AI Fear and Adoption: Modelling the Connection

Anthony Caldwell
University College Dublin
Ireland

Abstract

In the rapidly evolving landscape of technology, the integration of artificial intelligence (AI) into various facets of our lives has sparked both fascination and concern. Nowhere is this dichotomy more pronounced than in the realm of cybersecurity, where the fear of AI-driven threats has taken center stage. As AI continues to advance, so too does the anxiety surrounding its potential misuse and the vulnerabilities it may introduce to our digital defenses. Preliminary data on the model shows that there is some caution regarding AI tools and perceived threats associated with the acceptance that automation technologies such as AI are expected to expand significantly in the near future.

1. Introduction

Technophobia is defined as an 'abnormal fear of or anxiety about the effects of advanced technology [1]. Automation powered by AI enables attackers to execute sophisticated and large-scale operations with unprecedented efficiency. Tasks such as reconnaissance, vulnerability identification, and even the execution of attacks can be automated, allowing adversaries to mount assaults at a speed and scale that human operators would struggle to match. This acceleration of cyber threats raises concerns about the efficacy of current defense mechanisms and the ability of cybersecurity professionals to keep pace with the evolving threat landscape. Furthermore, the fear of AI in cybersecurity is exacerbated by the potential for AI to be weaponized for offensive purposes. As AI technologies become more accessible, the risk of non-state actors and cybercriminals utilizing AI tools to amplify the impact of their attacks grows. The prospect of AI-driven malware, capable of autonomously adapting to changing circumstances and identifying new vulnerabilities, adds a layer of complexity to the challenge of securing digital infrastructures.

There are ethical considerations that contribute to the apprehension surrounding AI in cybersecurity. Questions about the responsible development and deployment of AI technologies linger, with concerns about unintended consequences and the potential for biased decision-making by AI systems. The fear of an uncontrollable and unpredictable AI, acting outside the intended bounds set by its creators, underscores the need for robust ethical frameworks and governance mechanisms in the realm of AI-driven cybersecurity. Despite these fears, it is essential to recognize the positive role AI can play in enhancing cybersecurity defenses. AI technologies can augment the capabilities of cybersecurity professionals by automating routine tasks, detecting anomalies in network traffic, and rapidly responding to emerging threats. The key lies in striking a balance between leveraging AI for defensive purposes and mitigating the risks associated with its potential misuse. From the psychological perspective, a fear appeal serves to trigger the end-user that a threat exists but also the severity of the threat and their susceptibility to the threat. In this respect, once an individual is conscious of a threat, beliefs are established as regards the seriousness of the threat and the likelihood of personally experiencing the threat. Leventhal, (1971) argued that when an individual's emotions drive the response to a fear communication, a fear control process is engaged [2]. In this paper, the modelling of artificial fear pertains specifically to the fear of AI adoption as mediated through the perception of threats and threat efficacy. Indeed, the fear of artificial intelligence within the context of cybersecurity is multifaceted and deeply rooted in the transformative capabilities of AI. The concerns range from the adaptability and scale of AI-driven threats to the ethical considerations surrounding the development of AI. While acknowledging the challenges, it is crucial to approach the integration of AI in cybersecurity with a strategic and ethical mindset, fostering innovation while simultaneously safeguarding against potential risks. By doing so, we can harness the power of AI to strengthen our digital defenses and navigate the evolving landscape of cybersecurity with resilience and responsibility. As noted in a 2022 Forbes article, there are difficulties with defining what AI as a field is and while the promises (in the future) are impressive, for the moment, these AI-related cybersecurity incidents can be a cause for much concern [3]. Several models have attempted to predict user behaviours within the context of technology with varying degrees of success and in many different contexts. Explaining end-user's intentions to engage with computer security actions have been shown to be impacted by perceived threats

 | DOI: 10.20533/ijicr.2042.4655.2024.0153

thus act as a starting point to model artificial intelligence fear.

