SAFEGUARDING AGAINST CYBERSECURITY THREATS A COMPARATIVE ANALYSIS OF INSIDER THREATS, SOCIAL ENGINEERING, AND PHISHING ATTACKS

Marshet Zewdie, Adama Science and Technology University, Marshet.tamirat@astu.edu.et
Anteneh Girma, University Of the district of Colombia, Anteneh.girma@udc.edu
Tilahun Sitote, Adama Science and Technology University, Tilahun.melak@astu.edu.et

ABSTRACT

This paper delves into and compares the identification of insider threats, social engineering attacks, and phishing attacks within the realm of cybersecurity. The escalating prevalence of these threats poses considerable difficulties in the successful detection and mitigation of cybersecurity risks. In the present era, cyber attacks not only disrupt normal business operations but also result in alarming corporate customer data breaches. Unfortunately, the current detection systems primarily concentrate on technological aspects and overlook the pivotal role of human behavior in threat detection. This oversight compels corporations to assume substantial risks. Consequently, there is an urgent requirement for comprehensive detection methods that encompass insider threats, social engineering attacks, and phishing attacks. These threats possess unique characteristics and necessitate a fresh approach to comprehensive behavior analysis, particularly through the utilization of deep learning techniques. By integrating deep learning, organizations can enhance their capacity to effectively identify and counteract these threats. However, it is crucial to address the limitations of machine learning models and ensure the quality and representativeness of training data. The article concludes by summarizing the findings and underscoring the importance of adopting a comprehensive deep learning approach to fortify cybersecurity defenses and safeguard against these threats.

ANALYSIS OF IOT SECURITY VULNERABILITY AND THE NEED FOR CYBERSECURITY GOVERNANCE ON IOT DEVICES

Anteneh Girma, University of the District of Columbia,
anteneh.girma@udc.edu
Antione Searcy, University of the District of Columbia,
antione.searcy@udc.edu
Nurus Safa, University of the District of Columbia, nurus.safa@udc.edu

ABSTRACT

The Internet of Things (IoT) refers to systems that involve computation, sensing, communication, and actuation. IoT involves the connection between humans, non-human physical objects, and cyber objects, enabling monitoring, automation, and decision making. The connection is complex and inherits a core set of trust concerns, most of which have no current resolution. Organizations will increasingly use IoT devices for the mission benefits they can offer, but care must be taken in the acquisition and implementation of IoT devices. With the advancement of newer technology, Artificial intelligence, machine learning, the potential risks for hackers to gain access is not if it occurs, but when, and how to mitigate these vulnerabilities. This research paper will address the ongoing threat regarding Internet of Things, and the shortcomings and failures to adapt an overall governance model for securing these devices.

AI-POWERED CLOUD-BASED E-COMMERCE: DRIVING DIGITAL BUSINESS TRANSFORMATION INITIATIVES

Jamshir Qureshi, Purdue University Global, jamshirqureshi@alumni.purdue.edu

ABSTRACT

The digital landscape is rapidly reshaping under the influence of AI-powered cloud-based e-commerce platforms (PCEPs**).** These platforms leverage the transformative power of AI to personalize customer experiences, optimize pricing strategies, enhance security, and streamline operations, offering businesses a significant competitive edge. However, challenges surrounding data privacy, algorithmic bias, and potential job displacement raise crucial ethical questions regarding widespread AI adoption in e-commerce.

This study delves into the untapped potential and ethical considerations of PCEPs, distinguishing itself by proposing practical strategies for responsible development and ethical implementation.

OBJECTIVES

1. Investigate the transformative potential of PCEPs:
   - Personalized product recommendations: Analyze effectiveness and potential bias.
   - Dynamic pricing strategies: Explore impact on consumer fairness and market stability.
   - Enhanced fraud detection: Evaluate accuracy and privacy implications.
   - Optimized supply chain management: Assess efficiency gains and job displacement risks.

2. Critically analyze the ethical considerations of AI in e-commerce:
   - Data privacy: Assess current practices and develop mitigation strategies.
   - Algorithmic bias: Identify potential sources and propose solutions for fairer decision-making.
   - Job displacement: Evaluate impacts and propose reskilling initiatives.

3. Propose comprehensive and practical strategies for responsible PCEP development and implementation:
   - Transparency: Enhance user awareness and control over data usage.
   - Fairness: Design AI systems to mitigate bias and uphold consumer rights.
   - Accountability: Establish clear guidelines and oversight mechanisms for ethical AI development.

CONCLUSION

While PCEPs offer a plethora of transformative benefits, their ethical implementation is paramount. By adhering to principles of transparency, fairness, and accountability, businesses can unlock the full potential of PCEPs while minimizing potential risks and shaping the future of online commerce in a sustainable and equitable manner.

A PANEL REPORT ON AI IN HIGHER EDUCATION FROM THE PERSPECTIVE OF CIOS

Steven A. Schilhabel University of Wisconsin Oshkosh, Steve.Schilhabel@gmail.com

ABSTRACT

The panel's report examines how artificial intelligence (AI), especially generative AI, affects higher education. It is predicated on Midwest College Chief Information Officers (CIOs) observations. The panel report investigates how colleges may match their objectives and aims with the strategic integration of artificial intelligence. It demonstrates how artificial intelligence (AI) may improve teaching methods, boost student engagement, and promote administrative and academic efficiency. The panel report highlights the significance of strategic planning policy creation and addressing ethical standards and data security concerns, and it demonstrates that colleges have differing degrees of preparedness for implementing AI. The report recognizes artificial intelligence's (AI) promise to revolutionize education and the associated obstacles.

INTRODUCTION

Rapid technology breakthroughs are transforming the higher education scene, and artificial intelligence (AI), especially generative AI, is at the vanguard of this change. The results of Ellucian (Beltran, 2023) highlight this evolution, showing that administrators are becoming increasingly optimistic about AI's potential contribution to institutional operation despite the technology's still emerging and isolated use. The potential of generative AI to revolutionize the higher education sector is becoming increasingly evident as it showcases its ability to generate novel content and extract valuable insights from vast datasets (Michel-Villarreal et al., 2023).

The rise of artificial intelligence (AI) as a major force behind innovation and technological advancement transforms how higher education is taught. To future-proof their academic and administrative operations, universities are proactively adjusting to these developments, demonstrating their dedication to innovation and strategic planning. According to Tyton Partners' adoption trends (NeJame et al., 2023), integrating advanced analytics, natural language processing, and machine learning is expected to improve educational delivery and operations. This movement reflects a desire to stay ahead of the curve in the quickly changing educational landscape.

To fully realize AI's transformational potential, it is increasingly essential to strategically integrate AI into university systems in line with academic missions and aims. Recent studies highlight that these initiatives aim to promote inclusive and dynamic learning settings, increase research capabilities, and improve academic quality. They also acknowledge the importance of ethical AI implementation and strong data governance (Beltran, 2023).

AI impacts every stage of the student life cycle, not just the curriculum, by providing individualized learning and career guidance, personalized learning, and admissions. The objective is to create an integrated AI ecosystem that greatly increases student pleasure and achievement, taking into account the disparities in university readiness for AI adoption as well as issues like data privacy and the digital divide (AlDhaen, 2022; Aldosari, 2020; Harry, 2023).

The panel on AI in higher education, which met to debate the changing role of AI in academic settings, provided the basis for this panel report. Chief Information Officers (CIOs) from various universities came together for the panel, and each one brought special views and experiences to the table. These executives in digital strategy and information technology talked about the state of artificial intelligence (AI) in higher education and its possible obstacles and opportunities.

This report's format is intended to coherently provide the panelists' conclusions and debates. After the introduction, Section 2 explores the rationale for this panel's formation and the importance of AI in the contemporary educational landscape. The distinguished panelists are introduced in Section 3 (Panelists), providing an overview of their backgrounds and positions within their respective organizations. Section 4 (Panel Discussion) presents the report's core, which summarizes the panelists' insightful observations, major topics, and lively exchanges. The viewpoints on incorporating AI into academic environments are abundantly available in this section. Section 5 (Conclusion), which concludes the research, summarizes these observations into important conclusions and offers a forecast for the development of AI in higher education. Additionally, acknowledgments and references for sources used to enrich this report are included in Section 6 (Acknowledgements).

MOTIVATION

To learn more about the expanding importance of artificial intelligence (AI) in higher education, I, Steve Schilhabel, collaborated with a panel of university CIOs to organize this panel interview. Collecting and evaluating the perspectives of important figures spearheading these technological techniques in higher education has become crucial as technology, especially artificial intelligence, continues to transform educational systems.

The panel was thoughtfully assembled to tackle crucial inquiries about incorporating artificial intelligence in higher education. These crucial inquiries for our conversation sought to ascertain:

- **AI Integration and Strategic Vision: Our** goal was to ascertain how higher education institutions integrate AI in line with their strategic goals and ambitions. The emphasis was on evaluating AI's role in improving administrative and academic productivity, shifting the technology from an operational tool to a strategic educational asset.
- **AI's Place in the Revolution of Education:** This round of the discussion aimed to assess how AI is changing the dynamics of education. Our goal was to investigate how AI may improve student services, enhance educational opportunities, and increase overall success while adhering to data security and ethical guidelines.
- **Emerging AI Trends in Higher Education:** Considering the rapid pace at which AI technologies are advancing, we were motivated to catalog and analyze the most pertinent and forthcoming AI trends. The goal of this discussion was to learn how universities are preparing to use these advances in AI, with an emphasis on information security and digital literacy.

University Readiness for AI Adoption: Determining the institutions' level of preparedness for implementing AI was a crucial component of our discussion. Our goal was to pinpoint the elements that encourage hope for AI in higher education while also comprehending the worries, especially those about ethical dilemmas and IT security.

PANELISTS

Three of the University of Wisconsin system's most eminent IT leaders, all committed to promoting AI in higher education, were brought together by the esteemed panel. Their combined knowledge offers a road map for deeply incorporating AI to improve the ecosystem for education. The panelists shed light on the important role that AI has had in the advancement of administrative, instructional, and learning processes. The UW system is in a position to create a standard for AI integration in academia under their direction, emphasizing the value of innovation while guaranteeing the moral use of AI in education. Below is a brief bio of each panelist.

- **Mark Clements:** At UW Oshkosh, Assistant Vice Chancellor of Information Technology, Mark Clements is leading the charge to integrate AI into the institution's curricula. His knowledge guarantees that the use of AI is strategically in line with the academic objectives of the university, improving both the educational experience and the institution's standing in the eyes of the public while maintaining security and privacy.
- **Michael Bubolz:** Leading the effort to incorporate AI into UW Green Bay's information technology infrastructure is Michael Bubolz. To provide staff and students with cutting-edge learning environments and the digital fluency they will need in the future, his strategic vision for AI in education is essential.
- **Edward Murphy:** The UW System Administration's Associate Vice President and CISO, Edward Murphy, is essential to guaranteeing the safe integration of AI technologies. His cybersecurity acumen is essential to defending the university's AI projects and guaranteeing a secure learning environment in the digital era.

PANEL DISCUSSION

Q1: AI Integration and Strategic Vision

Topic/Question: How does integrating AI technologies at your institution align with its strategic vision and objectives? In what ways do you foresee AI contributing to enhancing academic and administrative efficiency?

UW Oshkosh's Mark Clements: Mark Clements highlighted the strategic change in AI integration at UW Oshkosh, stressing how it went from being an operational tool to a strategic academic and administrative one.

He said, "The integration of AI must be viewed through the lens of strategic enhancement rather than just operational convenience."

Clements went into detail on how artificial intelligence (AI) is changing how the university delivers instruction and how efficiently it runs, in line with creating a technologically cutting-edge learning environment. This reflects a larger trend in higher education, where AI is turning into a tactical tool essential to pedagogy and institutional operations.

> UW Green Bay's Michael Bubolz: Speaking on AI's revolutionary role at UW Green Bay, Michael Bubolz emphasized the importance of technology in the school's digital transformation process. He said, *"AI is not just a tool but a strategic partner in our journey towards digital transformation."*

Bubolz's viewpoint aligns with the need to see AI as a crucial component of institutional strategy. He also discussed successfully applying adaptive learning platforms, including Arizona State University's ALEKS platform, to highlight how AI may improve academic results and facilitate individualized learning.

Edward Murphy (UW System Administration): Edward Murphy promoted a comprehensive AI strategy that aligns with ethical norms and educational objectives by providing a system-wide viewpoint. His observations emphasize the necessity of a coordinated strategy to utilize AI's capabilities while adhering to moral norms fully. He emphasized the significance of guaranteeing impartial and equitable AI technologies, particularly in delicate domains such as student admissions, assessments, and performance tracking.

According to Alenezi, the digital transformation of modern higher education institutions entails implementing new technology and changing procedures, business models, and practices (Alenezi, 2021). This change aligns with higher education's goal, which is to produce more sophisticated and efficient procedures and processes. This viewpoint is consistent with what Mark Clements and Michael Bubolz have been saying about strategically incorporating AI into the larger goals of their respective universities.

The previous transition of higher education institutions (HEIs) to digital universities is explained by Fernandez (Fernández et al., 2023). This involves adopting new technology such as artificial intelligence (AI) and an organizational transformation involving information, processes, and human elements. This aligns with the scale of digital transformation initiatives and the path to digital maturity, mirroring Edward Murphy's strategic vision for AI integration and the requirement for an all-encompassing digital strategy.

Q2: AI's Role in Educational Transformation

Topic/Question: From your perspective, how can AI transform education dynamics at your university? What potential does AI have in improving student services, learning experiences, and overall success while maintaining ethical standards and data security?

UW Green Bay's Michael Bubolz: Speaking on AI's revolutionary potential, Michael Bubolz of UW Green Bay emphasized how it may completely change classroom instruction and student services.

> *"Our focus is on harnessing AI's potential while safeguarding ethical standards and data integrity,"* he said, arguing in favor of an ethical and balanced approach to integrating AI into education.

The use of adaptive learning systems in higher education is one of AI's more significant potential uses. These systems can adapt the learning process to each student's individual pace, preferences, and performance by using algorithms.

The use of the adaptive learning platform "ALEKS" (Assessment and Learning in Knowledge Spaces) by Arizona State University (ASU) in their introductory math courses is a notable example. ALEKS's real-time assessment of student knowledge and its dynamic adaptation to individual strengths and weaknesses are prime examples of an efficient, personalized learning process. Increased pass rates and better retention in future courses prove that ASU's implementation of ALEKS greatly improved student results. For example, after ALEKS was implemented, pass rates in a collegiate mathematics course increased from 64% to 75%. This approach showed how AI can change conventional teaching methods by enabling teachers to recognize and assist students with difficulties early in the course (Tyson & Sauers, 2021).

The UW System Administration's Edward Murphy: Edward Murphy explored the profound implications of generative AI technologies, such as Bing Enterprise Chat, on pedagogy and learning approaches. He emphasized that integrating AI requires careful consideration, especially when safeguarding private student data.

Murphy brought up an important issue: "There are instructors on all our campuses wrestling with issues related to generative AI, such as, you know, do I prohibit my students from using generative AI?"

This claim emphasizes the continuous discussions and difficulties surrounding AI's morally and practically acceptable integration in educational environments.

Mark Clements (UW Oshkosh): Mark Clements stated that AI has been essential in changing UW Oshkosh's educational methods. He underlined how educational institutions must adapt their practices and offerings to new developments in AI while upholding the highest moral standards. Clements' viewpoint is consistent with the larger trend in education toward the creative and responsible use of AI.

Q3: Emerging AI Trends in Higher Education

Topic/Question: What emerging trends in AI technology do you find most relevant for higher education? How is your university preparing to embrace these advancements, especially regarding digital literacy and information security?

The UW System Administration's Edward Murphy: Focusing on the promise of generative AI to change student services, Edward Murphy underlined the requirement of painstaking caution in AI integration, especially involving student data.

> He emphasized that *"we must approach AI integration with meticulous care, especially when dealing with student data,"* emphasizing the need for high schools to embrace AI technology while striking a critical balance between innovation and security.

UW Green Bay's Michael Bubolz: Michael Bubolz addressed the dualistic character of artificial intelligence and the opportunities and challenges it brings.

> *"AI presents both a challenge and an opportunity - it's about finding the right balance*," he said, arguing in favor of a calculated strategy prioritizing increased digital literacy and strong information security protocols.

Mark Clements (UW Oshkosh): Addressing issues of digital literacy and security, Mark Clements reiterated the comments about utilizing AI's potential in the administrative and academic spheres.

Further investigation of Data Security and Ethical Considerations resulted from this question. According to Edward Murphy, the ethical implications of AI have received a lot of attention, especially in managing sensitive student data. He discussed how higher education is becoming more conscious of the ethical ramifications of AI, including data security and student privacy. These worries are becoming more and more pertinent as large volumes of student data are analyzed by AI systems in education, which calls for strong privacy protection and data breach prevention methods.

In keeping with a larger educational trend that supports the ethical application of AI, Michael Bubolz underlined the necessity of ethical frameworks and rules that strike a balance between innovation and responsibility. Using Georgia Tech's AI ethics course as an example; he emphasized the significance of educating the ethical design of AI systems.

The talks between Murphy and Bubolz highlight the crucial balance that must be struck when implementing AI: taking advantage of its promise for efficient data-driven decision-making and personalized learning while upholding ethical oversight, openness, and justice.

As noted by Borenstein et al., integrating raises difficult ethical issues in several spheres of human existence, including education (Borenstein & Howard, 2021). They stress the significance of preparing upcoming AI experts to consider how AI affects people's lives and take on responsibilities for maximizing benefits while minimizing possible risks. This aligns with Michael Bubolz's focus on the necessity of ethical frameworks in the use of AI, arguing that ethics should be taught in AI curricula and through interdisciplinary teams.

Q4: University Readiness for AI Adoption
Topic/Question for All Panelists: Based on your insights and experiences, how would you evaluate your university's readiness for adopting AI technologies? What aspects make you most optimistic, and what concerns, if any, do you have, particularly regarding IT security? In navigating the AI landscape, Mark Clements (UW Oshkosh) underlined the significance of strategic planning.

> As he pointed out, *"We're navigating uncharted waters with AI, and strategic planning is key to our successful adoption,"* proactive policy formulation and alignment with institutional objectives are critical.

In his discussion of AI preparedness, Michael Bubolz (UW Green Bay) concentrated on identifying the potential of AI and creating strategic plans for its successful integration.

> *"It's about aligning our AI initiatives with our mission while upholding our commitment to ethical standards,"* said Bubolz, emphasizing the significance of doing so. Bubolz also emphasized the need to maintain high ethical standards.

The importance of creating adaptable AI regulations to control AI's expanding interest and applications in the educational sector was highlighted by Edward Murphy (UW System

Administration). He emphasized the necessity of a system-wide strategy and the significance of strategic adoption and cooperation across the educational landscape.

As reported by Crompton's systematic review, the substantial growth in publications on AI in higher education suggests a quickening of interest and advancement in this topic (Crompton & Burke, 2023). The review revealed some trends, including a greater emphasis on language acquisition and undergraduate students and the application of AI in tutoring, assessment, prediction, and assistance. These results demonstrate the variety of uses of AI in higher education and give context to Mark Clements' discussion of adoption readiness.

This question prompted further investigation of the Opportunities and Challenges in AI Integration. The conversation between Michael Bubolz and Mark Clements highlights the challenges of incorporating AI into systems of higher learning. The significance of preparation and strategic planning for the effective integration of AI addresses a range of AI uses, including intelligent tutoring systems, predictive analytics, assessment, evaluation, and student learning management.

These varied applications draw attention to the necessity of all-encompassing approaches that balance institutional preparedness, ethical issues, and technical potential. For instance, predictive analytics in artificial intelligence presents ethical questions about handling sensitive data and is essential for predicting patterns like dropout rates and school performance.

The subject of System-Wide Coordination and Strategy was then brought up. Edward Murphy's observations regarding the need for an all-encompassing strategy when using AI technologies speak to a larger issue facing the industry. This strategy addresses policy, ethical issues, data security, and stakeholder involvement at the university system level while integrating technology.

Taking care of the digital gap and ensuring that all educational institutions have equal access to cutting-edge AI technologies and resources are important components of this strategy. This is essential to guarantee that the benefits of AI are shared fairly and to avoid escalating the gaps in educational outcomes.

Harry discusses how artificial intelligence (AI) can potentially change higher education. Still, he also highlights some current barriers, including potential bias, expense, lack of trust, and privacy and security issues (Harry, 2023). Focus is placed on the importance of ethical considerations, which include making sure AI-based systems are accessible, transparent, and equitable. This emphasizes the necessity to weigh the advantages and disadvantages of integrating AI into educational settings, consistent with Edward Murphy's focus on the ethical aspects of AI managing sensitive student data.

CONCLUSION

The panelists' combined experiences presented the higher education industry at a critical point in its embrace of AI. Their observations demonstrate a deep understanding of the significance of ethical issues, strategic alignment, and AI integration readiness. These themes are not isolated; they are a part of a larger story in higher education, where technology is becoming increasingly

recognized as essential to operational effectiveness, instructional innovation, and institutional strategy.
The conversation made it evident that although there is hope for AI's potential, there is also a clear understanding of its drawbacks. Because of this, the panelists' perspectives provide a road map for navigating AI's potential in higher education, highlighting the significance of methodical, calculated, and moral methods.

KEY FINDINGS

The opinions from our panel of experts have shed light on the dynamic and changing role of AI in higher education. Chief Information Officers (CIOs) must concentrate on a few crucial areas as colleges traverse this crucial time to adequately meet the problems posed by AI and realize its full potential. These domains consist of:

- **Strategic Alignment with Institutional Goals:** AI projects need to be closely aligned with the purpose and goals of universities. This necessitates incorporating AI into institutions' pedagogy and fundamental operations, ensuring that these technologies advance the overarching strategic vision.
- **Ethical Issues with AI Deployment:** Adhering to ethical guidelines is critical when implementing AI, especially concerning data protection, bias, and transparency. CIOs need to take the lead in creating guidelines and regulations that support ethical AI use and educate the academic community for higher education on the moral implications of AI.
- **Readiness for AI Integration:** Investing in infrastructure, promoting innovation, and improving digital literacy are all necessary steps in getting ready for AI adoption. CIOs play a critical role in equipping the university community to effectively use AI technology by helping to develop AI competencies among staff and students.
- **Reducing the Digital Divide:** It is essential to guarantee equitable access to AI resources. CIOs must work to close the digital gap by supporting policies that give all faculty and students fair access to AI tools.
- **System-Wide Coordination and Collaboration:** Because AI integration is complicated, university divisions must work together in a coordinated manner. CIOs should encourage cooperation and knowledge exchange to maximize AI adoption and impact.

Our research team found that CIOs are critical in helping institutions navigate the AI-driven era in our panel report. They must manage cooperative efforts, ethical deployment, community preparedness, equitable access, and strategic alignment.

DIRECTIONS FOR FUTURE WORK

Future research should examine faculty and student perspectives on artificial intelligence's impact on higher education, according to our collaborative panel, which includes me (Steve Schilhabel) and the distinguished panel of Chief Information Officers. One can acquire a fuller understanding of the diverse impact of AI. This strategy will make it easier to compare and contrast these viewpoints with those of the IT and administrative leadership, improving our understanding of AI's place in the educational system.

