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

Raza Nowrozy

Abstract: ChatGPT, a Large Language Model (LLM) utilizing Natural Language Processing (NLP), has caused concerns about its impact on job sectors, including cybersecurity. This study assesses ChatGPT’s impacts in non-managerial cybersecurity roles using the NICE Framework and Technological Displacement theory. It also explores its potential to pass top cybersecurity certification exams. Findings reveal ChatGPT’s promise to streamline some jobs, especially those requiring memorization. Moreover, this paper highlights 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. A shift in focus from memorization to critical thinking, and collaboration between LLM developers and cybersecurity professionals, is recommended.

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

1. Introduction

The rapid advancements in LLM technology raise critical questions about their potential impacts on various job sectors, particularly non-managerial roles in cybersecurity. This study aims to investigate these impacts, focusing on job displacement, skill obsolescence, and the need for new skill sets in the cybersecurity workforce.

Chat Generative Pre-trained Transformer (ChatGPT) is a Large Language Model (LLM) trained by OpenAI™, based on the GPT-4 architecture. 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. It is designed to understand and generate human-like text in response to natural language inputs [1,2]. 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 [3], content creation [4–7], and language translation [1,8,9]. 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 [10–16].

Despite these challenges, ChatGPT has the potential to revolutionize the way the world interacts with machines and each other, opening up new possibilities for communication, creativity, and innovation [1,5–9,17–19]. The rise of generative AI, including ChatGPT, has also raised concerns about the potential impact on human jobs, including in the field of cybersecurity. Some experts argue that these AI generative technologies have the potential to automate a wide range of cybersecurity tasks, from threat detection and incident response to vulnerability detection.
and penetration testing [20,21]. This could lead to significant job displacement and require cybersecurity professionals to acquire new skills to remain employable in the rapidly evolving job market. However, proponents of generative AI argue that these technologies could improve human productivity and enable cybersecurity professionals to focus on higher-level tasks such as policy development and risk management [5–9,22]. Furthermore, the use of generative AI in cybersecurity could help scale up cybersecurity defenses, particularly in smaller organizations with limited human resources [7,17–19]. As an industry that heavily relies on and actively pursues the latest technology, the cybersecurity industry has a vested interest in exploring the potential impact of generative AI, especially LLM, on itself. In the absence of such a study that focuses on the cybersecurity industry, this study aims to provide some results for industry discussions.

The key contributions of this study are as follows:

- The scope of exposure to ChatGPT, as previously defined in [1,2], has been broadened to encompass several non-managerial cybersecurity industry positions and certifications.
- The NICE Framework was employed 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. The potential utilization of ChatGPT to pass cybersecurity certificate examinations was also studied.
- The challenges and limitations obtained from this study were identified, and a shift from emphasizing memorization to fostering critical thinking skills for the industry, education, and certification institutions that might be exposed by ChatGPT was suggested.

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

2. Related Works

Although there are limited publications on ChatGPT, there are many studies on the NICE framework, which serves as a key reference to define cybersecurity roles, responsibilities, and required skillsets [14,23]. Numerous studies have highlighted the effectiveness of the framework in various contexts, including the development of academic curricula [11–16], workforce training programs [23–26], and organizational role mapping in cybersecurity [27,28]. Researchers have also noted the flexibility of the NICE framework in adapting to the dynamic cybersecurity landscape while emphasizing the importance of continuous updates and revisions to maintain its relevance [15,29,30]. 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 address the ever-growing demand for skilled cybersecurity professionals [15,31–33]. In general, the literature underscores the importance of the NICE framework as a critical tool to build and sustain a robust cybersecurity workforce capable of tackling the diverse challenges in this rapidly evolving field.

In addition, several studies have explored the application of generative AI tools, including ChatGPT, in cybersecurity. For example, research by [1] examined the labor market impact of large language models, while Truong et al. [17] discussed the offensive and defensive uses of AI in cybersecurity. These studies highlight the potential for generative AI to automate routine tasks, enhance threat detection, and improve incident response, thus transforming the cybersecurity landscape. This study builds on these works
by specifically assessing the impact of ChatGPT on non-managerial cybersecurity roles and certifications [5–9].

3. Research Motivation

This section presents the background information that has motivated this investigation.

