Interdisciplinary Final paper

By: Sahmer Khaled Ismael

Dr: Pete Baker

IDS300W

December 1,2023

Can AI be sophisticated enough to replace humans in the field of cyber security?

One of the most diverse discussions globally for the past couple of years has been the emergence of AI (artificial intelligence), and whether it can replace humans in fields of technology base, such as cyber security. Cyber security attacks have caused drastic damage to the economy, in which they have caused major debt for governments across the globe with over 6.9 Billon dollars in damages due to cyber related crimes worldwide in 2021 (Griffiths,2023). Many various disciplines have extensively researched the pros and the cons of incorporating AI into Cyber security. However, none of these studies have predicted the likelihood of AI making a full shift in the realm of Cyber security. The second step, in the Interdisciplinary approach, is to justify if the question can be looked into from a interdisciplinary scope, which it can be.

The reasoning of why the question can be viewed in a interdisciplinary approach, is that the combination of AI, into a field such as cyber security, professionals must consider not only the technological components, but also the social, legal, ethical and human factors(Griffiths,2023). Cybersecruity attacks are ongoing and, continue to happen around the world every single day, with damaging effects. This calls for many disciplines to, be able to discover the matter of the issue. Not one discipline is able to embark on the areas of this question, without the aid of many other disciplines, which leads the question to becoming very complex and difficult to solve, which is looked at, in the perspective of, interdisciplinary issue.

The third step in the interdisciplinary process is to identify, the relevant disciplines in which, would help to aid my question from an interdisciplinary view. I can also implement the 5 step in the interdisciplinary process as well, which is to develop adequacy in each relevant discipline. There are many discipline insights in which aid into the topic of, can AI be sophisticated enough to replace humans in Cyber security? Although, the disciplines in which are

relevant to the research question are, Computer science, economics, sociology, ethics, and Cybersecruity. The paper will center its attention into only the disciplines of computer science, economics, and sociology. While other disciplines can assist in the research process of the, presented issue of AI in Cybersecruity, the disciplines which are focused throughout the paper, develop the most bountiful and critical information for the research question.

Literature review

The fourth step in the interdisciplinary process is conducting a literature review, on the disciplines that will be discussed around the research question. Within the computer science discipline, the discussion of whether if AI "Will be sophisticated enough to replace humans in Cyber security?" is cut in half essentially, with support from both sides of the issue. Both sides of the argument within the discipline agree that since hackers can ambush organizations and banks, security vulnerabilities' very casually, AI and Cybersecurity have expanded and become more convenient with each other due, to recent events of cybercrime (Bhargava et al.,2021). However, individuals against AI argue, AI is suffering from the dynamic and weak understanding of human life (Bhargava et al.,2021). This dynamic is to grasp, and pertain information and display decision making, through years of experience and expertise, in which AI is unable to do in a field of Cyber security (Bhargava et al.,2021). Furthermore individuals, against AI conclude that, as cyberthreats are continuing to develop, and be more efficient, the tools in AI must be updated on a daily basis (Corradini,2020). This leads to the issue, that there is no clarity for how AI will be able to mitigate security problems, without causing new ones to occur at the same time (Corradini,2020). Besides the matter in question, of AI causing new security problems to occur, cyber criminals can also use their methods of work, to exploit, the scalable use of AI systems (Corradini,2020). Computer scientist considered what follows next, in

which they transcribed which are gaps when it comes to AI (artificial intelligence) and the protection of sensitive information in cyber security (das & Sandhane, 2021).

Computer scientist state that hackers are trying to attempt to gain access to the computers by finding gaps in security in which, will not be detected by AI (artificial intelligence), and by the time it has been located, the hacker would have been long gone, with the sensitive information as well.