AI's role in higher education will not be limited to transforming teaching and learning. It will entail changing labor markets, rethinking educational models, and restructuring institutional frameworks. Universities can take the lead in educating students for a workforce driven by AI and develop into hubs for innovation in technology and community involvement.

REFERENCES

AlDhaen, F. (2022). The Use of Artificial Intelligence in Higher Education - Systematic Review. In COVID-19 Challenges to University Information Technology Governance. https://doi.org/10.1007/978-3-031-13351-0_13

Aldosari, S. A. M. (2020). The future of higher education in the light of artificial intelligence transformations. International Journal of Higher Education, 9(3). https://doi.org/10.5430/ijhe.v9n3p145

Alenezi, M. (2021). Deep dive into digital transformation in higher education institutions. Education Sciences, 11(12). https://doi.org/10.3390/educsci11120770

Beltran, K. (2023). Higher Education Leaders Eager to Embrace AI and Transform Campus Operations. https://www.ellucian.com/assets/en/article/higher-education-leaders-eager-embrace-ai-transform-campus-operations.pdf

Borenstein, J., & Howard, A. (2021). Emerging challenges in AI and the need for AI ethics education. AI and Ethics, 1(1). https://doi.org/10.1007/s43681-020-00002-7

Crompton, H., & Burke, D. (2023). Artificial intelligence in higher education: the state of the field. International Journal of Educational Technology in Higher Education, 20(1). https://doi.org/10.1186/s41239-023-00392-8

Fernández, A., Gómez, B., Binjaku, K., & Meçe, E. K. (2023). Digital transformation initiatives in higher education institutions: A multivocal literature review. Education and Information Technologies, 28(10). https://doi.org/10.1007/s10639-022-11544-0

Harry, A. (2023). Role of AI in Education. Interdiciplinary Journal and Hummanity (INJURITY), 2(3). https://doi.org/10.58631/injurity.v2i3.52

Michel-Villarreal, R., Vilalta-Perdomo, E., Salinas-Navarro, D. E., Thierry-Aguilera, R., & Gerardou, F. S. (2023). Challenges and Opportunities of Generative AI for Higher Education as Explained by ChatGPT. Education Sciences, 13(9). https://doi.org/10.3390/educsci13090856

NeJame, L., Bharadwa, Dr. R., Shaw, C., & Fox, K. (2023, April 25). Generative AI in Higher Education: From Fear to Experimentation, Embracing AI's Potential. Tyton Partners, Blog Post.

Tyson, M. M., & Sauers, N. J. (2021). School leaders' adoption and implementation of artificial intelligence. Journal of Educational Administration, 59(3). https://doi.org/10.1108/JEA-10-2020-0221

LEARNING BY DOING: ACQUIRING THE TACIT KNOWLEDGE OF HOW TO CONDUCT AN OPEN-SOURCE INTELLIGENCE COLLECTION AND ANALYSIS PROJECT

Fred Hoffman, fhoffman@mercyhurst.edu

ABSTRACT

Intelligence professionals working in analytic jobs in the U.S. intelligence community, in law enforcement intelligence, or in the competitive intelligence field can increasingly expect to participate in, or even lead, intelligence project teams. At Mercyhurst University, the first-ever intelligence studies program in the United States, resident graduate students in Applied Intelligence prepare for intelligence careers by taking the mandatory Strategic Intelligence capstone course. This course enables them to gain valuable tacit knowledge by conducting a semester-long, intelligence collection and analysis project for a real-world, external client. Based on a positivist intellectual paradigm and consistent with the theory of Social Constructivism, students learn to operate effectively as a team, acquire and apply project management skills, communicate with external clients, articulate Key Information Topics and Key Information Questions, scope a project, use specialized, commercially-available software and tradecraft to conduct open-source intelligence collection, aggregate and share acquired intelligence, comply with Intelligence Community Directive 203 (Analytic Standards), select and use appropriate structured analytic techniques, evaluate sources and information, write a final estimative intelligence product using probabilistic language, and present timely, actionable intelligence and findings to different types of audiences.

INTRODUCTION

The growth of intelligence as an academic field of study.

Intelligence studies is a burgeoning field in academia, with over 150 institutions now teaching intelligence in the United States alone (Dexter et al., p. 2017). In colleges and universities, intelligence has become “an academic complement to the practice of national security intelligence” (Marrin, 2016, p. 266). Today, there are many different degree programs in the intelligence field: Depending on which college or university they attend, students in the United States could earn a bachelor’s or master’s degree, in residence or online, in such degree programs as Homeland Security, Security Studies, Cyber Intelligence and Security, or Global Security; they could also minor in Defense Studies, Diplomatic and Military History, or Technical Intelligence. Mercyhurst University, which boasts the oldest intelligence studies department in the United States, prepares undergraduate and graduate students to transition after graduation into intelligence jobs in national security, intelligence support to law enforcement, or competitive intelligence.

RESEARCH OBJECTIVE

This study sought to answer the question, “How does a real-world intelligence research project enable graduate students to leverage explicit knowledge acquired from a master’s program in applied intelligence and gain the tacit knowledge necessary to perform effectively on an intelligence project team?”

Mu's Master Of Science In Applied Intelligence

At Mercyhurst University, undergraduate students can enrol in a resident undergraduate degree program in Intelligence Studies, while graduate students can earn a Master of Science in Applied Intelligence either online or in residence. One of the goals of the Mercyhurst master's degree program in Applied Intelligence is to teach graduate students how to effectively conduct intelligence collection and analysis while serving on, or leading, an intelligence project team. A master's degree program is not the same as a training program; yes, students learn about the intelligence profession, its history, and how intelligence is collected, analyzed, and reported. But most of all, students are taught how to think creatively and how to adapt to different intelligence requirements and needs.

Most of the students in the Mercyhurst master's degree program in Applied Intelligence do not have undergraduate degrees in Intelligence Studies, and it is a rarity in the resident program to have students who worked in the intelligence field prior to participating in the graduate degree program. For these reasons, for students enrolled in Mercyhurst's two-year-long master's degree program, the experience can be a lot like drinking from a fire hose. In contrast to students in the four-year-long undergraduate degree program, graduate students have only *two* years to learn about the intelligence profession, develop, write, and defend a master's degree, and then draw upon their accumulated knowledge and skills in a project-based Strategic Intelligence class. Strategic Intelligence is a capstone course that requires second-year graduate students to apply the knowledge gained over the previous year and a half to a real-world, semester-long intelligence project in support of an external client.

The Strategic Intelligence course

What is strategic intelligence? More than six decades ago, Sherman Kent (1949) distinguished between *intelligence* and *strategic intelligence* by asserting that the latter refers to "knowledge vital for national survival" (p. vii). With this distinction in mind, Strategic Intelligence course students draw upon all they have learned from various intelligence courses in the program and apply that knowledge as part of an intelligence project team supporting an external client, performing such tasks as:

- Receive a customer's initially stated intelligence needs and translate those into mutually comprehensible, executable, and achievable collection requirements;
- Formulate clear Key Intelligence Topics and Key Intelligence Questions (KIT/KIQ);
- Present KIT/KIQ to the client in a Terms of Reference (TOR) document;
- Engage in open-source intelligence (OSINT) collection;
- Engage in human intelligence (HUMINT) collection;
- Evaluate sources and information in accordance with intelligence community practices;
- Aggregate, store, access, and analyze intelligence;
- Recognize and mitigate analytic bias;
- Select and use appropriate structured analytic techniques;
- Write different types of intelligence reports;
- Properly write an estimative intelligence report with key judgments written in probabilistic language;
- Prepare and submit project deliverables;
- Professionally present intelligence project findings, both orally and in writing.

REVIEW OF THE LITERATURE

Growing academic interest in intelligence

Just as there has been an expansion in intelligence as a field of academic study, there has been a similar growth in the number of intelligence-related scholarly publications. CIA analyst Sherman Kent (1955) advocated for an increase in intelligence literature. As Marrin (2016) observed, although "intelligence studies literature is quite large, and growing," this "was not always true" (p. 267). However, the volume of intelligence literature has increased, especially since the start of this century. In fact, as Van Puyvelde and Curtis (2016) observed, it has recently reached the point where, "Students of intelligence can now rely on a substantial body of literature to inform their research and contribute to knowledge in this specific field of study," (p. 1040). Based on their examination of intelligence literature, Coulthart and Rorissa (2023) identified three distinct eras for the production of intelligence literature: The *practitioner era* (1950-1985), the *scholarly emergence era* (1986-2001), and the *exponential growth era* (2002-2020). It is in this most recent era that there has been a proliferation of scholarly articles about intelligence: "The last ten years alone (2010–2020) have seen more article-based knowledge production than the previous sixty years combined (1950–2010)" (Coulthart & Rorissa, 2023, p. 1003). Scott and Jackson (2004) noted how the terror attacks of 11 September 2001, and the alleged distortion of intelligence information to justify the 2003 invasion of Iraq, resulted in greater public interest in intelligence and contributed to the "development of intelligence studies" (p. 140). Scott and Jackson (2004) also asserted that, "The rapid growth of intelligence as a focus of academic enquiry will surely continue" (p. 140).

Academic interest in intelligence analysis

Coulthart and Rorissa (2023) noted that intelligence analysis was of particular interest to a large number of scholars writing on intelligence topics. Contributing to this increase in academic and scholarly interest in intelligence analysis are periodic conferences attended by intelligence scholars, such as the Strategic Consortium of Intelligence Professionals (SCIP) and the International Association for Intelligence Education (IAFIE) (Coulthart & Rorissa, 2023). Intelligence analysis is also of growing interest in the private sector (García-Madurga & Esteban-Navarro) and also in law enforcement intelligence (Guerette et al., 2021).

What is intelligence analysis, and how should it be performed?

The meaning of the terms *intelligence* and *intelligence analysis*, and the purpose of intelligence, continue to evolve. As Marrin (2016) asserted, there still is no universally agreed-upon definition of what intelligence is, or what its purpose might be. In the 20th century, intelligence evolved "from a staff function focused on information collection and collation, mainly for military commanders," to an "institution that reports tailored operational information" to military, government, and corporate decision-makers (Pili, 2023, p. 129).

Ben Jaffel and Larsson (2023) pointed out how, in this century, intelligence practices have spread to other professions and practitioners. Walsh and Harrison (2021) examined the roles played by leadership, organizational culture, cognitive factors, and technology in influencing the evolution of how strategic intelligence is performed in Australia since the 9/11 attacks. Marrin (2016) opined that as the field of intelligence studies grows in academia, this will enable an improved understanding of the intelligence and the intelligence field, both within the government and within the private sector. Scott and Jackson (2004) asserted that "the essence of intelligence lies at the level of analysis or assessment" (p. 142). Pili (2023) observed that although intelligence analysis was "one of the most explored topics in intelligence studies", it is also true that "decoding its nature is still challenging" (p. 128). Pili (2023) also argued that what is often called intelligence analysis "is much more synthesis – namely, structuring sensory data collection – than analysis" (p. 128). Delagenière (2021) argued there should be a critical discourse analysis approach in addition to the evidence-based reasoning methodology contained in Sherman Kent's positivist epistemology. Arcos and Palacios (2020) stated that, "Intelligence analysis is widely considered one of the cornerstones of the intelligence function" (p. 73). Teirilä (2024) noted that in addition to thinking about how strategic intelligence analysis is performed, and what the desirable qualities of an intelligence analyst should be, more attention must be paid to how an analyst is trained and developed.

The professionalization of intelligence analysis

Established in 2000, the Sherman Kent Center for Intelligence Analysis, located on CIA's Langley, Virginia campus, is named after the former Yale professor and CIA analyst who had been largely responsible for the professionalization of intelligence analysis within the Central Intelligence Agency during the 1950s and 1960s (Davis, 2002). As Davis (2002) noted, "Kent's *Strategic Intelligence* and the articles and letters he wrote around the time of CIA's establishment, about the need to ensure that the US intelligence effort attracts the country's best minds, had a profound effect on the early Directors and their top aides" (p. 6). As shown in table 1 (below), Frans Bax, founding Dean at the Kent School and later President of CIA University, identified nine characteristics of Kent's professional code for intelligence analysts (Davis, 2002, p. 8).

Table 1. Sherman Kent's professional code for intelligence analysis (Davis, 2002, p. 8).

1	Focus on policymaker concerns
2	Avoidance of a personal policy agenda
3	Intellectual rigor
4	Conscious effort to avoid analytic biases
5	Willingness to consider other judgments
6	Systematic use of outside experts
7	Collective responsibility for judgment
8	Effective communication of policy-support information and judgments
9	Candid admission of mistakes

Different approaches to teaching intelligence analysis

With respect to the teaching of intelligence analysis, Kilroy (2017) noted "how academics and practitioners often differ in their views of intelligence analysis" and asked, "is it an art or science?; tradecraft or training?; creative or critical thinking?" (p. 71). A gathering of intelligence educators from five universities "shared their views on how they approach the teaching of intelligence analysis within their specific academic departments and disciplines" (Kilroy, 2017, p. 73). Kilroy (2017) explained how methodologies used at these five universities to teach intelligence analysis included intensive readings, learning structured analytic techniques, working in teams, learning how to effectively communicate with decision-makers and intelligence product end users, being given tasks where they "can fail, adopt, and succeed" (p. 78) "implement the research design by learning in a trial and error way (like riding a bike)" (p. 79), and use estimative language. One of the professors in Kilroy's (2017) study noted how undergraduates frequently fail to read assigned materials.

METHODOLOGY

Theoretical foundation

In Mercyhurst's Strategic Intelligence course for second-year graduate students, the research orientation is a *positivist intellectual paradigm*, a paradigm that Phythian (2021) described as "one committed to the idea of the possibilities of producing neutral, objective, intelligence based on the accumulation of facts and dispassionate analysis of them" (p. 314). The theoretical underpinning of our approach to intelligence in the master's program in Applied Intelligence is *social constructivism*, an approach which Dexter et al. (2017) described as viewing "teachers and students as partners engaged in a joint enterprise of knowledge production" (p. 924). Rather than simply being passive recipients of classroom lectures, students in the Strategic Intelligence capstone course are instead active participants with both the professor and foreign intelligence partners in the active creation and execution of an intelligence activity.

Learning by doing

One of the concepts embraced by the U.S. military is that of "Be-Know-Do", which incorporates what a military servicemember must *be*, must *know*, and must *do* (Sangwan & Raj, 2021). Polanyi (1966) asserted that there are two types of knowledge, *explicit* and *tacit*. Explicit knowledge is easily conveyed and easily learned. Tacit knowledge is harder to convey, and therefore harder to learn. Learning how to play soccer, or ride a bicycle, is an example of tacit knowledge (Fruehauf et al., 2014). Learning how to conceptualize, plan, and execute an intelligence activity involves the acquisition of tacit knowledge because it is a "socially constructed phenomenon" (Fruehauf et al., 2014, p. 103). As Dexter et al. (2017) asserted, "people learn best through doing" (p. 924). Apprenticeships are a common method for transferring tacit knowledge from experienced practitioners to those who are new to a profession. Similarly, "using intelligence professionals in academic activity is a means of transferring expertise and institutional culture to future theoreticians and practitioners" (Coldea, 2019, p. 81). As Dexter et al. (2017) asserted, "Student interaction, then, is the key to active learning" (p. 925).

The value of working as a project team

"Learning is a collaborative process," as Dexter et al. (2017) observed (p. 925). Working as part of an intelligence project team in Strategic Intelligence is not only beneficial for effective learning, but as preparation for the demands of a career as an intelligence analyst: Whether working in one of the 18 organizational entities that currently comprise the U.S. intelligence community, as an intelligence practitioner in federal or state law enforcement, or in the private sector field of competitive intelligence, analysts increasingly find themselves working as members of a project team. As Heuer and Pherson (2011) pointed out, "This is a major change from the traditional concept of analysis as largely an individual activity" (p. 21).

Creating and enabling a project team

Tuckman (1965), a psychologist, introduced the four-step construct of group behavior that he referred to as *forming*, *storming*, *norming*, and *performing*. According to Tuckman (1965), *forming* is where group members establish relationships "with leaders, other group members, or preexisting standards" (p. 396). *Storming* is characterized by friction in the early phase of the project, as team members carve out responsibilities (Tuckman, 1965). As resistance and friction is overcome, the group enters the *norming* phase. In the *performing* phase, “interpersonal structure becomes the tool of task activities. Roles become flexible and functional, and group energy is channeled into the task” (Tuckman, 1965, p. 396). Hackman (2011) identified six enabling conditions necessary for creating an optimal intelligence project team: (1) Create a real team; (2) specify a compelling team purpose; (3) put the right people on the team; (4) establish clear norms of conduct; (5) provide organizational supports for teamwork, and (6) provide well-timed team coaching.

Intelligence project management

Successfully managing an intelligence project requires that project team members be familiar with some basic project management principles. García-Madurga and Esteban-Navarro (2020) examined how project management principles outlined by the Project Management Institute (PMI) were useful for human intelligence teams conducting collection and analysis for competitive intelligence firms. To be successful, effective intelligence analysts and managers require certain rudimentary project management skills. Such skills include:

- Conduct an effective “kick-off” meeting
- Conceptualize and plan how to perform collection, analysis, and production tasks in the time available
- Task organize the project team
- Develop a work breakdown structure
- Developing a project schedule, with milestones and interim objectives
- Manage an intelligence project while remaining attentive to the “triple constraint” of cost, schedule, and scope

Working with a foreign partner

At the start of the project, the external customer provides the team with an unclassified, open-source intelligence (OSINT) collection requirement. Sometimes the external customer is a foreign entity, which adds additional complexity to the project. Whitford and Prunckun (2017) examined the pedagogical, linguistic, and cultural challenges associated with teaching foreign non-governmental organizations (NGO) how to gather and analyze intelligence information, and noted the “difference in world view” reflected in the use of intelligence language (p. 54). Fortunately for the most recent student project team, the foreign counterpart consisted of professional military intelligence officers from a NATO partner country who possessed a comparable understanding of, and attitude towards, intelligence collection and analysis. Communication between the student team and the foreign partner was successfully accomplished via regularly scheduled Zoom calls and email.

The kick-off meeting

Kent (1949) wrote, “There is no phase of the intelligence business which is more important than the proper relationship between intelligence itself and the people who use its product. Oddly enough, this relationship, which one would expect to establish itself automatically, does not do this” (p. 180). It is at the kick-off meeting that the relationship between the intelligence project team (who will provide the intelligence) and the customer (who will use the intelligence) is formed. In the most recent project, the student team received and reviewed the customer’s original intelligence requirements and then organized a “kick-off meeting” with the foreign customer to review and refine the tasking. The team then provided the customer with their proposed KIT and

KIQ, a series of questions that the team would seek to answer during the course of the research project. KIT and KIQ are not only used in the U.S. intelligence community, but also by competitive intelligence professionals in the private sector for the purpose of effectively scoping a research project and ensuring a shared understanding between the client and the team regarding the intelligence project's objectives (Herring, 1999).

Scoping the project

One of the earliest tasks for the student project team is scoping the project so that it can be successfully completed within a 14-week-long semester. One of the principles of project management is the tyranny of the so-called "triple constraint" of cost, time, and scope: It is not possible to change one of these without impacting the other two (Van Wyngaard et al., 2012).

The pros and cons of open-source intelligence (OSINT) collection

According to *Army Techniques Publication* (ATP) 2-22.9 (2012), the Army's current manual for open-source intelligence collection, OSINT collection may be conducted in public speaking fora, public documents, public broadcasts, and Internet web sites. Open-source intelligence is more than just poking around on the Internet with one's preferred search engine; one must know where, and how, to look for information: Less than five percent of the Internet is indexed for search engine retrieval (Kobayashi & Takeda, 2000). In order to securely access websites in sensitive foreign countries, student project team members must have access to specialized, commercially-available software, employ managed attribution, and be familiar with appropriate online OSINT tradecraft (Fuchs & Lemon, 2019). Because not all Internet-based information is equally reliable, or valid (*Army Techniques*, 2012), the student project team used the Army's alphanumeric system for assessing acquired information. Wherever possible, the team strove to maximize efficiency and effectiveness. For example, they established collection lanes in the road to avoid the duplication of effort. They established a shared folder system for storing collected intelligence, enabling them to quickly ascertain whether something a team member came across had already been collected. Team members named files with standardized dates and names to simplify recovery and retrieval and used commercially-available social media apps (such as Signal, Microsoft Teams, and WhatsApp) to rapidly communicate and exchange information.

Complying with ICD 203, Analytic Standards

In previous courses, team members learned structured analytic techniques (SAT), a collection of analytic techniques intended to improve the quality of intelligence analysis, mitigate analytic bias, and increase transparency by enabling analysts to show their work and explain how they reached the conclusions they had reached (Heuer & Pherson, 2011). The purpose of structured analytic techniques is to "divide an intelligence problem into simple pieces and solve them accordingly" (Pili, 2023, p. 130). Although the *term* structured analytic techniques is relatively new, first used in the Intelligence Community in 2005 (Heuer & Pherson, 2011), a "review of hundreds of declassified national intelligence assessments from 1947 through the 1990s reveals elements of most" of them (Marchio, 2014, p. 159). Artner et al. (2016) noted how the intelligence community has made increased use of structured analytic techniques (SAT) "in the years following the intelligence failures on Iraqi weapons of mass destruction" (p. 3).

The Office of the Director of National Intelligence (ODNI) first disseminated Intelligence Community Directive 203, *Analytic Standards*, in 2007 (ICD 203, 2007). The stated purpose of this directive was to "promote rigorous analysis, lessen the risk of intelligence failure, and make analysts' reasoning more transparent to consumers" (Artner et al., 2016, p. 1). The most recent iteration of ICD 203, published in 2022, states that its purpose is to express "the responsibility of intelligence analysts to strive for excellent, integrity, and rigor in their analytic thinking and work practices" (ICD 203, 2022, p. 1). To achieve this goal, ICD 203 (2022) identifies five analytic standards and nine analytic tradecraft standards that U.S. intelligence community analysts should follow. According to ICD 203 (2022), the five analytic standards are that intelligence products should be: (1) Objective, (2) independent of political consideration, (3) timely, (4) based on all available sources of intelligence information, and (5) based on analytic tradecraft standards. The nine analytic tradecraft standards listed in ICD 203 (2022) are that an intelligence product: "(1) Properly describes quality and credibility of underlying sources, data, and methodologies; (2) Properly expresses and explains uncertainties associated with major analytic judgments; (3) Properly distinguishes between underlying intelligence information and analysts' assumptions and judgments; (4) Incorporates analysis of alternatives; (5) Demonstrates customer relevance and addresses implications; (6) Uses clear and logical argumentation; (7) Explains change to or consistency of analytic judgments; (8) Makes accurate judgments and assessments; and (9) Incorporates effective visual information where appropriate" (p. 4-5).