3.1. Media Coverage of ChatGPT

As a generative AI language model, ChatGPT has gained significant attention from various media outlets around the world [7,18–20,34]. Its advanced language processing capabilities and the ability to engage in human-like conversations have been the subject of numerous news articles and features in print, online, and broadcast media [7–9,35]. 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 drawn the interest of the media and trade [35]. Additionally, ChatGPT’s performance in Natural Language Processing (NLP) competitions and its ability to generate realistic and coherent text have been highlighted in numerous academic and research publications [1,2,34,35]. Despite its occasional unreliability [36], ChatGPT can efficiently handle repetitive tasks such as customer service that involve data entry, allowing humans to focus on more complex and creative tasks [1,14–16]. The 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 much interest and debate in the cybersecurity industry. Some believe that technology can be used to improve security measures by automating tasks such as threat detection and response, allowing human analysts to focus on more complex and strategic tasks (https://sekuro.io/blog/chatgpt-cybersecurity-benefits-and-risks/, accessed on 22 February 2023). However, others express concerns about the potential for generative AI to be used maliciously, such as in the creation of fake videos or social engineering attacks (https://www.businessinsider.com/how-to-detect-ai-generated-content-text-chatgpt-deepfake-videos-2023-3, accessed on 9 May 2023). 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, accelerating threat detection and response, and augmenting the capabilities of human security professionals [37]. 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 (https://www.microsoft.com/en-au/security/business/siem-and-xdr/microsoft-sentinel, accessed on 7 July 2024). However, 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 supervision [38]. Generative AI solutions such as ChatGPT have great potential in improving the accuracy and reliability of automation in cybersecurity defense, using their NLP capabilities to understand and interpret large amounts of data related to cyber threats, analyzing the patterns and behaviors of cyber attackers, and identifying potential vulnerabilities in the system [1,34]. Therefore, it would be worthwhile to
investigate how generative AI can enhance automation in cybersecurity and help create more resilient and reliable methods to mitigate increasing cyber threats.

4. Research Methods

This section demonstrates how the impact of ChatGPT on cybersecurity industry jobs and certifications was evaluated, based on the National Initiative for Cybersecurity Education (NICE) Framework (https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center, accessed on 7 July 2024) by the National Institute of Standards and Technology (NIST) [23,39].

4.1. The NICE Framework

The NICE Framework by NIST is a comprehensive guide that categorizes and describes cybersecurity work, with the aim of improving the understanding of cybersecurity roles, responsibilities, and skill requirements, and providing a common language for discussing cybersecurity work [23,39]. It is a structured approach widely used by organizations, educators and the cybersecurity workforce to identify the needs and skill gaps of the cybersecurity workforce, develop consistent training and education programs, create career paths and opportunities for cybersecurity professionals, and improve recruitment, hiring and retention efforts [39]. The NICE Framework was selected for this study due to its widespread acceptance and applicability across various organizations and educational institutions. It provides a structured approach to defining and assessing cybersecurity roles, making it an ideal choice for evaluating the impact of emerging technologies like ChatGPT.

The main building blocks within NICE are the Tasks, Knowledge, and Skills (TKS), or can be expressed as:

\[ \text{Tasks} = \text{Knowledge} \times \text{Skills} \] (1)

According to [7,18–20,23,34,39], 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 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 empirical study focuses on the second step by reviewing cybersecurity industry jobs and the third step by examining cybersecurity certifications.

4.2. Selection of Cybersecurity Industry Jobs

This study focuses on some of the non-managerial jobs that are the 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. LinkedIn (Australia) and Seek.com.au, the top websites used by Australians to perform job searches, were used for this purpose. For each role, the top five search results (sorted by relevance) were used to extract the commonality of their primary tasks that were not employer-specific, and information not directly related to job tasks, knowledge, or skills (e.g., location of positions, remuneration levels) was ignored. Their brief job descriptions are listed below:

- GRC consultants help organizations 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.

Furthermore, positions such as threat hunters and digital forensic investigators, which are critical in identifying and responding to cyber threats, could also be significantly impacted by LLMs. Future studies could further explore the specific challenges and opportunities for these roles.

4.3. Selection of Cybersecurity Certifications

This study focused on some of the most sought-after cybersecurity certifications in the industry, selected based on their popularity in the Australian job market:

Certified Information Systems Security Professional (CISSP) by (ISC)², Certified Ethical Hacker (CEH) by EC-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 (https://www.seek.com.au/, accessed on 7 July 2024) have been summarized in Table 1.

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

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Abbr.</th>
<th>Full Name</th>
<th>Min Work Experience</th>
<th>Popularity LinkedIn</th>
<th>Popularity Seek</th>
</tr>
</thead>
<tbody>
<tr>
<td>(ISC)²</td>
<td>CISSP</td>
<td>Certified Information Systems Security Professional</td>
<td>5 years</td>
<td>9282</td>
<td>1133</td>
</tr>
<tr>
<td>ISACA</td>
<td>CISA</td>
<td>Certified Information Systems Auditor</td>
<td>5 years</td>
<td>1359</td>
<td>696</td>
</tr>
<tr>
<td>EC-Council</td>
<td>CEH</td>
<td>Certified Ethical Hacker</td>
<td>2 years</td>
<td>445</td>
<td>320</td>
</tr>
<tr>
<td>ISACA</td>
<td>CISM</td>
<td>Certified Information Security Manager</td>
<td>5 years</td>
<td>308</td>
<td>511</td>
</tr>
<tr>
<td>Offensive Security</td>
<td>OSCP</td>
<td>Offensive Security Certified Professional</td>
<td>N/A</td>
<td>370</td>
<td>486</td>
</tr>
</tbody>
</table>

To evaluate the exposure of these certifications to ChatGPT, a series of tests were performed using official sample questions from each certification exam. These tests involved entering sample questions into ChatGPT and recording its performance. The results, summarized in Section 5.1.4, demonstrate the extent to which ChatGPT can correctly answer exam questions and simulate the certification process.