2. Fear Acceptance

Technology adoption theories such as the technology acceptance model (TAM) and the unified theory of acceptance and use of technology (UTAUT) are complex models aimed at predicting user behavior within the domain of information technology acceptance. Limitations lie in their ability to explain the acceptance and use of security technology due to a gap in the models concept of threat and the models; usage being primarily aimed at productivity-based applications. Fear appeals have seen much success in exploiting the end-user. Early research in to fear by Hovland et al. (1953) suggested that fear induces a feeling of unpleasantness, which the recipient will act to resolve or reduce [4]. Fear has been used in several contexts to manipulate human behaviors and reactions, either to persuade people to cease or reduce particular negative behaviors, or initiate helpful behaviors. The degree to which companies, malicious users and technology professionals can align the actions of end users with their respective goals dictates the level of success mitigating threats thus, the use of fear has been met with varying degrees of success [5]. A fear appeal serves to trigger the end-user that a threat exists but also that the severity of the threat and their susceptibility to the threat. Once an end-user is conscious of a threat, beliefs and the seriousness of the threat and the likelihood of personally experiencing the threat become more established. Indeed, early models suggested that when an individual's emotions drive the response to a fear communication, a fear control process is engaged [2] leading to the individual's cognition of the threat to dominate their responses, referred to a form of danger control [2]. Protection Motivation Theory (PMT) [6] illustrates two sequential appraisals consistent with the structure of the fear appeal message (see Figure.1).

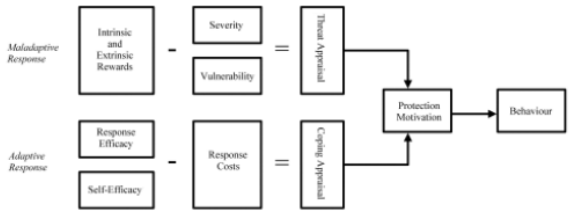

Figure 1. Protection Motivation Theory [6]

The first appraisal deals with the threat, while the second appraisal deals with the efficacy of the recommended threat response. Specifically, if a threat is perceived to be relevant and potentially harmful then an appraisal of efficacy will occur. If an end-user is exposed to a fear appeal that does not provoke a relevant perception of threat, then no further information processing/appraisal occurs. Where a perceived threat is accompanied by a moderate-to-high degree of perceived efficacy, individuals will take action to mitigate the threat, a type of behavior described as a danger control process. The danger control process can lead to beneficial outcomes such as when managers and directors wish to enforce compliance with security policies in an organization.

The Fear Appeal Model [5] explains user's intentions to engage in individual computer security actions recommended in fear inducing persuasive communications and extends the danger control process described in the PMT. A direct determinant of behavioral intent is social influence which assists in predicting intentions to accept a security technology (see Figure. 2).

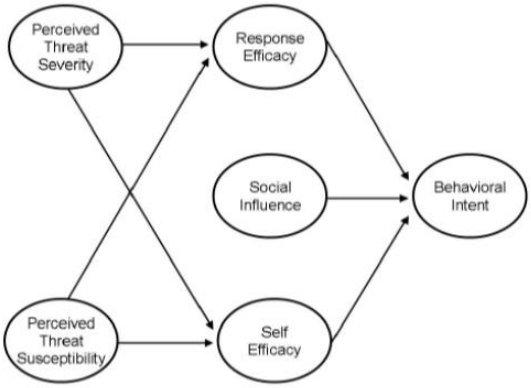

Figure 2. Fear Appeals Model [5]

The FAM shows that the perception of threat is a crucial element in the motivation to use protective software. More broadly, [7] showed that the experience of terror becomes more acute when the perceived threat approaches [7], [1]. Extending this model by introducing these fear appeals and their impact on behavior the Extended Parallel Process Model (EPPM) includes components of the Protection Motivation Theory (PMT) [8]. For example, Maush et al. [9] examined how the EPPM with its constructs threat and efficacy were shown to positively influence behavioral intention, i.e., participants who have been positively influenced by these two constructs tend to behave more securely (see Figure 3).

