Impact of AI on Cybersecurity

BY: BRYANT WATKINS

Table of Contents

Abstract

This research will serve the purpose of examining and predicting the impact of Artificial Intelligence on the cybersecurity field. The cybersecurity field is incredibly vast, so this research will specifically examine the following areas – cybersecurity job market, cyber warfare operations, and laws and regulations. The long-term impact of Artificial Intelligence is largely unresearched, particularly as it pertains to the area of cybersecurity. Research will be conducted with the acquisition of statistical data and consumption of established written pieces (i.e. articles, journals, reports, etc.) in a combination of quantitative and qualitative information.

There are numerous observations of key findings for this research. The staggering request for a 24,000% budget increase for autonomous warfare capabilities by the U.S military illustrates the global desire for autonomous cyber warfare. The growing autonomous surveillance and intelligence-gathering globally is reinforcing lawful regulatory concerns over accountability and consumer privacy. The predicted 50% decrease in employer desired specialized skills in entry-level cybersecurity positions by 2028 demonstrates the vast cybersecurity job market transformation to come. The impact of Artificial Intelligence on cybersecurity appears to be a largely uncertain mixture of excitatory innovative developments and adverse effects.

Introduction

Artificial Intelligence has announced its presence like few technological advancements in human history. “Artificial intelligence (AI) is technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy” (Stryker & Kavlakoglu, n.d.). Humans have spent nearly a century developing Artificial Intelligence, with its history dating back to the 1950’s. Alan Turing, a renown computer scientist and mathematician, was a pioneer in the early development of Artificial Intelligence. Turing would kickstart the first documented thought experiment on machine intelligence.

Turing conducted a test to determine if machines were capable of exhibiting human intelligence, eventually coining his famous phrase, “Can machines think?” (1949-1950). His test would go on to be known as the Turing test, and it is revolutionary to the history of Artificial Intelligence. For the testing, “a human interrogator would try to distinguish between a computer and human text response” (Stryker & Kavlakoglu, n.d.). Over the years, the Turing test would undergo scrutiny and criticism of its usefulness. Artificial intelligence’s history, however, had just begun.

The term, Artificial intelligence, would officially be coined in 1956 by John McCarthy. 1956 is when the first-ever Artificial Intelligence conference took place, taking place at Dartmouth College. The proceeding 1960’s and 70’s would provide numerous landmarks for the development of Artificial Intelligence. *ELIZA*, the world’s first chatbot, was developed by Joseph Weizenbaum in 1966 (Coursera staff, 2025). The late 1960’s to early 1970’s gave the world

Shakey the Robot, a robot system developed by the Artificial Intelligence Center at the Stanford Research Initiative.

The American Association of Artificial Intelligence would also be founded during this period. After these groundbreaking developments, however, came the *AI Winter*. The AI Winter would not be coined until the mid-1980's, but it is used to describe a period of relatively slowed development of Artificial Intelligence from the late 1970's to early 1990's. This period entailed a "gap between AI expectations and the technology's shortcomings" (Coursera, 2025). While development seemed stagnant, it would go on to enjoy a resurgence following the early 1990's.

From a driverless car to a chess-playing machine – the late 80's through the 90's did have some Artificial Intelligence innovations. Certainly, far from modern autonomous self-driving vehicles today, Ernst Dickmanns' invention was groundbreaking for its time. Dickmanns invented a car outfitted with cameras and sensors, allowing the vehicle to drive with a human driver. IBM would also have a groundbreaking development in its invention of Deep Blue, a computer system designed to play chess against humans. The next two and a half decades, however, would advance Artificial Intelligence like no other period.

NASA's rover was developed in the early 21st century with the ability to navigate with Artificial Intelligence decision-making, doing so without human intervention. IBM Watson was a revolutionary development in 2011, a computer program capable of answering questions on the famous *Jeopardy* TV show. Then came Siri and Alexa onto the scene, software programs designed to process verbal human input in what's known as the *command-and-control* system. While these were major innovations in the history of Artificial Intelligence – nothing quite matches the industry boom experienced from the early 2020's to present day.

The 2020's have brought to us era defining platforms, such as – OpenAI, ChatGPT, CoPilot, and Gemini to name a few. Platforms such as these have ushered in an era of what is known as Generative Artificial Intelligence. Generative Artificial Intelligence refers to Artificial Intelligence that can "generate text, images, and videos in response to text prompts" (Coursera, 2025). This era has not just brought new innovations, however, but also new questions. Many are asking what impact Artificial Intelligence has on humanity. As for a cybersecurity professional such as myself, I am asking, what impact will Artificial Intelligence have on cybersecurity?