Selection and use of structured analytic techniques

Over the years, many intelligence analysts have created and used specialized tools and techniques to improve the efficiency and accuracy of their work; however, in recent years, there has been an attempt to capture, codify, and standardize the use of what has become known as structured analytic techniques (Artner et al., 2016, p. 3). One of the most familiar references currently used by intelligence analysts has been Heuer and Pherson's (2011) Structured analytic techniques for intelligence analysis. The Mercyhurst project team made use of the following a described in that book:

Brainstorming

Brainstorming is a structured analytic technique that most people have heard of, but have probably done incorrectly (Heuer & Pherson, 2011). Structured Brainstorming, or Divergent/Convergent Thinking, is a 12-step process originally developed for CIA's Sherman Kent School for Intelligence Analysis (Heuer & Pherson, 2011). Done correctly, brainstorming requires a facilitator and for brainstorming session participants to write down, rather than verbalize, their responses to facilitator questions. This serves to mitigate Groupthink and prevents more vocal session members from dominating the conversation.

Hypothesis Generation

A hypothesis is "a potential explanation or conclusion that is to be tested by collecting and presenting evidence" (Heuer & Pherson, 2011, p. 122). Based on what they have observed and know, an analytic team articulates a hypothesis as a statement (rather than as a question). The hypothesis "contains a dependent and an independent variable. The dependent variable is the phenomenon being explained. The independent variable does the explaining" (Heuer & Pherson, 2011, p. 122).

Key Assumptions Check

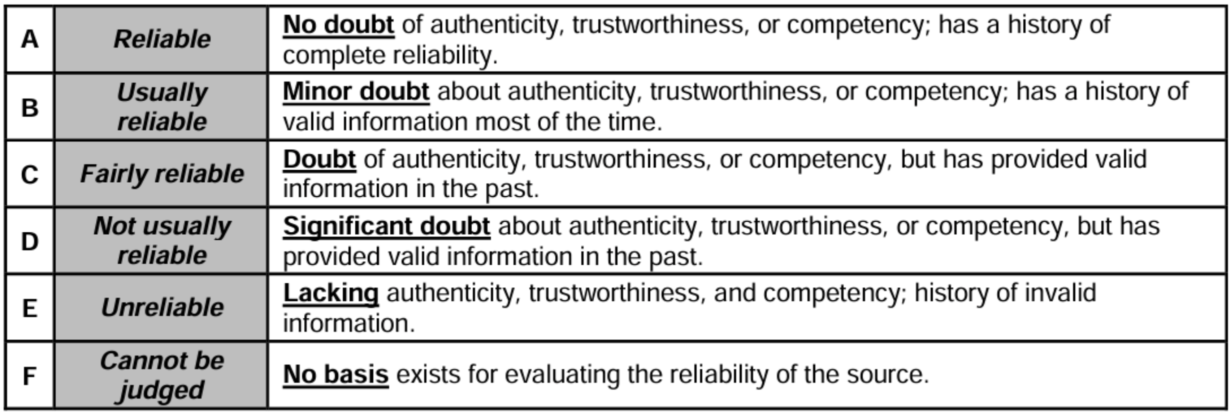
Heuer and Pherson (2011) describe this technique as “a systematic effort to make explicit and question the assumptions (the mental model) that guide an analyst’s interpretation of evidence and reasoning about any particular problem” (p. 148). Explicitly articulating assumptions in a written document is part of the team’s effort to show their work, as ICD 203 (2022) requires. Failing to acknowledge assumptions can have catastrophic consequences for an analytic team. For example, in the 2002 DC sniper case, law enforcement officials mistakenly assumed the perpetrator was a white male with military experience, driving a white van (Beebe & Pherson, 2015).

Source identification and assessment

Artner et al. (2016) noted how ICD 203 (2007) asserted that a finished intelligence product “properly describes quality and reliability of underlying sources” (p. 12). The importance of this requirement was reflected by the fact that, in addition to issuing the original ICF 203 in 2007, the Office of the Director of National Intelligence (ODNI) also issued ICD 206 (2007), *Sourcing Requirements for Disseminated Analytic Products*. ICD 206 (2007) requires analysts to provide a **source reference citation**, or SRC, to identify sources of information or analytic judgments. Sourcing information should be provided in the form of source reference citations, appended reference citations, source descriptors, and source summary statements. As ICD 206 (2007) instructed, “Analysts should use a combination of these mechanisms to optimize clarity and reader understanding” (p. 3).

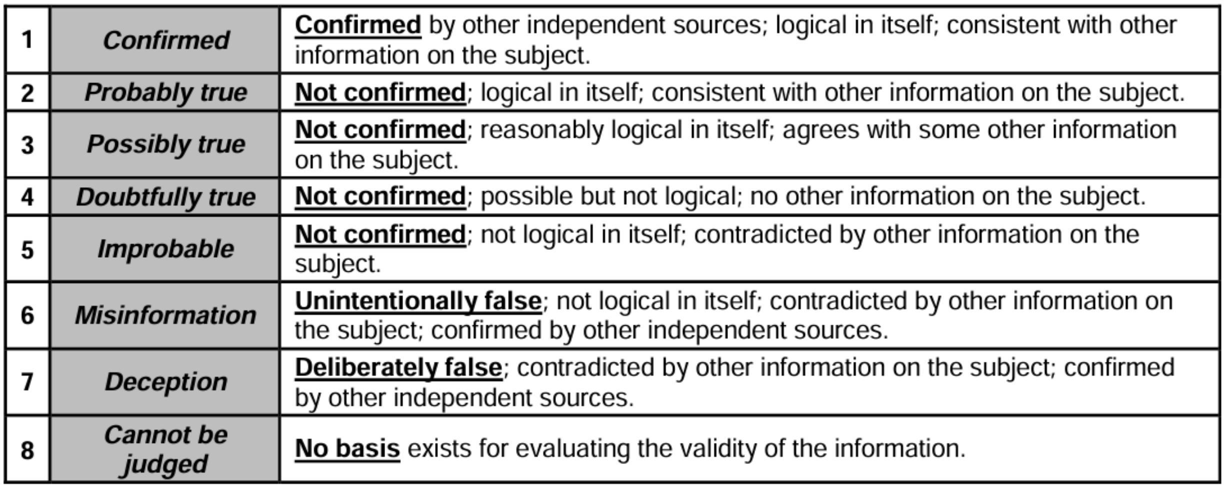
Alphanumeric source descriptions

ICD 206 (2007) encouraged analysts to provide **source summary statements** “to provide a holistic assessment of sourcing that supports a covered analytic product” (p. 3). Not all OSINT reporting is of equal quality or legitimacy; for this reason, the analytic team rated individual information sources using the U.S. Army’s alphanumeric code for evaluating both **source reliability** and **source credibility**. For example, as shown in figures 1 and 2, an F-8 code might be given to a source for which there is no means for evaluating either the source’s reliability or the reliability of the reported information (*Army Techniques*, 2012).



A	***Reliable***	**No doubt** of authenticity, trustworthiness, or competency; has a history of complete reliability.
B	***Usually reliable***	**Minor doubt** about authenticity, trustworthiness, or competency; has a history of valid information most of the time.
C	***Fairly reliable***	**Doubt** of authenticity, trustworthiness, or competency, but has provided valid information in the past.
D	***Not usually reliable***	**Significant doubt** about authenticity, trustworthiness, or competency, but has provided valid information in the past.
E	***Unreliable***	**Lacking** authenticity, trustworthiness, and competency; history of invalid information.
F	***Cannot be judged***	**No basis** exists for evaluating the reliability of the source.

Figure 1. Open-source reliability ratings. ATP 2-22-9 (2012), p. 22.



1	*Confirmed*	**Confirmed** by other independent sources; logical in itself; consistent with other information on the subject.
2	*Probably true*	**Not confirmed**; logical in itself; consistent with other information on the subject.
3	*Possibly true*	**Not confirmed**; reasonably logical in itself; agrees with some other information on the subject.
4	*Doubtfully true*	**Not confirmed**; possible but not logical; no other information on the subject.
5	*Improbable*	**Not confirmed**; not logical in itself; contradicted by other information on the subject.
6	*Misinformation*	**Unintentionally false**; not logical in itself; contradicted by other information on the subject; confirmed by other independent sources.
7	*Deception*	**Deliberately false**; contradicted by other information on the subject; confirmed by other independent sources.
8	*Cannot be judged*	**No basis** exists for evaluating the validity of the information.

Figure 2. Open-source information content credibility. ATP 2-22-9 (2012), p. 22.

Deciding on an appropriate intelligence product and reporting format

There are many different types of intelligence products, such as basic intelligence, current intelligence, and estimative intelligence (Lowenthal, 2017). Depending on a customer's intelligence needs, a student project team will decide on which type of intelligence product is appropriate and create products appropriate for that category. In the most recent case, the student project team opted to engage in estimative intelligence and craft products consistent with this type of intelligence. This decision was driven by the fact that the customer wanted to know what a peer competitor had been doing over time and what implications that might have for that competitor's future activities.

Estimative intelligence, key judgments, and probabilistic language

The student project team decided to use a modified national intelligence estimate (NIE) format to deliver Key Judgments to the customer, following the "BLUF" principle ("bottom line up front"). The NIE and its key judgments must have relevance for a time-constrained leader attempting to make the most informed decision possible in response to a particular problem or challenge. To create an estimative intelligence product, analysts look at past and current data to make predictions about what is likely to happen in the future. One of the premier intelligence products within the U.S. intelligence community is the National Intelligence Estimate (NIE). Two characteristic features of an NIE were incorporated into this team's final product: Key judgments, and probabilistic (or estimative) language. Heuer (1981) described a *judgment* as "what we use to fill gaps in our knowledge. It entails going beyond the available information and is our principal means of coping with uncertainty. It always involves an analytical leap, from the known into the unknown" (p. 65). Key judgments written in probabilistic language contain two key components: The *degree of confidence* analysts have in a stated projection, and the *likelihood* that the predicted action will actually occur.

Desired end state: Actionable intelligence

Pedantic writing has no place in intelligence writing. Instead, simplicity, directness, and conciseness are all valued in an intelligence product. Whether an intelligence team's customer is on the battlefield, in the White House, or in a corporate board room, the delivered intelligence product must be timely, relevant, comprehensible, and *actionable* (Rao, 2003). Actionable intelligence does not mean a decision-maker *must* act on the intelligence received; in fact, an informed decision to take no action at all is absolutely legitimate. However, the goal of intelligence professionals is to equip the decision-maker with the most complete picture possible of a given situation. The intelligence product must also meet the "so what?" test, answering the question, "What significance does this intelligence have for me (or us)?" (Bernhardt, 2003).

DISCUSSION

As Polanyi (1966) asserted, tacit knowledge is the type of knowledge that is most effectively acquired via experiential learning, through personal experience. The acquisition of tacit knowledge is the goal for graduate students who participate in intelligence collection and analysis projects during the Strategic Intelligence capstone course in Mercyhurst University's Applied Intelligence program. These students are afforded the opportunity to take the explicit knowledge they have acquired in a classroom setting over the previous year and a half and apply it working a real-world intelligence product in support of an external client. This experience helps prepare them for careers as intelligence professionals in the U.S. intelligence community, law enforcement, or competitive intelligence.

REFERENCES

Arcos, R., and J.-M. Palacios. "EU INTCEN: A Transnational European Culture of Intelligence Analysis?" *Intelligence and National Security 35*, no. 1 (2020): 72–94. doi:10.1080/02684527.2019.1649912.

Artner, S., R. S. Girven, and J. B. Bruce. "Assessing the Value of Structured Analytic Techniques in the U.S. intelligence Community." (2016). *RAND*. https://www.rand.org/pubs/research_reports/RR1408.html

Army Techniques Publication (ATP) 2-22.9. *Open-Source Intelligence*. (2012). Washington, DC: Department of the Army.

Beebe, S. M., and R. H. Pherson. *Cases in Intelligence Analysis: Structured Analytic Techniques in Action*. Los Angeles: Sage, 2015.

Ben Jaffel, H. and S. Larsson. "Why Do We Need a New Research Agenda for the Study of Intelligence?" *International Journal of Intelligence and CounterIntelligence*, (06 Jul 2023). DOI: 10.1080/08850607.2023.2222342

Bernhardt, D. *Competitive intelligence*. London: Prentice Hall, 2003.

Coldea, F. "Case studies in teaching intelligence: Pros and cons." *Romanian Intelligence Studies Review 21*. (2019): 79-92.

Coulthart, S., and A. Rorissa. "Growth, diversification, and disconnection: an analysis of 70 years of intelligence scholarship (1950-2020)." *Intelligence and National Security 38*, no. 6 (2023): 1003-1019.

Davis, J. "Sherman Kent and the Profession of Intelligence Analysis." *Occasional Papers 1*, no 5 (2002): 1-13.

Delagenière, B. "Intelligence Analysis as Cryptic Hermeneutics." *Intelligence & National Security 36*, no. 4 (2021): 541-554.

Dexter, H., M. Phythian, and D. Strachan-Morriset. "The What, Why, Who, and How of Teaching Intelligence: The Leicester approach." *Intelligence and National Security 32*, no. 7 (2017): 920-934.

Fellman, P. V. “The Complexity of Intelligence Estimates.” In *Proceedings of the 8th International Conference on Complex Systems, New England Complex Systems Institute, Quincy MA*. (2011, June).

Fruehauf, J., F. G. Kohun, and R. J. Skovira. “A Discussion Focusing on Polanyi’s ‘Tacit Knowing.’” *Online Journal of Applied Knowledge Management 3*, no 2 (2014): 100-114.

Fuchs, M., & J. Lemon. “Sans 2019 threat hunting survey: The differing needs of new and experienced hunters.” *SANS Institute Information Reading Room*. (2019).

García-Madurga, M.-Á. and M.-Á Esteban-Navarro. “A Project Management Approach to Competitive Intelligence.” *Journal of Intelligence Studies in Business 10*, no. 3 (2020): 8-23.

Guerette, R. T., K. Przeszlowski, J. Lee-Silcox, and K. M. Zgoba. “Improving Policing through Better Analysis: An Empirical Assessment of a Crime Analysis Training and Enhancement Project within an Urban Police Department.” *Police Practice & Research 22*, no. 4 (2021): 1425-1442.

Hackman, J. R. *Collaborative Intelligence: Using Teams to Solve Hard Problems*. San Francisco: Berrett-Koehler Publishers, 2011.

Herring, J. P. “Key Intelligence Topics: A Process to Identify and Define Intelligence Needs.” *Competitive Intelligence Review 10*, no. 2 (1999): 4-15.

Heuer, R. J. “Strategies for Analytical Judgment.” *Studies in Intelligence 25*, no. 2 (Summer 1981): 65–78.

Heuer, R. J., and R. H. Pherson. *Structured analytic techniques for intelligence analysis*. Washington, DC: CQ Press, 2011.

Intelligence Community Directive (ICD) 203. *Analytic Standards*. (2007 – June 21).

Intelligence Community Directive (ICD) 203. *Analytic Standards*. (2022 – December 21).

Intelligence Community Directive (ICD) 206. *Sourcing Requirements for Disseminated Analytic Products*. (2007 – October 17).

Kent, S. *Strategic Intelligence for American World Policy*. Princeton, NJ: Princeton University Press, 1949.

Kent, S. “The need for an intelligence literature.” *Studies in Intelligence 1*, no. 1, (1955): 1–11.

Kilroy, R. J. “Teaching Intelligence Analysis: An Academic and Practitioner Discussion.” *Global Security & Intelligence Studies 2*, no. 2 (2017): 71-85.

Kobayashi, M., & K. Takeda. “Information Retrieval on the Web.” *ACM computing surveys (CSUR) 32*, no. 2 (2000): 144-173.

Lowenthal, M. M. *Intelligence: From secrets to policy*. Los Angeles: Sage, 2017.

Marchio, J. “Analytic Tradecraft and the Intelligence Community: Enduring Value, Intermittent Emphasis.” *Intelligence and National Security 29*, no. 2 (2014): 159–183. http://dx.doi.org/10.1080/02684527.2012.746415

Marrin, S. “Improving Intelligence Studies as an Academic Discipline.” *Intelligence and National Security 31*, no. 2 (2016): 266-279.

Phythian, M. “Conclusion: The Development of Critical Intelligence Studies.” *Intelligence and National Security 36*, no. 4 (2021): 615-620.

Pili, G. “Deciphering Intelligence Analysis: The Synthetic Nature of the Core Intelligence Function.” *Intelligence & National Security 38*, no. 1 (2023): 128-142.

Polanyi, M. *The tacit dimension*. Chicago: The University of Chicago Press, 1966.

Rao, R. “From Unstructured Data to Actionable Intelligence.” *IT professional 5*, no. 6 (2003): 29-35.

Sangwan, D., Raj, P. "The Philosophy of Be, Know, and Do in Forming the 21st-Century Military War-front Competencies: A Systematic Review." *Defence Studies 21*, no. 3 (2021): 375-424.

Scott, L., and P. Jackson. The study of intelligence in theory and practice. *Intelligence and National Security 19*, no. 2 (2004): 139-169.

Teirilä, O. J. "The Optimal Analyst: Balancing the Width and Depth in Strategic Intelligence." *International Journal of Intelligence & Counterintelligence 37*, no. 1 (2024): 1-12.

Tuckman, B. "Developmental Sequence in Small Groups." *Psychological Bulletin 63*, no. 6 (1965): 384-399. https://doi.org/10.1037/h0022100

Van Puyvelde, D. and S. Curtis. "'Standing on the shoulders of giants': Diversity and scholarship in intelligence studies." *Intelligence and National Security 31*, no. 7 (2016): 1040-1054.

Van Wyngaard, C. J., J. H. C., Pretorius, & L. Pretorius. "Theory of the Triple Constraint—A Conceptual Review." In *2012 IEEE International Conference on Industrial Engineering and Engineering Management* (1991-1997). IEEE, (2012, December).

Walsh, P. F., and M. Harrison. "Strategic Intelligence Practice in the Australian Intelligence Community: Evolution, Constraints and Progress." *Intelligence & National Security 36*, no. 5 (2021): 660-675.

Whitford, T., and H. Prunckun. "Discreet, Not Covert: Reflections on Teaching Intelligence Analysis in a Non-government Setting." *Salus Journal 5*, no. 1 (2017): 48-61.

CYBERSECURITY NEEDS FOR SMES

Assion Kuyona Tetteh, University of Maryland, atetteh3@umd.edu

ABSTRACT

Small and Medium-sized Enterprises (SMEs) all over the world are the very heart of economic growth. SMEs drive economic growth worldwide. However, unlike most behemoths, they lack the resources and experience to tackle cybersecurity threats compared to large organizations with well-established security infrastructure. This exposure renders them vulnerable to danger and ideal targets for cybercriminals. Contrary to yesterday's digital attacks, cyberattacks nowadays are not the sole realm of professional hackers using expensive tools to target huge organizations, but ordinary organizations have also become victims of these malicious attacks. This paper explores the unique cybersecurity challenges faced by SMEs and offers practical solutions to enhance their security posture. The research delves into various dimensions of cybersecurity issues that SMEs encounter, such as inadequate threat awareness, insufficient training for employees, and reliance on outdated technology. It examines the types of cyberattacks most frequently directed at SMEs, including phishing scams, ransomware, and insider threats, and analyzes the impact of these attacks on business operations, financial stability, and reputation. To address these challenges, the paper presents a comprehensive set of practical solutions aimed at enhancing the cybersecurity posture of SMEs. These solutions encompass both technological and non-technological measures. The paper also explores the role of government and industry associations in supporting SMEs' cybersecurity efforts. It highlights various programs and resources available to SMEs, such as training workshops, grants for cybersecurity improvements, and informational guides.

TEACHING THE PROBLEM-SOLVING PROCESS IN INFORMATION SYSTEMS AND MANAGEMENT CLASSROOMS: AN ASSESSMENT OF THE SOCRATIC METHOD

Donald "Breck" Terheide, Ball State University, dbterheide@bsu.edu
Allen D. Truell, Ball State University, atruell@bsu.edu
Eric S. Green, Ball State University, esgreen2@bsu.edu

ABSTRACT

There is little doubt that problem-solving is among the most sought-after skills of information systems and management program graduates. Thus, information systems and management faculty are constantly assessing teaching strategies to enhance the problem-solving skills of program graduates. Therefore, the purposes of this presentation are threefold: (1) to provide an overview of the Socratic Method, (2) to examine identified strengths of the Socratic Method, and (3) to explore reported weaknesses of the Socratic Method. A few of the identified strengths of the Socratic Method include (1) relevant problem-solving, (2) learner interaction, (3) listening skill development, and (4) improved reading comprehension. Several of the reported weaknesses of the Socratic Method include (1) not addressing diverse learning styles, (2) groupthink, (3) instructor emotional and intellectual manipulation, (4) ambiguity, and (5) poor instructor questioning skills. The presentation will highlight insights from a local management faculty expert who has successfully applied the Socratic Method's strengths while minimizing its weaknesses for decades.

Keywords: information systems, management, problem-solving, Socratic Method

OPPORTUNITIES AND CHALLENGES OF ARTIFICIAL INTELLIGENCE APPLICATIONS IN HIGHER EDUCATION: IMPLICATIONS FOR INFORMATION SYSTEMS AND OPERATIONS MANAGEMENT FACULTY

Allen D. Truell, Ball State University, atruell@bsu.edu
Eric S. Green, Ball State University, esgreen2@bsu.edu
Christopher B. Davison, Ball State University, cbdavison@bsu.edu
Edward J. Lazaros, Ball State University, ejlazaros@bsu.edu

ABSTRACT

There is little doubt that artificial intelligence has permeated many areas of higher education. As such, information systems and operations management faculty are constantly refining their integration and response to artificial intelligence integration into numerous aspects of higher education. Thus, the purpose of this presentation is multifold: (1) to share an overview of artificial intelligence and how it has permeated higher education, (2) to share opportunities for integrating artificial intelligence into higher education for information systems and operations management faculty, and (3) to share challenges of integrating artificial intelligence into higher education for information systems and operations management faculty. Sample artificial intelligence applications that can be used by information systems and operations management faculty and their students will be reviewed. Lessons learned, and adjustments made for integrating artificial intelligence applications will be offered at critical points from information systems and operations management faculty and student perspectives.

Keywords: artificial intelligence, faculty, higher education, information systems

THE UTILITY OF E-LEARNING PLATFORM INTEGRATION BY FACULTY IN AN AACSB-ACCREDITED BUSINESS COLLEGE

Allen D. Truell, Ball State University, atruell@bsu.edu
Eric S. Green, Ball State University, esgreen2@bsu.edu
Edward J. Lazaros, Ball State University, ejlazaros@bsu.edu
Christopher B. Davison, Ball State University, cbdavison@bsu.edu

ABSTRACT

There is little doubt that using textbook publisher-aligned e-learning platforms has saturated many classrooms, including those in AACSB-accredited business colleges. As such, AACSB-accredited business college faculty are constantly refining their integration of textbook publisher-affiliated e-learning platforms into their courses. Thus, the purpose of this presentation is threefold: (1) to share an overview of textbook publisher-aligned e-learning platforms, (2) to examine the opportunities for faculty and students of textbook publisher-aligned e-learning platform integration into courses, and (3) to examine the challenges for faculty and students of textbook publisher-affiliated e-learning platform integration into courses. Frequently noted benefits of integrating textbook publisher-aligned e-learning platforms include (1) assessment monitoring tools, (2) seamless learning management system integration, and (3) significant publisher support. Some of the more commonly reported benefits for students include (1) adaptive learning, (2) detailed feedback, and (3) immediate access to materials. Lessons learned and adjustments made for continuous improvement will be offered throughout the presentation.