The contending side of computer scientist in which, support the use of AI, taking over some jobs in the field of Cyber security, conclude that, AI systems and predictive analytics, for example provide opportunities for thoughtful calculations in synthesizing large volume of data in Cyber security(Jarrahi,2018). The issue that came into mind when AI started to gain recognition for advancing, was that can it adapt to the field of Cyber security in a costly effective manner and mitigate issues that occur. They further conclude that AI based tools, will provide testing and help with evaluating alternative course of action as well, using algorithms, rather than humans using, gut feeling (Jarrahi,2018). Nevertheless, a significant amount of human thinking and decision-making emerges from instinct, that comes from the subconscious rather than purposeful information gathering and analyzing that AI concludes (Dane et al., 2012). Being able to generate direct information or understanding to arrive at decisions without depending on reason or logic. This can be a real issue for a cyber security firm in which, employees might depend on a gut feeling, or instinct in which they will guess how a product will turn out (Jarrahi,2018).

Another reasoning in which, why, experts argue that, the addition of AI into Cyber security is going to be a big boost in the technology era, is due to it making, crucial decisions in a very complex situation, which even the smartest human, can’t even make , in such a timely manner (Jarrahi,2018). AI is also very useful tool for infrastructural security as well, which it performs to

the greatest degree, when the products they utilize is created on the database of Cyber security devices (Sharma, 2021, p. 3). AI then will be able to focus on being square, cautious and able to recognize any abnormalities that are occurring in the system (Sharma, 2021, p. 3).

From an economic perspective, the addition of AI taking over jobs in the field of Cyber security, present many benefits, in which aid the cyberworld. Which economist argue with computer scientist, that the addition of AI in cyber security would help the digital world rather than hurt it. According to Sarma (2017), the use of AI methods and tools for dealing with certain cyber security issues, like for instance advanced malware and the rapid growth of cyberattacks, offers solutions to mitigating the problems emerging for economist (Sarma et al., 2017). Economist argue that One argument states, the involvement of AI into the economy could help to offer solutions for the protection of vital industries like health, education, and cyber security (Sarma et al., 2017). The way in which this occurs, is that it offers a new path to innovation and entrepreneurship by collaboration plus communication, in the merging knowledge of the economy (Sarma et al., 2017). According to recent studies, the use of machine learning and artificial intelligence, have been used more frequently in the field of Cybersecruity since 2012(Kshetri,2021). According to research done, from a market research firm, they have concluded that the addition of AI in Cyber security, will boost the market value in 2019 which was 8.6 billion, all the way up to a predicted all-time high of 101.8 billion by 2030(Kshetri, 2021). This is all due to the factor of Artificial intelligence being able to detect cyber threats faster and at a higher rate, then a human team would, and to stop they cyber-attack as soon as possible (Kshetri, 2021). The effect of AI tripling almost the cost of what was spent in 2021, in just a field like Cyber security, could cause dramatic damage for individuals involved in the field (Kshetri, 2021). Moreover, according to a study that was conducted in 2018 by the pomeron

institute, the mass amount of businesses that are using AI for Cyber security, which was 69 percent, said that the ability to detect cyber threats was two times faster than the previous 3 years (Kshetri,2021).

Sociologist have shared similar views to that of, computer scientist, in which they argue, that, technology such as AI, is more of a technical issue, and is not one in which exist unchangeable from human or social control(Musik & Bogner,2019). Sociologist also argue, although AI has many abilities in which they can perform mechanical task such as pattern recognition, and specified task, they are still unable to understand context, such as to "see" and "understand" which is a fundamental aspect of humans in a field such as Cyber security (Liu ,2021). Sociologist argue that, we should not see human factor as a problem, but as a part of the solution, since individuals are essential to the functioning of the socio-technical system (Zimmermann and Renaud 2019. The reasoning behind this is that humans can comprehend, issues that are accruing in the field of Cybersecruity and are able to act upon that issue, the next time they encounter it (Liu ,2021). Humans as well provide knowledge of context, and the background knowledge in which AI are unable to do (Liu ,2021). This is drastically important due to the field of Cybersecruity continuing to transition and evolve every single year. However a economist would argue that, the advancement in AI, helps to alleviate the issue in which sociologist are arguing, AI can't do which is be able to adapt, to the change of see and understand as a human would. Due to the reasoning of AI being able to adapt to new threats in the filed of Cybersecruity and being able to mitigate against the issues, the way in which a human would cyber activity (Liu ,2021). Economist continue to argue the fact, in which AI, over humans, is cost effective, and do not need break in which a human would need throughout work (Kshetri,2021).