In addition to performing tests using official sample questions, domain experts were involved in evaluating ChatGPT’s responses. These experts assessed the accuracy, relevance, and utility of ChatGPT’s answers, providing quantitative data on the potential defensive uses of ChatGPT in cybersecurity. Their evaluations helped validate the findings and ensure that the analysis was grounded in practical experience.

The table below illustrates the evaluation of ChatGPT’s responses by domain experts in various areas of cybersecurity. Each expert assessed the precision, relevance, and utility of the responses, providing five scores together with qualitative comments. This evaluation helps validate the effectiveness of ChatGPT in performing cybersecurity tasks [7,18–20,34].
Table 2 below illustrates the evaluation of ChatGPT’s responses by domain experts in various areas of cybersecurity. Each expert assessed the precision, relevance, and utility of the responses, providing five scores together with qualitative comments. This evaluation helps validate the effectiveness of ChatGPT in performing cybersecurity tasks.

Table 2. Domain Experts’ Evaluation of ChatGPT’s Responses.

<table>
<thead>
<tr>
<th>Expert ID</th>
<th>Area of Expertise</th>
<th>Criteria Assessed</th>
<th>Evaluation Score (Out of 5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1</td>
<td>Governance, Risk, and Compliance</td>
<td>Accuracy, Relevance, Utility</td>
<td>4.5</td>
</tr>
<tr>
<td>E2</td>
<td>Security Operations</td>
<td>Accuracy, Relevance, Utility</td>
<td>4.0</td>
</tr>
<tr>
<td>E3</td>
<td>Network and Cloud Security</td>
<td>Accuracy, Relevance, Utility</td>
<td>4.2</td>
</tr>
<tr>
<td>E4</td>
<td>Penetration Testing</td>
<td>Accuracy, Relevance, Utility</td>
<td>3.8</td>
</tr>
<tr>
<td>E5</td>
<td>Cybersecurity Certifications</td>
<td>Accuracy, Relevance, Utility</td>
<td>4.7</td>
</tr>
</tbody>
</table>

Comments

- Expert E1: ChatGPT’s responses were accurate and relevant, with minor gaps in utility for complex scenarios.
- Expert E2: The responses were generally accurate and relevant, but some lacked depth in incident response details.
- Expert E3: ChatGPT provided accurate information, but occasionally missed context-specific nuances.
- Expert E4: The responses were accurate, but sometimes lacked practical applicability and detailed technical insights.
- Expert E5: ChatGPT excelled in providing relevant and useful information for certification exam questions.

4.4. Defining Exposure to ChatGPT

In [1], exposure was defined as a metric that determined whether accessing a ChatGPT or GPT-powered system would result in at least a 50% decrease in the time required for a human to perform a particular Detailed Work Activity (DWA) or task. Ref. [1] defined three 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 the 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 three categories of extensions for ChatGPT: Web browsing, Python code interpreter, and semantic search.

In this study, their definition of exposure for cybersecurity jobs is inherited and expanded, and redefined in Table 3. Arbitrary values were assigned as follows: 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 the LLM. For a particular task on the job (t), the estimated exposure of the task is T. Each task can be assigned to several knowledge points (k) and skills (s).

If the exposure of the i\textsuperscript{th} knowledge point is k\textsubscript{i}, the overall exposure of the body of knowledge, K is given by

$$K = \frac{1}{m} \sum_{i=1}^{m} k_i.$$  \hspace{1cm} (2)

Using Equation (2), human-specific knowledge is obtained,
where \( m_1 \in 1, 2, 3, \ldots, N_1 \).

Similarly, using Equation (2), LLM-assisted knowledge is obtained,

\[
K_{LLM} = \frac{1}{m_2} \sum_{i=1}^{m_2} k_i
\]

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

\[
S = \frac{1}{n} \sum_{i=1}^{n} s_i
\]

where \( n \in 1, 2, 3, \ldots, M \).

Using Equations (3)–(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:

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

where \( K = K_h + K_{LLM} \).

Table 3. Redefinition of exposure against job tasks and certifications.

<table>
<thead>
<tr>
<th>Exposure</th>
<th>Job task</th>
<th>Knowledge</th>
<th>Certifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>No exposure (0)</td>
<td>LLM does not reduce the time to perform the skill.</td>
<td>LLM does not help with knowledge presentation.</td>
<td>LLM cannot be used to pass the exam.</td>
</tr>
<tr>
<td>LLM+ exposure (0.5)</td>
<td>LLM combined with additional software can partially (≥50%) perform the skill.</td>
<td>LLM combined with additional software can partially (≥50%) present the knowledge.</td>
<td>LLM combined with additional software can be used to pass the exam.</td>
</tr>
<tr>
<td>Direct exposure (1)</td>
<td>LLM alone can partially (≥50%) perform the skill.</td>
<td>LLM alone can partially (≥50%) or fully present knowledge.</td>
<td>LLM alone can pass the exam.</td>
</tr>
</tbody>
</table>

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 that are necessary to complete them in various real-world situations. In addition, discouraging LLM-assisted knowledge in exams contributes to upholding the fairness and integrity of the grading process.

