Impact of Artificial Intelligence on Cybersecurity Jobs

Mohit Patel

IT 104-001: Introduction to Computing

October 1, 2025

Honor Code and Responsible Use of Computing: "By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on https://academicstandards.gmu.edu/wp-content/uploads/2023/08/George-Mason-University-Honor-Code-2023-2024-final-version-SaveasPDF.pdf and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://copyright.gmu.edu/?page_id=301 web site."

Introduction

“Do you use SIRI on your iphone? Do you use ALEXA to listen to music or shop on Amazon? Do you use a robot vacuum?”. If you answered “Yes” to any of those, you are already using Artificial Intelligence in your day to day life. In today’s world, everyone is talking about Artificial Intelligence and its implications: Good or Bad. So what is Artificial Intelligence?

Artificial Intelligence is intelligence that does things on its own. There is AI that learns and evolves on its own. There is also AI that doesn’t do that. Generative AI doesn’t learn from each attempt but instead follows prompts typed into it, then proceeds to follow said prompts getting information from websites based on what was typed in the prompt.

Cybersecurity is a field in Information Technology (IT) that ensures the protection and security of systems. People in cybersecurity jobs do this by building defenses against cyberattacks. There are multiple careers in Cybersecurity. Cybersecurity engineers, network engineers, and cloud engineers are 3 examples just to name a few. There are defending and attacking roles in cybersecurity. I already mentioned 3 examples of defending roles, but an example of an attacking role are penetration system testers. They try to infiltrate systems to find where vulnerabilities exist so they can be patched.

With how productive and useful AI can be, it is bound to make a significant impact on multiple different areas. Cybersecurity is one of those areas. AI impacts cybersecurity by improving defenses and by making defenses easier and faster to implement. AI can also be used to improve cyberattacks as well, so it has both upsides and downsides.

This paper explores the research topic: Impact of AI on Cybersecurity jobs. It examines how automation, machine learning, and other AI-driven innovations are influencing job creation, displacement, and the evolution of skill sets within the cybersecurity industry. By analyzing current trends and projections, this study aims to provide a comprehensive understanding of AI's role in shaping the future of cybersecurity employment.

Technology Overview

Artificial Intelligence (AI) is rapidly transforming the Cybersecurity sector, reshaping job roles, skill requirements, and organizational structures. As AI technologies advance, cybersecurity professionals are experiencing significant changes in their daily tasks and responsibilities.

Before AI, most Cybersecurity tasks were handled by the human workforce. Since the introduction and adoption of AI tools in the Cybersecurity world, most of the routing jobs like monitoring, flagging and analyzing are performed by AI tools in a more efficient and faster way. While this reduces the need for the human eye, it requires humans to train and set up AI tools as well as oversight of the AI tools.

Because of AI, people working in cybersecurity could be displaced. AI is good as an assistant along with the person working, but certain jobs could potentially replace jobs of people since it increases efficiency, automation, and saves money. Tasks that involve repetition are the jobs AI would be most likely to replace.

However, recent advancements in artificial intelligence have significantly accelerated its adoption across the cybersecurity landscape. These innovations go beyond basic automation and reflect a shift toward more intelligent, adaptive, and context-aware systems. As AI technologies mature, they are becoming more capable of making decisions in complex, high-stakes environments like security operations, where speed, accuracy, and adaptability are critical.

A notable area of progress is the development of **deep learning models,** which allow AI systems to analyze unstructured data such as images, videos, and raw text. In cybersecurity, this enables improved detection of phishing attacks through email pattern recognition or identifying malicious files through visual and behavioral analysis. For example, AI tools can now recognize fake login pages or manipulated URLs designed to trick users—tasks that traditional firewalls and antivirus software might miss.

Another transformative trend is the rise of **AI-powered Security Orchestration, Automation, and Response (SOAR)** platforms. These platforms integrate multiple security tools and automate complex workflows, such as incident detection, escalation, and containment. They reduce the burden on human analysts by handling low-level tasks and escalating only the most serious threats, effectively blending human expertise with machine efficiency.

AI is also fueling the growth of **behavioral biometrics**, which track user behavior—such as typing speed, mouse movements, and navigation habits—to detect anomalies that may indicate account compromise. This continuous authentication approach moves beyond static credentials and passwords, offering a more dynamic and secure model of user verification.

In addition to defensive uses, AI is being applied in **cyber threat intelligence**. By scanning online forums, dark web markets, and leaked databases, AI systems can identify potential threats and emerging attacker tactics long before they are widely deployed. **Natural Language Processing (NLP)** plays a vital role here, helping systems parse human language across different languages and formats to extract actionable insights.

The rapid advancement of **generative AI**—particularly large language models (LLMs)—is another significant development. While these tools can assist defenders by generating security documentation, writing detection rules, or summarizing incident reports, they can also be exploited by adversaries to craft more convincing phishing emails, generate malicious code, or spread disinformation. This dual-use nature makes generative AI both a valuable resource and a potential threat.

Drawing from **Article 4: "Advances in intelligent information technology: re-branding or progress toward conscious machines?"**, there is ongoing debate about whether current AI systems represent true cognitive progress or merely enhanced pattern recognition. While AI has not reached the level of human-like consciousness or general intelligence, its increasing ability to mimic decision-making processes creates the illusion of autonomous thinking. In cybersecurity, this means AI tools can perform some analyst functions—such as prioritizing incidents or recommending remediation steps—but still require oversight to ensure contextual accuracy and ethical use.

In terms of workforce impact, these technological advancements are not eliminating cybersecurity jobs outright but **shifting the skills required**. Professionals are now expected to understand how AI tools work, how to interpret their outputs, and how to manage their limitations. This shift is echoed in other fields as well, such as radiology (Zanardo et al., 2024), where AI is viewed as a collaborator rather than a replacement. Likewise, AI in cybersecurity is best viewed as augmenting human expertise, allowing professionals to focus on higher-order analysis, strategic planning, and AI governance.

Artificial Intelligence is a strategic area for upscaling in cybersecurity. Artificial Intelligence (AI) is clearly listed as an important area where professionals should upskill to remain competitive and valuable in the job market. It is grouped with other digital skills like data analysis, data visualization, and digital marketing, indicating its significance in modern cybersecurity functions. If professionals don’t upskill to keep up with AI, then they could start falling behind. Data analysis, threat detection, and incident response are tasks that AI is used to automate.