Cybersecurity is being impacted by Artificial Intelligence just like any other facet of the world. From the cybersecurity job market and national defense – to cyber law and cyber operations and techniques, cybersecurity is being greatly impacted. Artificial Intelligence is a major technological development for the world, and cybersecurity will face ramifications from it like any other in history. I want to evaluate what these ramifications will entail, as there is not extensive long-term outlook on Artificial Intelligence's cybersecurity impact.

We are seeing Artificial Intelligence's impact on cybersecurity in real-time. The United States Department of Defense and military is in conflict with Artificial Intelligence company Anthropic. Cybersecurity college graduates are increasingly wary of a muddled cybersecurity job market. Politicians and lawmakers worldwide are conflicted on how to address the regulation of Artificial Intelligence. Artificial Intelligence tools are becoming available to cybersecurity professionals that are untested or unproven. These factors illustrate the large degree of relevance for Artificial Intelligence on cybersecurity.

This research assignment will serve as an in-depth examination of many of these factors. Cybersecurity will have to undergo long-term corrective action. It will take the efforts of everyone to implement and understand these needed corrective actions. Artificial Intelligence

will not only require adjustments from society – but from the whole cybersecurity industry as well.

Literature Review

Certain areas of Artificial Intelligence's impact on cybersecurity have been explored. Research has been done on how Artificial Intelligence is reshaping the cyber threat landscape, the use of Artificial Intelligence by cybersecurity professionals, and how cybersecurity can defend against emerging Artificial Intelligence threats. I still find, however, numerous areas with little research conducted thus far that I wish to inquire. We currently do not have deep insight into how Artificial Intelligence will impact national defense and cyber warfare. Challenges posed to the cybersecurity job market by Artificial Intelligence have not been explored. Artificial Intelligence cyber laws and regulations are also not deeply explored. I plan to inquire about these areas for a more comprehensive understanding of the impact of Artificial Intelligence on cybersecurity.

The National Cyber Security Centre of the United Kingdom has conducted critical research on how Artificial Intelligence is shifting the threat landscape for cybersecurity. Their detailed report includes numerous relevant findings. Bad actors will increasingly utilize and acquire Artificial Intelligence tools to infiltrate and disrupt systems. Artificial intelligence is being developed at a rapid pace, and with this rapid development comes rapid proliferation and skill development. The efficiency and effectiveness of cyber intrusions will be greatly increased in coming years, leading to increased frequency and intensity of attacks, according to the National Cyber Security Centre of the United Kingdom.

It also appears that cybersecurity will struggle to keep sufficient pace with the rapidly developing Artificial Intelligence threat landscape. According to the National Cyber Security Centre of the United Kingdom, Zero-day exploits will increase in frequency along with the prioritization of development speed in conflict with security considerations by companies. These suggestions indicate that the cybersecurity industry will need to speed up its adaptations to effectively counter emerging threats. Cybersecurity will also need be prioritized to the same level as Artificial Intelligence development, as a lapse in the two will leave cybersecurity at a severe disadvantage.

There is extensive research on mitigation techniques and methods cybersecurity will have to deploy against Artificial Intelligence, with strong findings uncovered by Syracuse University. Sajjad Bhuiyan and Joon S. Park, of Syracuse University, have conducted research on *Cybersecurity Threats and Mitigation Strategies in AI Applications*. They uncovered numerous significant findings for how cybersecurity professionals will have to counter Artificial Intelligence cyber threats. From Explainable Artificial Intelligence (XAI) and "AI-powered cyber defense" – Bhuiyan and Park cover critical areas of defending against emerging Artificial Intelligence cyber threats.

Trust, transparency, and integration appear to prove critical for the future of cyber defense against emerging Artificial Intelligence threats. Explainable Artificial Intelligence establishes this trust and transparency by identifying the decision-making process of a Machine Learning model, making it an effective defensive tool. It is also important to take advantage of the benefits provided by Artificial Intelligence. Intrusion Detection systems, amongst other tools, have greatly benefited from the incorporation of Artificial Intelligence. Intrusion Detection systems and automation with Artificial Intelligence provide highly valuable tools and tactics for

defensive operations. Utilizing Artificial Intelligence tools and tactics enhances the consistency and efficiency of defensive operations.

Methodology

For this research, I am attempting to predict what impact Artificial Intelligence will have on the cybersecurity industry. The areas of cybersecurity receiving the focus will be the following – cyber warfare, cybersecurity jobs, and laws and regulations. Since Artificial Intelligence is relatively new in its current iteration, it is imperative that humans conduct study on its future impact on a major component to global operations – that is cybersecurity. Artificial Intelligence's impact on cybersecurity is not just for those in that profession, politicians, or military leaders. This research will provide findings that impact all of humanity, as the effects will reverberate throughout global order.