A failure of cybersecurity could also lead to psychological harm, especially when fear appeals are deployed repeatedly. This might be the case when the person being targeted is already anxious about other things, or does not feel competent to take the recommended action, leading to a form of threat fatigue. If the perception of threat is a crucial element of the motivation to use protective software such as anti-virus as noted by Petersen and Liaras [7].

 | DOI: 10.20533/ijicr.2042.4655.2024.0153

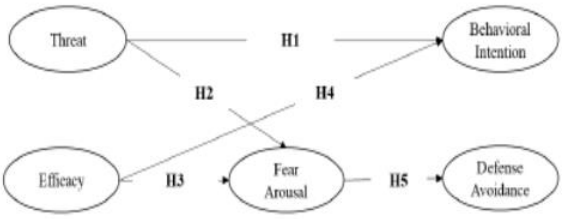

Figure 3. The Extended Parallel Process Model [9]

consider now the potential for AI to be weaponized for offensive purposes has become more accessible and accordingly, the risk of cybercriminals utilizing AI tools to enhance and amplify the impact of their attacks grows [7].

3. Artificial Fear

In 2015 a British Science Association survey found that 60 per cent think that the use of robots or programmes equipped with artificial intelligence (AI) will lead to fewer jobs within ten years and 36 per cent of the public believe that the development of AI poses a threat to the long term survival of humanity [10]. AI anxiety characterized as an overall, affective response of anxiety or fear that may restrict interactions with AI [11]. The prospect of AI-driven malware, capable of autonomously adapting to changing circumstances and identifying new vulnerabilities, adds a layer of complexity to the challenge of securing digital infrastructures. AI tools often expose various fears deeply rooted in human psychology and societal dynamics. The loss of control, particularly those capable of autonomous decision-making, may raise concerns about relinquishing control to machines. We may come to fear that AI will make decisions or take actions that conflict with their interests or values, leading to a loss of autonomy and agency. Accordingly, the widespread adoption of AI tools across various industries has led to fears of job displacement and economic instability. As AI automation replaces certain tasks traditionally performed by humans, individuals may fear unemployment or the need to acquire new skills to remain relevant in the workforce. As previously mentioned, AI algorithms are often trained on historical data, which may contain biases reflecting societal inequalities. Consequently, there are concerns about AI perpetuating or exacerbating biases in decision-making processes, such as hiring, lending, or criminal justice. The fear is that AI tools may amplify existing disparities and perpetuate discrimination against certain groups. In the realm of surveillance and data analysis, AI raises fears about the erosion of privacy. Individuals may feel apprehensive about the collection, analysis, and utilization of their personal data by AI systems, leading to concerns about surveillance, manipulation, and breaches of privacy. Existential fears regarding the potential consequences of highly advanced AI systems surpassing human intelligence and capabilities, known as the singularity, raise existential questions about the future of humanity, including scenarios of AI domination or existential risks. Confronted with complex ethical dilemmas, such as determining responsibility and accountability for AI-driven decisions shows that navigating the ethical boundaries of AI applications may evoke fears about the consequences of AI technologies on society and individuals. Consider for a moment the customer service or caregiving domains. There are fears about the dehumanizing effects of AI-mediated interactions. Particularly AI replacing human connection, empathy and interpersonal relationships leading to fears of social isolation and alienation. All of these fears underscore the complex interplay between technology and human psychology, highlighting the need for ethical, transparent, and responsible development and deployment of AI tools to address societal concerns and mitigate potential risks [12].

4. Modelling Fear in AI

While Adams notes that Dihal and Cave's (2019) modelling of intelligent machines rested upon four hopes (immortality, ease, gratification and dominance) there were four corresponding fears (inhumanity, obsolescence, alienation and uprising) including a loss of human control thus exposing the fear associated with AI, or intelligent machines [13]. What is notable is that the affective responses to intelligent machines where such technologies represent the utopian ideals of what the human race can achieve is accompanied by the fear that they will turn against us [11]. In a 2022 model of AI Anxiety (AIA), the construct incorporates components such as learning, AI configuration, job placement and sociotechnical blindness (unique to the AIA construct) [14].