A solution is proposed to optimize human-specific knowledge and minimize LLM-assisted ability. A list of symbols in the proposed model can be found in Table 4.

\[
\max_{\psi \in X} (1 - \beta)K_h(\psi) - \beta K_{LLM}(\psi).
\]

It is ensured that both \( K_h(\psi) > 0 \) and \( K_{LLM}(\psi) > 0 \) for each exam, using the assessments \( X = \psi_1, \psi_2, \ldots, \psi_\phi \) and weight factor, \( \beta \in [0, 1] \).

The objective is to develop assessments to maximize the use of human-specific knowledge, \( K_h(\psi) \), while reducing the dependence on LLM-assisted information, \( K_{LLM}(\psi) \).
Table 4. List of symbols used in the proposed model.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>Tasks</td>
</tr>
<tr>
<td>$K$</td>
<td>Number of knowledge points</td>
</tr>
<tr>
<td>$S$</td>
<td>Skills</td>
</tr>
<tr>
<td>$K_h$</td>
<td>Human specific knowledge</td>
</tr>
<tr>
<td>$K_{LLM}$</td>
<td>LLM assisted knowledge</td>
</tr>
<tr>
<td>$N_1$</td>
<td>Number of human-specific knowledge available, where $m_1 \in 1, 2, 3, \ldots, N_1$</td>
</tr>
<tr>
<td>$N_2$</td>
<td>Number of LLM-assisted knowledge available, where $m_2 \in 1, 2, 3, \ldots, N_2$</td>
</tr>
<tr>
<td>$M$</td>
<td>Number of skills available, where $n \in 1, 2, 3, \ldots, M$</td>
</tr>
<tr>
<td>$\beta$</td>
<td>Weight factor</td>
</tr>
<tr>
<td>$\psi$</td>
<td>Assessments, where $X = \psi_1, \psi_2, \ldots, \psi_\psi$</td>
</tr>
</tbody>
</table>

4.6. Defining Exposure to ChatGPT

In [1], exposure was defined as a metric that determined whether accessing a ChatGPT or GPT-powered system would result in at least a 50% decrease in the time required for a human to perform a particular detailed work activity (DWA) or task. Ref. [1] defined three 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 the 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 three categories of extensions for ChatGPT: Web browsing, Python code interpreter, and semantic search.

In this study, their definition of exposure for cybersecurity jobs is inherited and expanded, and redefined in Table 3. Arbitrary values were assigned as follows: 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 the LLM. For a particular task on the job ($t$), the estimated exposure of the task is $T$. Each task can be assigned to several knowledge points ($k$) and skills ($s$).

Simple Explanation: The mathematical presentation shows how the extent to which ChatGPT can help with different cybersecurity tasks is measured by using a specific formula. This helps determine how useful ChatGPT can be in various scenarios.

4.7. 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 [40–43]. This study interprets the results by examining the following aspects in the context of cybersecurity.

- Job Loss: 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, will be explored.
- Skill Obsolescence: The speed at which the skills of impacted professionals may become outdated, as well as the potential need for reskilling or upskilling will be investigated.
• Labor Market Shifts: 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 will be estimated.

• Socioeconomic Impact: The wider socioeconomic ramifications of technological displacement in cybersecurity, such as its influence on productivity, wages, and income inequality will be explored.

Using this theory as a framework, a deeper understanding of ChatGPT’s potential to replace certain cybersecurity jobs and place empirical findings within the larger conversation surrounding technology-driven changes in the labor market will be sought.

5. Alignment of Cybersecurity Jobs and Certifications with GPT Capabilities

This section aligns cybersecurity jobs and certifications with GPT capabilities.

5.1. Industry Jobs

This subsection evaluates the main job tasks associated with various cybersecurity roles by breaking them down into skills and knowledge requirements. The aim is to determine to what extent these roles may be exposed to, or even potentially augmented by, the capabilities of ChatGPT. By analyzing the degree to which LLM can influence or impact these professions, a better understanding of the future landscape of the cybersecurity industry can be achieved.

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, cybersecurity fundamentals, compliance and regulations, and legal knowledge and ethics can be obtained directly by ChatGPT, while the knowledge of the client can be extracted and summarized using LLM from records of client interviews. Among the skillset expected of GRC consultants, risk management and project management can be LLM+ exposed to ChatGPT via bridging software to perform data collection, cleansing and transformation. Therefore, the overall exposure to the body of knowledge is estimated to be 1, the exposure to the skill set is estimated to be 0.67, and the overall exposure to the task is estimated to be 0.67 (Table 5).

Table 5. Evaluation of the TKS exposure of GRC Consultants to ChatGPT.