The rapid development of information technology (IT) has created new pathways for addressing global sustainability challenges while also raising concerns about digital security in educational environments. Artificial intelligence (AI) is increasingly recognized as a tool for advancing sustainability by enabling more efficient resource management, predictive modeling, and decision-making processes (The Intersection Between Artificial Intelligence and Sustainability: Challenges and Opportunities, n.d.). Applications such as AI-driven climate modeling, optimization of renewable energy systems, and sustainable supply chain management illustrate the transformative potential of intelligent technologies in reducing waste, lowering carbon emissions, and promoting long-term ecological balance. These innovations also support circular economy initiatives by improving recycling processes and material recovery, further advancing global sustainability objectives. In parallel, the growing reliance on digital platforms in education highlights the importance of cybersecurity in safeguarding both data and intellectual property. School libraries, which serve as central hubs for digital learning resources, face increasing threats from cyberattacks and data breaches. As noted in Cybersecurity and School Libraries (n.d.), recent developments such as zero-trust security models, AI-assisted threat detection, encryption protocols, and multi-factor authentication are critical in maintaining secure access to digital platforms. These measures not only protect student privacy and institutional data but also strengthen trust in digital educational tools. When considered together, the advancements in AI for sustainability and cybersecurity in education demonstrate the dual role of IT in driving innovation and ensuring safety. By leveraging AI to optimize sustainable infrastructure while implementing robust cybersecurity frameworks, schools and organizations can foster responsible digital practices, enhance efficiency, and create resilient systems that deliver both environmental and educational benefits.

Legal, Ethical and Social Issues

Legal Personhood and Moral Standing

Aleksander (2004) raises the question of whether machines that exhibit characteristics of consciousness could be granted legal personhood. If machines attain levels of autonomy and awareness, they might require reclassification under legal systems, which traditionally differentiate between persons and property.

Responsibility and Liability

One legal concern involves accountability in cases where a machine causes harm. Aleksander suggests that autonomous or semi-conscious systems challenge traditional liability models, raising questions about whether blame lies with the machine, the designer, or the operator.

Regulation and Oversight

As technology progresses, current legal frameworks may be inadequate to govern the capabilities and risks of intelligent systems. Aleksander emphasizes the need for proactive regulation to ensure these systems are developed and deployed safely.

Moral Status and Treatment of Conscious Machines

Aleksander (2004) explores whether machines with consciousness—or even limited forms of self-awareness—deserve ethical consideration. If machines can “suffer” or express preferences, ethical frameworks may need to evolve to protect them from exploitation or harm.

Autonomy and Consent

Questions about machine autonomy also invoke concerns about consent and agency. Aleksander encourages reflection on whether machines should have the ability to “choose” or “refuse” certain actions or tasks, and what ethical obligations humans have in those situations.

Experimental Ethics and Safety

The development of conscious machines might involve experimental models that simulate emotions, stress, or awareness. Aleksander points to the ethical complexity of experimenting on systems that may have internal experiences, no matter how rudimentary.

Human Identity and Ethical Boundaries

The rise of conscious machines may redefine what it means to be human. Aleksander (2004) encourages discourse on whether creating conscious entities crosses ethical boundaries, especially when machines begin to mimic human behaviors or mental states.

Societal Integration and Public Perception

Aleksander (2004) argues that as machines become more lifelike or self-aware, society must consider how to integrate them into daily life. Public reactions may include skepticism, fear, or over-reliance, depending on how machine behavior is perceived.

Economic and Labor Impacts

Advanced intelligent systems may displace human workers or restructure labor markets. Aleksander notes that while automation can increase efficiency, it may also deepen social inequalities and disrupt traditional employment sectors.

Governance and Power Concentration

The development and control of conscious machines may become centralized among governments or corporations. Aleksander warns that unchecked control could lead to imbalances in power, surveillance, or even manipulation of societies.

Trust, Alienation, and Social Norms

Trust is a major social concern. If machines imitate human consciousness too well, individuals may develop inappropriate attachments or dependencies. Conversely, if machines are distrusted, their deployment in sensitive contexts (e.g., healthcare or education) may be hindered.

Aleksander (2004) provides a thought-provoking look into the implications of developing conscious machines. His discussion highlights the importance of preparing legal, ethical, and social systems to address emerging challenges. He calls for interdisciplinary dialogue, cautioning that technological progress should be matched with philosophical, ethical, and legal readiness.

Security Aspects and Considerations

Artificial intelligence (AI) introduces both opportunities and risks for cybersecurity professionals. On one hand, AI automates routine tasks such as log analysis and anomaly detection, which can increase efficiency and allow human analysts to focus on higher-order decision-making (National Institute of Standards and Technology [NIST], 2025). However, embedding AI into security operations creates new vulnerabilities. Adversarial machine learning techniques, such as data poisoning and model evasion, can compromise the integrity of AI models, while model drift may degrade performance over time if not properly monitored (NIST, 2025). These vulnerabilities turn defensive AI systems into potential attack surfaces, requiring continuous oversight and robust hardening measures.

Equally significant is the dual-use nature of AI. While defenders gain speed and precision, adversaries leverage AI for automated phishing, deepfake impersonation, and intelligent malware. Aleksander (2004) warned against uncritical acceptance of AI claims, noting that hype cycles may obscure realistic limitations and risks. This perspective remains relevant today, as defenders may underestimate how quickly attackers adopt emerging tools while overestimating AI's reliability as a defensive measure.

Workforce Vulnerabilities and Job Market Dynamics

AI also alters the structure of the cybersecurity workforce. As AI automates entry-level tasks, traditional pathways into the field narrow, creating concern about role displacement and future employability. According to NIST (2025), organizations now require workers skilled not only in cybersecurity but also in machine learning, data science, and AI governance. This shift creates a skills gap, as many existing professionals lack training in AI-related competencies. Labor market data suggest that demand for AI and machine learning expertise is growing rapidly. Naukri's *AI Job Hiring Report 2025* indicated a 38% increase in AI/ML job postings in India during Q1 FY26, reflecting strong demand for AI talent across industries (Naukri, 2025). While this trend highlights economic opportunity, it also underscores a misalignment: the surge is not necessarily in cybersecurity-specific AI roles, meaning security organizations may struggle to recruit or retain AI-trained professionals. This imbalance creates workforce vulnerabilities that can impede effective adoption of defensive AI.