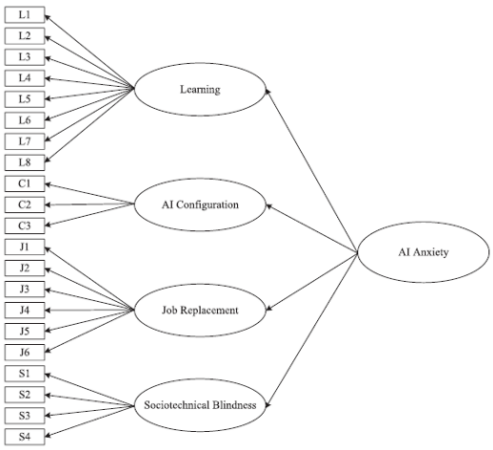

Figure 4. The AIA Model [14]

 | DOI: 10.20533/ijicr.2042.4655.2024.0153

AI anxiety generally results from an exclusive focus on AI programs leaving human beings out and replace that same human behavior to prioritize and assign meaning to AI program operations. In the paper presented here, it is proposed here that AI fear may be mediated through the constructs of threat and thereat efficacy, leading a behavioural intention to reject AI [9, 13]. This is proposed as follows,

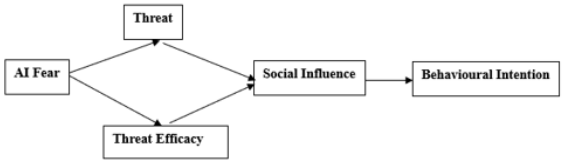

Figure 5. AI Fear Model

Threat and their susceptibility to the threat via threat efficacy represent may positively influence behavioral intention, i.e., participants who have been positively influenced by these two constructs tend to behave more securely and vice versa. Social influence assists in predicting intentions to accept an AI technology. In this case, the fear of AI such as AI programs leaving human beings and human behavior out of the decision making process. It is predicted that with the increase in AI fear will lead to a decrease in the behavioural intention to adopt AI or AI like processes and tools. Based on extant literature several hypotheses are suggested in Table 1.

Table 1. AI Fear Hypotheses

Hypothesis	Description
H^1	The perception of a threat coupled with the efficacy with which that threat may cause harm, will impact the behavioural intention to accept or reject an AI technology.
H^2	The social influence surrounding an AI threat will impact the behavioural intention to accept or reject an AI technology.

5. Preliminary Data

Some preliminary data has been gathered on the model proposed. Seventeen responses from a cohort ranging in age from 19 to 56 were gathered from people in the Republic of Ireland. Given the low number of responses at this point, only descriptive statistics can be presented. The questionnaire items that load onto the variables in the model are listed in Table 2.

Table 2: Questionnaire Items and Variable.

Question	Variable
T1: I feel threatened by AI	Threat
T2: I need AI defenses on my device/laptop	Threat
T3: AI is a threat to my family and friends	Threat
T4: AI is a global threat	Threat
T5: AI malware and viruses are a bigger threat today	Threat
TE1: AI could easily overcome my device/laptop defenses	Threat Efficacy
TE2: I could easily detect an AI generated image or piece of text	Threat Efficacy
S1: If my friends and family trust AI I will also trust it	Social Influence
S2: Society in general trusts AI	Social Influence
S3: The media does not do enough to highlight the threats posed by AI	Social Influence
B1: I intend to use AI tools on my laptop/device	Behavioural Intention
B2: I will recommend the use of AI tools to my friends and family	Behavioural Intention

Table 3 below lists the percentage of responses associated with a five-point Likert scale ranging from strongly disagree to agree.

Table 3: Preliminary Questionnaire Data.

