complex judgments based on real-world experience and abstract concepts. Its responses are generated based on patterns in the data on which it has been trained, which does not always equate to true critical thinking.

6.1.2. Jobs and Certifications Relying Heavily on Static Knowledge More Exposed to ChatGPT

Cybersecurity jobs (Figure 1) and certifications that rely heavily on static knowledge are becoming more exposed to the capabilities of LLMs like ChatGPT. As these LLMs continue to develop and

---

6 https://help.offensive-security.com/hc/en-us/articles/360040165632-OSCP-Exam-Guide
7 https://cloud.connect.isc2.org/cissp-quiz
8 https://www.isaca.org/credentialing/cisa/cisa-practice-quiz
9 https://iclass.eccouncil.org/our-courses/certified-ethical-hacker-ceh/ceh-readiness-quiz/
10 https://www.isaca.org/credentialing/cism/cism-practice-quiz

 doi:10.20944/preprints202404.1600.v1

improve, their ability to understand and process information rapidly and accurately is leading to significant implications for the cybersecurity landscape. Certifications that focus on the acquisition of static knowledge may lose their relevance and value, as LLMs can quickly access and process information, prompting the need for certifications to promote critical thinking, hands-on experience, and adaptable problem-solving skills, rather than purely memorization of static cybersecurity concepts and parameters. Cybersecurity professionals should adapt to an environment where LLMs like ChatGPT will inevitably play a larger role, resulting in a gradual shift towards roles that require more strategic thinking, creativity, and an understanding of human behaviors. Nevertheless, instead of viewing LLMs as threats to cybersecurity jobs or certifications, cybersecurity professionals can harness the power of LLMs to enhance their capabilities, to create new roles and opportunities, *e.g.*, by developing and maintaining secure LLM systems, and to audit their ethical usage.