<table>
<thead>
<tr>
<th>Task List</th>
<th>Body of Knowledge</th>
<th>Skillsets</th>
<th>Exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish and maintain effective GRC frameworks</td>
<td>Cybersecurity fundamentals</td>
<td>Risk management</td>
<td>LLM+ exposed (0.5)</td>
</tr>
<tr>
<td>Compliance and regulations</td>
<td>Direct (1)</td>
<td>Problem solving and time management</td>
<td>No exposure (0)</td>
</tr>
<tr>
<td>Legal knowledge and ethics</td>
<td>Direct (1)</td>
<td>Governance and policy development</td>
<td>Direct (1)</td>
</tr>
<tr>
<td></td>
<td>Auditing and assessment</td>
<td>Direct (1)</td>
<td></td>
</tr>
<tr>
<td>Knowledge of the client, their environment and preferences</td>
<td>Direct (1)</td>
<td>Communication, presentation and media literacy</td>
<td>Direct (1)</td>
</tr>
<tr>
<td></td>
<td>Project management</td>
<td>LLM+ exposed (0.5)</td>
<td></td>
</tr>
</tbody>
</table>

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 such as sentiment analysis, topic modeling, or extracting insights from unstructured data sources. It can assist in the writing or editing of 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 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 output before relying on them. The use of ChatGPT can also raise concerns related to privacy, security, and fairness, which GRC consultants must consider when integrating it into their workflow.

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 automation scripts and help improve communication and presentation, but it 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, 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 exposure to the task of monitoring and analyzing security events and incidents is estimated to be 0.39 (Table 6).

Table 6. Evaluation of the TKS exposure of SOC Analysts to ChatGPT.

<table>
<thead>
<tr>
<th>Task List</th>
<th>Body of Knowledge</th>
<th>Skillsets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor and analyze security</td>
<td>Advanced cybersecurity</td>
<td>Using SIEM tools</td>
</tr>
<tr>
<td>events and incidents</td>
<td>Direct (1)</td>
<td>LLM+ exposed (0.5)</td>
</tr>
<tr>
<td></td>
<td>Threat intelligence</td>
<td>Incident detection</td>
</tr>
<tr>
<td></td>
<td>LLM+ exposed (0.5)</td>
<td>and response</td>
</tr>
<tr>
<td></td>
<td>Knowledge of the client</td>
<td>Basic forensic analysis</td>
</tr>
<tr>
<td></td>
<td>and their baseline norms</td>
<td>LLM+ exposed (0.5)</td>
</tr>
<tr>
<td></td>
<td>LLM+ exposed (0.5)</td>
<td>Scripting and automation</td>
</tr>
<tr>
<td></td>
<td>Communication skills</td>
<td>Direct (1)</td>
</tr>
<tr>
<td></td>
<td>Problem solving and time</td>
<td>No exposure (0)</td>
</tr>
<tr>
<td></td>
<td>management</td>
<td></td>
</tr>
</tbody>
</table>

SOC analysts can improve their work experience 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, which is helpful in tasks such as 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 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 output before relying on them. It can raise concerns related to privacy, security, and fairness, which SOC analysts must consider when integrating ChatGPT into their workflow.

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 these skills, ChatGPT can generate scripting for automation, 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, the overall exposure to the body of knowledge is 1, the overall exposure to skills is 0.8, and the overall exposure to tasks of designing, implementing, and maintaining secure network and cloud infrastructures is 0.8 (Table 7).

### Table 7. Evaluation of the TKS exposure of Network and cloud security engineers to ChatGPT.

<table>
<thead>
<tr>
<th>Task List</th>
<th>Body of Knowledge</th>
<th>Skillsets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design, implement and maintain secure network and cloud infrastructures</td>
<td>Advanced cybersecurity</td>
<td>Incident detection</td>
</tr>
<tr>
<td></td>
<td>Network and cloud technologies and best practice</td>
<td>Network or cloud diagnoses</td>
</tr>
<tr>
<td></td>
<td>Identity and asset management</td>
<td>Scripting and automation</td>
</tr>
<tr>
<td></td>
<td>Data protection</td>
<td>Communication skills</td>
</tr>
<tr>
<td></td>
<td>Legal and regulatory compliance</td>
<td>Problem solving and time management</td>
</tr>
</tbody>
</table>

Network and cloud cybersecurity engineers can benefit from using LLMs such as 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 from its usual issues of limited information 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 remediation recommendations, written for both management and technical audiences. Among its body of knowledge, cybersecurity knowledge, legal knowledge and ethics are directly exposed to ChatGPT through simple queries. The client’s knowledge via reconnaissance and Open Source Intelligence (OSINT) cannot be directly obtained by ChatGPT, because it has no 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 a basic level of analytics. It is highly capable of generating a professional report and presenting it to the public with a high level of media literacy. Therefore, the overall exposure of the body of knowledge is estimated to be 0.67, the exposure of skills is estimated to be 0.4, and the overall exposure of the pentest and reporting task is estimated to be 0.27 (Table 8).

Table 8. Evaluation of the TKS exposure of Penetration Testers to ChatGPT.