My data will be both quantitative and qualitative. Since this matter has so much complexity, there is an abundance of relevant numerical data as well as non-numerical data to obtain and analyze. Collecting both sets of data will likely provide a more comprehensive overview of the research findings. The numerical data will establish conclusive and objective findings that can be tracked through its evolutions through the past, present and future years. The non-numerical data will address the human experience aspect of the research.

Cyber warfare has numerical statistics that may be tracked over time, such as the number of strikes conducted with the assistance of Artificial Intelligence. There is also qualitative information to be gained on Artificial Intelligence in cyber warfare, such as interviews or articles on the relationship between the two. Cybersecurity job data is stored and calculated numerically

like many other industries, but there are also numerous reports and interviews examining the current and future state of this job market. Laws and regulations are mainly informationally documented in a qualitative manner, though they may also be tracked numerically.

Findings

I was successfully able to uncover significant data and information for my research. Vulpe, Rughinis, Turcanu, and Rosner penned an excellent piece that addresses the impact of Artificial Intelligence on Cybersecurity. I took away numerous relevant findings from their work. The pure uncertainties in Artificial Intelligence proliferation globally are somewhat paralyzing for many. There also appears to be a severe lack of guidance or regulation on the use and implementation of Artificial Intelligence on both a national and global level. Artificial Intelligence is also impacting job markets, with the implementation of Artificial Intelligence tools into hiring processes and entry-level work tasks.

Job postings for entry-level graduate professionals have dropped by 15% from 2024 to 2025 (revelio labs). Artificial intelligence impacted job employment has dropped by 16% for Gen Z since 2022 (Selingo, 2026). There has been a 6% decline in employment opportunities for those aged 22 to 25 between 2022 and 2025 (Brynjolfsson, Chanda, & Chen, 2025). Job openings for mid-and-senior level workers have increased. Postings increased by 2% from July 2024 to January 2025 and are trending upwards.

Jaiswal and Mishra provide relevant findings on Artificial Intelligence in cyber warfare from their informational piece. The largest legal implications for the use of Artificial Intelligence in military operations stem from “liability, privacy, regulatory compliance” (Jaiswal & Mishra, 2024). The use of Artificial Intelligence in militaries around the world has grown immensely

over the past few years. Per Grand View Research, “the global artificial intelligence in military market size was estimated at USD 9.31 billion in 2024 and is projected to reach USD 19.29 billion by 2030”. The United States military is by far and away the global leader in spending on Artificial Intelligence for military use. The largest share of United States military spending in Artificial Intelligence pertains to information processing.

Artificial Intelligence also maintains a sizeable impact on the cybersecurity job market. There has been an exponentially increasing demand for cybersecurity professionals with specialized expertise in Artificial Intelligence. Criminals and bad actors are increasingly incorporating Artificial Intelligence into their tactics to increase speed, efficiency, and scale of attacks. Cybersecurity professionals are being asked to combat the rise of Artificial Intelligence by implementing strong Knowledge Management (KM) (Graham, 2025). Knowledge Management is, “the process of identifying, organizing, storing and disseminating information within an organization” (IBM).

Cybersecurity job availability has also been greatly impacted by the rapid proliferation of Artificial Intelligence. Employers are increasingly implementing Artificial Intelligence into many of their tasks that require repetitiveness. Employment for young people beginning their career, aged 22-25, has fallen precipitously. From late 2022 to July of 2025, young people experienced a 6% drop in employment with employers with high levels of exposure to Artificial Intelligence (Richard, 2025). Overall employment has risen in the presence of Artificial Intelligence adoption by many workplaces, but not for young people, most job opportunities added are benefitting mid and senior level professionals (Richard, 2025).

Discussion

The findings are incredibly telling on the impact of Artificial Intelligence on cybersecurity. Artificial Intelligence has completely shifted the landscape of cyber warfare. The United States military leading the world in Artificial Intelligence investment and implementation will likely place the United States military at the forefront of Artificial Intelligence cyber operational innovation. The request for 54 billion dollars towards the Defense Autonomous Warfare Group is a staggering 24,000% increase and a telling sign (Down, 2026). The United States military is determined make Artificial Intelligence the future of cyber warfare and operations.