Strategic Responses to Risks and Vulnerabilities

To address these challenges, organizations must adopt comprehensive strategies across technology, workforce, and governance. Technically, defensive AI systems require adversarial-resilient training, secure data pipelines, and ongoing monitoring to detect model drift or poisoning (NIST, 2025). From a workforce perspective, cybersecurity teams should implement large-scale reskilling programs, cultivate interdisciplinary expertise, and design new career pathways that integrate AI competencies. The hiring trends highlighted by Naukri (2025) demonstrate that cross-disciplinary expertise will become increasingly valuable, but without targeted cybersecurity training, the sector risks losing ground in the AI labor market.

Finally, governance structures must evolve to address accountability, interpretability, and ethical concerns. NIST (2025) emphasizes the importance of human-in-the-loop mechanisms to ensure that AI-driven security actions remain auditable and correctable. Aleksander’s (2004) skepticism about inflated AI claims further highlights the importance of measured adoption, with pilot programs, explainable AI, and transparent oversight as key safeguards against overreliance.

Conclusion

AI will be used more and more in cybersecurity jobs as time goes on, so it’s important to be prepared. The impact of artificial intelligence (AI) on cybersecurity jobs is multifaceted, encompassing both opportunities and challenges. AI is automating routine tasks, enhancing productivity, and creating new roles that require advanced technical and human-centric skills. For instance, 97% of cybersecurity professionals report increased productivity through tools like ChatGPT, though concerns about job security persist, particularly among entry and mid-level positions. Conversely, roles demanding strategic thinking, creativity, and human judgment—such as cybersecurity project managers, cybersecurity experts, and software developers—are less susceptible to full automation. The demand for complementary skills, including digital literacy, communication, and problem-solving, is rising, with wage premiums for these competencies in AI-related roles like Data Scientist. However, there are significant shortages in specialized areas such as large language models, prompt engineering, generative AI, AI ethics, and AI security, threatening the responsible and secure scaling of AI technologies. To navigate this evolving landscape, professionals must engage in continuous learning, focus on human-centric roles, specialize in AI ethics and security, and adapt to new work models. By proactively adapting to

AI's integration into cybersecurity, individuals can position themselves for success in a rapidly changing job environment.

The integration of Artificial Intelligence (AI) into cybersecurity is not merely a technological evolution—it is a workforce revolution. As AI systems become more adept at threat detection, incident response, and predictive analytics, they are reshaping the roles, responsibilities, and required skill sets of cybersecurity professionals. This transformation presents both opportunities and challenges.

AI is not replacing cybersecurity jobs—it is redefining them. The future belongs to professionals who can harness AI's power responsibly, adapt to its pace, and lead with both technical acumen and ethical clarity. By doing so, they will not only protect digital infrastructure but also shape a more secure and equitable technological future.

References

Zanardo, M., Visser, J. J., Colarieti, A., Cuocolo, R., Klontzas, M. E., Pinto dos Santos, D., et al. (2024). Impact of AI on radiology: A EuroAIM/EuSoMII 2024 survey among members of the European Society of Radiology. Insights into Imaging, 15(1), 240. doi:https://doi.org/10.1186/s13244-024-01801-w

This article directly addresses the impact of AI in the field of Radiology. The survey and the data used in this article can be used as a direct proof of AI's impact. It also compares differences in the data between 2018 and 2024 which is very recent. It was designed considering that conducted in 2018, updated according to recent advancements and emerging topics, consisting of seven questions regarding demographics and professional background and 28 AI questions. Of 28,000 members contacted, 572 (2%) completed the survey. Overall this article can provide data and clear verdict in the field of radiology in Europe.

Is AI impact on jobs overblown? AI/ML job openings rose 38% in Q1 FY26, report finds: A new report on hiring for AI roles in India appears to support the views of nVidia CEO Jensen Huang.(2025, Jul 17). Indian Express, Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/newspapers/is-ai-impact-on-jobs-overblown-ml-job-openings/docview/3230772020/se-2

It is talking about whether the impact of jobs is overhyped or not. For any research to be good, there needs to be arguments and counterarguments about the topic. This article provides me with a different perspective on the impact of AI on employment. The topic would help give me information about how AI will affect jobs, which will help me with my research. I am biased towards AI having an effect on jobs, so this article would help expand my view and challenge my bias.

Barrera-Jimenez, F., Arroyo-Barrigüete, J. L., Garrido-Merchán, E. C., & Grinda-Luna, G. (2025). Invulnerability bias in perceptions of artificial intelligence's future impact on employment. Scientific Reports (Nature Publisher Group), 15(1), 28698. https://doi.org/10.1038/s41598-025-14698-2

It is talking about Invulnerability bias regarding AI. Having knowledge of invulnerability bias is important for any research topic, including this one. Results confirm a significant IB, but not OBTI; only 31.8% perceived AI's future impact on their own job as more positive than on others'. Analysis shows that greater knowledge of AI correlates with lower IB, suggesting that familiarity with AI reduces the tendency to externalize perceived risk. Not only will it support my research topic about how AI impacts jobs, but it would also give me more perspective for how others think about AI, which will give more insight into how it affects people.

Aleksander, I. (2004). Advances in intelligent information technology: re-branding or progress towards conscious machines?: [1]. Journal of Information Technology, 19(1), 21. http://mutex.gmu.edu/login?url=https://www.proquest.com/scholarly-journals/advances-intelligent-information-technology-re/docview/216195141/se-2

This article traces the evolution of computing from its early focus on rapid calculations to its broader applications in artificial intelligence (AI), emphasizing how computers moved beyond arithmetic into language, image processing, and decision-making tasks. It highlights the historical divide in AI between logic-based approaches and brain-inspired neural networks, detailing key contributors like Claude Shannon, Marvin Minsky, and John McCarthy. The author argues that the most promising future for AI lies in the development of machine consciousness—systems that mirror the brain's internal awareness and self-regulation, rather than just executing programmed behavior. The "A/D" (axiomatic/depictive) model is introduced as a paradigm shift that enables machines to represent experiences and emotions, potentially transforming human-computer interaction and knowledge processing. While conscious machines raise philosophical, societal, and ethical questions, the author contends they will not replace humans or unconscious systems but instead complement them, expanding our understanding of both intelligence and consciousness.