Questionnaire Item	Percentage
T1: I feel threatened by AI	58.8.% Disagree 23.5% Neither 11.8% Agree 5.9% Strongly Agree
T2: I need AI defenses on my device/laptop	17.6% Disagree 64.7% Agree 17.6% Neither
T3: AI is a threat to my family and friends	5.9% Strongly Disagree 58.5% Disagree 17.6% Neither 5.9% Agree 11.8% Strongly Agree
T4: AI is a global threat	11.8% Disagree 52.9% Neither 17.6% Agree 17.6% Strongly Agree
T5: AI malware and viruses are a bigger threat today	17.6% Disagree 11.8% Neither 64.7% Agree 5.9% Strongly Agree
TE1: AI could easily overcome my device/laptop defenses	17.6% Neither 76.5%Agree 5.9% Strongly Agree
TE2: I could easily detect an AI generated image or piece of text	5.9% Strongly Disagree 47.1% Disagree 23.5% Neither 23.5% Agree
S1: If my friends and family trust AI I will also trust it	41.2% Strongly Disagree 35.3% Disagree 23.5% Neither
S2: Society in general trusts AI	47.1% Disagree 29.4% Neither 23.5% Agree

 | DOI: 10.20533/ijicr.2042.4655.2024.0153

S3: The media does not do enough to highlight the threats posed by AI	17.6% Disagree 17.6% Neither 47.1% Agree 17.6% Strongly Agree
B1: I intend to use AI tools on my laptop/device	5.9% Strongly Disagree 11.8% Disagree 11.8% Neither 58.8% Agree 11.8% Strongly Agree
B2: I will recommend the use of AI tools to my friends and family	11.8% Strongly Disagree 35.3% Neither 52.9% Agree

The data showed that several questions elicited a stronger response than others. For TE1, 'AI could easily overcome my device/laptop defenses', 76.5% agreed with this statement. For T5 'AI malware and viruses are a bigger threat today', 64.7% agreed with this statement and T2 'I need AI defenses on my device/laptop', 64.7% agreed with this statement both of which align with research which suggested that the development of AI poses a threat [10]. Evidence shows that younger people adopt new technologies better than older generations [11]. For T3 'AI is a threat to my family and friends', 58.8% disagreed with this statement which may be a reflection of the age profile of the sample which was predominantly in the 19 to 22 year old range. For B1 'I intend to use AI tools on my laptop/device', 58.8% agreed with this statement which may reflect an acceptance that automation technologies such as AI are expected to expand significantly in the near future [14]. As regards 'Which question in this list is AI generated?' showed that 29.4% stated that question S3 'The media does not do enough to highlight the threats posed by AI' was the most likely candidate. In truth, there were no AI generated questions. This was asked as a test which follows up on question TE2 'I could easily detect an AI generated image or piece of text' thus suggesting that the 23.5% of the respondents who responded agree could not easily detect an AI generated piece of text. Importantly, and more directly targeting the initial premise of the model regarding fear of AI, the data also suggest that while T1 'I feel threatened by AI' showed that 58.8% were not afraid of AI, 64.7% also responded that they needed AI defenses on their devices. On the questions regarding society S1, S2 and S3 41.2% strongly disagreed with the statement 'If family and friends trust AI I will also trust it', 47.1% disagreed with the statement that 'Society in general trusts AI'. This suggests family, friends and society in general are not a valid source from which to ascertain if AI tools can be trusted perhaps eluding to the question S3' The media does not do enough to highlight the threats posed by AI' where 47.1% agreed with this statement. As regards the behavioural intention, B1 and B2, 58.8% agreed with the statement that 'I intend to use AI tools on my laptop/device' and 52.9% agreed with the statement that 'I will recommend the use of AI tools to my friends and family. This indicates that rather than exposing a fear of AI, there is some acceptance of the technology perhaps supported by research suggesting that much of AI anxiety is overblown [15]. The model proposed suggests a susceptibility to the threat via threat efficacy represent may positively influence behavioral intention. The questions regarding this TE1 and TE2 showed that 76.5% agreed with the statement that 'AI could easily overcome my device/laptop defenses' and 47.1% disagreed with the statement that 'I could easily detect an AI generated image or piece of text'. There is insufficient data to support this link, but research suggests that where there is high levels of openness to broader interests, novelty and innovation, there tended resistance to technology while those less open tend to be unwilling to try new experiences unless they are forced to [1]. The data aimed at measuring perceptions of threat and their respondents perceived susceptibility. Questions T1 through T4 showed that T1 'I feel threatened by AI', 58.8% disagree, T2'I need AI defenses on my device/laptop', 64.7% agree, T3 'AI is a threat to my family and friends' 58.5% agree and T4 'AI is a global threat' 52.9% agree. While this agrees with some research which suggested that the introduction of AI poses a threat [10] it also suggests that there is a challenge to the effective use of AI technology in our increasingly technology-dependent lives [1].