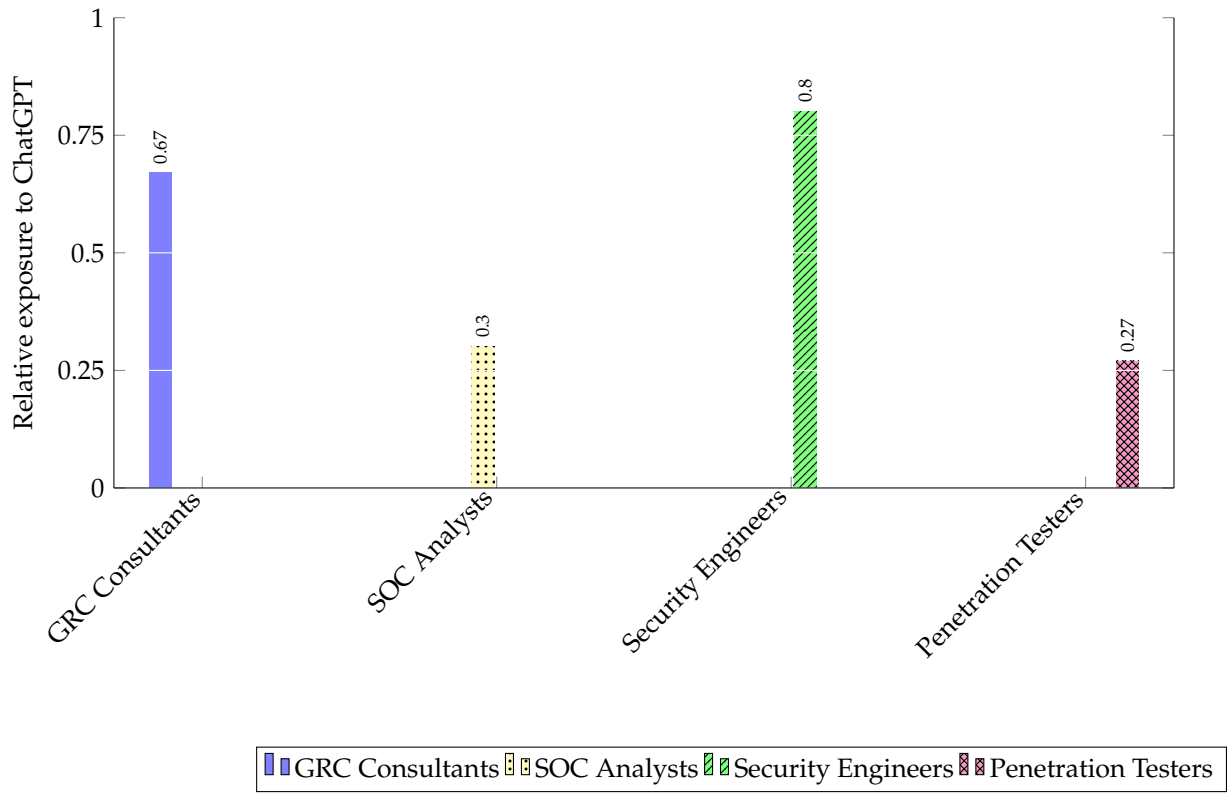

Figure 1. Comparison of estimated exposure of four cybersecurity jobs

6.2. Implications for the Industry

As LLMs like ChatGPT become more prevalent in the cybersecurity sector, both legitimately and illicitly, it is essential for the industry to assess their ethical utilization and prioritize data safety. LLMs may unintentionally reinforce biases and discrimination present in their training data, resulting in unjust and harmful outcomes. To ensure ethical and fair usage of LLMs, the cybersecurity industry must identify and address these biases using techniques such as re-sampling, re-weighting, and adversarial training. To safeguard sensitive data from data breaches during data ingestion by LLMs, the industry needs to establish strong data handling practices, including encryption, anonymization, and secure storage, and to implementing stringent access controls and monitoring systems to prevent unauthorized access and data breaches. It is highly likely that LLMs can be misused for malicious purposes, including generating phishing emails, spreading disinformation campaigns, or creating deepfakes. The cybersecurity industry should proactively evaluate potential risks and devise countermeasures to detect and counter such threats, and should collaborate with other stakeholders, such as governments, academic institutions, and private organizations, to form a coordinated response. The industry should

 doi:10.20944/preprints202404.1600.v1

aim to strike a balance between automation and human intervention, and ensure that LLMs serve as supportive tools for human decision-making, rather than replacing it.

6.3. Implications for the Education Sector Teaching Cybersecurity

In light of the rapid adoption of ChatGPT and similar LLMs, some educational institutes have chosen to ban the usage of ChatGPT, while others are watching its development before making decisions[11]. The ability of ChatGPT and similar LLMs to pass most cybersecurity certification exams has profound implications for the education sector, particularly for institutions teaching cybersecurity. These implications necessitate a reevaluation of teaching methodologies, curricula, and skill development approaches in order to maintain the relevance of cybersecurity education. cybersecurity education needs to shift its focus towards practical skills and hands-on experience, develop students' critical thinking and problem-solving abilities, and emphasize real-world scenarios, simulations, and exercises to develop students' abilities to apply their knowledge in dynamic cybersecurity environments. To prepare students for a future when LLMs can play a significant role in cybersecurity, the education sector should integrate AI and other emerging technologies into their cybersecurity curriculum, to help students understand the capabilities and limitations of AI, as well as learn how to effectively and ethically collaborate with AI-driven tools in their professional roles.

6.4. Long-Term Impact of ChatGPT on Cybersecurity Using the Technological Displacement Theory

The long-term impact of ChatGPT on the cybersecurity industry, as viewed through the lens of the *Technological Displacement* theory, can manifest in several ways, particularly in terms of job losses, skill obsolescence, labor market shifts, and mixed socioeconomic impacts (Figure 2).