Keywords: business colleges, e-learning platforms, student engagement, student learning

USING CHATGPT IN SYSTEMS ANALYSIS INSTRUCTION

Judy Wynekoop, Florida Gulf Coast University, jwynekoo@fgcu.edu

INTRODUCTION

Large language models (LLMs), such as ChatGPT, are in the early stage of use for systems development tasks such as identifying requirements or modeling software. The growing use of LLMs in systems development is expected to significantly impact the way software is developed, as well as software development education (Cámara et al, 2023). The use of LLMs to write code has been most studied (Cámara et al, 2023). Research on the use of LLMs for gathering, analyzing, and modeling software requirements has just begun (Cámara et al, 2023; Khojah, et al., 2024; Rajbhoj, et al., 2024; Rodriguez et al., 2024; Russo, 2024). We will present initial results from a pilot study of factors influencing students' perceptions and use of LLMs in software development, grounded in existing theory in the UTAUT framework (Venkatesh, 2022) and the Technology Acceptance Model (Davis, 1989; Russo, 2024). The pilot was undertaken to inform the development of an instrument to study specific factors impacting perceptions, adoption, and use of LLMs for software development.

THE STUDY

Students in a systems analysis and design class were asked to use ChatGPT to identify initial user needs and requirements for an application they would prototype in the class. Students first received a 20-minute lesson on how to write effective prompts for ChatGPT and were shown examples of prompts and resulting output to help them effectively use ChatGPT to identify user needs. Data related to personal characteristics, their perceptions of LLMs, and how open they would be to using LLMs professionally were collected via survey after they had used the technology.

Existing studies in this area have had diverse findings. Developers have been found to believe that LLMs can be used successfully through all phases of software development, although developer productivity may be diminished (Khojah et al., 2024). Russo's (2024) study of the relationship of technology characteristics and LLM use had mixed results. An initial review of responses from this pilot study indicates that students found ChatGPT to be useful for brainstorming and generally timesaving, although some thought they could have accomplished the task equally well and more quickly without ChatGPT, supporting Khojah's (2024) findings. Students with a generally positive view of the usefulness of LLMs seem to have had a better outcome using ChatGPT for requirements identification. These responses, as well as the relationship of technology and individual characteristics with LLM perception and use will be presented.

IMPLCATIONS AND CONCLUSION

Many IS programs such as ours cannot provide "real" cases with "real" users for systems analysis and design projects. Yet, students need to practice eliciting requirements working with users. Using ChatGPT as the users for a hypothetical system provides this practice. Understanding how students use ChatGPT for systems development tasks and factors impacting their successful use will help educators effectively integrate LLMs into systems development courses. These initial results will give some evidence of how an LLM may be used in a systems analysis and design class, as well as inform the future study of antecedents of their successful use.

REFERENCES

Cámara, J., Troya, J., Burgueño, L. & Vallecillo, A. (2023). On the assessment of generative AI in modeling tasks: an experience report with ChatGPT and UML. *Software and Systems Modeling*, *22*(3), 781-793.

Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.

Khojah, R. Mohamad, M., Leitner, P. & de Oliveira Neto, F.G. (2024). Beyond code generation: An observational study of ChatGPT usage in software engineering practice. arXiv preprint arXiv:2404.14901.

Rajbhoj, A., Somase, A., Kulkarni, P., Kulkarni, V. (2024). Accelerating software development using generative AI: ChatGPT Case Study. *ISEC 2024, February 22-24, 2024, Bangalore, India.*

Rodriguez, D. V., Lawrence, K., Gonzalez, J., Brandfield-Harvey, B., Xu, L., Tasneem, S., Levine, D.L. & Mann, D. (2024). Leveraging generative AI Tools to support the development of digital solutions in health care research: Case study. *JMIR Human Factors*, *11*(1), e52885.

Russo, D. (2024). Navigating the complexity of generative AI adoption in software engineering. *ACM Transactions on Software Engineering and Methodology*.

Venkatesh, V. (2022). Adoption and use of AI tools: a research agenda grounded in UTAUT. *Annals of Operations Research*, *308*(1), 641-652.

PRIVACY AND THE PROTECTION MOTIVATION THEORY: AN INTEGRATED MODEL

C. Bryan Foltz, University of Tennessee at Martin, cfoltz1@utm.edu
Laura G. Foltz, University of Tennessee at Martin, lfoltz@utm.edu

INTRODUCTION

In the seminal 1986 article, Mason identified privacy as an ethical issue facing the information age. Mason listed two primary threats to privacy: the growth of information technology “with its enhanced capacity for surveillance, communication, computation, storage, and retrieval” (p5) and the increasing value of information for decision-making (Mason, 1986). Mason’s concerns were well-placed. Today, massive amounts of data are collected from various sources, including Internet of Things devices, medical devices, and cell phones (Cichy et al, 2021); technologies such as big data and data analytics discover patterns and links within this data (Allen, 2016; Barth et al, 2023; West, 2019). The collection and examination of this data has led to an increasing concern with user privacy (Barth et al, 2023).

PROPOSED STUDY

This research seeks to further the understanding of the formation of privacy concerns by integrating a privacy concern model within a model of human behavior.

PRIVACY AND PRIVACY CONCERN

Privacy has been defined as “the right to select what personal information about me is known to what people” (Westin, 1968). Belanger and Crossler (2011) refined this definition to suggest that “Information privacy refers to the desire of individuals to control or have some influence over data about themselves.” Sfar et al (2018) suggested incorporating the collection, use, and sharing of data. This research will utilize the Sfar et al (2018) extension of the Belanger and Crossler (2011) definition. Within the literature, privacy concern is often used as a proxy for privacy and has been featured in multiple behavioral models (Xu et al, 2008). Privacy concern may be defined as “One’s concern about his or her personal data being used” (Chen et al, 2023, p2). Preibusch (2013) provides a summary of multiple instruments developed to measure privacy concern. For example, Xu et al (2012) created an instrument to focus on mobile users privacy concerns. This instrument is based on Communication Privacy Management theory and suggests that prior experience and three dimensions, perceived surveillance, perceived intrusion, and secondary use of information, create privacy concern (Xu et al, 2012).

HUMAN BEHAVIOR

Human behavior has been widely studied within the extant literature. The Protection Motivation Theory (PMT) (Rogers, 1975) has been utilized to understand and explain human behavior for “any threat for which there is an effective recommended response that can be carried out by the individual” (Floyd et al, 2000, p409).

This research seeks to understand the formation of privacy concerns by examining the Mobile Users Privacy Concerns model (Xu et al, 2012) from the perspective of Protection Motivation Theory (Rogers, 1975).

IMPLICATIONS AND CONCLUSION

Privacy is a growing concern as everyday devices gather massive amounts of data; the growth of related technologies such as data analytics and machine learning simply exaggerate the issue. This research seeks to better understand the formation of privacy concerns to help organizations and individuals better understand and cope with this ongoing concern.

REFERENCES

Allen, A. L. (2016), "Protecting One's Own Privacy in a Big Data Economy". *All Faculty Scholarship*. 1716. https://scholarship.law.upenn.edu/faculty_scholarship/1716

Barth, S., D. Ionita, and P. Hartel. (2023). “Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines.” *ACM Computing Surveys* 55 (3): 1–37.

Bélanger, F. and R. E. Crossler. (2011). “Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems.” *MIS Quarterly* 35 (4): 1017-1041.

Chen, M., H. Wang, and R. Zhang. (2023). “Using the Extended Theory of Planned Behavior to Predict Privacy-Protection Behavioral Intentions in the Big Data Era: The Role of Privacy Concern.” Edited by J. Hj Ahmad and J. Guo. *SHS Web of Conferences* 155: 03011.

Cichy, P., T.O. Salge, and R. Kohli, (2021). “Privacy Concerns and Data Sharing In The Internet Of Things: Mixed Methods Evidence From Connected Cars.” *MIS Quarterly*, *45*(4), 1863–1892.

Floyd, D. L., S. Prentice-Dunn, and R. W. Rogers. (2000). “A Meta-Analysis of Research on Protection Motivation Theory.” *Journal of Applied Social Psychology* 30 (2): 407–29.

Mason, R. O. (1986). “Four Ethical Issues of the Information Age.” *MIS Quarterly* 10 (1): 5–12.

Preibusch, S. (2013). “Guide to Measuring Privacy Concern: Review of Survey and Observational Instruments.” *International Journal of Human-Computer Studies* 71 (12): 1133–43.

Rogers, R.W. (1975). “A Protection Motivation Theory of Fear Appeals and Attitude Change.” *Journal of Psychology* 91 (1): 93–114.

Sfar, R., E. N. Arbia, Y. Challal, and Z. Chtourou. (2018). “A Roadmap for Security Challenges in the Internet of Things.” *Digital Communications and Networks* 4 (2): 118–37.

West, S. M. (2019). “Data Capitalism: Redefining the Logics of Surveillance and Privacy.” *Business & Society* 58 (1): 20–41.

Westin, A. F. (1968). “Privacy And Freedom.” Washington and Lee Law Review, 25(1).

Xu, H., T. Dinev, H. J. Smith, and P. Hart. (2008). “Examining the Formation of Individual’s Privacy Concerns: Toward an Integrative View.” In *Proceedings of International Conference on Information Systems*, 1–16.

ANALYZING THE IMPACT OF SNS AFFORDANCES ON PERUVIANS' PURCHASE INTENTIONS IN SOCIAL COMMERCE: IMPLICATIONS FOR SMES

Nicol Contreras-Mendoza, *Universidad del Pacífico, Lima-Peru, ng.contrerasm@alum.up.edu.pe*
Christian Fernando Libaque-Saenz, *Universidad del Pacífico, Lima-Peru, cf.libaques@up.edu.pe*

EXTENDED ABSTRACT

PROPOSED STUDY

The restrictions on mobility during the pandemic impacted businesses, especially small and medium-sized enterprises (SMEs) (Apedo-Amah et al., 2020), forcing them to migrate to digital channels. S-commerce, which uses social network site (SNS) platforms to facilitate buying and selling products (Almahameed & Obidat, 2023), has emerged as an alternative channel because of its growing number of users and low implementation costs. Although this medium is increasingly adopted as a purchasing channel, 58% of Peruvians who make online purchases still do not use it for this purpose (Datum Internacional, 2020). This study aims to determine the impact of SNS affordances (visibility, accessibility, triggering-attending, social connecting) on users' purchase intention through SNSs to provide SMEs with recommendations on how to use this channel efficiently. Based on the stimulus-organism-response (SOR) framework, a model is proposed to investigate the influence of SNS affordances on purchase intention in s-commerce. This topic may be of interest to the audience attending the International Association for Computer Information Systems (IACIS) conference because it may help to establish strategies to improve sellers' performance through SNS platforms as a digital channel.

BASIS OF THIS STUDY

This study targeted buyers in Peru who were at least 18 years old. In terms of specific behavior, this research included only those participants who had used SNSs to purchase products previously. This study used primary data collected through a survey technique using Google Forms. The survey was provided in Spanish and all variables were measured on a 5-point Likert scale. A snowball sampling technique was used, and a partial least squares (PLS) variance-based technique of structural equation modeling (SEM) was used for data analysis.

Data were collected from October to November 2023. A total of 219 valid responses were used for further analysis. Results support the positive effect of the following affordances: visibility, triggering-attendance, and social connecting as trust-building mechanisms, which in turn is positively related to intention and, thus, purchase.

DISCUSSION AND IMPLICATIONS

This study contributes to the literature by filling these two research gaps: 1) there is an unattended relationship between IT affordances and trust towards sellers, with limited evidence of the impact of the former in trust-building mechanisms, and 2) mixed results regarding the influence that trust in sellers has on s-commerce intention. In terms of practical implications, practical guidance is provided to sellers on using SNSs to increase trust, thereby increasing purchase intention and subsequent purchase. First, it is suggested that sellers improve the quality of their product images and videos and have a consistent publication frequency (visibility). Second, it is recommended that sellers send personalized notifications to keep customers informed about new products, promotions, and offers (triggering-attendance). Third, sellers can build "social proof" by inviting shoppers to share photos or videos of their purchases through incentives and encouraging reviews (social connecting).

CONCLUSIONS

This study aimed to determine the impact of SNS affordances on users' purchase intentions. The results indicate that visibility, triggering attendance, and social connection act as trust-building mechanisms, increasing buying intention and the likelihood of purchase. Furthermore, visibility, accessibility, and triggering-attendance were identified as enablers of the purchase process. Finally, practical recommendations were provided to help sellers improve their use of SNSs to sell their products.

REFERENCES

Almahameed, M., & Obidat, A. (2023). Exploring the critical success factors of s-commerce in social media platforms: The case of Jordan. *International Journal of Data and Network Science*, *7*(1), 163–174. https://doi.org/10.5267/j.ijdns.2022.11.006

Apedo-Amah, M., Avdiu, B., Cirera, X., Cruz, M., Davies, E., Grover, A., Iacovone, L., Kilinc, U., Medvedev, D., Maduko, F., Poupakis, S., Torres, J., & Tran, T. T. (2020). *Unmasking the Impact of COVID-19 on Businesses: Firm level evidence from across the world*. World Bank, Washington, DC. https://doi.org/10.1596/1813-9450-9434

Datum Internacional. (2020). *Emprendedores en contexto Covid-19*. https://www.datum.com.pe/new_web_files/files/pdf/Estudio%20Emprendedor%20COVID-19%20-v3_220405035510.pdf

OPEN DIGITAL PLATFORM FOR SMART HONEY VALUE CHAINS: IDENTIFYING DATA THROUGH BEEKEEPING EXPERTISE

Ewa W. Ziemba [0000-0002-1084-7497], University of Economics in Katowice, Poland
Ewa W. Maruszewska [0000-0003-0461-4133], University of Economics in Katowice, Poland
Anna Karmańska [0000-0001-5883-1243], University of Economics in Katowice, Poland
Mieczyslaw L. Owoc [0000-0003-1578-6934], Wroclaw University of Economics and Business, Poland
Mehmet N. Aydın [0000-0002-3995-6566], Kadir Has University, Türkiye
Şahin Aydın[0000-0001-7355-5339], Işık University, Türkiye
Samet Okuyan [0000-0002-4356-4733], Apiculture Research Institute, Ordu, Türkiye, Türkiye
Aleksejs Zacepins [0000-0002-6974-8653], Latvia University of Life Sciences and Technologies, Latvia
María Alejandra Palacio [0000-0002-9732-3070], National Agricultural Technology Institute, Argentina

EXTENDED ABSTRACT

The necessity for research on smart honey value chains is increasingly evident as consumer demand for transparency, quality, and sustainability grows (Dossou et al., 2022; Hidalgo et al., 2020; Rünzel et al., 2021). Advances in digital technology are transforming the ways in which trust is built and sustained within value chain relationships, including in the honey sector (Finlay-Smits et al., 2023; Rünzel et al., 2021). Within the international project "Trustable and Sustainable Open Platform for Smart Honey Value Chains[i]," efforts are being made to develop a reliable, sustainable, and adaptive digital open data platform to facilitate the efficient implementation of smart honey value chains. Stakeholders and the data they provide and utilize are crucial components of these chains, highlighting the importance of thorough data mapping and analysis (Dossou et al., 2022; Sparacino et al., 2022).

Despite the recognized need, existing literature lacks research on data mapping in smart honey value chains and the creation of a comprehensive data value map (Agerskans et al., 2023; Dossou et al., 2022) that includes data acquisition, data integration, data analysis, and data delivery (Nagle & Sammon, 2017). This gap underscores the importance of developing a detailed understanding of the types of data necessary for these chains and the methods for effectively acquiring and managing this data.

This article focuses on the first component of the data value map: data acquisition. The primary objective is to identify the types of data related to beekeeping activities that need to be acquired and collected within the honey value chain. By addressing this objective, the research aims to provide a foundational framework for future studies and practical applications in smart honey value chains.

The research methodology involved a comprehensive review of scientific and grey literature and the application of design thinking principles to develop an initial framework for data acquisition in the honey value chain. This preliminary framework was then validated through qualitative research, specifically interviews conducted with 30 beekeeping experts in Poland. The interviews aimed to gather detailed insights into the specific data required for a robust and transparent honey value chain.

The study's key findings confirmed that all collected data in a smart honey value chain can be categorized into four main groups: Beekeeper Description, Apiary Description, Honey Description

and Quality, Apiary Management, and Beekeeping Regulations and Standards. Within each group, specific data points were identified that need to be collected to ensure transparency and trust among stakeholders and enhance honey quality.

The research contributes to the academic field by providing a structured framework for data acquisition in smart honey value chains, addressing a significant gap in the literature. This framework serves as a basis for further research on data integration, analysis, and delivery within the value chain.

In practical terms, the findings offer valuable insights for stakeholders involved in honey production, enabling them to implement more effective data collection and management practices. By adopting these practices, the honey industry can improve product quality, ensure regulatory compliance, and build greater consumer trust.

Keywords: sustainability, honey value chains, beekeeping, data value map

Acknowledgment

The TOP4HoneyChains: Trustable and Sustainable Open Platform for Smart Honey Value Chains project has received funding from the European Union's Horizon 2020 research and innovation programme under the ERA-NET CO-FUND ICT-AGRI-FOOD (2022 Joint Call), under Grant Agreement No. 862665.

The project is co-funded by:
1. The National Centre for Research and Development (NCBIR) in Poland, under the agreement ICTAGRIFOOD/II/67/TOP4HoneyChain/2023;
2. Türkiye–TÜBİTAK, under the agreement 123N225;
3. The National Institute of Agricultural Technology (INTA) in Argentina, under the agreement Smart Honey Value Chain Analysis;
4. Ministry of Education and Science, Republic of Latvia.

References

Agerskans, N., Ashjaei, M., Bruch, J., Chirumalla, K. (2023). Critical Factors for Selecting and Integrating Digital Technologies to Enable Smart Production: A Data Value Chain Perspective. In: Alfnes, E., Romsdal, A., Strandhagen, J.O., von Cieminski, G., Romero, D. (eds) *Advances in Production Management Systems. Production Management Systems for Responsible Manufacturing, Service, and Logistics Futures*. APMS 2023. *IFIP Advances in Information and Communication Technology*, vol 689 (pp. 311-325). Springer, Cham. https://doi.org/10.1007/978-3-031-43662-8_23

Dossou, S. A. R., Adanguidi, J., Aoudji, A. K. N., & Gbedomon, R. C. (2022). Promotion of beekeeping: Insights from an empirical analysis of three honey value chains in Benin. *Natural Resources Forum*, *46*(1), 39–59. https://doi.org/10.1111/1477-8947.12238

Finlay-Smits, S., Ryan, A., de Vries, J.R., & Turner J. (2023). Chasing the honey money: Transparency, trust, and identity crafting in the Aotearoa New Zealand mānuka honey sector. *Journal of Rural Studies*, 103004. https://doi.org/10.1016/j.jrurstud.2023.03.012

Hidalgo, H.A., Nicolas, A.R., & Cedon, R. (2020). Development Barriers of Stingless Bee Honey Industry in Bicol, Philippines. *International Journal on Advanced Science*, *Engineering and Information Technology, 10*(3), 1245-1251. http://dx.doi.org/10.18517/ijaseit.10.3.4747

Nagle, T., & Sammon, D. (2017). 'The Data Value Map: A framework for developing shared understanding on data initiatives. In *ECIS 2017: Proceedings of the 25th European Conference on Information Systems*, Guimarães, Portugal, 5-10 June, pp. 1439-1452. https://aisel.aisnet.org/ecis2017_rp/93

Rünzel, M.A.S., Hassler, E.E., Rogers, R.E.L., Formato, G. & Cazier, J. A. (2021). Designing a Smart Honey Supply Chain for Sustainable Development. *IEEE Consumer Electronics Magazine*, *10*(4), 69-78. https://doi.org/10.1109/MCE.2021.3059955

Sparacino, A., Merlino, V.M., Blanc, S., Borra, D., Massaglia, S. (2022). A Choice Experiment Model for Honey Attributes: Italian Consumer Preferences and Socio-Demographic Profiles. *Nutrients 14*, 4797. https://doi.org/10.3390/nu14224797

ESTIMATING INTRINSIC DIMENSION TO ARCHITECT COMPACT NEURAL NETWORKS

James Bonacci, Robert Morris University, jxbst976@mail.rmu.edu
Peyton Lutchkus, Robert Morris University, pglst259@mail.rmu.edu
Reese Martin, Robert Morris University, rgmst170@mail.rmu.edu
Robert Pava, Robert Morris University, rjpst280@mail.rmu.edu
Dr. Ping Wang (Supervising Faculty), Robert Morris University, wangp@rmu.edu
Dr. Bradford Kline (Problem Mentor), National Security Agency, bjkline@uwe.nsa.gov

PROPOSED/COMPLETED STUDY DESCRIPTION

Information security professionals around the world are always looking for ways to improve the robustness of threat detection and response. A machine learning paradigm such as an autoencoder can be used to automate flagging and increase the accuracy of threat detection. Autoencoders are unsupervised neural networks that are able to take input data, encode and compress the data, and decompress the data into a reconstruction extremely similar to the original data (Badr, 2019). Compression schemes such as autoencoders need to encode input to a size that maximizes space savings while minimizing information loss – a size governed by the intrinsic dimension of the data. This research focuses on a suite of intrinsic dimension estimation techniques implemented in the Scikit-dimension Python package and subsequent use of the Pytorch package to develop an autoencoder model. This is an extremely important interplay because without the correct intrinsic dimension, adversaries can take advantage of the excess space in the autoencoder and insert malicious packets to the system. On the other hand, if the intrinsic dimension of an autoencoder is set too low, it will struggle to learn the representation of even normal, non-malicious data. It is for these reasons that it is imperative to discover a reliable method of intrinsic dimension estimation.

EXPLANATION OF THE STUDY

The data that was collected for this research was supplied by Dr. Bradford Kline from the National Security Agency (NSA). Dr. Kline produced 12 synthetic data sets, varying in distribution with some datasets being clean and others containing noise. While the authors acknowledge limitations in the use of synthetic data for generalizability of machine learning results, the present investigations required control of the data variability and knowledge of the exact intrinsic dimensions. The data was used to test 4 different algorithms from the Scikit-dimension Python package. Dr. Kline also provided datasets that had anomalous features and they were used to test the reliability of the autoencoder. The data analysis is expected to show whether or not the Scikit-dimension toolkit can be used to reliably estimate the intrinsic dimensions of various datasets, and therefore whether or not it can be used to supply the correct intrinsic dimension to autoencoders, thus providing reliable anomaly detection capabilities.

Once the intrinsic dimension is determined with the Scikit toolkit, the autoencoder can confirm that the result is true. The autoencoder would be trained on the same dataset that was used for the Scikit toolkit and have it reconstruct the data at the proposed intrinsic dimension. If it is the correct dimension, it will reconstruct with near 0% loss. If it is too low of a dimension, the autoencoder will struggle to get anywhere near 0% loss and fail to reconstruct the data. If it is too high of a dimension, the autoencoder will reconstruct it with 0% loss much faster than it should.