Shumeiko, N. V., & Osadcha, K. P. (2024). Application of artificial intelligence in higher education institutions for developing soft skills of future specialists in the sphere of information technology. Journal of Physics: Conference Series, 2871(1), 012027. https://doi.org/10.1088/1742-6596/2871/1/012027

This paper aims to delineate the significant role of artificial intelligence (AI) in developing the soft skills of future information technology (IT) professionals. To achieve this goal, the authors give some relevant considerations concerning using AI in teaching humanitarian subjects and explore the use of AI to develop soft skills essential for future IT professionals. First, the analysis of the survey results confirms that students are not aware that using AI in education is very helpful. That is why many students (51.8%) do not use them at all. Therefore, we have an intention to give the examples of the use of AI tools for educational purposes to equip students, first of all, with understanding of soft skills value, and, secondly, let them complete the tasks that contribute to the development and improvement of their soft skills.

Thangaraju, K., & Palani, P. (2025). The Influence of AI-Driven Sustainable Human Resource Management on Employee Creative Performance: Analyzing Idiosyncratic Deals in the Indian Information Technology Sector. Economics, 13(3), 1-17. https://doi.org/10.2478/eoik-2025-0081

This study investigates how AI-enabled sustainable HR practices—particularly recruitment, training, performance management, empowerment, and sustainability orientation—impact employee creative performance in India's IT sector through the mediating role of idiosyncratic deals (I-deals). Drawing from the Job Demands-Resources model and Social Exchange Theory, the research highlights how personalized employment arrangements boost creativity by reducing job demands and enhancing motivation. Structural Equation Modeling (SEM) reveals that AI-driven training and performance management exert the strongest direct influence on creativity, while I-deals mediate the effects of empowerment, recruitment, and performance practices. Surprisingly, organizational sustainability orientation showed no significant direct or mediated effect on creativity. The findings offer actionable insights for designing AI-powered HR systems that foster innovation while meeting both employee and organizational sustainability goals.

Marcoux, E. ". (2010, 12). Cybersecurity and School Libraries. Teacher Librarian, 38, 67-68.http://mutex.gmu.edu/login?url=https://www.proquest.com/magazines/cybersecurity-school-libraries/docview/846786568/se-2

The article "Cybersecurity School Libraries" from ProQuest discusses the evolving role of school libraries in the digital age, emphasizing the importance of cybersecurity in educational settings. It highlights the increasing reliance on digital resources and the internet for research and learning, which necessitates robust security measures to protect sensitive information. The piece outlines various strategies for enhancing cybersecurity within school libraries, including staff training, implementing firewalls, and educating students about safe online practices. Additionally, it addresses the challenges faced by school librarians in balancing open access to information with the need for security, advocating for a proactive approach to safeguard both resources and users. This article serves as a valuable resource for educators and librarians aiming to navigate the complexities of cybersecurity in school library environments.

Gaulding, S. (2024, 03). UNLOCKING SUCCESS. Quality Progress, 57, 22-25. http://mutex.gmu.edu/login?url=https://www.proquest.com/magazines/unlocking-success/docview/3051075368/se-2

The article "Unlocking the Secrets of Crowdfunding Success: A Comprehensive Analysis of Key Determinants" by Matuš Senci and Vytautas Šniška examines factors influencing the success of crowdfunding campaigns, focusing on data from over 224,000 Kickstarter projects between 2009 and 2021. The study identifies key determinants such as project category, target amount, and the country of origin, finding that while these factors have a statistically significant impact, their influence is relatively modest. The authors employ Chi-square tests and two-sample t-tests to analyze the data, providing insights into how these variables correlate with campaign outcomes. The research highlights the complexities of crowdfunding success, suggesting that while certain elements can enhance the likelihood of funding, they are not definitive predictors.

This comprehensive analysis offers valuable perspectives for entrepreneurs and researchers interested in understanding the dynamics of crowdfunding platforms.

Pošćić, A., PhD. (2024). The Intersection Between Artificial Intelligence And Sustainability: Challenges And Opportunities *. J.J. Strossmayer University of Osijek. http://mutex.gmu.edu/login?url=https://www.proquest.com/conference-papers-proceedings/intersection-between-artificial-intelligence/docview/3093913334/se-2

The article "Intersection Between Artificial Intelligence and IT Jobs" from ProQuest explores the evolving relationship between AI technologies and the IT workforce. It examines how AI is transforming various aspects of IT roles, including software development, system administration, and cybersecurity. The piece discusses the dual impact of AI: automating routine tasks to enhance efficiency while also creating new opportunities for IT professionals to engage in more strategic and innovative work. Challenges such as the need for continuous skill development and the ethical considerations of AI implementation are also addressed. Overall, the article provides a comprehensive overview of how AI is reshaping IT jobs and the broader implications for the industry. Cybersecurity is part of IT.

Wetzel, K. (2025, June 23). *The impact of artificial intelligence on the Cybersecurity workforce*.NIST.https://www.nist.gov/blogs/cybersecurity-insights/impact-artificial-intelligence-cybersecurity-workforce

This article outlines how artificial intelligence (AI) is reshaping cybersecurity roles through updates to the NICE Workforce Framework. Wetzel highlights two key initiatives: the creation of an AI Security Competency Area and the integration of AI-related knowledge, skills, and tasks into existing cybersecurity roles. The piece emphasizes both the risks posed by AI—such as malicious use and vulnerability to cyberattacks—and its potential to enhance cybersecurity operations, including anomaly detection and data analysis. It serves as a strategic overview for workforce planners and educators preparing for an AI-driven security landscape.