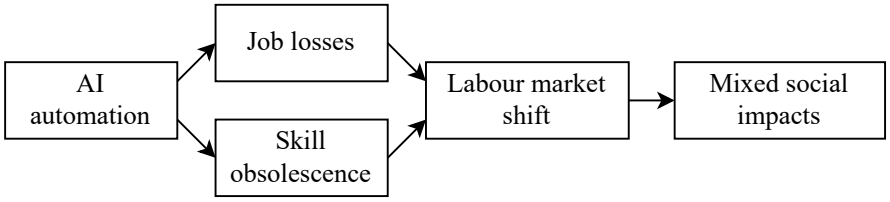

Figure 2. Long-term impact of ChatGPT on cybersecurity

6.4.1. Job Losses

The introduction of ChatGPT and its continuous advancements might contribute to a moderate level of job losses in the cybersecurity industry, particularly in positions that are more susceptible to it. As AI-powered solutions become more effective and economical, businesses may increasingly depend on them to automate tasks previously carried out by cybersecurity workers, like network and cloud security engineers or GRC consultants. This shift could lead to a decreased need for human labor in these roles, potentially alleviating the recurrent shortage of skilled cybersecurity professionals and the rising demand driven by the growing number of cyber threats, as noted in [36]. However, it may eventually contribute to increased unemployment rates within the cybersecurity sector, by reducing the demand for workers.

6.4.2. Skill Obsolescence

As ChatGPT and related technologies progress, the skill sets needed for specific cybersecurity roles, particularly those that depend on memorization rather than critical thinking, could become obsolete. For instance, recalling particular network ports and associated services or setting up firewalls following standard procedures might lose importance as AI-based solutions can efficiently and accurately retrieve

[11] https://www.businessinsider.com/chatgpt-schools-colleges-ban-plagiarism-misinformation-education-2023-1

 doi:10.20944/preprints202404.1600.v1

necessary information and perform these tasks. In light of this, cybersecurity professionals should concentrate on developing skills that complement AI technologies instead of competing against them. Human expertise will remain essential in areas such as threat intelligence analysis, incident response, strategic decision-making, and creating customized security policies. Professionals should emphasize critical thinking, problem-solving, and communication skills, along with the capacity to adapt to new technologies and incorporate AI-driven solutions into their work processes.

To ready the cybersecurity workforce for this transition, organizations and educational institutions must modify their training and development initiatives. Focus should be on nurturing higher-order skills like creative thinking, collaboration, and ethical considerations when addressing cyber threats. By fostering a culture of ongoing learning and accepting AI technologies as a fundamental component of the cybersecurity domain, we can establish a stronger and more resilient defense against the constantly evolving cyber threats faced by individuals, businesses, and governments worldwide.

6.4.3. Labor Market Shifts

The labor market in the cybersecurity industry may undergo significant changes as ChatGPT and related technologies advance. Demand for traditional cybersecurity roles, such as network and cloud security engineers, could decrease, while the need for professionals skilled in managing and maintaining AI-driven solutions may increase. Additionally, emerging job roles may focus on ethical considerations, AI governance, AI-auditing, and the creation of unbiased and transparent algorithms. Cybersecurity professionals may need to specialize in assessing AI models to prevent unintentional propagation of biases, discrimination against specific groups, or breaches of privacy standards. There might also be a higher demand for experts who can bridge the gap between AI development and cybersecurity, ensuring AI systems are designed with security and privacy as foundational elements. Consequently, the industry will likely see a shift towards skills and expertise compatible with AI advancements. In order to adapt, both professionals and organizations should prioritize continuous learning, interdisciplinary collaboration, and a heightened focus on the ethical and governance dimensions of AI technologies within the cybersecurity field.

6.4.4. Mixed Socioeconomic Impacts

The long-term socioeconomic outcomes of ChatGPT's effect on the cybersecurity sector can be complex and varied. On one hand, businesses might enjoy increased productivity and cost savings due to automation. For example, AI-driven solutions could identify and resolve security vulnerabilities more effectively than humans, leading to reduced response times and operational costs for the organizations. On the other hand, widespread job losses and outdated skills may contribute to growing unemployment rates and income inequality among cybersecurity employees. As conventional cybersecurity roles become less crucial, employees could face challenges finding new opportunities within the industry. This may disproportionately impact individuals with specialized or outdated skills that are exposed to LLMs, exacerbating the wealth gap between those who can adapt to AI-driven changes and those who cannot.