The Asia Pacific is not far behind Autonomous warfare innovation, while not as large a market as the United States, it is faster growing. Actors and nations globally are looking to Artificial Intelligence for much of their intelligence gathering as well as strategic planning. Governments will likely continue pushing for Artificial Intelligence development and seek ways to utilize autonomous tools to increase the efficiency and effectiveness of cyber warfare. The future of cyber operations, however, is not completely certain.

Laws and regulations on Artificial Intelligence are also a large factor in cybersecurity. In cyber warfare, who is to be held accountable for an autonomous weapon erroneously targeting civilians in an uncontrolled manner? This is where the state of laws and regulations globally come into play. Liability will have to be determined in the very near future, as simply blaming Artificial Intelligence will not suffice public sentiment. Society will also demand new regulatory frameworks on user privacy, as the increase in autonomous intelligence gathering will surely cause immense unease globally.

Artificial intelligence will likely cause privacy to be at the forefront of public discourse, with many feeling a severe lack of privacy. Cybersecurity will have to adjust defensive tactics to

counter increasingly invasive autonomous surveillance measures. Professionals in cybersecurity will increasingly be tasked with ensuring regulatory compliance with new laws and regulations to come. Ensuring regulatory compliance is just one of many alterations to the cybersecurity job market due to Artificial Intelligence.

Over the coming years, the cybersecurity job market will prove vastly different in the wake of Artificial Intelligence global proliferation. Job roles will increasingly demand skills and expertise in Artificial Intelligence for cybersecurity professionals. Deepfakes, a generative Artificial Intelligence tool that impersonates the characteristics of individuals, are going to increase in frequency and sophistication. Deepfakes will significantly enhance social engineering attacks by bad actors, which will lead organizations to demand cybersecurity professionals with extensive expertise in mitigating such Artificial Intelligence tactics.

Cybersecurity professional roles for entry-level talent are also going through a major disruption. Many organizations are implementing Artificial Intelligence for tasks that have been completed by entry-level professionals fresh out of college in recent years. These moves by organizations have led to a chain effect, where entry-level roles are increasingly requiring mid-level experience. Mid-level cybersecurity professionals are settling for entry-level roles; this will continue to have an immensely adverse impact on the early career development of cybersecurity professionals. Young and entry-level professionals will struggle to obtain employment and relevant experience in their field of cybersecurity.

All cybersecurity job market shifts will not be bleak, however. It will be up to many disenfranchised young and entry-level cybersecurity graduates to adjust their expectations and expertise. Cybersecurity roles specializing in Artificial Intelligence will continue to become increasingly available, which will provide a vast network of opportunities for young people to

acquire employment. New graduates will have to transition their skillset to developing and defending against Artificial Intelligence. Doing so will transform the cybersecurity job market, and I predict provide corrective action as well for the market.

Conclusion

While there are many uncertainties on the impact Artificial Intelligence will have on cybersecurity – there are numerous predictive and anticipatory conclusions that may be drawn from relevant information and data. Cyber warfare and operations appear to be heading toward an immensely autonomous state with Artificial Intelligence development akin to a global arms race. Lawmakers worldwide will begin taking legislative action on regulating Artificial Intelligence, as consumer concerns over privacy and accountability will grow vastly in the years to come. The cybersecurity job market will continue to undergo the largest transformation that we have seen in recent times, as employers are increasingly searching for skillsets centered on Artificial Intelligence and incorporate this technology into their practices and diminish historically entry-level tasks.

Much research is still needed, however, on other areas where Artificial Intelligence may impact cybersecurity. The identity management and security of machines will require insightful assessment, as there remains a large gap in research and development (Northeast Technical Institute, 2026). Cybersecurity ethics have not been extensively researched, with many concerns and questions swirling around on this subject matter. The risks and repercussions associated with the use of Artificial Intelligence by script kiddies also must be explored, as a lack of expertise on Artificial Intelligence may cause inexperienced bad actors to unknowingly unleash threats that have never been seen before. Questions and concerns of Artificial Intelligence will only increase

over time, and it will ultimately be up to the cybersecurity industry to adjust, defend, and develop to help ensure the safety and security of our civilization.