6. Conclusion

The model proposes that the stronger the perception of a threat being real coupled with the high efficacy with which that threat may cause harm will lead to a behavioural intention to reject AI. Much of AI anxiety and fear may be attributed to three factors: an exclusive focus on AI programs that excludes humans, confusion about autonomy in computation and an exaggerated perception of technological development. There are good reasons to worry about AI but not for the reasons advanced by AI alarmists [15]. To the original point that a rejection of AI based upon fear is dependent upon such theoretical constructs as threat, threat efficacy and social influence, the preliminary data seem to suggest several things. AI defenses and tools are perceived as needed because AI malware and viruses are a larger threat today and could easily overcome a standard laptop's defenses, but conversely, many did not consider AI a threat to peers. The proliferation of AI-like technologies demands careful consideration of ethical implications and ongoing efforts to stay ahead of adversaries. As the cybersecurity landscape continues to evolve, embracing AI technologies responsibly and ethically is essential to ensuring a secure digital future. The premise of creating the AI assistant and future GAI is to take from us those tasks we don't want to think about. This inevitably increases the number of things we can do without thinking. To take these away is to take away certain

 | DOI: 10.20533/ijicr.2042.4655.2024.0153

thinking patterns and imbue the AI with them, more broadly, increasing the number of things that we do without thinking is dangerous, thus our fear of AI may be our own self-fulfilling prophecy. From a practical perspective, reactions to AI merits study for managing workplace habits and practices.

7. References

[1] Anthony, L., M., Clarke, M., C. and Anderson,S. J. (2000). Technophobia and personality subtypes in a sample of South African university students. Computers in Human Behavior, vol. 16, pp. 31-44.

[2] Leventhal, H. (1971). Fear Appeals and Persuasion: The Differentiation of a Motivational Construct. American Journal of Public Health, vol. 61, pp. 1208-1224.

[3] Katari, G. (2022).AI Trends For 2023: Industry Experts (And ChatGPT AI) Make Their Predictions. Forbes.

[4] Hovland, C., Janis, I., L. and Kelly, H. (1953). Communication and Persuasion, New Haven, CT: Yale University Press.

[5] Johnston, A., C. and Warketin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly, vol. 34, no. 3, pp. 549-566.

[6] Rogers, R., W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. Journal of Psychology., vol. 91, pp. 93-114.

[7] Petersen, R. and Liaras, E. (2006). Countering Fear in War: The Strategic Use of Emotion. Journal of Military Ethics, vol. 5, no. 4, pp. 317-333.

[8] Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model, Comminication Monographs, vol. 59, no. 4, pp. 329-349.

[9] Maush, K., Hengstler, S., Schulze, L, and Trang, S. (2021). The Impact of Threat and Efficacy on Information Security Behavior:Applying an Extended Parallel Process Model to the Fear of Ransomware., in Proceedings of the 54th Hawaii International Conference on System Sciences.

[10] British Science Association (2015). One in three believe that the rise of artificial intelligence is a threat to humanity, British Science Association.

[11] Ha, J. G., Page, T. and Thorsteinsson G. (2011). A study on technophobia and mobile device design., International Journal of Contents, vol. 7, no. 2, pp. 17-25.