To address these challenges, governments and educational institutions might need to invest in retraining programs and educational reforms. These efforts should focus on equipping displaced workers with the necessary skills to move into emerging job roles, such as AI model evaluation, AI governance, and ethical AI solution creation. By fostering a culture of continuous learning and adaptation, these initiatives can help individuals remain competitive in the job market and support economic growth. Furthermore, collaboration between public and private sectors could play a vital role in shaping the future cybersecurity workforce. This may include creating new job opportunities, funding research and development in AI-compatible cybersecurity solutions, and enacting policies that encourage ethical and sustainable AI adoption. By taking a proactive approach, stakeholders can work together to navigate the socioeconomic ramifications of ChatGPT's impact on the cybersecurity sector and ensure a more equitable and thriving future for all workers.

 doi:10.20944/preprints202404.1600.v1

6.4.5. Summary

In summary, our analysis using the *Technological Displacement* theory on ChatGPT's long-term impact on cybersecurity revealed inevitable potential for job losses, skill obsolescence, labor market shifts, and mixed socioeconomic impact on the society. We highlighted the importance of preparing for these changes, by investing in upskilling, reskilling, and job reinventions, to mitigate potential negative outcomes and to foster a sustainable and inclusive labor market.

6.5. Limitations of This Study

This empirical cybersecurity study has limitations that may affect the scope and applicability of its findings. First, it omits managerial aspects of cybersecurity jobs, potentially leading to an incomplete understanding of the skills required for success. Second, it doesn't cover the full range of cybersecurity roles, limiting the study's representativeness of the broader industry. Lastly, the study doesn't consider factors like organizational culture, industry requirements, the different weight of each knowledge point or skill per task, and geographical variations, which could oversimplify the field and overlook key differences between roles and environments. Future research in this area should strive to address these limitations and provide a more comprehensive understanding of the cybersecurity landscape to better inform practitioners, educators, and policymakers about the potential impacts of ChatGPT and other LLMs on cybersecurity, and get prepared before its mass adoption.

7. Conclusion

Our empirical study has found that ChatGPT has exhibited huge potential in streamlining and optimizing many parts of the non-managerial cybersecurity jobs, and can perform well in cybersecurity certification exams that mainly test on memorizing knowledge. The proper augmentation of LLMs like ChatGPT with the existing cybersecurity workforce can potentially relief the skill shortage, and help the workforce make better cybersecurity decisions. However, there may exist several considerations and challenges to be addressed to fully harness the capabilities of LLMs in cybersecurity, including ethical concerns and data safety, and limitations of LLMs in processing more nuanced, context-specific tasks that involve critical thinking and problem-solving. Additionally, LLMs like ChatGPT have the potential to displace cybersecurity jobs, by causing job losses, skill obsolescence, labor market shifts, and mixed socioeconomic impact on the society in the long term. Ultimately, the impact of LLMs like ChatGPT on the cybersecurity job market is still uncertain, and it is likely to require ongoing discussions and collaboration between industry leaders, policymakers, and cybersecurity professionals to ensure a smooth and equitable transition. In this study, we specifically targeted cybersecurity educational institutions. However, the findings and outcomes of this study could be applied to other educational domains, such as medicine, mathematics, commerce, and arts with adaptation.

Funding: This research received no external funding.

Data Availability Statement: No data has been captured as part of this research.

Conflicts of Interest: The author declare no conflicts of interest.

 doi:10.20944/preprints202404.1600.v1

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CEH	Certified Ethical Hacker
DWA	Detailed Work Activities
DOI	Digital Object Identifier
GRC	Governance, Risk, and Compliance
ISC	International Information System Security Certification Consortium
LLM	Large Language Model
MCQ	Multiple-Choice Questions
MDPI	Multidisciplinary Digital Publishing Institute
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
OSCP	Offensive Security Certified Professional
OSINT	Open Source Intelligence
PDF	Portable Document Format
SIEM	Security Information and Event Management
SOC	Security Operations Center
XDR	Extended Detection and Response