<table>
<thead>
<tr>
<th>Task List</th>
<th>Body of Knowledge</th>
<th>Skillsets</th>
<th>Exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pentesting and reporting</td>
<td>Advanced cybersecurity</td>
<td>Using forensic tools and software</td>
<td>No exposure (0)</td>
</tr>
<tr>
<td></td>
<td>(Direct (1))</td>
<td>Problem solving and time management</td>
<td>No exposure (0)</td>
</tr>
<tr>
<td></td>
<td>Legal knowledge and ethics</td>
<td>Timelne analysis and artifact correlation</td>
<td>LLM+ exposed (0.5)</td>
</tr>
<tr>
<td></td>
<td>(Direct (1))</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Knowledge of the client via reconnaissance and OSINT</td>
<td>Analytical skills</td>
<td>LLM+ exposed (0.5)</td>
</tr>
<tr>
<td></td>
<td>(No exposure (0))</td>
<td>Communication skills and storytelling, presentation and media literacy</td>
<td>Direct (1)</td>
</tr>
</tbody>
</table>

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

5.2. Certifications

In this subsection, a series of tests and evaluations were conducted to determine whether ChatGPT possesses the necessary knowledge and skills required to pass the cybersecurity certification exams. The exact questions from the certification exams cannot be used, as this would compromise the integrity of the exam and violate the exam security policies. Instead, existing official sample questions, if provided by the vendors, which are similar in nature and difficulty to those found in the actual certification exams were used. The official sample test questions of OSCP by Offensive Security were not available, but according to the OSCP exam guide (https://help.offensive-security.com/hc/en-us/articles/360040165632-OSCP-Exam-Guide, accessed on 7 July 2024), it only contains laboratory-based challenge tasks, without MCQ. Therefore, it is reasonable to assume that the current version of ChatGPT will fail this lab-based exam, see Table 9. Other official sample questions used are listed below.
• CISSP: The free CISSP practice quiz (https://cloud.connect.isc2.org/cissp-quiz, accessed on 7 July 2024) is publicly available on the (ISC)² website and is made up of 10 questions.
• CISA: The free CISA practice quiz (https://www.isaca.org/credentialing/cisa/cisa-practice-quiz, accessed on 7 July 2024) consisted of 10 questions, and ISACA explicitly claimed that they were at the same difficulty level of the actual exams.
• CISM: The free CISM practice quiz (https://www.isaca.org/credentialing/cism/cism-practice-quiz, accessed on 7 July 2024) consisted of 10 questions, and ISACA also explicitly claimed that they were at the same difficulty level as the actual tests.

Table 9. Certification exam details and the results by ChatGPT on their practice questions.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Abbr.</th>
<th>Exam Format</th>
<th>Exam Marking</th>
<th>ChatGPT Attempts with Practice Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>(ISC)²</td>
<td>CISSP</td>
<td>MCQ</td>
<td>Lowest: 0</td>
<td>Highest: 1000 Passing: 700 ✓ Direct: 9/10 pass</td>
</tr>
<tr>
<td>ISACA</td>
<td>CISA</td>
<td>MCQ</td>
<td>Lowest: 200</td>
<td>Highest: 800 Passing: 450 ✓ Direct: 10/10 pass</td>
</tr>
<tr>
<td>ISACA</td>
<td>CISM</td>
<td>MCQ</td>
<td>Lowest: 200</td>
<td>Highest: 800 Passing: 450 ✓ Direct: 7/10 pass</td>
</tr>
<tr>
<td>EC-Council</td>
<td>CEH</td>
<td>MCQ</td>
<td>Lowest: 0</td>
<td>Highest: 1000 Passing: 700 ✓ Direct: 4/5 pass</td>
</tr>
<tr>
<td>Offensive Security</td>
<td>OSCP</td>
<td>Lab-based</td>
<td>Lowest: 0</td>
<td>Highest: 100 Passing: 700 ✓ No exposure N/A fail</td>
</tr>
</tbody>
</table>

6. Discussion

ChatGPT tends to excel in tasks related to NLP, such as presenting factual cybersecurity 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 can be difficult to assess the true impact of a cybersecurity vulnerability, prioritize risk mitigation strategies, or make decisions about which mitigation strategy is the most optimal in a given scenario. These tasks often require human expertise, situational awareness, and the ability to critically think about potential outcomes and consequences.

Furthermore, while ChatGPT and other LLMs can generate efficient text or code snippets, their effectiveness is significantly enhanced when the user possesses sufficient subject knowledge. Users without adequate expertise might find it challenging to identify errors or utilize the outputs generated by these models effectively. This limitation underscores the importance of human oversight and the necessity for cybersecurity professionals to maintain a high level of expertise to effectively use AI tools.

In practical terms, while ChatGPT can provide substantial assistance in generating content and offering suggestions, it cannot replace the nuanced understanding and practical application of knowledge that cybersecurity professionals bring to their roles. Implementing cybersecurity strategies requires a comprehensive approach that includes knowledge application, real-time problem solving, and adaptability to dynamic threat landscapes, areas where human expertise remains indispensable.

The mathematical presentations and tables provided by LLMs, while interesting, might not always be straightforward to interpret without a solid understanding of the underlying concepts. Therefore, enhancing the clarity and accessibility of these presentations is crucial to ensure that they are valuable to security engineers and other professionals.