[12] Lemay, D. J., B. R. B. and Doleck, T. (2020). Fearing the Robot Apocalypse: Correlates of AI Anxiety, International Journal of Learning Analytics and Artificial Intelligence for Education, vol. 2, no. 2, pp. 24-33.

[13] Adams, R. (2019). Helen A'Loy and other tales of female automata: a gendered reading of the narratives of hopes and fears of intelligent machines and artificial intelligence, AI and Society, Journal of Knowledge, Culture and Communication, vol. 35, pp. 569-579.

[14] Wang, Y. Y., and Wang, Y. S. (2022). Development and validation of an artificial intelligence anxiety scale: an initial application in predicting motivated learning behavior, Interactive Learning Environments, vol. 30, no. 4, pp. 619-634.

[15] Johnson D. and Verdicchio, M. (2017). Fearing the Robot Apocalypse. Correlates of AI Anxiety, Journal of the Association for Information Science and Technology, vol. 68, no. 9, pp. 2267-2270.

[16] Chatham House. (2022). Challenges of AI. https://www.chathamhouse.org/2022/03/challenges-ai (Acc -ess Date: 2 February 2024).

[17] Darktrace, (2023). Generative AI: Impact on Email Cyber-Attacks. https://darktrace.com/resources/generative-ai-impact-on-email-cyber-attacks (Access Date: 4 April 2024).

[18] Hayes, J. (2023). AI defenders ready to foil AI-armed attackers, The Register. https://www.theregister.com/2023 /04/20/ai_defenders_ready_to_foil/ (Access Date: 6 August 2024).

[19] Amazon, (2023). Free Machine Learning Services on AWS. https://aws.amazon.com/free/machine-learning/(Access Date 22 February 2024).

[20] C2PA, (2023). Coalition for Content Provenance and Authenticity (C2PA),, Shttps://c2pa.org/ (Access Date: 5 March 2024).

[21] Akter,S. McCarthy, G., Sajib, S., Michael, L., Divedi, Y.K., D'Ambra, J., and Shen, K. N. (2021). Algorithmic bias in data-driven innovation in the age of AI, International Journal of Information Management, vol. 60.

[22] Siau K. and Wang, W. (2020). Artificial Intelligence (AI) Ethics: Ethics of AI and Ethical AI., Journal of Database Management, vol. 31, no. 2, pp. 74-78.

[23] Messerschmidt, J. (2013). Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm, Columbia Journal of Transnational Law.

[24] Liu, Q. Li, P., Zhao, W., Cai, W., Yu S. and Leung, V. C. M. (2018). A survey on security threats and defensive techniques of machine learning: A data driven view, IEEE Access, vol. 6, pp. 12103-12117.

[25] Khanzode K. C. A. and Sarode, R. D. (2020). Advantages and Disadvantages of Artificial Intelligence and Machine Learning: A Literature Review, International Journal of Library and Information Science (IJLIS), vol. 9, no. 1, pp. 30-36.

[26] Baidoo-Anu D. and Owusu Ana, L. (2023). Education in the Era of Generative Artificial Intelligence (AI): Understanding the Potential Benefits of ChatGPT in Promoting Teaching and Learning.

[27] Taddeao, M., McClutcheon T., and Floridi, L., (2019). Trusting artificial intelligence in cybersecurity is a double-

 | DOI: 10.20533/ijicr.2042.4655.2024.0153

edged sword, Nature Machine Intelligence, vol. 1, pp. 557-560.

[28] Wu, H., Haiting, H., Wang, X. and Sun, S. (2020). Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey, IEEE Access, vol. 8, pp. 153826-158848.

8. Acknowledgements

I wish to acknowledge the help of Dr. Gerry McWilliams of the Atlantic Technical College in Letterkenny, Co. Donegal for his help in gathering data for the questionnaire.

 | DOI: 10.20533/ijicr.2042.4655.2024.0153