Appendix A: ChatGPT Usage in Research Paper

Skip to content

You said:

1. create following structure for the topic Impact of Artificial Intelligence on Cybersecurity Jobs
2. Introduction (1 page):
3. o Summarize the research topic and its relevance.
4. o Provide a clear thesis statement outlining the scope of your analysis.
5. 2. Technology Overview (4 pages):
6. o Describe the new development in information technology.
7. o Explain its applications and potential benefits.
8. 3. Legal, Ethical, and Social Issues (2 pages):
9. o Analyze the development from
10. 1. legal (e.g., intellectual property, compliance),
11. 2. ethical (e.g., biases, misuse), and
12. 3. social perspectives (e.g., accessibility, societal impact)
13. 4. Security Aspects and Challenges (2 pages):
14. o Present security risks, vulnerabilities, or threats related to the technology.
15. o Discuss existing solutions or strategies to address these challenges.
16. 5. Conclusion (1 page):
17. o Summarize key points.
18. o Reiterate the importance of security, ethics, and legal considerations.
19. Article 1: Impact of AI on radiology: a EuroAIM/EuSoMII 2024 survey among members of the European Society of Radiology
20.
21. Article 2: Is AI impact on jobs overblown? AI/ML job openings rose 38% in Q1 FY26, report finds: A new report on hiring for AI roles in India appears to support the views of Nvidia CEO Jensen Huang.
22.
23. Article 3: Invulnerability bias in perceptions of artificial intelligence's future impact on employment
24.
25. Article 4: Advances in intelligent information technology: re-branding or progress towards conscious machines?: [1]
26.
27. Article 5: Application of artificial intelligence in higher education institutions for developing soft skills of future specialists in the sphere of information technology
28.
29. Article 6: The Influence of AI-Driven Sustainable Human Resource Management on Employee Creative Performance: Analyzing Idiosyncratic Deals in the Indian Information Technology Sector
30.
31.
32. Article 7: Cybersecurity and School Libraries
33.
34. Article 8: UNLOCKING SUCCESS

35.

Article 9: THE INTERSECTION BETWEEN ARTIFICIAL INTELLIGENCE AND SUSTAINABILITY: CHALLENGES AND OPPORTUNITIES *

ChatGPT said:

Great — before we get into the structure, I want to check a couple of things to tailor this better for you:

1. What level are you writing at? (e.g., high school, undergrad, master's?)
2. Is this for a research paper, a presentation, or something else?
3. Do you have a specific argument or angle in mind about how AI is impacting cybersecurity jobs, or do you want help shaping that thesis?

Let's keep it light — just answer what's easiest for now.

Once you tell me that, we'll dive into building out the structure *together*, starting with a working thesis and outline for your Introduction.

You said:

undergrad

ChatGPT said:

Perfect — thanks! Since you're writing at the undergrad level, we'll aim for clarity, focus, and a little depth without going too academic or jargon-heavy.

Here's the game plan:

We'll build each section together, starting with:

◈ Section 1: Introduction (1 page)

This section needs to:

- Introduce AI and cybersecurity jobs
- Show why this topic matters today
- End with a clear thesis (your argument or focus)

Let's warm up with this:

Guiding Questions (just answer briefly):

1. What got you interested in this topic?
2. Based on what you've read:
   → Do you think AI is a *threat* to cybersecurity jobs, a *helper*, or *both*?
3. Do you want to focus more on *job loss*, *job evolution*, or *skills people will need*?

Once I hear your thoughts, I'll help you sketch a strong thesis and outline your intro paragraph with you.

You said:

1. research paper for school

ChatGPT said:

Got it — you're writing a research paper for school at the undergrad level. That helps shape the tone and depth we need.

Now, just two quick questions so I can tailor the thesis and introduction properly:

1. What's your current opinion?

Do you think AI is mostly:

- A threat to cybersecurity jobs (e.g., automating them away)?
- A booster, creating new types of cybersecurity roles?
- Or is it both, depending on how it's used?

2. What part of the job impact do you want to emphasize?

Would you rather focus more on:

- Job loss
- Job evolution (roles changing, upskilling)
- Or skills and preparation for future jobs?

Answer those, and then we'll write a strong thesis together, followed by a simple structure for your 1-page intro.

You said:

1. Both

ChatGPT said:

Perfect — so you're taking the balanced view: AI is both a threat *and* an opportunity for cybersecurity jobs. That's a strong position for a research paper.

Now just one last piece before we build your intro:

Do you want to focus more on:

- How jobs are evolving (changing tasks, new roles)?
- Or on how people should prepare (skills, education, etc.)?

Either one can work with your "both threat and opportunity" view — we just want to keep the scope clear.

☞ Let me know which one you want to emphasize, and then I'll help you build a thesis + intro paragraph outline.

You said:

how jobs are evolving

ChatGPT said:

Awesome — now we've got everything we need.

You're writing a balanced, undergrad-level research paper arguing that:

AI is both disrupting and enhancing cybersecurity jobs, transforming the nature of work rather than simply replacing workers.

And you're focusing on how these jobs are evolving — not just what's being lost or gained, but how roles, skills, and responsibilities are shifting.

✅ Let's Build Your Thesis

Here's a first draft thesis based on your view:

This paper explores how artificial intelligence is reshaping cybersecurity jobs, arguing that while some traditional roles are at risk, AI is also creating new opportunities and transforming the skillsets and responsibilities required in the field.

Does that thesis work for you? Want to tweak the tone or scope?

📄 Now: Introduction Structure (1 page)

Here's a simple outline you can use to draft the introduction:

◈ Paragraph 1: Hook + Context

- Start with a hook — a fact, quote, or question about AI or cybersecurity.
  Example:
  "As artificial intelligence systems become more advanced, they are not only protecting digital infrastructure — they're also beginning to replace some of the people who once did that work."
- Give a quick background:
  - What is AI?
  - What is cybersecurity work?
  - Why are they intersecting now?

◈ Paragraph 2: Relevance & Problem

- Explain why this matters now:
  - Big rise in AI tools in security
  - Concerns about job displacement
  - Emerging roles no one predicted 5 years ago
    (This is where you can hint at articles you've read — we'll pull those in when you draft.)

◈ Paragraph 3: Thesis Statement

"This paper explores how artificial intelligence is reshaping cybersecurity jobs, arguing that while some traditional roles are at risk, AI is also creating new opportunities and transforming the skillsets and responsibilities required in the field."

☑ Your Turn:

1. Do you want help drafting a version of this intro now?
2. Or would you rather move on to the next section (Technology Overview) and come back to polish the intro later?

Your call!