References

Stryker, C., & Kavlakoglu, E. (2026, April 1). *What is Artificial Intelligence (AI)?*. IBM. https://www.ibm.com/think/topics/artificial-intelligence

Peralta, R. (2025, February 11). *Alan Turing's everlasting contributions to computing, AI and cryptography*. NIST. https://www.nist.gov/blogs/taking-measure/alan-turings-everlasting-contributions-computing-ai-and-cryptography

Staff, C. (2025, October 15). *The history of AI: A Timeline of Artificial Intelligence*. Coursera. https://www.coursera.org/articles/history-of-ai

Impact of AI on Cyber threat from now to 2027. National Cyber Security Centre. (2025, May 7). https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027

Bhuiyan, S., & Park, J. S. (2025). Cybersecurity threats and mitigation strategies in AI applications. *Journal of The Colloquium for Information Systems Security Education*, *12*(1), 1. https://doi.org/10.53735/cisse.v12i1.199

Vulpe S-N, Rughiniș R, Țurcanu D and Rosner D (2024) AI and cybersecurity: a risk society perspective. Front. Comput. Sci. 6:1462250. doi: 10.3389/fcomp.2024.1462250

Jaiswal, A., & Mishra, P. C. (2024). ARTIFICIAL INTELLIGENCE (AI) AND CYBERSECURITY LAW: LEGAL ISSUES IN AI-DRIVEN CYBER DEFENSE AND OFFENSE. *ShodhKosh: Journal of Visual and Performing Arts*, *5*(6). https://doi.org/10.29121/shodhkosh.v5.i6.2024.4144

Artificial Intelligence in military market | industry report, 2030. (n.d.). https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-military-market-report

Graham CM (2025), "AI skills in cybersecurity: global job trends analysis". *Information and Computer Security*, Vol. 33 No. 5 pp. 673–689, doi: https://doi-org.proxy.lib.odu.edu/10.1108/ICS-09-2024-0235

IBM. (2025, November 17). *What is knowledge management?* https://www.ibm.com/think/topics/knowledge-management

Elgan, M. (2025, November 18). *Is Ai saving jobs... or taking them?*. IBM. https://www.ibm.com/think/insights/is-ai-saving-jobs-or-taking-them#:~:text=It's%20clear%20that%20AI%20is,field%20are%20myriad%20and%20expanding.

Richardson, N. (2025, October 6). *Yes, Ai is affecting employment. here's the data.* ADP Research. https://www.adpresearch.com/yes-ai-is-affecting-employment-heres-the-data/

Down, A. (2026, April 22). *Pentagon asks for $54bn in pivot towards Ai-Powered War*. The Guardian. https://www.theguardian.com/us-news/2026/apr/22/pentagon-asks-for-54bn-in-pivot-towards-ai-powered-war?CMP=share_btn_url

Admin, N. (2026, February 18). *AI-powered attacks expose critical security gaps: 2026 cybersecurity warning*. Northeast Technical Institute. https://ntinow.edu/ai-powered-attacks-expose-critical-security-gaps/#:~:text=%23%20Uncategorized-,AI%2DPowered%20Attacks%20Expose%20Critical%20Security%20Gaps:%202026%20Cybersecurity%20Warning,this%20security%20gap%20widens%20further.

Poremba, S. (2025, November 18). *ISC2 cybersecurity workforce study: Shortage of AI skilled workers*. IBM. https://www.ibm.com/think/insights/isc2-cybersecurity-workforce-study-shortage-ai-skilled-workers#:~:text=In%20its%20study%20AI%20in,need%20for%20non%2Dtechnical%20skills.

Artificial Intelligence in Military Market Size, Share, Report, 2034. (2025). Fortunebusinessinsights.com. https://www.fortunebusinessinsights.com/artificial-intelligence-in-military-market-113094

Tajammul Pangarkar. (2024, April 15). *Artificial Intelligence in Military Statistics 2024 By Efficiency, Tech*. Market.us Scoop. https://scoop.market.us/artificial-intelligence-in-military-statistics/

What Is College for in the Age of AI? Young graduates can't find jobs. Colleges know they have to do something. But what? | Office of Academic Affairs. (2026). Osu.edu. https://oaa.osu.edu/news/2026/01/20/what-college-age-ai-young-graduates-cant-find-jobs-colleges-know-they-have-do

ISC2. (2024, February 21). *The real-world impact of AI on cybersecurity professionals*. Www.isc2.org. https://www.isc2.org/Insights/2024/02/The-Real-World-Impact-of-AI-on-Cybersecurity-Professionals

reveliolabs. (2025). *Is AI responsible for the rise in entry-level unemployment? | Revelio Labs*. Revelio Labs. https://www.reveliolabs.com/news/macro/is-ai-responsible-for-the-rise-in-entry-level-unemployment/

Brynjolfsson, E., Chandar, B., & Chen, R. (2026, April 3). *Canaries in the coal mine? Six facts about the recent employment effects of Artificial Intelligence*. Stanford Digital Economy Lab.

https://digitaleconomy.stanford.edu/publication/canaries-in-the-coal-mine-six-facts-about-the-recent-employment-effects-of-artificial-intelligence/