IMPLICATIONS AND CONCLUSION

Autoencoders reinforce the importance of knowing the correct intrinsic dimension because if the dimension is too high, malicious actors can inject bad traffic for the autoencoder to train on. This will result in the failure to detect anomalous traffic.

Note: This project is supported by Grant H98230-21-1-0317.

REFERENCES

Bac, J., et al. (2021). Scikit-Dimension: a Python Package for Intrinsic Dimension Estimation. *Entropy*, 23(10), 1368. https://doi.org/10.48550/arXiv.2109.02596

Badr, W. (2019, July 1). *Auto-encoder: What is it? and what is it used for? (part 1)*. Medium. https://towardsdatascience.com/auto-encoder-what-is-it-and-what-is-it-used-for-part-1-3e5c6f017726

Campadelli, P., Casiraghi, E., Ceruti, C., & Rozza, A. (2015, October 19). *Intrinsic dimension estimation: Relevant techniques and a benchmark framework*. Mathematical Problems in Engineering. https://www.hindawi.com/journals/mpe/2015/759567/

Kvalheim, M. D., & Sontag, E. D. (2024). Why should autoencoders work?. Ithaca: https://reddog.rmu.edu/login?url=https://www.proquest.com/working-papers/why-should-autoencoders-work/docview/2872517484/se

Scikit-dimension - intrinsic dimension estimation in Python. Documentation. (2024, January). https://scikit-dimension.readthedocs.io/en/latest/

Torabi, H., Mirtaheri, S. L., & Greco, S. (2023). Practical autoencoder based anomaly detection by using vector reconstruction error. *Cybersecurity, 6*(1). https://doi.org/10.1186/s42400-022-00134-9

EXPLORING THE INTERSECTION OF AI, TRUST, FEAR, AND ART: A SURVEY

Roger Finnegan, PhD, Metro State University, roger.finnegan@metrostate.edu

STUDY DESCRIPTION

Recent articles have noted that as artificial intelligence (AI) advances people have become more concerned about its capabilities (Ezrati, 2023). People are not sure that they understand AI and they are not sure if they trust AI. While some people are excited about the new capabilities, others are feeling nervous about them. Many people do see the benefits of AI but things such as deepfake images have them concerned. Many people need to know if an image was generated by AI or not in order to have trust. In addition, the new AI capabilities to create art have some people concerned. People may or may not consider AI generated art to truly be art (Getty Images, 2024). This has importance since as AI advances in capabilities people will need to be comfortable with those advances.

BASIS OF THE STUDY

As AI grows in importance and capabilities how people react to it is very important. People may fear that AI may replace their job (Hanna, n.d.) or even replace them (Mollick, 2024). People may be growing concerned about deepfake images (Herrick & Ismaylov, n.d.). How concerned people are about AI secretly generating images should be determined. Also, part of this new AI capability will be the ability to create art and entertainment (Getty Images, 2024). How people perceive this AI generated art should also be studied.

A recent survey of 107 adults was conducted to determine the feeling of participants towards AI. Specifically, the study wanted to gauge the nervousness of people towards the advances of AI. The study also asked if people feel they are familiar with AI. The study asked people if they feel that there are benefits to the advancement of AI and if they felt excited about the new AI capabilities. The study also asked if participants wanted to know if an image had been generated by AI. Lastly, the study asked participants if they felt that art generated by AI was truly art.

STUDY IMPLICATIONS

The survey found that over 64% of participants are nervous about the increasing capabilities of AI. Over 50% of participants feel that they are familiar with AI and over 71% of participants agreed or strongly agreed that there are benefits to AI. Over 52% of participants were excited about these new AI capabilities. In addition, almost 77% of participants do want to know if an image was generated by AI. Regarding the question of whether AI generated art is real art the participants were split almost evenly. Just over 41% disagreed or strongly disagreed that it was art and over 37% agreed or strongly disagreed that it was art. The remaining 22% neither agreed nor disagreed.

CONCLUSIONS

The results indicate that people do feel nervous about new AI capabilities but at the same time they see the possibilities and are excited about them. There is a great deal of concern about images being AI generated without it being disclosed. Perhaps the most intriguing finding in the survey is that people are accepting of the idea that AI can generate true art.

REFERENCES

Ezrati, M. (April 7, 2023). No Reason to Fear AI. Forbes. https://www.forbes.com/sites/miltonezrati/2023/04/07/no-reason-to-fear-ai/?sh=7fe842607ba6

Getty Images (2024). Building Trust in the Age of AI. http://reports.gettyimages.com/VisualGPS-Building-Trust-In-AI.pdf.

Hanna, K. (n.d.). What is a Luddite? [Review of What is a Luddite?]. Tech Target. https://www.techtarget.com/whatis/definition/Luddite.

Herrick, D. & Ismaylov, R. (n.d.). Deepfakes Pose Business Risks – Here's what to know. Booz Allen Hamilton. https://www.boozallen.com/insights/ai/deepfakes-pose-businesses-risks-heres-what-to-know.html

Mallick, E. (April 1, 2024). We're Focusing on the Wrong Kind of AI Apocalypse. Time. https://time.com/6961559/ethan-mollick-ai-apocalypse-essay/

USING ARTIFICIAL INTELLIGENCE (AI) TECHNIQUES TO UNCOVER FUNDAMENTAL DRIVERS OF ACADEMIC SUCCESS

Jenq-Foung Yao, Georgia College & State University, jf.yao@gcsu.edu
Yu-Hsiang (John) Huang, Georgia College & State University, john.huang@gcsu.edu
Cheng-Ying Yang, University of Taipei, cyang@utaipei.edu
Tsu-Ming Chiang, Georgia College & State University, tm.chiang@gcsu.edu

ABSTRACT

Academic success in higher education is shaped by multiple factors, including student engagement, institutional policies, and individual student attributes (Kuh et al., 2006). York et al. (2015) extensively investigated the concept of academic success in higher education, exploring diverse definitions and the complexities in effectively measuring it. Several studies have tackled the challenge of measuring academic success by examining the correlation between class attendance and academic performance through linear regression analysis (e.g., LeBlanc, 2005; Broucek & Bass, 2008; Yadav, 2022), offering valuable insights into the intricate interplay between class attendance and academic achievement across various fields. However, we believe the results have not been fully captured by linear regression analysis. Further analyses can employ artificial intelligence (AI) techniques to uncover the fundamental drivers of academic performance. Specifically, our study scrutinizes the factors influencing students' cumulative grades across diverse courses. This analysis employs multiple AI methodologies, including (1) Artificial Neural Networks, (2) Decision Trees, and (3) Naïve Bayes. Through this approach, we identify several distinct scenarios leading to different grade categories. These findings will broaden our understanding of student success.

REFERENCES

Broucek, W. G., & Bass, W. (2008). Attendance feedback in an academic setting: preliminary results. *College Teaching Methods & Styles Journal* , *4*(1), 45-48.

Kuh, G. D., Kinzie, J. L., Buckley, J. A., Bridges, B. K., & Hayek, J. C. (2006). *What matters to student success: A review of the literature* (Vol. 8). Washington, DC: National Postsecondary Education Cooperative.

LeBlanc, H. P. (2005). The relationship between attendance and grades in the college classrooms. In *Proceedings of the 17th Annual Meeting of the International Academy of Business Disciplines*. Pittsburgh, PA.

Yadav, R. S. (2022). A study of relationship to absentees and score using machine learning method: A case study of linear regression analysis. *IARS' International Research Journal*, *12*(1), 33-39.

Yao, J. F., & Chiang, T. M. (2011). Correlation between class attendance and grade. *Journal of Computing Sciences in Colleges*, *27*(2), 142-147.

York, T. T., Gibson, C., & Rankin, S. (2015). Defining and measuring academic success. *Practical Assessment, Research & Evaluation, 20*(5), 1–20.

EMPOWERING ARTIFICIAL INTELLIGENCE FOR KNOWLEDGE MANAGEMENT AUGMENTATION

Edward Chen, University of Massachusetts Lowell, edward_chen@uml.edu

ABSTRACT

This study investigates the transformative potential of artificial intelligence (AI) in enhancing knowledge management (KM) systems. Organizations face challenges with vast data accumulations and fragmented knowledge silos that traditional management systems cannot efficiently address. This research highlights how knowledge capture, retrieval, and synthesis can be automated to improve organizational performance.

AI in knowledge management promises to automate tedious tasks like data tagging and categorization, enhance efficiency, and save employee time. By breaking down informational silos, AI-driven systems facilitate improved collaboration across organizational and geographical boundaries. These systems also support better decision-making by providing timely and relevant insights. To **integrate AI effectively**, organizations must conduct thorough needs assessments to identify pain points and user preferences, select suitable AI technologies, and develop customized solutions that align with organizational workflows. Ensuring robust data privacy and offering comprehensive training programs are essential to encourage adoption and maximize the benefits of AI tools.

Looking forward, the successful integration of AI into knowledge management is anticipated to herald advanced applications like AI-powered virtual assistants, predictive analytics, and augmented reality, all while navigating ethical considerations to ensure fairness and transparency. This research endeavors to unlock AI's potential, propelling organizations towards a future where knowledge management is efficient, inherently collaborative, and astutely informed, marking a significant evolution in organizational dynamics in the digital age.

Keywords: Artificial Intelligence, Decision-Making, Generative Artificial Intelligence, Knowledge Management, Organizational Performance, Problem-Solving

INTRODUCTION

The most comprehensive definition of knowledge management refers to a range of practices used by organizations to identify, create, represent, and distribute knowledge for reuse, awareness, and learning across the organization (Glick, 2007).

In other words, it refers not only to mere knowledge but also to a very forward-looking process of sharing tacit knowledge possessed by employees within the organization and creating the next step. It is a management method that aims to create innovations by utilizing the knowledge and experience of individuals throughout the organization. Recently, this method has become widely known and has attracted attention in business, where the collapse of lifetime employment has made it difficult for companies to pass on their knowledge and know-how. The key point is to convert tacit knowledge into formal knowledge through verbalization and visualization and share it throughout the organization.

The concept of AI dates back to ancient times, with myths and legends about artificial beings with intelligence and consciousness. Surprisingly, artificial intelligence is based on the assumption that human thought processes can be reproduced by machines, and the history of mechanical or formal reasoning goes back to Chinese, Indian, and Greek philosophers. Aristotle, for example, formulated and analyzed the three-stage argument; Hourisme developed algebra, whose name remains as "algorithm." However, since the modern field of AI research was established in the 1950s, we will now look at the history of modern AI. The main events and developments in the History of Artificial Intelligence are as follows:

1950s: The term artificial intelligence was coined by John McCarthy at the Dartmouth Conference in 1956. Early pioneers such as Alan Turing, John McCarthy, Marvin Minsky, and Claude Shannon began exploring fundamental concepts such as artificial neural networks and machine learning (ML). They are considered the key programmers of the first decade of AI research.

1960s-1970s: the "first AI boom," a period of rapid progress and optimism in AI. Researchers focused on areas such as reasoning and problem-solving. However, by the mid-1970s, progress slowed, funding was cut, and the "AI winter" set in. AI was then subjected to criticism and funding cuts, AI researchers failed to properly assess the difficulty of the problems they were facing, expectations of expected results were raised too high out of optimism to produce results, and funding for research largely dried up. In addition, the low performance of computers, at least concerning the processing of AI, was a very significant barrier.

The 1980s: The "second AI boom" was driven by the development of expert systems that could replicate human decision-making. These systems, however, were limited in their ability to do so because they were derived from built-in expert knowledge and because the knowledge had to be programmed by hand. Just as quickly, as in 1981, Japan's Ministry of International Trade and Industry launched a 57 billion yen fifth-generation computer project. The goal was to build programs and machines that could achieve a variety of goals, such as interacting with humans in natural language, machine translation, image recognition, human-like reasoning, etc., etc., which led to a worldwide AI boom.

2000s-present: Powerful hardware, large data sets, and the rise of new machine learning algorithms such as deep learning using autoencoders by Jeffrey Hinton led to the "third AI boom, AI has made great strides in areas such as natural language processing, computer vision, and gameplay. Deep learning, in particular, was a breakthrough in artificial intelligence, as it eliminated the need for human knowledge representation in terms of feature extraction without human intervention.

Then, in 2022, the release of ChatGPT, a large-scale language model developed by OpenAI, demonstrated the transformative potential of AI in communication and interaction with machines. Generative AI is now an integral part of our lives. Overall, the History of Artificial Intelligence has been characterized by cycles of progress, setbacks, and renewed optimism as the field has evolved over the past 70 years. 2050, or 2045 at the latest, will be the year when artificial intelligence will far surpass humans in terms of knowledge and intelligence and will be the main driver of scientific and technological progress and transform the world. It is no exaggeration to say that the era in which we now live is on the verge of an even earlier Singularity.

Knowledge management enhancement refers to a variety of strategies and techniques used to improve and optimize an organization's knowledge management. Some important aspects include centralizing knowledge content, leveraging technology and AI, building a knowledge-sharing culture, and measuring and optimizing performance, companies can implement these best practices to drive productivity, innovation, and a better customer experience. A study identifying drivers of innovativeness in a furniture manufacturing company reported that a hybrid of technology management and knowledge management works to promote innovation. The study showed that if the goal is to maximize product or process innovation, the focus should be on improving modification and computational efficiency, and if the priority is the immediate improvement of innovativeness, the focus should be on improving contextualization efficiency. Thus, knowledge management is also one way to strengthen innovativeness to gain a competitive advantage in business (Reddy et al., 2023).

INTERPLAY OF ARTIFICIAL INTELLIGENCE AND KNOWLEDGE MANAGEMENT

Artificial intelligence and knowledge management are closely related, with knowledge management providing context, structure, and understanding to AI algorithms, while AI leverages machine learning to accelerate knowledge discovery, streamline content curation, and personalize information delivery to enhance the practice of knowledge management. This convergence represents a paradigm shift and opens new possibilities to drive productivity, innovation, and competitive advantage. AI-powered knowledge management tools and platforms analyze vast amounts of data in real time to provide valuable insights to the business but to achieve the best results, human and AI collaboration is essential. Careful attention must also be paid to ethical considerations related to data privacy, security, and the balance between automation and the contribution of human knowledge, successful AI adoption requires seamless integration that bridges the gap between human expertise and AI capabilities, user-friendly interfaces, and employee skill development is necessary.

A significant number of studies have been conducted in the past to explore the relationship between AI/ML and KM systems. However, these studies have focused on the impact of definitive technologies and a small number of AI/ML algorithms, neglecting their other roles and how they impact KM systems to achieve organizational goals. KM systems can be significantly enhanced by AI/ML, especially in knowledge acquisition and knowledge creation, and other knowledge management processes can take advantage of different types of AI/ML algorithms that can enhance an organization's competitiveness. Finding that most of the previous studies agree that there is a positive correlation between AI/ML and knowledge management and discussing the pivotal role that AI/ML plays in the overall improvement of KM systems, also attests to this (Vadari and Desik, 2021).

RECENT KNOWLEDGE MANAGEMENT PROBLEMS

In the modern domain of knowledge management, organizations are inundated with vast amounts of data, creating a major barrier to employees identifying the right information quickly and efficiently. This problem is compounded by the fact that knowledge is often siloed and scattered across various departments and individuals, greatly hindering the potential for collaboration and the fluid exchange of insights. Further complicating matter is the dynamic nature of knowledge itself. As knowledge ages, it tends to become obsolete, leading to inaccurate and inefficient decision-making processes. This temporal decay of knowledge underscores the need for systems that not only capture and store information but also keep it current and relevant over time.

In addition to these challenges, traditional KM systems are inadequate to provide a customized experience. Such systems often fail to provide personalized recommendations in line with the unique needs and preferences of individual users, thus limiting the usefulness and reach of knowledge within the organization. While knowledge management systems are still widely applied and researched in the business sector, research on the use of knowledge management systems in the public sector remains an open question. Furthermore, it explains that the commonly discussed models related to organizational learning relate to elements of management and leadership, culture, knowledge, information and communication systems, and organizational structure and that the topics related to organizational learning are social processes, corporate values, organizational memory change, operational performance, organizational effectiveness, and total quality management, to name a few variables, and there still seems to be an opportunity to propose a comprehensive model using structural equation model analysis that includes knowledge management systems, organizational learning, innovation, and performance (Fitriastuti et al., 2019).

Taken together, these issues highlight the pressing need for a more sophisticated and nuanced approach to knowledge management. Organizations are called upon to critically evaluate their knowledge management practices and infrastructure and identify bottlenecks and opportunities for innovation to handle the knowledge lifecycle in a more enlightened and efficient manner.

ORGANIZATIONAL IMPACTS

The integration of artificial intelligence into knowledge management practices is expected to transform organizational operations across several dimensions. Specifically, it will increase efficiency, enhance collaboration, improve decision-making, and promote continuous learning. The following is a summary of each dimension based on the results of several studies (Taherdoost and Madanchian, 2023).

Increased Efficiency

Increased efficiency: AI's ability to automate repetitive tasks in knowledge management represents a pivotal shift toward increased organizational efficiency. By minimizing manual labor, AI will allow organizations to focus more on strategic tasks. In addition, advanced search and retrieval capabilities ensure fast and accurate access to information, thus optimizing the flow of knowledge. AI's role extends to organizing and curating vast knowledge bases by employing intelligent algorithms to classify and personalize content, simplify navigation, and improve manageability. The use of AI in this context will not only accelerate productivity but also strengthen the infrastructure underlying the knowledge management process (Taherdoost and Madanchian, 2023).

Enhanced Collaboration

AI-driven systems act as catalysts to improve collaboration within an organization. By suggesting relevant documents, pinpointing subject matter experts, and establishing valuable connections, AI enhances synergy across teams and departments. Implementing AI-powered chatbots and virtual assistants can offload routine inquiries from human staff. AI can enable more in-depth decision-making support and allow managers to engage in more complex problem-solving activities. In addition, AI's analytical ability to decipher communication patterns and knowledge flows will discover new pathways for collaborative innovation and foster a more interconnected and unified workforce (Taherdoost and Madanchian, 2023). The rapid proliferation of Generative Artificial Intelligence has revolutionized the way employees interact with KM systems by providing rapid access to a vast knowledge base. This impact has also raised questions about the balance between human-derived tacit knowledge and AI-generated formal knowledge (Alavi, Leidner, and Mousavi, 2023).

Improved Decision-Making

At the core of AI's impact on knowledge management is its ability to derive actionable insights from vast data sets, enabling decision-makers to better understand underlying trends and correlations. Predictive analytics from AI will increase organizational foresight, reveal future trajectories, and facilitate proactive strategy development. The KM system will also be monitored by an AI system that will be used to monitor the KM system. AI's vigilance in monitoring the KM system will also enhance regulatory compliance, uncover potential inconsistencies, and support a framework for strategic, sustainable, ethical, and informed decision-making (Tettra, 2024). Knowledge management of knowledge based on experience and intuition, or so-called tacit knowledge, is derived from four dimensions: socialization, externalization, cohesion, and internalization. Tacit knowledge management has been shown to have a significant impact on organizational performance. However, of the four dimensions of socialization, internalization, externalization, and cohesion, tacit knowledge management had a significant impact on organizational performance only for socialization and internalization (Muthuveloo, Shanmugam, and Teoh, 2017).

Continuous Learning

AI systems embody the principle of perpetual growth, continually learn from ongoing interactions, and adapt their knowledge repository to reflect the latest conditions. This adaptive learning ensures that disseminated knowledge remains relevant and valuable to users. By tailoring content to the needs and preferences of individual users, AI redefines the personalization of knowledge provision. Proactively identifying knowledge gaps paves the way for timely enhancement and creates an organizational culture that values continuous progress and intellectual curiosity (Elium, 2024). One point of caution, however, is the impact on organizations of the rapid proliferation of Generative Artificial Intelligence beginning in 2022 while generative AI undoubtedly improves processing and cognitive functions in the process of knowledge creation, storage, transfer, and application. Generative AI facilitates both individual and organizational learning. There are risks of AI bias and human social discrimination. However, there is also the risk caused by AI bias and the marginalization of young knowledge workers. In terms of knowledge application, generative AI is seen as a tool to increase productivity and innovation, but issues such as misuse of knowledge, intellectual property, and ethical considerations are important (Alavi, Leidner, and Mousavi, 2023).

SUGGESTIONS FOR KNOWLEDGE MANAGEMENT ENHANCEMENT

To enhance knowledge management with artificial intelligence, organizations should undertake a series of strategic steps. First, conduct a comprehensive analysis of knowledge requirements and address specific pain points and user preferences so that AI solutions can accurately address these needs. Furthermore, as the organization gains experience in transforming information into knowledge, it will be able to govern more influentially and efficiently as the future vision of knowledge erupts. It is crucial to recognize that it is challenging to anticipate all the processing that will be necessary for a specific organization. This is because the aggregation of individual sources of information and knowledge requirements is intricate and undergoes constant evolution (Pai et al., 2022). Second, carefully select AI technologies such as natural language processing and machine learning that are aligned with the organization's objectives to provide the most effective solution. Many types of applications and software exist for visualization tools. Such resources do not manage knowledge by themselves. Knowledge management is not just a “technology” per se. Creating a knowledge management “framework” requires a blend and combination of individuals, cultures, and technologies (Pai et al., 2022). Third, customize these AI-driven systems to seamlessly integrate with existing organizational workflows to increase efficiency and consistency. Fourth, establish robust data privacy measures to comply with regulations and protect sensitive information, protecting both the organization and its stakeholders. IT support systems based on artificial intelligence have emerged as crucial elements for organizational innovation, efficiency, and effectiveness. A unified, automated framework to manage the necessary infrastructure, data, IT assets, and lifecycle management is essential for ensuring sustainability, security, compatibility, compliance, and adherence to legal regulations. The primary challenge lies in keeping pace with ongoing advancements in both infrastructure and software technology (Pai et al., 2022). Finally, provide targeted training programs for employees to facilitate the adoption and effective use of AI tools and maximize their potential benefits. Collectively, these steps are a blueprint for leveraging AI to revolutionize knowledge management practices and make organizations more agile, informed, and competitive in the digital age. In addition, there is an interesting finding about using ChatGPT. It suggests that when students perceive the usefulness of ChatGPT for learning, they experience higher levels of satisfaction and are more likely to continue using ChatGPT. Furthermore, knowledge acquisition has a significant impact on both satisfaction and continued use of ChatGPT, while knowledge sharing and application only affect user satisfaction. This indicates that students prioritize knowledge acquisition over knowledge sharing and application through ChatGPT. Theoretically, utilizing the expectation confirmation model and integrating knowledge management elements would contribute to the understanding and continued use of ChatGPT. User satisfaction not only can be found in education but also in business training (Ngo et al., 2024).

FUTURE IMPLICATIONS

The successful deployment of AI-enhanced knowledge management systems is anticipated to pave the way for developments such as AI-driven virtual assistants, advanced predictive analytics, augmented reality integration, and the need for ethical practices ensuring fairness and transparency in operations. Incorporating knowledge management as a strategic business approach is likely to provide firms with a significant competitive advantage, enabling them to surpass their rivals. Effective KM implementation can lead to increased revenues, reduced resource consumption, significant cost savings, and heightened user acceptance. KM also supports the establishment of an environment conducive to teaching and learning, with both elements recognized as vital corporate assets. Employees are often inspired to pursue continuous personal development, enhance their skills, and take on leadership positions.