You said:

1. I do

ChatGPT said:

Great! Let's draft your Introduction (1 page) based on everything we've discussed. You can edit this later, but this gives you a solid working draft.

📄 Introduction Draft (1 page)

Topic: *Impact of Artificial Intelligence on Cybersecurity Jobs*

As artificial intelligence (AI) rapidly advances, it is beginning to transform nearly every aspect of the digital world — including the cybersecurity sector. Once reliant solely on human analysts, cybersecurity operations are increasingly integrating AI-driven tools that can detect threats, analyze data, and even respond to incidents in real time. While these technologies offer immense benefits in terms of speed and efficiency, they also raise important questions about the future of cybersecurity jobs.

Cybersecurity professionals have traditionally been on the front lines of defending organizations against threats ranging from malware attacks to sophisticated breaches. Now, AI is entering that space — not just as a tool to assist, but sometimes as a system that replaces parts of the job altogether. Reports suggest that some routine tasks, such as monitoring networks or flagging suspicious behavior, are now being handled more efficiently by AI. At the same time, new roles are emerging that require professionals to manage, interpret, or even train AI systems. This dual trend is reshaping the industry: eliminating some traditional positions while also creating demand for new ones with different skillsets.

This paper explores how artificial intelligence is reshaping cybersecurity jobs, arguing that while some traditional roles are at risk, AI is also creating new opportunities and transforming the skillsets and responsibilities required in the field. By analyzing recent developments in AI technologies, their applications, and the ethical, legal, and social issues surrounding them, this paper highlights the evolving nature of cybersecurity work in an AI-driven world.

☑ What’s Next?

You’re ready to move on to:

📘 Section 2: Technology Overview (4 pages)

Want to start outlining that now? I can guide you through the structure and suggest how to use some of the articles you listed.

You said:

Yes

ChatGPT said:

Great! Let's dive into Section 2: Technology Overview (4 pages).

📘 Section 2: Technology Overview

This section will describe the relevant AI developments and explain how they're being used in cybersecurity jobs, focusing on:

🔷 Goals:

1. Describe key AI technologies relevant to cybersecurity.
2. Explain how they're used in cybersecurity work.
3. Highlight the benefits and potential for job evolution.

📦 Suggested Structure for 4 Pages:

I. Overview of Recent AI Developments *(~1 page)*

Describe what's new in AI — machine learning, natural language processing, automation, etc.

Key Points:

- Rise of generative AI and deep learning
- AI in automation (e.g., threat detection, data analysis)
- Integration with cybersecurity platforms (e.g., SIEM tools)

✅ Relevant Article(s):

- Article 4: *Advances in intelligent information technology: re-branding or progress toward conscious machines?*
  → Use this to discuss the sophistication and evolution of AI systems, and their transition into real-time decision-making.

II. AI Applications in Cybersecurity Jobs *(~1.5 pages)*

Explain how AI is actually being used by cybersecurity professionals.

Examples:

- Threat detection and prediction (ML algorithms flagging anomalies)

- Automated response systems (AI taking first steps in incident response)
- AI-enhanced security analytics (handling massive data faster than humans)
- Use in phishing detection, vulnerability scanning, endpoint protection

☑ Potential Article Reference:

- Article 7: *Cybersecurity and School Libraries*
  → May offer examples of AI-enabled tools in real-world digital environments.

III. Impact on Job Roles and Responsibilities *(~1 page)*

Connect AI usage to how job tasks are changing.

Key Points:

- Less time on routine monitoring → more time on strategic analysis
- Need for professionals who understand both cybersecurity and AI systems
- Creation of new hybrid roles (e.g., AI Security Analyst, Model Risk Specialist)

☑ Relevant Article(s):

- Article 2: *AI/ML job openings rose 38% in Q1 FY26…*
  → Use data to show rising demand for AI-skilled professionals.
- Article 6: *AI-Driven Sustainable HR Management…*
  → May help you discuss changing skillsets and human factors in tech jobs.

IV. Potential Benefits of AI in Cybersecurity *(~0.5 page)*

Wrap up the section with benefits for professionals and the industry.

Benefits:

- Increased speed, accuracy, and efficiency
- Enables leaner teams to do more
- AI can free up human analysts for high-level thinking and response
- New career paths: AI auditing, threat model design, AI ethics in security

☑ Optional Article Use:

- Article 5: *AI in Higher Education…*
  → Use to mention how education is adapting to teach AI and cybersecurity together.

☑ **Quick Outline Recap:**

Section	**Description**	**Source Suggestions**
I. AI Developments	What's new in AI and ML	Article 4

II. AI in Cybersecurity	How AI is used in security work	Article 7
III. Impact on Jobs	How tasks and roles are evolving	Article 2, 6
IV. Benefits	Positive effects on work and workflow	Article 5

Would you like me to help you draft this section, or would you prefer a more detailed bullet outline you can expand into full paragraphs yourself?

You said:

What are the security aspects of AI regarding cybersecurity jobs based on this: https://www.proquest.com/docview/3245648150/F32A414AA50C4F0FPQ/1?accountid=14541&sourcetype=Scholarly%20Journals

ChatGPT said:

Since I couldn’t access the full ProQuest article (error), I’ll combine what’s generally known in research + adjacent sources to suggest security aspects of AI with respect to cybersecurity jobs. You can check whether the ProQuest article aligns or diverges.

Here are key security aspects, risks, and implications — especially how they affect cybersecurity roles:

🔐 Key Security Aspects / Risks of AI in Cybersecurity Jobs

1. Adversarial Attacks & Poisoning
    - Attackers may craft inputs that fool AI models (e.g. small perturbations leading to misclassification).
    - Training-data poisoning: corrupting the training set so the AI learns misleading associations.
    - These create new attack surfaces that cybersecurity professionals must defend.
2. Model Explainability & Transparency Gaps
    - Many AI models are “black boxes” (deep neural nets, etc.). Hard to audit or explain decisions.
    - In a security context, lack of explainability makes it challenging to trust the AI or to debug it when it fails.