In general, ChatGPT and similar tools should be viewed as additional resources rather than replacements for human expertise in cybersecurity. By recognizing the limitations and strengths of these tools, professionals can better integrate them into their workflows, improving efficiency while maintaining high standards of accuracy and reliability.
Based on the analysis in Section 5, the following observations were made and summarized 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 factual cybersecurity 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 can be difficult to assess the true impact of a cybersecurity vulnerability, prioritize risk mitigation strategies, or make decisions about which mitigation strategy is the most optimal in a given scenario. These tasks often require human expertise, situational awareness, and the ability to critically think about 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 are heavily based on static knowledge are becoming more exposed to the capabilities of LLMs like ChatGPT. As these LLMs continue to develop and improve, their ability to understand and process information rapidly and accurately has 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 understanding of human behaviors. However, instead of viewing LLMs as threats to cybersecurity jobs or certifications, cybersecurity professionals can harness the power of LLMs to enhance their capabilities, and create new roles and opportunities, for example, by developing and maintaining secure LLM systems, and auditing their ethical use.
6.2. Implications for the Industry

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

Ethical Dimensions and Implications:

Given the sensitive nature of cybersecurity, the ethical dimensions and implications of using ChatGPT must be thoroughly examined. The potential for AI-driven tools to reinforce biases, make unfair decisions, and violate privacy requires careful consideration. Ethical guidelines and best practices must be established to ensure that generative AI is used responsibly. Collaboration between AI developers, policymakers, and cybersecurity professionals is crucial to address these concerns and to develop frameworks that promote the ethical use of AI while protecting sensitive information.

6.3. Implications for the Education Sector Teaching Cybersecurity

In light of the rapid adoption of ChatGPT and similar LLM, some educational institutes have chosen to ban the use of ChatGPT, while others are watching its development before making decisions (https://www.businessinsider.com/chatgpt-schools-colleges-ban-
plagiarism-misinformation-education-2023-1, accessed on 7 July 2024). 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 require the adoption of teaching methodologies, curricula, and skill development to understand the relevance of cybersecurity education. Cybersecurity education should shift its focus to 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 an important 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, and learn how to collaborate effectively and ethically with AI-driven tools in their professional roles.

Detailed mitigations could include the implementation of advanced threat detection systems, the continuous monitoring of AI-generated content for malicious activities, and the development of robust incident response protocols. In addition, promoting cybersecurity awareness and training among employees can help identify and mitigate the threats posed by AI tools. Regular updates to AI models to address new vulnerabilities and ensure strict access controls and data encryption are also critical measures.

Offensive Use of ChatGPT in Cybersecurity:

The offensive use of ChatGPT in cybersecurity poses significant risks that need to be addressed. Generative AI tools can be used to create sophisticated phishing emails, generate malicious code, and conduct social engineering attacks with high levels of realism. Studies such as those by [17] have discussed the potential for AI-driven offensive capabilities. To mitigate these risks, cybersecurity professionals must develop advanced detection and response strategies, promote awareness of AI-generated threats, and collaborate with AI developers to implement safeguards that prevent misuse.

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

The long-term impact of ChatGPT on the cybersecurity industry, 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.](image)

6.4.1. Job Losses

The introduction of ChatGPT and its ongoing improvements could contribute to a moderate level of job loss in the cybersecurity industry, particularly in positions that are more susceptible to it. As AI-powered solutions become more effective and economical, businesses can increasingly depend on them to automate tasks previously performed by cybersecurity workers, such as network and cloud security engineers or GRC consultants. This shift could lead to a decreased need for human labor in these roles, which could alleviate the recurrent shortage of skilled cybersecurity professionals and the growing demand driven by the increasing number of cyber threats, as noted in [44]. However, it may eventually contribute to higher 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 example, 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 necessary information and perform these tasks. In light of this, cybersecurity professionals should focus 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 ability to adapt to new technologies and incorporate AI-driven solutions into their work processes.

To prepare the cybersecurity workforce for this transition, organizations and educational institutions must modify their training and development initiatives. The focus should be on nurturing higher-order skills, such as 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, a stronger and more resilient defense against the constantly evolving cyber threats faced by individuals, businesses, and governments worldwide can be established.

6.4.3. Labor Market Shifts

The labor market in the cybersecurity industry may undergo significant changes as ChatGPT and related technologies advance. The 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. In addition, emerging job roles can 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 may also be a higher demand for experts who can bridge the gap between AI development and cybersecurity, ensuring that 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 greater 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 the 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 organizations. However, widespread job losses and outdated skills can contribute to growing unemployment rates and income inequality among cybersecurity workers. As conventional cybersecurity roles become less crucial, employees could face the challenge of finding new opportunities within the industry. This may disproportionately affect people with specialized or outdated skills who 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 skills necessary to move into emerging job roles, such as evaluating AI models, AI governance, and creating ethical AI solutions. By fostering a culture of continuous learning and adaptation, these initiatives can help
people remain competitive in the job market and support economic growth. Furthermore, collaboration between the 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 adoption of AI. By taking a proactive approach, stakeholders can work together to navigate the socio-economic ramifications of ChatGPT’s impact on the cybersecurity sector and ensure a more equitable and thriving future for all workers.

6.5. Stakeholder Perspectives

The analysis of ChatGPT’s impact on cybersecurity should consider the perspectives of key stakeholders such as users, developers, and policymakers. Users must understand the potential benefits and risks of AI tools, while developers must focus on creating ethical and secure AI solutions. Policymakers should establish regulations and guidelines to ensure responsible usage of AI. By incorporating these perspectives, a comprehensive approach can be developed to address the challenges and solutions related to the integration of ChatGPT into the cybersecurity industry.