Furthermore, the rise of remote working has underscored the importance of robust KM systems more than ever before. In the contemporary digital age, defined by rapid advancements in information technology, SNS (social networking, blogs, etc.), and artificial intelligence, the workforce and knowledge assets of organizations comprise a diverse array of generational cohorts, including Post-war Generation, Transition Generation, Digital Natives, and Internet Generation. This diversity necessitates a reevaluation of an organization’s memory and intellectual prowess (Viterouli et al., 2023). Achieving a long-term competitive edge will depend critically on the efficacy of knowledge management. The management and organization of the knowledge management process, which encompasses the generation of knowledge, dissemination, transmission, assimilation, archiving, access, and utilization, are of vital importance for operational success. This study has endeavored to tap into AI's potential to foster organizations that are not only efficient and collaborative but also well-informed in the digital landscape. The expected impact of such AI-driven KM systems extends across various industries. They affect multiple generations of employees and alter organizational practices (Pai et al., 2022).

CONCLUSION

In this paper, we have explored the profound impact of artificial intelligence on knowledge management systems. We illustrate how AI can transform traditional knowledge management practices into dynamic and efficient processes. As organizations continue to grapple with vast data accumulations and fragmented knowledge silos, AI emerges as a pivotal technology capable of revolutionizing how knowledge is captured, retrieved, and synthesized. This conclusion synthesizes the findings from our research and anticipates future directions in this evolving field.

AI's integration into KM practices has demonstrated significant potential to enhance organizational efficiency by automating routine tasks such as data tagging, indexing, and categorization. This automation not only speeds up access to relevant information but also alleviates the manual burden on employees, allowing them to engage in more value-adding activities. Furthermore, AI-driven systems have been crucial in breaking down informational silos, promoting an environment of enhanced collaboration across different departments and even geographical locations. By facilitating seamless information flow, these systems contribute to a more cohesive organizational knowledge ecosystem. The decision-making process within organizations has also seen remarkable improvements due to AI’s ability to provide timely and fairly accurate insights. Through advanced analytics and predictive modeling, AI aids in uncovering hidden patterns and forecasting future trends, thereby enabling more informed and strategic decision-making.

Additionally, AI’s role in ensuring compliance and ethical governance in KM practices cannot be overstated, as it helps organizations navigate the complexities of data privacy and security with greater precision. An equally important aspect of AI in KM is its capability to foster continuous learning and adaptation. AI systems are designed to learn from new data inputs continuously, ensuring that the organizational knowledge base remains up-to-date and relevant. This feature is indispensable in today’s fast-paced business environments where information becomes obsolete quickly. AI’s ability to personalize knowledge delivery according to individual user preferences further enhances the effectiveness of KM systems, making them more user-centric and responsive. Looking ahead, the successful implementation of AI-powered KM systems is poised to lead to even more sophisticated applications such as AI-powered virtual assistants, enhanced predictive analytics, and augmented reality integrations. These advancements are expected to drive significant shifts in organizational practices and push the boundaries of what is possible in knowledge management. As organizations adopt knowledge management as a strategic business tool, they are likely to experience substantial benefits, including increased revenue, reduced resource utilization, and improved operational efficiencies. Moreover, the rise of remote work has underscored the importance of robust KM systems, which are crucial for supporting a dispersed workforce. In the era of digital transformation, where the workforce comprises multiple generations, rethinking an organization's knowledge strategy and tools is essential to maintain competitiveness and innovation.

In conclusion, this thesis not only highlights the current benefits of integrating AI into KM systems but also sets the stage for future research in this field. By continuously evaluating and adapting AI strategies in knowledge management, organizations can look forward to not only keeping pace with technological advancements but also setting new standards for efficiency, collaboration, and innovation in the digital age.

REFERENCES

Alavi, M., Leidner, D. E., & Mousavi, R. (2023). A knowledge management perspective of generative artificial intelligence. *Journal of the Association for Information Systems, 25*(1), 1-12.

Elium. (2024). *Unlocking synergy: The dynamic relationship between knowledge management and AI*. https://elium.com/blog/unlocking-synergy-the-dynamic-relationship-between-knowledge-management-and-ai/

Fitriastuti, L. I., Sujoko, Sujoko, Herawan, T., & Vemberi, Y. (2019). Knowledge management system usage and organization learning: Recent trends and open problems. *Journal of Advanced Research in Law and Economics (JARLE), 10*(6), 1832-1849. HeinOnline.

Glick, S. (2007). What is knowledge management and how can marketing directors have a role in managing the knowledge in their firms? CPA Practice Management Forum, 3(4), 11-12.

Muthuveloo, R., Shanmugam, N., & Teoh, A. P. (2017). The impact of tacit knowledge management on organizational performance: Evidence from Malaysia. *Asia Pacific Management Review, 22*(4), 192-201.

Ngo, T. T. A., Tran, T. T., An, G. K., & Nguyen, P. T. (2024). ChatGPT for educational purposes: Investigating the impact of knowledge management factors on student satisfaction and continuous usage. *IEEE Transactions on Learning Technologies, 17*, 1367-1378.

Pai, R. Y., Shetty, A., Shetty, A. D., Bhandary, R., Shetty, J., Nayak, S., Dinesh, T. K., & D'souza, K. J. (2022). Integrating artificial intelligence for knowledge management systems – synergy among people and technology: A systematic review of the evidence, 7043-7065. https://www.tandfonline.com/doi/full/10.1080/1331677X.2022.2058976

Reddy, S., Babu, M. N., Yamuna, G., Madhavi, T., Bizon, C. C., Bizon, N., & Thounthong, P. (2023). Hybridizing technology management and knowledge management to spur innovation: A system dynamics approach. *Organizations & Markets in Emerging Economies, 14*(3), 696-720. https://doi.org/10.15388/omee.2023.14.11

Taherdoost, H., & Madanchian, M. (2023, March 31). *Artificial Intelligence and Knowledge Management: Impacts, benefits, and implementation*. MDPI. https://www.mdpi.com/2073-431X/12/4/72

Tettra. (2024). *How AI knowledge management will impact your business*. https://tettra.com/article/ai-knowledge-management/

Vadari, S., & Desik, P. H. A. (2021). The role of AI/ML in enhancing knowledge management systems. *IUP Journal of Knowledge Management*, *19*(2), 7-31.

Viterouli, M., Belias, D., Koustelios, A., & Tsigilis, N. (2023). Linking adult learning to knowledge management in a multigenerational workforce. *Proceedings of the European Conference on Knowledge Management, 24*(2), 1410-1420.

AN ANALYSIS OF AMERICAN'S ATTITUDES ABOUT ARTIFICIAL INTELLIGENCE AND THEIR IMPLICATIONS FOR SOCIETY

Chandrashekar Challa, Virginia State University, cchalla@vsu.edu
Ephrem Eyob, Virginia State University, eeyob@vsu.edu

PROPOSED STUDY

Artificial intelligence is a rapidly expanding field. The evolution of AI has seen remarkable advancements in natural language processing (NLP). Today's AI can understand, interpret, and generate human language with unprecedented accuracy, which is evident in sophisticated chatbots, language translation services, and voice-activated assistants (Ideta, 2024) This paper explores Americans' evolving perceptions of artificial intelligence (AI) and discusses the broader social implications of these attitudes. By examining AI's historical development, current applications, and potential future, this study offers insights into AI's challenges and opportunities for society (Galaxy Information Technologies, 2024). We propose to summarize the analysis conducted by these organizations and recommend guidelines for future research in artificial intelligence. AI is an important and timely topic for IACIS 2024 conference participants, as the results of our study will provide participants with possible ideas and avenues for their future research in AI, use of AI in teaching computer programming, systems analysis & design, networking, and courses that have language translation components.

Keywords: artificial intelligence, AI attitudes, AI implications, AI research, AI & society

BASIS OF THE STUDY

The history of AI marks significant milestones that illustrate its development from theoretical foundations to practical applications. The history of artificial intelligence traces back to British scientist Alan Turing, who, in his 1950s research paper, explored the mathematical possibility of artificial intelligence (Anyoha, 2017). Turing suggested that humans use available information and reason to solve problems and make decisions, so why can't machines do the same thing? (Turing, 1950). Alan Turing published his work "Computing Machinery and Intelligence," which eventually became the Turing Test, a method used to measure computer intelligence. The term "artificial intelligence" was coined and used widely (McCarthy et al., 1956). John McCarthy, an American scientist, was a prominent computer and cognitive scientist who is equally considered the founder of artificial intelligence. The summer 1956 conference at Dartmouth College (funded by the Rockefeller Institute) is regarded as the discipline's founding event (McCarthy et al., 1956). Premier research universities, institutes, and centers like Pew Research, Stanford University, Northeastern University, and Brookings Institute conducted studies to analyze American attitudes toward artificial intelligence. AI has advanced from basic algorithms to complex systems that can learn and make decisions independently (VNext, 2024). AI has gone through several phases: initial rule-based systems, integration of machine learning, the rise of deep learning, and the current exploration of AI ethics and autonomous decision-making systems (Claytex, 2024).

The journey of artificial intelligence (AI) from its conceptual beginnings to today's advanced systems showcases a rich trajectory filled with notable advancements, setbacks, and invaluable lessons (Claytex, 2024). Understanding the predisposition of humans toward this critical technology, which is revolutionizing customer experience (CX) in various fields such as business, industry, education, entertainment, medicine, sports, and many other areas, is crucial in designing products and services that will match and enhance customer experience.

The data source is a dataset from the Pew Research Center, which collects objective data that meets the highest standards. We will analyze the data using various statistical tools and techniques to understand American attitudes toward artificial intelligence and its societal implications. The data analysis will reveal insights into public views in America, which will determine the technologies to use and the challenges expected. Such detailed insights also allow companies and organizations to design products and services that meet the expectations of Americans without compromising societal implications. Additional insights from the study would be related to the risks of AI to society, including employment issues, abuse of AI by bad actors, the use of AI in the movie and music industry, deployment of driverless cars, use of algorithms to identify false information on social media, human enhancement practices in the areas of genetics, medicine, and the enhancement of cognitive function using computer chip implants in the brain.

REFERENCES

Anyoha, R. (2017). Special edition on artificial intelligence. *Science in the News*. https://sitn.hms.harvard.edu/special-edition-artificial-intelligence/

Claytex. (2024). Neural networks archives. *Claytex*. https://www.claytex.com/tag/neural-networks/

Galaxy Information Technologies. (2024). The future is now: Understanding artificial intelligence and its impact on society. *Galaxy Information Technologies*. https://galaxyit.net/the-future-is-now-understanding-artificial-intelligence-and-its-impact-on-society/

Ideta. (2024). How artificial intelligence has evolved over the years. *Ideta*. https://www.ideta.io/blog-posts-english/how-artificial-intelligence-has-evolved-over-the-years

McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (1956). A proposal for the Dartmouth summer research project on artificial intelligence.

Turing, A. M. (1950). Computing machinery and intelligence. *Mind, 59*(236), 433-460.

RISK MANAGEMENT POLICIES FOR GENERATIVE ARTIFICIAL INTELLIGENCE IN THE CLASSROOM

Donna M. Schaeffer, PhD Marymount University donna.schaeffer@marymount.edu
Mashianeh Dehghanpour Marymount University m0d39143@marymount.edu
Patrick C. Olson, PhD National University polson@nu.edu

ABSTRACT

This is an exploratory study of Generative Artificial Intelligence (GenAI) policies at colleges and universities designated as National Centers of Academic Excellence (NCAE) for cybersecurity degrees in the United States. These colleges and universities comprise an interesting set to study because the cybersecurity ecosystem has been a leader in competency-based assessment. Through a content thematic analysis of existing policies and correspondence interviews with academic administrators, we developed recommendations for student use of GenAI in classwork. The intended audience of this paper, which includes faculty and academic administrators, will need to write and adopt policies and procedures for acceptable use. The research methodology may also be modified and applied to other emerging technologies and pedagogies.

INTRODUCTION

This study aims to understand existing Generative AI (GenAI) policies for several National Centers of Academic Excellence (NCAE) in Cybersecurity Bachelor's degree programs. These organizations are at the forefront of cybersecurity research and the progression of curriculum and pedagogy. This mixed method study consists of content analysis of policies and correspondence interview analyses. The goal is to introduce the concepts a Gen AI policy should include for appropriate student technology usage. The two primary research questions are:

Q1. What are current trends and policies among NCAE entities related to student usage of generative AI tools?
Q2. How can universities improve their existing or develop a student usage of Gen AI policy?

There are sound reasons for studying the GenAI policies at NCAE institutions. In 1999, The National Security Agency (NSA) founded and still manages the National Centers of Academic Excellence in Cyber Security (NCAE-C) program alongside several partners such as the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA). The program supports colleges and universities in the United States that offer cybersecurity education programs by setting curriculum standards, fostering outreach initiatives, and researching how to improve cybersecurity education. The curricula in NCAE cybersecurity degree programs are ethically oriented, and the program administrators routinely share knowledge and lead by example. The NCAE schools have shown a solid commitment to responding to the ever-developing and growing cybersecurity challenges through curriculum development efforts and implementing new pedagogies in the classroom and labs.

Competency-based Education

One hallmark of modern cybersecurity curricula is competency-based education. This pedagogy has been used in other disciplines, as well. Competency-based education (CBE) is often referenced across various industries with slightly different definitions (Frank *et al.*, 2010). A broad definition, for example, comes from health care -- the American Association of Critical-Care Nurses defines competency-based education as "a system of instruction, assessment, feedback, self-reflection, and academic reporting based on students demonstrating that they have learned the knowledge, attitudes, motivations, self-perceptions, and skills expected of them as they progress through their education" (American Association of Colleges of Nursing, n.d.). In healthcare, competency-based education may also be called outcome-based education (OBE).

Competency-based education has a complement. When criteria are formulated as competencies, which integrate knowledge, skills, and attitudes, assessment criteria may be designed as performance indicators (Fastré *et al.*, 2010).

CBE's origins can be traced back to 1957 when the Soviet Union launched Sputnik I. This event catalyzed the United States to focus on science and mathematics in the American educational system and facilitated the launch of training programs. This impetus created a mindset that curriculum design should focus on specific objectives to produce student behavior changes. Students' overall learning is most meaningful when they accomplish skills that can be applied in real life (Morcke *et al.*, 2012). Thus, skills-based learning is a cornerstone of CBE and suggests that it is more important for learners to validate that they know the information required for their target jobs through their sheer skills and validation of credentials. CBE challenges the idea that students must spend certain hours or earn a specified number of credits to learn particular concepts (Baker-Stein *et al.*, 2020).

Learning theories such as CBE allow pre-professionals to be adequately trained in the specific concepts related to the work they will be conducting and to get as much hands-on and interactive experience as possible. Learners should actively work to improve their knowledge, as active cognition is more beneficial to learners than simply passively acquiring knowledge. CBE supports that learning objectives should be relevant to the learner, learning should occur in an environment that mirrors the real world, and teachers should serve as guides rather than simply instructors (Doolittle & Camp, 2017).

Competency-Based Education (CBE) in Cybersecurity

The National Institute of Standards and Technology (NIST) called for employers to be more open toward CBE regarding cybersecurity assessments. Baker-Stein *et al.* (2022) suggest that skills-based learning and hiring should be more common across the public and private sectors and that this practice is already growing across both sectors. Companies across all industries have highly leveraged traditional university degrees as a prerequisite and pivotal element in hiring and promotion decisions. However, Executive Order 13932, issued by then-President Donald Trump on June 26, 2020, has focused on modernizing and reforming the assessment and hiring of federal job candidates. A potential hire's competency and specific skills may be more important than degrees in the future (Baker-Stein *et al.*, 2022).

For the cybersecurity industry, CBE is a direct response to the education-to-hiring portion of the ecosystem. It supports improved hiring opportunities for non-traditional aspiring cybersecurity professionals who may need a relevant university degree. Given that CBE is centered around learners being able to grow in confidence and expertise for specific job roles, this model "gives credit where credit is due" (Baker-Stein *et al*., 2022, p. 1). Employers also find that the more motivated and capable a candidate is to learn, the more they will invest in training a candidate for the proper role. As a theory, CBE supports individuals looking to expand their cybersecurity expertise in technical and soft skills (Baker-Stein *et al.*, 2022).

Scenario-based learning is a method within CBE. Ghosh and Francia (2021) report that it effectively assesses an individual's competency.

Artificial Intelligence (AI), Cybersecurity, and Competency-Based Education (CBE)

Artificial intelligence (AI) and Cybersecurity are topics of interest in the current societal landscape. Their interconnection supports the knowledge economy, as AI's use in Cybersecurity can protect critical infrastructure and boost the economy. AI has a vast expanse of use cases in Cybersecurity, such as detecting potential malicious events, malware, and more. AI supports advancements in various industries, such as healthcare, and drives innovation and economic growth (Sarma *et al.*, n.d.). Generative artificial intelligence (GenAI) is a form of AI that can develop content such as text, images, videos, and audio based on prompts or inputs that the AI system can process. With advances in machine learning, which trains the AI system on data from various sources, this process can occur rapidly and allow for novel content generation (Polito and Pupillo, 2024).

One of the most recognized GenAI tools is ChatGPT, which members of the public often use for various use cases, such as developing a travel itinerary or looking up answers based on specific prompts. GenAI can be a big time-saver for cybersecurity professionals, as it aids in identifying trends and solving complex problems and can even support training simulations (Polito and Pupillo, 2024). Privacy and security needs within Cybersecurity make using applications like ChatGPT tricky. Since GenAI tools can learn from information inputted in response to prompts, users must be wary of what they input into these systems and ensure none is proprietary or sensitive data.

GenAI tools such as ChatGPT can be leveraged for training and tutoring within CBE. These tools can gamify the learning experience and allow for simulation engagement and unique novel outputs to aid students. Given the considerable risks associated with using AI technology in education, students must understand how to use these tools responsibly. GenAI highlights the importance of educational institutions outlining the acceptable use of such tools. Aside from the more significant ethical risks associated with using GenAI in the educational space, students may unknowingly engage in plagiarism, relying upon outputs that may not be entirely accurate or even hindering their learning process by not fact-checking information produced by such tools. Acceptable student use policies should be clearly outlined and made available to students as they continue to navigate the responsible use of these technologies.

Examples of ChatGPT Use in Cybersecurity Class Assignments

Cybersecurity faculty often incorporate new and emerging tools into the curriculum. Kallonas, Piki, and Stavrou (2024) describe teaching cybersecurity students how to write effective ChatGPT prompts to build training plans for specific job roles, such as threat intelligence analysts. Marquardson (2024) describes positive results from allowing students to use ChatGPT 3.5.

Students reported it was a helpful learning aid and plan to use ChatGPT for self-directed learning after graduating college. He reports that the students did not violate academic integrity policies.

Santhi and Srinivasan (2024) used the ChatGPT to enhance the learn-apply-create model of pedagogy. Students provide prompts and learn from the computer's responses. The learned concepts are then applied to the mathematical modeling of cyberattacks, and detection schemas are created. They found that incorporating ChatGPT provided students with essential skills in modern industry.

Mitra and Ro (2023) describe the conversational role-playing exercise they developed for a course. Using ChatGPT to simulate attack vectors, students played the Chief Information Security Officer role and developed responses. The assignment fostered holistic competencies as well as technical skills. Students reported having more confidence to apply their knowledge in a meaningful and impactful manner.

RESEARCH METHODOLOGY

This study's population drew from the 401 institutions the NCAE accredits for their Cyber Defense programs. The National Centers of Academic Excellence in Cybersecurity website briefly describes all current CAE programs in the United States. Our search for the terms "competency-based learning" and "artificial intelligence" yielded twelve (12) CAE-C institutions. We were able to locate some policies on public-facing websites. When we could not locate a publicly available GenAI policy, we emailed a brief correspondence interview to the cybersecurity program administrator to gather additional information on their current or potential acceptable use policies for GenAI.

Survey of NCAE Institutions

The twelve (12) institutions we gathered information about represent a geographic diversity across the United States and comprise both public and private institutions. Marymount University's Institutional Review Board deemed the correspondence interview protocol exempted from review on 28 May 2024. The correspondence interview protocol has six questions:

1) Does your educational institution have a policy for student use of generative artificial intelligence (AI) tools such as ChatGPT?
2) If yes, what brought about the creation of this policy, and what did the process for creating it look like, e.g., was it created by a committee or an individual?
3) Is the policy disseminated to students? If yes, how, when, and how often? Have students provided feedback regarding this policy?
4) Do you view the policy as having positive or negative impacts on generative AI use at your educational institution?
5) Please provide the URL where we can access the policy or attach the policy as a reply to this email.
6) If your institution does not have a policy, is there a reason why, or do you plan on implementing a policy within the coming academic year?

We employed a constructivist worldview for this exploratory study as we plan to continue gathering data and then develop a theory. "A constructivist believe[s] that individuals seek understanding of the world in which they live and work. Individuals develop subjective meanings of their experiences … these meanings are varied and multiple, leading the researcher to look for the complexity of views rather than narrowing meanings into a few categories or ideas" (Creswell and Creswell, 2022, p. 9). After analysis of the policies using MAXQDA software, we derived takeaways regarding current trends for GenAI policies, and the critical information that needs to be included in GenAI usage policy. This will be discussed in the Conclusion of the paper.

RESULTS

Based on the policies currently in place at the institutions, the preliminary analysis resulted in 13 codes used 77 times in all documents. The most popular code was artificial intelligence or AI, used 30 times. Additionally, ChatGPT was referred to by name seven times. All 12 institutions agreed that students should use GenAI only with the instructors' permission. Misuse or unauthorized use was closely aligned with violations of academic integrity and intellectual honesty. Terms such as academic misconduct, plagiarism, and cheating were often used. A few policies noted the benefits that GenAI provides as an aid but cautioned students to use it ethically and consider the risks.

Responses to the correspondence interview indicate that those institutions that do not currently have policies on GenAI use by students plan to implement one within the coming academic year.

A program director from a large state university said the need for their policy was driven by the rapid advances in large language model technologies and the fact that AI tools are readily available and free. He said, "The policies are meant to promote ethical and open/fair use of GenAI tools, where permissible by instructors and committees. The intent is to allow students to leverage them to enhance their work where possible and do this transparently and openly."