References

1. Eloundou, T.; Manning, S.; Mishkin, P.; Rock, D. GPTs are GPTs: An Early Look at the Labor Market Impact Potential of Large Language Models. *arXiv preprint arXiv:2303.10130* **2023**.
2. Zamfirescu-Pereira, J.; Wong, R.; Hartmann, B.; Yang, Q. Why Johnny can't prompt: how non-AI experts try (and fail) to design LLM prompts. Proceedings of the 2023 CHI conference on human factors in computing systems (CHI'23), 2023.
3. MacNeil, S.; Tran, A.; Hellas, A.; Kim, J.; Sarsa, S.; Denny, P.; Bernstein, S.; Leinonen, J. Experiences from using code explanations generated by large language models in a web software development e-book. Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1, 2023, pp. 931–937.
4. Martin, C.; DeStefano, K.; Haran, H.; Zink, S.; Dai, J.; Ahmed, D.; Razzak, A.; Lin, K.; Kogler, A.; Waller, J.; others. The ethical considerations including inclusion and biases, data protection, and proper implementation among AI in radiology and potential implications. *Intelligence-Based Medicine* **2022**, p. 100073.
5. Smith, G. The intelligent solution: automation, the skills shortage and cyber-security. *Computer Fraud & Security* **2018**, *2018*, 6–9.
6. Atiku, S.B.; Aaron, A.U.; Job, G.K.; Shittu, F.; Yakubu, I.Z. Survey on the applications of artificial intelligence in cyber security. *International Journal of Scientistic and Technology Research* **2020**, *9*, 165–170.
7. Bécue, A.; Praça, I.; Gama, J. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review* **2021**, *54*, 3849–3886.
8. Truong, T.C.; Diep, Q.B.; Zelinka, I. Artificial intelligence in the cyber domain: Offense and defense. *Symmetry* **2020**, *12*, 410.
9. Newhouse, W.; Keith, S.; Scribner, B.; Witte, G. National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST special publication* **2017**, *800*, 181.
10. Petersen, R.; Santos, D.; Wetzel, K.; Smith, M.; Witte, G. Workforce framework for cybersecurity (NICE framework) **2020**.
11. Fowler, J.; Evans, N. Using the NICE framework as a metric to analyze student competencies. Journal Of The Colloquium For Information Systems Security Education, 2020, Vol. 7, pp. 18–18.