Creating common ground

The evidence concludes that, humans can be replaced in Cybersecruity, due to many reasons. Both computer scientist, who support AI and economist, can agree that the transition of AI in Cybersecruity over humans, is one that will be faster in responding to incidence response. These issues conclude, such as threats that have been detected in the system, which would take months for a group human's workers to solve. While other disciplines have argued that the implantation of AI, is one that comes with risk, since hackers are so strategic in being able to breach a system, with new threats. Sociologist and economist both argue that AI, is more than capable of adapting to new threats and challenges in the field of Cyber security and coming up with solutions for them.

Both economist and computer scientist both agree that the implantation of Cybersecruity inside a firm, is one that is cost effective due to multiple reason such as, AI being able to operate without, breaks. Also implementing AI in an organization, would help mitigate against attacks, that are caused by humans such as social engineering attacks, which are the most used tactics in Cybersecruity today, and cause the most damages to businesses (Kshetri,2021). Both sociologist and economist agree, Cyber security firms as talked about before, have adjusted to using AI tools in which to help mitigate the attacks in which they face. Both economics and sociology disciplines agree that, the collaboration of both disciplines can help develop a comprehensive understanding, of economics and cyber hygiene, within the field of Cyber security.

The field of Cybersecruity will continue to progress in which it will continue to rely heavily on AI for solutions, in battling ongoing new Cyber security attacks to cooperation’s.

Reference Page

Artificial Intelligence and cyber security: A new pathway for growth in ... (n.d.-a). https://worldscientific.com/doi/10.1142/9789811221750_0004

Author links open overlay panelMohammad Hossein Jarrahi, AbstractArtificial intelligence (AI) has penetrated many organizational processes, Dane, E., Gardner, W. L., Hung, S.-Y., Mumford, E., Accenture, Bishop, P., Brynjolfsson, E., Buchanan, L., Burke, L. A., Choo, C. W., Cross, R., Davenport, T. H., Guszcza, J., & Hayashi, A. M. (2018, April 12). Artificial Intelligence and the future of work: Human-AI symbiosis in organizational decision making. Business Horizons. https://www.sciencedirect.com/science/article/pii/S0007681318300387#sec0030

Corradini, I. (1970, January 1). Redefining the approach to cybersecurity. SpringerLink. https://link.springer.com/chapter/10.1007/978-3-030-43999-6_3#chapter-info

Das1, R., & Sandhane1, R. (2021, July 1). IOPscience. Journal of Physics: Conference Series. https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042072

Economics of Artificial Intelligence in cybersecurity | IEEE journals ... (n.d.-b). https://ieeexplore.ieee.org/abstract/document/9568267/

The latest Cyber Crime Statistics (updated December 2023): Aag it support. AAG IT Services. (2023, December 1). https://aag-it.com/the-latest-cyber-crime-statistics/

Musik, C., & Bogner, A. (2019, May 27). Book title: Digitalization & society - österreichische zeitschrift für soziologie. SpringerLink. https://link.springer.com/article/10.1007/s11614-019-00344-5

Role of artificial intelligence in Cyber ... - Wiley Online Library. (n.d.-c). https://onlinelibrary.wiley.com/doi/10.1002/9781119760429.ch3

Sociological perspectives on artificial ... - wiley online library. (n.d.-d). https://compass.onlinelibrary.wiley.com/doi/full/10.1111/soc4.12851

Tai, M. C.-T. (2020, August 14). The impact of Artificial Intelligence on Human Society and Bioethics. Tzu chi medical journal. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7605294/