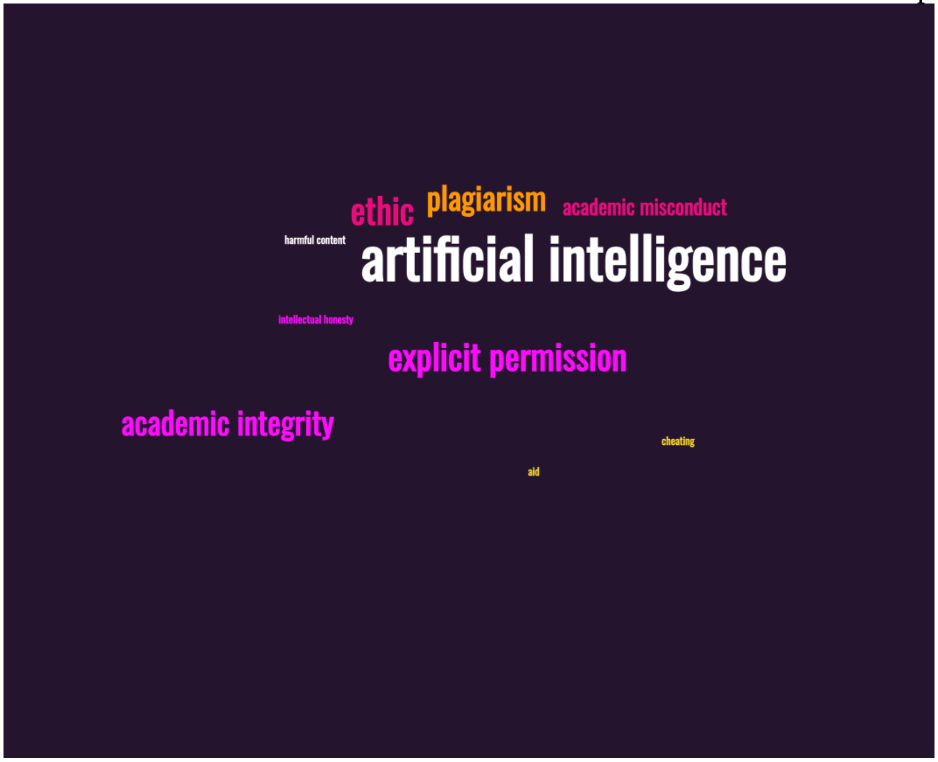
Each institution indicated that the policies were, are being, or will be developed by committees. Almost all policies were written in collaboration with or after discussions with the faculty. At one public college, the respondent said, "… there is a committee state-wide to dig more into what AI means for us."

Once adopted, the policies are disseminated by course instructors at the start of each semester, typically via course syllabi.

Some colleges and universities may integrate GenAI policies with other academic policies. One respondent noted that their academic integrity policy implicitly covers GenAI tools. Their policy is intentionally designed to allow instructors to define what is "authorized" vs. "unauthorized" and what constitutes "plagiarism" and "cheating." In several policies we looked at, the use of GenAI tools was at the discretion of the course's instructor.

Two institutions do not have an official policy but suggest language for faculty to use and adapt for their courses.

Figure 1 shows a word cloud based on the themes we identified in the GenAI policies.



CONCLUSION

As the use of GenAI diffuses through our culture, several use policies could be appropriate. However, as new technologies diffuse, the best means to ensure broad and equitable adoption is to have a policy that addresses all the ways the organization is being affected. The following components need to be addressed in a GenAI.

A Preamble section should acknowledge the existence of and recognize the benefits of emerging technologies such as GenAI. The Preamble should also remind readers of the risks the use of GenAI may bring, such as improperly crediting sources and spreading misinformation. Next, it is essential to define terms. What software tools fall under the umbrella term "Generative AI"? Scope and conditions can be noted, such as statements that using GenAI is acceptable with the instructor's permission.

While this paper focused on students' classroom use of GenAI, colleges and universities will deploy the tools elsewhere in operations. Risk Management Frameworks can provide insights into their use with prospective students, alumni, and faculty/staff. Ultimately, high-level administrators and Boards will have to make decisions about the policies that are adopted.

REFERENCES

American Association of Colleges of Nursing. (n.d.) *What is Competency-Based education? https://www.aacnnursing.org/essentials/tool-kit/competency-based-education*

Baker-Stein, M., Paradise, B., & Petersen, R. (2022, October 25). *Why employers should embrace competency-based learning in Cybersecurity*. National Institute of Standards and

Technology. https://www.nist.gov/blogs/cybersecurity-insights/why-employers-should-embrace-competency-based-learning-cybersecurity

Creswell, Creswell, J. W. and Creswell, J. D. (2022). *Research design: Qualitative, quantitative, and mixed methods approaches*. 6th ed. Thousand Oaks, CA: SAGE Publications.

Doolittle, P.E. and Camp, W.G., 1999. Constructivism: The career and technical education perspective. *Journal of vocational and technical education*, *16*(1), pp.23–46.

Fastré, G.M.J., Van der Klink, M.R. and Van Merriënboer, J.J., 2010. The effects of performance-based assessment criteria on student performance and self-assessment skills. *Advances in Health Sciences Education*, *15*, pp.517-532.

Frank, J.R., Snell, L.S., Cate, O.T., Holmboe, E.S., Carraccio, C., Swing, S.R., Harris, P., Glasgow, N.J., Campbell, C., Dath, D. and Harden, R.M., 2010. Competency-based medical education: theory to practice. *Medical teacher*, *32*(8), pp.638–645.

Ghosh, T. and Francia III, G., 2021. Assessing competencies using scenario-based learning in Cybersecurity. *Journal of Cybersecurity and Privacy*, *1*(4), pp.539–552.

Kallonas, C., Piki, A. and Stavrou, E., 2024, May. Empowering professionals: a generative AI approach to personalized cybersecurity learning. In *2024 IEEE Global Engineering Education Conference (EDUCON)* (pp. 1-10). IEEE.

Marquardson, J., 2024. Embracing Artificial Intelligence to Improve Self-Directed Learning: A Cybersecurity Classroom Study. *Information Systems Education Journal*, *22*(1), pp.4–13.

Mitra, R., Schwieger, D. and Roy, I., 2023. Educating the Next Generation of CSOs: An Exercise in Conversational Role Play with ChatGPT. In *Proceedings of the ISCAP Conference ISSN* (Vol. 2473, p. 4901).

Morcke, A.M., Dornan, T. and Eika, B., 2013. Outcome (competency) based education: an exploration of its origins, theoretical basis, and empirical evidence. *Advances in Health Sciences Education*, *18*, pp.851-863.

Polito, C. and Pupillo, L., 2024. Artificial Intelligence and Cybersecurity. *Intereconomics*, *59*(1), pp.10–13.

Santhi, T.M. and Srinivasan, K., 2024. Chat-GPT Based Learning Platform for Creation of Different Attack Model Signatures and Development of Defense Algorithm for Cyberattack Detection. *IEEE Transactions on Learning Technologies*.

Sarma, M., Matheus, T. and Senaratne, C., 2021. Artificial intelligence and cyber security: a new pathway for growth in emerging economies via the knowledge economy? In *Business Practices, Growth and Economic Policy in Emerging Markets* (pp. 51-67).

PANEL DISCUSSION

THE CURRENT STATE OF ARTIFICIAL INTELLIGENCE (AI) IN HIGHER EDUCATION

Alex Koohang, *Middle Georgia State University*, *USA*, *alex.koohang@mga.edu*
Rod McRae, *Middle Georgia State University*, *USA*, *rod.mcrae@mga.edu*
Carol Springer Sargent, *Mercer University*, *USA*, *sargent_cs@mercer.edu*
Allen Truell, *Ball State University*, *USA*, *atruell@bsu.edu*
Patrick Harris, University System of Georgia, USA, *patrick.harris@usg.edu*
Joanna Paliszkiewicz, *SGGW University*, *Poland*, *joanna_paliszkiewicz@sggw.edu.pl*

ABSTRACT

Higher education is on the cusp of a significant transformation driven by artificial intelligence. This panel discussion will explore how AI can personalize the learning experience, improve student support, and streamline administrative tasks, making education more efficient and accessible for all. We'll explore the exciting possibilities of AI-powered tutoring, enhanced learning materials, and automated administrative processes. The panel will also address ethical considerations surrounding AI use, the need for faculty training, and the importance of safeguarding student data privacy.

Keywords: AI, higher education, AI opportunities, AI challenges

THE CYBERSECURITY JOB MARKET AND ARTIFICIAL INTELLIGENCE: AN ANALYSIS OF SKILL LISTINGS IN CYBERSECURITY JOB ADVERTISEMENTS

Timothy Greer, Middle Tennessee State University, tim.greer@mtsu.edu
Nita Brooks, Middle Tennessee State University, nita.brooks@mtsu.edu

ABSTRACT

The importance of a robust cybersecurity workforce cannot be overstated. Technology continues to permeate every facet of life, from personal banking to national security, the need for skilled professionals who can protect, and secure sensitive information has become critical. The demand for cybersecurity experts is driven by an ever-evolving threat landscape where cyber threats become more sophisticated and pervasive. As a result, the skills required for careers in cybersecurity are diverse and complex, encompassing both technical and non-technical areas.

Artificial Intelligence (AI) is having a significant impact in the workplace. Bhaskar and Peng (2023) found that AI is reshaping the skill requirements in the modern workplace, shifting from routine, manual tasks to more complex, cognitive responsibilities. AI presents revolutionary potentials, it requires careful implementation and management to truly enhance organizational knowledge management effectively. Alavi, Leidner, & Mousavi (2024) noted that AI presents revolutionary potentials, it requires careful implementation and management to truly enhance organizational knowledge management effectively. AI offers remarkable opportunities for enhancing knowledge work and creativity, it also necessitates careful management to mitigate potential risks and ensure it complements human skills effectively Benbya, H., Strich, F., & Tamm, T. (2024).

This study looks at 500 cybersecurity job ads to determine the potential impact of artificial intelligence on the expectations of the cybersecurity workforce. One observation that stands out is simply the average number of skills associated with cybersecurity job ad, 29.65 skills listed. Forty two of those 500 cybersecurity jobs ads list “artificial intelligence” as a desired skill in a candidate. This study will also look at those skills associated with artificial intelligence in each of those job listings. This results of this study would benefit students, faculty, and university as it would help them identify trends and expectations in the cybersecurity workforce.

REFERENCES

Alavi, M., Leidner, D. E., & Mousavi, R. (2024/01//). Knowledge management perspective of generative artificial intelligence. *Journal of the Association for Information Systems, 25*(1), 1-12. doi:https://doi.org/10.17705/1jais.00859

Benbya, H., Strich, F., & Tamm, T. (2024/01//). Navigating generative artificial intelligence promises and perils for knowledge and creative work. *Journal of the Association for Information Systems*, *25*(1), 23-36. doi:https://doi.org/10.17705/1jais.00861

Bhaskar, R., & Peng, G. (2023). Artificial intelligence and machine learning for job automation: A review and integration. *Journal of Database Management*, *34*(1), 1-12. doi:https://doi.org/10.4018/JDM.318455

LEARNING DATABASE WHILE HAVING FUN: STUDYING THE EFFECT OF INTRINSIC MOTIVATION ON TEACHING EFFECTIVENESS

Wei Sha, Pittsburg State University, wsha@pittstate.edu
Jack Qu, Pittsburg State University, xqu@gus.pittstate.edu

EXTENDED ABSTRACT

INTRODUCTION

Learning database concepts such entity relationship diagrams, subtypes, normalization and SQL etc. can be challenging for students. Even students with majors in computer information systems or computer science could struggle in grasping the concepts and applying the analysis skills. Therefore, improving teaching effectiveness becomes imperative to database instructors. This research proposes that boosting a student's intrinsic motivation toward learning through incorporating fun elements in the curriculum can be an effective way in improving student learning database concepts and skills.

THE STUDY

Intrinsic motivation (IM) has a long history in the information system research literature. This construct is usually defined as someone willing to perform a task for its own sake for satisfactions and pleasures inherent in the task performing process (Wu and Lu, 2013). IM is mainly studied as computer enjoyment in Information Systems research literature. Computer enjoyment is about the degree to which a person experiences positive emotions while this person interacts with a computing environment. It is an emotional state that "using a specific is perceived to be enjoyable in its own right, aside from any performance consequences resulting from system use" (Venkatesh, 2000).

Research has shown that people can be more engaged while they are having fun. Venkatesh (1999) argued that through framing, training can be disguised as game-based training, it is possible "not only to create a positive impact on perceived ease of use but also to have a strong impact on the effect of perceived ease of use on behavioral intention". Ways of learning database concepts can be conducted through fun and engaging exercises. For example, learning database concepts can be conducted by playing a jeopardy game. Students can also use their SQL skills to rescue people from an island. We believe these kinds of activities would significantly increase a student's enjoyment which would in turn increase their perceived effectiveness of their learning experience.

Data would be collected through an experiment and surveys. Quantitative data will be summarized and analyzed through structural equation modeling techniques. The instruments for designated constructs will be validated through a nomological network approach. Student traits such as playfulness will be evaluated before and after the experiment. Computer enjoyment will be measured during the experiment and students' attitude and intentions toward learning will be assessed as measures for teaching effectiveness. Contributions and limitations of the research will also be presented.

IMPLICATIONS

This study intends to introduce fun into the database curriculum by means of games and intriguing exercises to boost students' willingness to have better understanding of various database concepts. This study would provide an opportunity to examine the effect of intrinsic motivation on intentions in a higher education learning environment. The results would be beneficial to improve database curriculum design and teaching effectiveness.

REFERENCES

Venkatesh, V. (1999). Creating Favorable User Perceptions: Exploring the Role of Intrinsic Motivation. MIS Quarterly, 23:2, 239-260.

Venkatesh, V. (2000). Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation and Emotion into the Technology Acceptance Model. Information Systems Research, 11:4, pp. 342 – 365.

Wu, J & Lu, X (2013). Effects of Extrinsic and Intrinsic Motivators on Using Utilitarian, Hedonic and Dual-Purposed Information Systems: A Meta-Analysis. Journal of the Association for Information Systems, 14:3, pp. 153-191.

STATE-OF-THE-ART MACHINE LEARNING APPROACHES FOR CANCER PREDICTION

Shilpa Balan, California State University, Los Angeles, sbalan@calstatela.edu
Sumali Conlon, University of Mississippi, sconlon@bus.olemiss.edu

EXTENDED ABSTRACT

PURPOSE OF THE STUDY

Cancer is one of the deadliest diseases in the world and is responsible for numerous deaths worldwide (Win et al., 2014). Even though cancer is preventable in the early stages, many patients are diagnosed with cancer much later. Therefore, it is of prime importance to predict cancer recurrence so that specific treatments can be sought. Predicting cancer disease is an important task in the cancer discovery process. For example, distinguishing between benign and malignant tumors helps to advance the medical diagnosis of cancer (Turki, 2018). In this work, a review of machine learning approaches applied in the prediction of cancer is presented with the aim to improve cancer patient outcomes.

BASIS OF THE STUDY

The early diagnosis of the cancer type and stage has become an important need in cancer research. We conducted a comprehensive literature review on machine learning technologies in cancer. We considered a set of relevant keywords to collect information on progress in cancer from healthcare journals and articles from 2000 to 2022. Sources of data collection include Cancer Informatics, BMC Bioinformatics, Frontiers, International Journal of Oncology, Computational and Structural Biotechnology, Artificial Intelligence in Medicine, International Journal of Artificial Intelligence and Applications, Decision Support Systems, Journal of Medical Systems. News articles originated from sources such as Nature, MIT News, Medium and the Guardian.

IMPLICATIONS

Advances in digital medicine have shifted the landscape for cancer risk prediction models (Alfayez et al., 2021). The past decade has witnessed a continuous development of cancer related research (Hanahan and Weinberg, 2011). Scientists have applied different machine learning (ML) methods for the early prediction of cancer treatment outcome. From previous studies, it is seen that machine learning methods can be used to improve the accuracy of predicting cancer susceptibility. Essentially, machine learning helps to model the progression and treatment of cancer. These techniques can identify patterns and relationships between them, from complex datasets, while they are able to effectively predict future outcomes of a cancer type. Artificial Neural Networks (ANN), Decision Tree, Support Vector Machines (SVM), and Naïve Bayes techniques are mostly used to determine recurrence. Clustering techniques are used to determine survivability. ANN's are popularly used to detect breast cancer survivability. This study contributes to cancer prediction by presenting a summary of the popular ML techniques highlighted in the literature.

CONCLUSION

The role of artificial intelligence and machine learning in cancer research offers several advantages primarily assisting with clinical decision-making. A variety of machine learning techniques such as Artificial Neural Networks, Bayesian Networks, Support Vector Machines and Decision

Trees have been broadly applied in predictive models for cancer research. A number of trends are identified with respect to the types of machine learning methods being used and the overall performance of these methods in predicting cancer susceptibility or outcomes. While ANNs still predominate it is evident that a growing variety of alternate machine learning strategies are being used and that they are being applied to many types of cancers to predict outcomes. Machine learning methods are helping to improve the performance of most diagnoses.

REFERENCES

Alfayez, A., Kunz, H., Lai, A. (2021). Predicting the risk of cancer in adults using supervised machine learning: a scoping review. BMJ. pp.1-11

Hanahan, D., Weinberg, RA. (2011). Hallmarks of cancer: the next generation. *Cell*;144(5):646-74.

Turki, T. (2018). An empirical study of machine learning algorithms for cancer identification. IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), Zhuhai, China, pp. 1-5.

Win. S., Htike, Z., Yusof, F., Noorbatcha, I. (2014). Cancer Recurrence Prediction Using Machine Learning. International Journal of Computational Science and Information Technology (IJCSITY), Vol.2, No.2

DATA CLASSIFICATION FOR AI MODELING

Elena Alikhachkina, TE Connectivity, elena.alikhachkina@te.com
Pankaj Nagpal, Arkansas State University, pnagpal@astate.edu

SUMMARY

As Artificial Intelligence (AI), specifically Generative Artificial Intelligence (Gen AI) and Large Language Model (LLM) adoption accelerates in enterprises, data classification is important for AI and ML model quality. The proposed study endeavors to study how data classification impacts AI and ML model performance. The study will cover challenges in data classification for AI, based on the authors' experience in addressing the complexities of large and diverse datasets for Fortune 500 companies. This includes managing data sensitivity and privacy concerns. We will discuss techniques for categorizing data based on sensitivity, usage, and relevance. Other possible relevant topics include the utilization of automated tools and algorithms for data classification. Examples of data classification implementations at Fortune 500 companies will be referenced to utilize the case study method.

PROPOSED STUDY AND MOTIVATION

This topic is highly relevant for IACIS conference participants as it tackles one of the fundamental aspects of AI and ML implementation: data quality. Understanding how to classify data effectively can lead to better model outcomes, more robust data governance, and enhanced compliance with privacy regulations. As organizations increasingly rely on AI and ML for decision-making, the insights from this paper will be invaluable for both academic researchers and industry practitioners seeking to optimize their AI strategies.

BASIS OF THE STUDY

This study will be grounded in both empirical experience and theoretical frameworks. Data for the study will be drawn from case studies and examples of data classification implementations in Fortune 500 companies. The paper will examine the methods that these companies use to handle data sensitivity, usage, and relevance in their AI models. Additionally, literature on data classification techniques and tools, particularly in the context of AI and ML, could provide a foundational understanding of current best practices and emerging trends.

IMPLICATIONS AND CONCLUSION

The findings of this study will have significant implications for the implementation of AI and ML in enterprises. Effective data classification can lead to more accurate and reliable AI models, improved data governance, and enhanced compliance with privacy regulations. Organizations can leverage these insights to refine their data strategies, ensuring that their AI initiatives are both effective and responsible.

In conclusion, data classification is a vital component of AI and ML model quality. This paper highlights the challenges and best practices associated with data classification, offering valuable insights for enterprises seeking to optimize their AI strategies. By addressing data sensitivity and privacy concerns through effective classification, organizations can achieve better model performance and compliance. This research contributes to the broader understanding of data management in AI, and provides a foundation for future studies and practical applications.

DUAL DIGITAL TWINS FOR ENHANCED CYBERSECURITY POSTURE

Chase Peterson, MBA, CISSP, Metropolitan State University, chase.peterson@metrostate.edu

INTRODUCTION

The threat of a costly cyberattack prompts companies to ask how they can predict future attacks and minimize their impact. Unfortunately, according to ChatGPT, we are at least a few decades and a number of computational and quantum miracles from a crystal ball that can accurately predict the future. A more feasible answer may lie in a set of Digital Twins emulating the constant attack and defense of the company.

BACKGROUND

The exponential growth of the internet has seen the growth of vulnerabilities and attack surfaces (CSIS, 2024). The world economic forum estimated the cost of cybercrime in 2023 as 11.5 trillion USD and forecast it to grow to 23.82 trillion by 2027 (Charlton, 2024). This poses a significant problem for organizations around the world; In a recent survey conducted by Cisco (2024) about 54% of companies reported being the target of a successful attack, a little more than half (52%) of the compromised companies reported that the incident cost the company at least $300,000 USD, with 12% saying that their impact was over a million USD. 73% of companies believe that within the next 24 months they will suffer a significant disruption due to a cyberattack (Cisco, 2024). Current techniques for forecasting cyber defense are more reactive than proactive, and research into using Machine Learning has demonstrated that it is able to forecast with roughly 70% accuracy at best.

LITERATURE

In 2003, Grieves learned about Digital Twins (DT) from NASA's John Vickers and later used it in his University of Michigan Executive Course on Product Lifecycle Management. In it he defined the potential to simulate the manufacturing process and optimize the product lifecycle (Grieves, 2014). He discussed that a DT is composed of three key parts; physical products in physical space, virtual products in virtual space, and a data link between the two. Building on that work and expanding the concept of a DT into a cyber focused equivalent, Luzzi et al (2024) conducted a systematic literature review that identifies the majority of existing literature focused on a Cyber-Cyber System(CCS), as opposed to a Cyber-Physical System(CPS). They also discuss the current prevailing strategies for predicting cyberattacks; what the current uses of DTs in the field of cybersecurity are; and what role DTs can play in enhancing the prediction of an attack. Additionally they highlight three advantages of the CCS over a CPS; complete malleability meaning that any changes made to the DT can be implemented, true-twins showcase the blending and seamless transition between real and simulated and a simulation hierarchy meaning that a DT can replicate itself for further testing and investigation. The use of machine learning for a proactive approach to forecasting cyber threats has been explored by Almahmoud et al. and discuss the benefits of a forward thinking approach as opposed to a traditional reactive approach (2023). They offer both a novel dataset constructed of big unstructured data and outline how their approach can predict threat trends up to three years in advance with up to 70% accuracy across a wide range of attacks including univariate and multivariate analysis for 42 different cyber attacks. This offers an attractive benchmark that can be used to validate future DT testing and applications.

DISCUSSION

The research regarding DTs and their application in a CCS is sparse compared to research with a more AI and ML centric view, however Dietz et al.(2022) demonstrate the ability of DT to engage in security by design system testing and show how DTs can be used in an industrial control system to prevent a pressure tank from exploding. Somma et al. (2020) introduce a potential framework for their DT implementation in cybersecurity utilizing five layers consisting of the Physical Twin(PT) layer representing the CPS, the PT-DT layer manages the data generated from the PT, the DT layer that replicates the network using Mininet, specifically MiniCPS(Antonioli and Tippenhauer, 2017), the DT-Serv layer which manages the data generated by the DT and last the Service layer where different security services are hosted. Suhail et al. (2023) highlight the potential threats that a DT may pose due to their interconnected nature with the CPS and propose a method of gamification that aims to secure the CPS through the use of AI/ML adversarial testing showing how their framework can be utilized to strengthen and introduce an explainable element for validation and verification. Hadar et al. (2020) show that DTs can be used to analyze and gather requirements for necessary security controls as well as to optimize and identify current or missing controls, outlining how DTs can be utilized within the design process to identify and rectify missing security controls. Current literature identifies the threat actor and defensive component of a given CCS DT as being one system and interacting as one system (Hader et al, 2020; Somma et al, 2020; Suhail et al, 2023, Luzzi et al, 2024). Somma et al, (2020) outline their five layers to implementing a proof of concept DT in a simulated network, representing the different devices in the network. and by utilizing the forecasting benchmark and dataset outlined by Almahmoud et al, (2023) we can establish a baseline for future twin sets to be measured against for efficacy.