6.6. Theoretical Knowledge vs. Practical Application

Although tools like ChatGPT can answer basic concepts and provide advice on potential issues, implementing effective cybersecurity strategies requires a deeper level of expertise and hands-on experience. It is crucial to recognize that theoretical knowledge is only one aspect of cybersecurity, and applying that knowledge in practical scenarios is an entirely different challenge.

In this study, the valuable role that ChatGPT can play in helping cybersecurity professionals is acknowledged. It can streamline information retrieval, generate reports, and offer suggestions based on a vast database of knowledge. However, the practical implementation of cybersecurity strategies involves complex decision-making, real-time problem-solving, and a nuanced understanding of an organization’s specific context and needs.

Cybersecurity is an inherently dynamic field, where threats continuously evolve, and attackers employ increasingly sophisticated techniques. Human expertise is indispensable in interpreting and responding to these threats. Professionals must leverage their experience, intuition, and critical thinking to develop and implement robust security measures that address current and emerging risks. In addition, effective cybersecurity strategies require coordination across various organizational levels and functions. It involves collaboration between IT departments, management, and external stakeholders to ensure complete protection. This level of coordination and integration goes beyond the capabilities of any single tool or model.

In light of these considerations, this article emphasizes that while ChatGPT and similar LLMs can enhance the capabilities of cybersecurity professionals, they are not a replacement for human expertise. Instead, they should be viewed as supplementary tools that support and enhance the efforts of skilled practitioners. By providing quick access to information and generating preliminary insights, ChatGPT allows professionals to focus on more strategic and high-value tasks that require human judgment and expertise. The discussion has been expanded to highlight the distinction between theoretical knowledge and practical application, underscoring the importance of hands-on experience and the irreplaceable value of human expertise in cybersecurity. The goal is to present a balanced view that acknowledges the benefits of AI tools while recognizing their limitations in the practical implementation of cybersecurity strategies.

Summary:

In summary, our analysis using the Technological Displacement theory on ChatGPT’s long-term impact on cybersecurity revealed the inevitable potential for job losses, skill obsolescence, labor market shifts, and mixed socioeconomic impacts on society. The importance of preparing for these changes was highlighted, emphasizing the need to invest
in upskilling, reskilling, and job reinvention to mitigate potential negative outcomes and foster a sustainable and inclusive labor market.

6.7. Limitations of This Study

This empirical cybersecurity study has limitations that may affect the scope and applicability of its findings. First, it omits the managerial aspects of cybersecurity jobs, which could lead to an incomplete understanding of the skills required for success. Second, it does not cover the full range of cybersecurity roles, limiting the study’s representativeness of the broader industry. Lastly, the study does not consider factors such as 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 prepare before its mass adoption.

7. Conclusions

Our empirical study has found that ChatGPT has exhibited great potential to streamline and optimize many parts of non-managerial cybersecurity jobs and can perform well on cybersecurity certification exams that mainly test memorizing knowledge. Key findings include ChatGPT’s ability to automate routine tasks, its limitations in critical thinking, and the necessity for a shift from memorization to critical thinking in education and certifications. Proper augmentation of LLMs like ChatGPT with the existing cybersecurity workforce can potentially alleviate the skill shortage and help the workforce make better cybersecurity decisions. However, there may be 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. Furthermore, LLMs such as ChatGPT have the potential to displace cybersecurity jobs by causing job losses, skill obsolescence, labor market shifts, and mixed socioeconomic impacts on society in the long term. Ultimately, the impact of LLMs such as ChatGPT on the cybersecurity job market is still uncertain and will likely require ongoing discussions and collaboration between industry leaders, policymakers, and cybersecurity professionals to ensure a smooth and equitable transition. In this study, the study specifically targeted cybersecurity educational institutions. However, the findings and results of this study could be applied to other educational domains, such as medicine, mathematics, commerce, and the arts with adaptation.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable

Informed Consent Statement: Not applicable

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

Acknowledgments: I would like to extend my heartfelt thanks to Khandakar Ahmed, Email: khandakar.ahmed@vu.edu.au and Hua Wang, Email: hua.wang@vu.edu.au of the College of Engineering and Science at Victoria University. Their guidance and mentorship were invaluable throughout the course of my doctoral studies, providing critical insights while respecting my independent approach to both my research and the development of my manuscript. Their support helped to facilitate a research environment that encouraged personal growth and autonomy. I am also grateful for the administrative and technical support received from Victoria University, which was instrumental in my academic endeavors.

Conflicts of Interest: Author Raza Nowroz is employed by the untapped Holdings Pty Ltd. The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.
Abbreviations
The following abbreviations are used in this manuscript:

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

References

7. Sai, S.; Yashvardhan, U.; Chamola, V.; Sikdar, B. Generative ai for cyber security: Analyzing the potential of chatgpt, dall-e and other models for enhancing the security space. *IEEE Access* 2024, 12, 53497–53516. [CrossRef]


17. Truong, T.C.; Diep, Q.B.; Zelinka, I. Artificial intelligence in the cyber domain: Offense and defense. *Symmetry* 2020, 12, 410. [CrossRef]


Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.