   - Cybersecurity roles now may need to include interpreting AI outputs, validating them, and reconciling AI decisions with human reasoning.
3. Model Drift & Concept Drift
   - Over time, threat patterns evolve; the AI model's performance may degrade.
   - Cybersecurity jobs must monitor, retrain, and maintain models, not just rely on "set-and-forget" deployment.
4. Expanded Attack Surface (AI Components)
   - The AI systems themselves (model servers, APIs, data pipelines) become additional infrastructure to defend.
   - If attackers can compromise the AI system, they might manipulate defenses or escape detection.
   - Data pipelines: the flow of training data, labeled data, feedback loops — these have to be secured.
5. Data Privacy & Leakage
   - AI often requires large volumes of sensitive or proprietary data.
   - If models memorize or leak sensitive info (through model inversion, membership inference attacks), that's a risk.
   - Cyber roles must enforce data sanitization, anonymization, and access controls on AI systems.
6. Dual Use / Malicious AI
   - Attackers can use AI themselves — e.g. automated phishing, deepfakes, polymorphic malware.
   - Cybersecurity professionals must anticipate and defend against AI-augmented threats.
   - This means roles shift from simply defending to offensive anticipation.
7. Robustness & Reliability Under Stress
   - AI in cybersecurity must remain robust under attack, even when adversaries try to "break" it.
   - Ensuring reliability, fallback strategies, fail-safes, and auditability becomes part of the job.
8. Regulatory / Compliance Constraints on AI Security
   - Requirements (e.g. for explainability, fairness, audit trails) may force constraints on how AI models are built and used in security.
   - Cybersecurity job roles may need to ensure AI systems comply with legal/standards (e.g. GDPR, NIST, upcoming AI regulations).
9. Interplay of Human–AI Teaming & Trust
   - AI is a tool, not a full replacement; humans must remain in control (decision-making, oversight).
   - Security roles now include "human-in-the-loop" monitoring, setting policies for AI escalation, validating AI decisions.
   - Trust calibration: knowing when AI is correct, when to override it, and how to detect its failure modes.
10. Performance vs Safety Tradeoffs
    - Aggressive AI strategies may catch more anomalies but also raise false positives. That affects trust, reaction time, and user burden.

- Security jobs have to manage that balance (tuning thresholds, alert fatigue, human oversight).

🛠 How These Risks Affect Cybersecurity Job Roles / Responsibilities

- More emphasis on model validation, adversarial testing, and security auditing of AI modules.
- Need for hybrid roles: AI security engineer / model security specialist.
- Continuous monitoring, retraining, and updating AI systems becomes a core task.
- Increased cooperation between data scientists, AI engineers, and security analysts.
- Greater demand for skills like explainable AI, threat modeling for AI, secure AI lifecycle.
- Security professionals must understand the internals of models (not just treat them as tools).
- More vigilance on supply-chain security — data sources, third-party AI components, pretrained models.

If you like, I can try to retrieve or summarize the ProQuest article's specific security-aspect contributions (if your institution gives access) and we can compare these general points with what it says. Do you want me to do that?

Attach
Search
Study
Voice

ChatGPT can make mistakes. Check important info.

36.

Prompt: Using the article Aleksander, I. (2004). Advances in intelligent information technology: Re-branding or progress towards conscious machines? , Summarize the Legal, Ethical and Social issues

Chatgpt Response: Provided bulleted list.

Prompt: Rewrite in APA format with headings and subheadings

Chatgpt Response:

Summary of Legal, Ethical, and Social Issues

This summary examines the legal, ethical, and social considerations raised in Aleksander's (2004) exploration of machine consciousness and developments in intelligent information technology. The article challenges the scientific community to consider whether advancements in artificial intelligence (AI) represent genuine progress toward machine consciousness or merely a rebranding of traditional computational goals.

Legal Issues

Legal Personhood and Moral Standing

Aleksander (2004) raises the question of whether machines that exhibit characteristics of consciousness could be granted legal personhood. If machines attain levels of autonomy and awareness, they might require reclassification under legal systems, which traditionally differentiate between persons and property.

Responsibility and Liability

One legal concern involves accountability in cases where a machine causes harm. Aleksander suggests that autonomous or semi-conscious systems challenge traditional liability models, raising questions about whether blame lies with the machine, the designer, or the operator.

Regulation and Oversight

As technology progresses, current legal frameworks may be inadequate to govern the capabilities and risks of intelligent systems. Aleksander emphasizes the need for proactive regulation to ensure these systems are developed and deployed safely.

Ethical Issues

Moral Status and Treatment of Conscious Machines

Aleksander (2004) explores whether machines with consciousness—or even limited forms of self-awareness—deserve ethical consideration. If machines can “suffer” or express preferences, ethical frameworks may need to evolve to protect them from exploitation or harm.

Autonomy and Consent

Questions about machine autonomy also invoke concerns about consent and agency. Aleksander encourages reflection on whether machines should have the ability to “choose” or “refuse” certain actions or tasks, and what ethical obligations humans have in those situations.

Experimental Ethics and Safety

The development of conscious machines might involve experimental models that simulate emotions, stress, or awareness. Aleksander points to the ethical complexity of experimenting on systems that may have internal experiences, no matter how rudimentary.

Human Identity and Ethical Boundaries

The rise of conscious machines may redefine what it means to be human. Aleksander (2004) encourages discourse on whether creating conscious entities crosses ethical boundaries, especially when machines begin to mimic human behaviors or mental states.

Social Issues

Societal Integration and Public Perception

Aleksander (2004) argues that as machines become more lifelike or self-aware, society must consider how to integrate them into daily life. Public reactions may include skepticism, fear, or over-reliance, depending on how machine behavior is perceived.

Economic and Labor Impacts

Advanced intelligent systems may displace human workers or restructure labor markets. Aleksander notes that while automation can increase efficiency, it may also deepen social inequalities and disrupt traditional employment sectors.

Governance and Power Concentration

The development and control of conscious machines may become centralized among governments or corporations. Aleksander warns that unchecked control could lead to imbalances in power, surveillance, or even manipulation of societies.

Trust, Alienation, and Social Norms

Trust is a major social concern. If machines imitate human consciousness too well, individuals may develop inappropriate attachments or dependencies. Conversely, if machines are distrusted, their deployment in sensitive contexts (e.g., healthcare or education) may be hindered.

Conclusion

Aleksander (2004) provides a thought-provoking look into the implications of developing conscious machines. His discussion highlights the importance of preparing legal, ethical, and social systems to address emerging challenges. He calls for interdisciplinary dialogue, cautioning that technological progress should be matched with philosophical, ethical, and legal readiness.