 doi:10.20944/preprints202404.1600.v1

12. Jones, K.S.; Namin, A.S.; Armstrong, M.E. 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)* **2018**, *18*, 1–12.
13. Ngambeki, I.B.; Rogers, M.; Bates, S.J.; Piper, M.C. Curricular Improvement Through Course Mapping: An Application of the NICE Framework. 2021 ASEE Virtual Annual Conference Content Access, 2021.
14. Patnayakuni, N.; Patnayakuni, R. A Professions Based Approach to Cybersecurity Education and the NICE Framework. *Investigating Framework Adoption, Adaptation, or Extension National CyberWatch Center Digital Press ID NCC-2020-CSJ-02 csj. nationalcyberwatch. org* **2020**, p. 82.
15. Saharinen, K.; Viinikanoja, J.; Huotari, J. Researching Graduated Cyber Security Students–Reflecting Employment and Job Responsibilities through NICE framework. European Conference on Cyber Warfare and Security, 2022, Vol. 21, pp. 247–255.
16. Dash, B.; Ansari, M.F. An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy. *Int. Res. J. Eng. Technol.(IRJET)* **2022**, *9*.
17. Jacob, J.; Wei, W.; Sha, K.; Davari, S.; Yang, T.A. Is the nice cybersecurity workforce framework (ncwf) effective for a workforce comprising of interdisciplinary majors? Proceedings of the 16th International Conference on Scientific Computing (CSC'18). Las Vegas, USA., 2018.
18. Paulsen, C.; McDuffie, E.; Newhouse, W.; Toth, P. NICE: Creating a cybersecurity workforce and aware public. *IEEE Security & Privacy* **2012**, *10*, 76–79.
19. Coulson, T.; Mason, M.; Nestler, V. Cyber capability planning and the need for an expanded cybersecurity workforce. *Communications of the IIMA* **2018**, *16*, 2.
20. Hott, J.A.; Stailey, S.D.; Haderlie, D.M.; Ley, R.F. Extending the National Initiative for Cybersecurity Education (NICE) Framework Across Organizational Security. *Investigating Framework Adoption, Adaptation, or Extension National CyberWatch Center Digital Press ID NCC-2020-CSJ-02 csj. nationalcyberwatch. org* **2020**, p. 7.
21. Estes, A.C.; Kim, D.J.; Yang, T.A. Exploring how the NICE Cybersecurity Workforce Framework aligns cybersecurity jobs with potential candidates. The 14th International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS'18). Las Vegas, USA., 2018.
22. Teoh, C.S.; Mahmood, A.K. Cybersecurity workforce development for digital economy. *The Educational Review, USA* **2018**, *2*, 136–146.
23. Baker, M. State of cyber workforce development. Technical report, Carnegie Mellon University, 2013.
24. Dawson, M.; Taveras, P.; Taylor, D. Applying software assurance and cybersecurity nice job tasks through secure software engineering labs. *Procedia Computer Science* **2019**, *164*, 301–312.
25. Liu, F.; Tu, M. An Analysis Framework of Portable and Measurable Higher Education for Future Cybersecurity Workforce Development. *Journal of Education and Learning (EduLearn)* **2020**, *14*, 322–330.
26. Dwivedi, Y.K.; Kshetri, N.; Hughes, L.; Slade, E.L.; Jeyaraj, A.; Kar, A.K.; Baabdullah, A.M.; Koohang, A.; Raghavan, V.; Ahuja, M.; others. "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management* **2023**, *71*, 102642.
27. Bozkurt, A.; Xiao, J.; Lambert, S.; Pazurek, A.; Crompton, H.; Koseoglu, S.; Farrow, R.; Bond, M.; Nerantzi, C.; Honeychurch, S.; others. Speculative Futures on ChatGPT and Generative Artificial Intelligence (AI): A Collective Reflection from the Educational Landscape. *Asian Journal of Distance Education* **2023**.
28. Jakesch, M.; Hancock, J.T.; Naaman, M. Human heuristics for AI-generated language are flawed. *Proceedings of the National Academy of Sciences* **2023**, *120*, e2208839120.
29. Ali, A.; Septyanto, A.W.; Chaudhary, I.; Al Hamadi, H.; Alzoubi, H.M.; Khan, Z.F. Applied Artificial Intelligence as Event Horizon Of Cyber Security. 2022 International Conference on Business Analytics for Technology and Security (ICBATS). IEEE, 2022, pp. 1–7.
30. Rajasekharaiah, K.; Dule, C.S.; Sudarshan, E. Cyber security challenges and its emerging trends on latest technologies. IOP Conference Series: Materials Science and Engineering. IOP Publishing, 2020, Vol. 981, p. 022062.
31. Alsmadi, I.; Easttom, C. *The NICE cyber security framework*; Springer, 2020.
32. Collins, R. Technological displacement and capitalist crises: escapes and dead ends. *Political Conceptology* **2010**, *1*, 23–34.

 doi:10.20944/preprints202404.1600.v1

33. Hyötyläinen, M. Labour-saving technology and advanced marginality–A study of unemployed workers' experiences of displacement in Finland. *Critical Social Policy* **2022**, *42*, 285–305.
34. McGuinness, S.; Pouliakas, K.; Redmond, P. Skills-displacing technological change and its impact on jobs: challenging technological alarmism? *Economics of Innovation and New Technology* **2021**, pp. 1–23.
35. Sorells, B.; others. Will robotization really cause technological unemployment? The rate and extent of potential job displacement caused by workplace automation. *Psychosociological Issues in Human Resource Management* **2018**, *6*, 68–73.
36. Fourie, L.; Pang, S.; Kingston, T.; Hettema, H.; Watters, P.; Sarrafzadeh, H. The global cyber security workforce: an ongoing human capital crisis **2014**.