Prompt: summary and analysis of the security risks, vulnerabilities, and strategic responses to artificial intelligence (AI) in cybersecurity and workforce development, drawing from three key sources: NIST's blog on The Impact of Artificial Intelligence on the Cybersecurity Workforce

Igor Aleksander's article on Advances in Intelligent Information Technology

Naukri's AI Job Hiring Report 2025 on workforce trends in India

Write with APA-formatted section headings and in-text citations.

Chatgpt response: Below is a structured summary of **Security Aspects and Challenges** for *cybersecurity jobs* derived from the three articles you mentioned:

Artificial Intelligence in Cybersecurity: Risks, Vulnerabilities, and Strategic Responses

Security Risks Introduced by AI

Artificial intelligence (AI) introduces both opportunities and risks for cybersecurity professionals. On one hand, AI automates routine tasks such as log analysis and anomaly detection, which can increase efficiency and allow human analysts to focus on higher-order decision-making (National Institute of Standards and Technology [NIST], 2025). However, embedding AI into security operations creates new vulnerabilities. Adversarial machine learning techniques, such as data poisoning and model evasion, can compromise the integrity of AI models, while model drift may degrade performance over time if not properly monitored (NIST, 2025). These vulnerabilities turn defensive AI systems into potential attack surfaces, requiring continuous oversight and robust hardening measures.

Equally significant is the dual-use nature of AI. While defenders gain speed and precision, adversaries leverage AI for automated phishing, deepfake impersonation, and intelligent malware. Aleksander (2004) warned against uncritical acceptance of AI claims, noting that hype cycles may obscure realistic limitations and risks. This perspective remains relevant today, as defenders may underestimate how quickly attackers adopt emerging tools while overestimating AI's reliability as a defensive measure.

Workforce Vulnerabilities and Job Market Dynamics

AI also alters the structure of the cybersecurity workforce. As AI automates entry-level tasks, traditional pathways into the field narrow, creating concern about role displacement and future employability. According to NIST (2025), organizations now require workers skilled not only in cybersecurity but also in machine learning, data science, and AI governance. This shift creates a skills gap, as many existing professionals lack training in AI-related competencies.

Labor market data suggest that demand for AI and machine learning expertise is growing rapidly. Naukri's *AI Job Hiring Report 2025* indicated a 38% increase in AI/ML job postings in India during Q1 FY26, reflecting strong demand for AI talent across industries (Naukri, 2025). While this trend highlights economic opportunity, it also underscores a misalignment: the surge is not necessarily in cybersecurity-specific AI roles, meaning security organizations may struggle to recruit or retain AI-trained professionals. This imbalance creates workforce vulnerabilities that can impede effective adoption of defensive AI.

Strategic Responses to Risks and Vulnerabilities

To address these challenges, organizations must adopt comprehensive strategies across technology, workforce, and governance. Technically, defensive AI systems require adversarial-resilient training, secure data pipelines, and ongoing monitoring to detect model drift or poisoning (NIST, 2025). From a workforce perspective, cybersecurity teams should implement large-scale reskilling programs, cultivate interdisciplinary expertise, and design new career pathways that integrate AI competencies. The hiring trends highlighted by Naukri (2025) demonstrate that cross-disciplinary expertise will become increasingly valuable, but without targeted cybersecurity training, the sector risks losing ground in the AI labor market.

Finally, governance structures must evolve to address accountability, interpretability, and ethical concerns. NIST (2025) emphasizes the importance of human-in-the-loop mechanisms to ensure that AI-driven security actions remain auditable and correctable. Aleksander's (2004) skepticism about inflated AI claims further highlights the importance of measured adoption, with pilot programs, explainable AI, and transparent oversight as key safeguards against overreliance.

Conclusion

Artificial intelligence presents both a powerful tool and a potential liability in cybersecurity. Its risks include adversarial attacks on AI systems, the dual-use capabilities of generative technologies, and workforce disruptions caused by rapid automation. Vulnerabilities manifest in technical, organizational, and workforce domains, with a widening skills gap as a pressing concern. Strategic responses—spanning technical hardening, reskilling, and governance—will determine whether AI strengthens or destabilizes cybersecurity operations. Coordinating education, hiring, and policy efforts will be essential to aligning AI advancements with the resilience of the cybersecurity workforce.

Prompt: create technical overview based on articles The Intersection Between Artificial Intelligence And Sustainability: Challenges And Opportunities *. and Cybersecurity and school libraries. Teacher Librarian to create Technical Overview with new development in IT as well as its applications and potential benefits. Write in APA paragraph format without subheadings. Include in text citations

Chatgpt Response:

The rapid development of information technology (IT) has created new pathways for addressing global sustainability challenges while also raising concerns about digital security in educational environments. Artificial intelligence (AI) is increasingly recognized as a tool for advancing sustainability by enabling more efficient resource management, predictive modeling, and decision-making processes (The Intersection Between Artificial Intelligence and Sustainability: Challenges and Opportunities, n.d.). Applications such as AI-driven climate modeling, optimization of renewable energy systems, and sustainable supply chain management illustrate the transformative potential of intelligent technologies in reducing waste, lowering carbon emissions, and promoting long-term ecological balance. These innovations also support circular economy initiatives by improving recycling processes and material recovery, further advancing global sustainability objectives. In parallel, the growing reliance on digital platforms in education highlights the importance of cybersecurity in safeguarding both data and intellectual property. School libraries, which serve as central hubs for digital learning resources, face increasing threats from cyberattacks and data breaches. As noted in *Cybersecurity and School Libraries* (n.d.), recent developments such as zero-trust security models, AI-assisted threat detection, encryption protocols, and multi-factor authentication are critical in maintaining secure access to digital platforms. These measures not only protect student privacy and institutional data but also strengthen trust in digital educational tools. When considered together, the advancements in AI for sustainability and cybersecurity in education demonstrate the dual role of IT in driving innovation and ensuring safety. By leveraging AI to optimize sustainable infrastructure while implementing robust cybersecurity frameworks, schools and organizations can foster responsible digital practices, enhance efficiency, and create resilient systems that deliver both environmental and educational benefits.