Additionally, to enhance the fidelity and accuracy of our digital twin (DT) simulation, we also aim to incorporate a comprehensive analysis of email as a significant vector for cybersecurity threats. This integration seeks to replicate human behavior in response to email-based attacks, reflecting the complexity of user interactions and decision-making processes. Our approach underlines the critical need to model and understand the nuances of human factors in cybersecurity, enabling the development of more effective, behaviorally-informed defense mechanisms within the DT framework.

Based on the prior research, DT could potentially serve as a method/tool for predicting cyberattacks enabled through a number of attack vectors such as phishing campaigns, improperly secured hardware or software accounts, and weak policies. We propose that separating the modeling of offensive and defensive aspects will allow for a greater degree of fidelity in highlighting weak points within a company that are the most likely to be exploited by threat actors. The separation would allow for a higher degree of control of the data incorporated into each twin. To simulate the implementation a laboratory experiment designed to emulate a business including key components to accurately replicate the network, hardware, environment and communication methods.

CONCLUSION

This research aims to underscore the potential of digital twins as predictive tools in cybersecurity, particularly against common vectors. By integrating detailed simulations of both technological and human elements, our digital twin framework hopes to enhance organizational resilience against cyber threats through improved forecasting and prediction capabilities allowing for greater clarity when making strategic decisions.

REFERENCES

Almahmoud, Zaid, et al. "A Holistic and Proactive Approach to Forecasting Cyber Threats." *A Holistic and Proactive Approach to Forecasting Cyber Threats*, vol. 13, no. 1, May 2023, https://doi.org/10.1038/s41598-023-35198-1. Accessed 29 May 2024.

Alshammari, Kaznah, et al. "Cybersecurity for Digital Twins in the Built Environment: Current Research and Future Directions." *Journal of Information Technology in Construction*, vol. 26, Apr. 2021, pp. 159–73, https://doi.org/10.36680/j.itcon.2021.010. Accessed 20 May 2024.

Antonioli, Daniele, and Nils Tippenhauer. *MiniCPS: A Toolkit for Security Research on CPS Networks*. 17 July 2015, arxiv.org/pdf/1507.04860. Accessed 1 June 2024.

Baiardi, Fabrizio, and Federico Tonelli. "Twin Based Continuous Patching to Minimize Cyber Risk." *European Journal for Security Research*, vol. 6, no. 2, Dec. 2021, pp. 211–27, https://doi.org/10.1007/s41125-022-00079-7. Accessed 26 May 2024.

Charlton, Emma. "2023 Was a Big Year for Cybercrime – Here's How We Can Make Our Systems Safer." *World Economic Forum*, 10 Jan. 2024, www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/. Accessed 28 May 2024.

Cisco. *Underprepared and Overconfident Companies Tackle an Evolving Landscape 2024 Cisco Cybersecurity Readiness Index*. 2024, newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf. Accessed 20 May 2024.

CSIS. "Significant Cyber Incidents | Center for Strategic and International Studies." *Www.csis.org*, Apr. 2024, www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Accessed 31 May 2024.

Dietz, Marietheres, et al. "Employing Digital Twins for Security-By-Design System Testing." *Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*, Apr. 2022, https://doi.org/10.1145/3510547.3517929.

Eckhart, Matthias, et al. "Enhancing Cyber Situational Awareness for Cyber-Physical Systems through Digital Twins." *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Sept. 2019, https://doi.org/10.1109/etfa.2019.8869197. Accessed 17 May 2024.

---. "Security-Enhancing Digital Twins: Characteristics, Indicators, and Future Perspectives." *IEEE Security & Privacy*, vol. 21, no. 6, Institute of Electrical and Electronics Engineers, Nov. 2023, pp. 64–75, https://doi.org/10.1109/msec.2023.3271225. Accessed 18 May 2024.

Faleiro, Rajiv, et al. "Digital Twin for Cybersecurity: Towards Enhancing Cyber Resilience." *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, 2022, pp. 57–76, https://doi.org/10.1007/978-3-030-93479-8_4. Accessed 29 May 2024.

Grieves, Michael. *Digital Twin: Manufacturing Excellence through Virtual Factory Replication*. 2014, www.3ds.com/fileadmin/PRODUCTS-

SERVICES/DELMIA/PDF/Whitepaper/DELMIA-APRISO-Digital-Twin-Whitepaper.pdf. Accessed 24 May 2024.

Hadar, Ethan, et al. "Cyber Digital Twin Simulator for Automatic Gathering and Prioritization of Security Controls' Requirements." *2020 IEEE 28th International Requirements Engineering Conference (RE)*, Aug. 2020, https://doi.org/10.1109/re48521.2020.00035. Accessed 21 May 2024.

Hearn, Mark, and Simon Rix. *Cybersecurity Considerations for Digital Twin Implementations*. Nov. 2019, www.iiconsortium.org/news-pdf/joi-articles/2019-November-JoI-Cybersecurity-Considerations-for-Digital-Twin-Implementations.pdf.

Homaei, Mohammadhossein, et al. *A Review of Digital Twins and Their Application in Cybersecurity Based on Artificial Intelligence*. 2023, arxiv.org/pdf/2311.01154. Accessed 25 May 2024.

Jiang, Yuning, et al. "Leveraging Digital Twin Technology for Enhanced Cybersecurity in Cyber–Physical Production Systems." *Future Internet*, vol. 16, no. 4, Multidisciplinary Digital Publishing Institute, Apr. 2024, pp. 134–34, https://doi.org/10.3390/fi16040134. Accessed 23 May 2024.

Jones, David, et al. "Characterising the Digital Twin: A Systematic Literature Review." *CIRP Journal of Manufacturing Science and Technology*, vol. 29, no. 1755-5817, May 2020, pp. 36–52, https://doi.org/10.1016/j.cirpj.2020.02.002. Accessed 21 May 2024.

Luzzi, Juan, et al. "SoK: A Holistic View of Cyberattacks Prediction with Digital Twins." *2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE)*, Feb. 2024, https://doi.org/10.1109/ic-etite58242.2024.10493514. Accessed 23 May 2024.

Malhotra, Parushi, et al. "Internet of Things: Evolution, Concerns and Security Challenges." *Sensors*, vol. 21, no. 5, Mar. 2021, p. 1809, https://doi.org/10.3390/s21051809. Accessed 29 May 2024.

Pokhrel, Abhishek, et al. "Digital Twin for Cybersecurity Incident Prediction." *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*, June 2020, https://doi.org/10.1145/3387940.3392199.

Schiffer, Alex. "How a Fish Tank Helped Hack a Casino." *Washington Post*, 21 July 2017, www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/. Accessed 25 May 2024.

Somma, Alessandra, et al. *A Cyber Digital Twin Framework to Support Cyber-Physical Systems Security*. 2023, www.mallouli.com/recherche/publications/dt2023.pdf. Accessed 18 May 2024.

Suhail, Sabah, et al. "Security Attacks and Solutions for Digital Twins." *Computers in Industry*, vol. 151, Oct. 2023, p. 103961, https://doi.org/10.1016/j.compind.2023.103961. Accessed 20 May 2024.

Wang, Yue, et al. "TWIN-GPT: Digital Twins for Clinical Trials via Large Language Model." *ArXiv (Cornell University)*, Cornell University, Apr. 2024, https://doi.org/10.48550/arxiv.2404.01273. Accessed 21 May 2024.

EXPLORING FACULTY ADOPTION OF AI IN EDUCATION: AN EXPERIMENTAL STUDY USING THE UNIFIED THEORY OF ACCEPTANCE AND USE OF TECHNOLOGY (UTAUT): A PILOT STUDY

Aurelia Nicholas-Donald, Virginia State University, adonald@vsu.edu

ABSTRACT

This experimental study investigates faculty adoption of Artificial Intelligence (AI) in educational contexts using the Unified Theory of Acceptance and Use of Technology (UTAUT) framework. As AI technologies offer promising opportunities to enhance teaching and learning practices, understanding factors influencing faculty acceptance and use of AI is crucial for successful implementation.

BUILDING BRIDGES: THE INAUGURAL INTER-UNIVERSITY VIRTUAL SQL SUMMIT

Robert J. Mills, Utah State University, bob.mills@usu.edu
Bryan Marshall, Georgia College & State University, bryan.marshall@gcsu.edu
Peter Cardon, University of Southern California, cardon@marshall.usc.edu
Tanya Beaulieu, University of Maine, tanya.beaulieu@maine.edu
Carl M. Rebman Jr., University of San Diego, carlr@sandiego.edu
Ari Schurig, Utah State University, ari.schurig@usu.edu

EXTENDED ABSTRACT

In a concerted effort to enhance collaboration among students and faculty from universities nationwide, we orchestrated the First Semi-annual Virtual Inter-University SQL Summit. This event, featuring three IACIS participating professors from Utah State University, Georgia College & State University, and the University of Southern California, successfully involved 80 students. The purpose of this presentation is to provide a comprehensive overview of the processes and procedures that facilitated this significant student participation in a virtual IACIS-like conference.

The initial SQL Summit was organized during the Spring semester of 2024 as an academic conference focused on SQL-related topics. Over 80 students submitted video presentations to one of two major conference tracks: “Closing the Loop” and “Expanding the Loop.” The “Closing the Loop” track concentrated on concepts and ideas that students have encountered in their textbooks, reinforcing foundational knowledge. Conversely, the “Expanding the Loop” track offered a platform for exploring innovative ideas and topics not thoroughly covered in class, encouraging further exploration and discovery. Appendix A describes the tracks in more detail.

Given the number of submissions, winnowing conference video submissions was a challenging process. Initially, each participating school was responsible for identifying the top five submissions based on an evaluation rubric. This process included both faculty and student representatives serving as reviewers. The top five submissions between the two schools represented the final conference presenters to be viewed by both institutions. The ten conference session videos were also sent to a professor at the University of Southern California to rank the conference videos to determine the 2024 Summit award recipients.

The top conference session was submitted by a student from Utah State University. The student’s presentation focused on offset window functions. The video presentation illustrated how to implement the four offset window functions. The demonstration showcased how window functions serve as a powerful tool for analyzing and summarizing data and are useful for analyzing and comparing sequential data in an output with the current row.

To introduce a new generation of professionals to IACIS, we plan to have top award recipients showcase excerpts from their video sessions at the annual IACIS conference. We also hope to discuss the following with IACIS members who attend the conference session:

1. In addition to the initial three participating faculty members, two additional faculty members from the University of Maine and the University of San Diego have joined the team. We are interested in knowing if other IACIS faculty members who teach SQL/database management are interested in joining. Would new members participate each semester or once a year? How would we efficiently scale the event?

2. We are interested in discussing the possibility of more formally integrating the Summit with IACIS, with the goal of increasing the number of students and faculty attending the conference.

3. The first SQL Summit involved video presentations to mimic a virtual academic conference focused on SQL-related topics. While effective, what other SQL collaboration opportunities are worth considering? While the student video presentations worked well, should the Summit activity vary based on a rotating conference chair, such as a data-wrangling competition?

WELCOME TO THE
INTER-UNIVERSITY SQL SUMMIT
GEORGIA COLLEGE & STATE UNIVERSITY
1865 THE UNIVERSITY OF MAINE
USC University of Southern California
University of San Diego
STATE U
UtahState University

NAVIGATING THE DIGITAL FRONTIER: GEN Z'S CHARACTERISTICS AND THE EMERGING THREATS TO EDUCATIONAL INSTITUTION TECHNOLOGY INFRASTRUCTURE

Olumide Malomo, Virginia State University, omalomo@vsu.edu
Ayse N. Balas, Virginia State University, abalas@vsu.edu
Adeyemi A. Adekoya, Virginia State University, aadekoya@vsu.edu
Ephrem Eyob, Virginia State University, eeyob@vsu.edu
Shanzhen Gao, Virginia State University, sgao@vsu.edu
Aurelia M. Donald, Virginia State University
Chandrasheker Challa Virginia State University
Christine Shikutwa, University Collegeville, cshikutwa001@csbsju.edu

ABSTRACT

Generation Z, often called Gen Z, is the first generation to grow up with the Internet and digital technology from a young age. They are proficient with various computing devices like smartphones and comfortable using social media platforms and other digital tools. The Internet and the evolution of cloud computing and web application technologies are the infrastructural building blocks and backbones of all Internet-based communications. They have immensely contributed to the increasing growth of emerging technologies and business innovations, driving the productivity for businesses to flourish and promoting products and services that benefit society at large. These technologies catalyze companies to innovate, leading to advancements in user interface design, mobile applications, and digital marketing strategies that enable Gen Z to be more ethnically and culturally diverse than previous generations. Gen Z’s comfort with technology is a characteristic and a driving force behind digital products and service innovations. Educational institutions use Gen Z's extensive online presence and familiarity with technology by creating online degree courses and integrating digital tools, expanding access to online resources, and improving communication and collaboration among students and faculty. Unfortunately, Gen Z's approach to cybersecurity is shaped by their perspectives on security and privacy. They have a high level of trust in technology companies and security tools to protect their data. Their familiarity and confidence in digital communications can sometimes lead to overconfidence in their ability to spot scams, making them less likely to scrutinize emails that appear legitimate or click on a phishing link. Consequently, cyber-attackers have found ways to exploit their trust in digital communications and social media platforms, as well as their digital habits and vulnerabilities on the internet, and by using cyber Tactics, Techniques, and Procedures (TTP) such as advanced phishing and social engineering to launch successful cyberattacks. Hence, their characteristics pose significant risks related to cybersecurity, not only to themselves but also to their surrounding environment, be it an organization or academic institution. The paper aims to explore Gen Z's digital characteristics and their potential threat to educational institution technology infrastructure. Highlighting the risks and our proposed framework for mitigation strategies, which is a crucial step in addressing the identified issues. We aim to create awareness for academic institutions and security professionals to focus on understanding and addressing the risks associated with Gen Z and using their tech-savvy nature to make them humans as firewalls, the last line of defense against cyber threats when IT security infrastructure fails for example to block sophisticated malicious emails.

Keywords: Generation Z, Cloud Computing, Web Technologies, Web Applications Cybersecurity, Humans as Firewalls, Information Technology, Zero Trust Architecture, Social Media Platform, Phishing, Social Engineering, Risk Management

ROLES OF UNCERTAINTY AVOIDANCE AND LONG-VERSUS SHORT-TERM ORIENTATION ON DECISION-MAKING STYLES: A SAMPLE FROM GERMANY

Fatih Çetin, Baskent University, Turkey, fcetin@baskent.edu.tr
Markus Launer, Ostfalia University of Applied Sciences, Germany, m-a.launer@ostfalia.de
H. Nejat Basım, Baskent University, Turkey, nbasim@baskent.edu.tr

ABSTRACT

This study explores the influence of cultural dimensions, specifically uncertainty avoidance and long- versus short-term orientation, on intuitive decision-making styles within a German sample. By integrating theories from cross-cultural psychology and decision-making research, we investigate how these cultural values impact rational, holistic, inferential, and emotional decision-making styles. Data were collected from 491 German participants through a comprehensive survey assessing their cultural values and decision-making preferences. Our findings indicate that high uncertainty avoidance negatively influences the preference for holistic and emotional decision-making. Additionally, long-term orientation is positively related to analytic decision-making, whereas short-term orientation is associated with emotional and inferential decision-making. These results underscore the importance of cultural context in shaping decision-making styles and offer insights for enhancing decision-making efficacy in multicultural environments. Implications for organizational practices and future research directions are discussed.

Keywords: Uncertainty avoidance, Long-term orientation, Short-term orientation, Decision-making styles, Germany

A PANEL REPORT ON AI IN HIGHER EDUCATION FROM THE PERSPECTIVE OF CIOS

Steven A. Schilhabel, Assistant Professor, University of Wisconsin Oshkosh, College of Business

Abstract

The panel's report examines how artificial intelligence (AI), especially generative AI, affects higher education. It is predicated on Midwest College Chief Information Officers (CIOs) observations. The panel report investigates how colleges may match their objectives and aims with the strategic integration of artificial intelligence. It demonstrates how artificial intelligence (AI) may improve teaching methods, boost student engagement, and promote administrative and academic efficiency. The panel report highlights the significance of strategic planning policy creation and addressing ethical standards and data security concerns, and it demonstrates that colleges have differing degrees of preparedness for implementing AI. The report recognizes artificial intelligence's (AI) promise to revolutionize education and the associated obstacles.

Keywords: Generative AI, Education, Higher Education Transformation, Academic Impact, AI Integration Strategies, University CIOs, panel report

Introduction

Rapid technology breakthroughs are transforming the higher education scene, and artificial intelligence (AI), especially generative AI, is at the vanguard of this change. The results of Ellucian (Beltran, 2023) highlight this evolution, showing that administrators are becoming increasingly optimistic about AI's potential contribution to institutional operation despite the technology's still emerging and isolated use. The potential of generative AI to revolutionize the higher education sector is becoming increasingly evident as it showcases its ability to generate novel content and extract valuable insights from vast datasets (Michel-Villarreal et al., 2023).

The rise of artificial intelligence (AI) as a major force behind innovation and technological advancement transforms how higher education is taught. To future-proof their academic and administrative operations, universities are proactively adjusting to these developments, demonstrating their dedication to innovation and strategic planning. According to Tyton Partners' adoption trends (NeJame et al., 2023), integrating advanced analytics, natural language processing, and machine learning is expected to improve educational delivery and operations. This movement reflects a desire to stay ahead of the curve in the quickly changing educational landscape.

To fully realize AI's transformational potential, it is increasingly essential to strategically integrate AI into university systems in line with academic missions and aims. Recent studies highlight that these initiatives aim to promote inclusive and dynamic learning settings, increase research capabilities, and improve academic quality. They also acknowledge the importance of ethical AI implementation and strong data governance (Beltran, 2023).

AI impacts every stage of the student life cycle, not just the curriculum, by providing individualized learning and career guidance, personalized learning, and admissions. The objective is to create an integrated AI ecosystem that greatly increases student pleasure and achievement, taking into account the disparities in university readiness for AI adoption as well as issues like data privacy and the digital divide (AlDhaen, 2022; Aldosari, 2020; Harry, 2023).

The panel on AI in higher education, which met to debate the changing role of AI in academic settings, provided the basis for this panel report. Chief Information Officers (CIOs) from various universities came together for the panel, and each one brought special views and experiences to the table. These executives in digital strategy and information technology talked about the state of artificial intelligence (AI) in higher education and its possible obstacles and opportunities.

This report's format is intended to coherently provide the panelists' conclusions and debates. After the introduction, Section 2 explores the rationale for this panel's formation and the importance of AI in the contemporary educational landscape. The distinguished panelists are introduced in Section 3 (Panelists), providing an overview of their backgrounds and positions within their respective organizations. Section 4 (Panel Discussion) presents the report's core, which summarizes the panelists' insightful observations, major topics, and lively exchanges. The viewpoints on incorporating AI into academic environments are abundantly available in this section. Section 5 (Conclusion), which concludes the research, summarizes these observations into important conclusions and offers a forecast for the development of AI in higher education. Additionally, acknowledgments and references for sources used to enrich this report are included in Section 6 (Acknowledgements).

Motivation

To learn more about the expanding importance of artificial intelligence (AI) in higher education, I, Steve Schilhabel, collaborated with a panel of university CIOs to organize this panel interview. Collecting and evaluating the perspectives of important figures spearheading these technological techniques in higher education has become crucial as technology, especially artificial intelligence, continues to transform educational systems.

The panel was thoughtfully assembled to tackle crucial inquiries about incorporating artificial intelligence in higher education. These crucial inquiries for our conversation sought to ascertain:

- **AI Integration and Strategic Vision: Our** goal was to ascertain how higher education institutions integrate AI in line with their strategic goals and ambitions. The emphasis was on evaluating AI's role in improving administrative and academic productivity, shifting the technology from an operational tool to a strategic educational asset.
- **AI's Place in the Revolution of Education:** This round of the discussion aimed to assess how AI is changing the dynamics of education. Our goal was to investigate how AI may improve

student services, enhance educational opportunities, and increase overall success while adhering to data security and ethical guidelines.
- **Emerging AI Trends in Higher Education:** Considering the rapid pace at which AI technologies are advancing, we were motivated to catalog and analyze the most pertinent and forthcoming AI trends. The goal of this discussion was to learn how universities are preparing to use these advances in AI, with an emphasis on information security and digital literacy.

University Readiness for AI Adoption: Determining the institutions' level of preparedness for implementing AI was a crucial component of our discussion. Our goal was to pinpoint the elements that encourage hope for AI in higher education while also comprehending the worries, especially those about ethical dilemmas and IT security.

Panelists

Three of the University of Wisconsin system's most eminent IT leaders, all committed to promoting AI in higher education, were brought together by the esteemed panel. Their combined knowledge offers a road map for deeply incorporating AI to improve the ecosystem for education. The panelists shed light on the important role that AI has had in the advancement of administrative, instructional, and learning processes. The UW system is in a position to create a standard for AI integration in academia under their direction, emphasizing the value of innovation while guaranteeing the moral use of AI in education. Below is a brief bio of each panelist.

- **Mark Clements:** At UW Oshkosh, Assistant Vice Chancellor of Information Technology, Mark Clements is leading the charge to integrate AI into the institution's curricula. His knowledge guarantees that the use of AI is strategically in line with the academic objectives of the university, improving both the educational experience and the institution's standing in the eyes of the public while maintaining security and privacy.
- **Michael Bubolz:** Leading the effort to incorporate AI into UW Green Bay's information technology infrastructure is Michael Bubolz. To provide staff and students with cutting-edge learning environments and the digital fluency they will need in the future, his strategic vision for AI in education is essential.
- **Edward Murphy:** The UW System Administration's Associate Vice President and CISO, Edward Murphy, is essential to guaranteeing the safe integration of AI technologies. His cybersecurity acumen is essential to defending the university's AI projects and guaranteeing a secure learning environment in the digital era.

Panel Discussion

Q1: AI Integration and Strategic Vision

Topic/Question: How does integrating AI technologies at your institution align with its strategic vision and objectives? In what ways do you foresee AI contributing to enhancing academic and administrative efficiency?

UW Oshkosh's Mark Clements: Mark Clements highlighted the strategic change in AI integration at UW Oshkosh, stressing how it went from being an operational tool to a strategic academic and administrative one.

He said, "The integration of AI must be viewed through the lens of strategic enhancement rather than just operational convenience."

Clements went into detail on how artificial intelligence (AI) is changing how the university delivers instruction and how efficiently it runs, in line with creating a technologically cutting-edge learning environment. This reflects a larger trend in higher education, where AI is turning into a tactical tool essential to pedagogy and institutional operations.

> UW Green Bay's Michael Bubolz: Speaking on AI's revolutionary role at UW Green Bay, Michael Bubolz emphasized the importance of technology in the school's digital transformation process. He said, *"AI is not just a tool but a strategic partner in our journey towards digital transformation."*

Bubolz's viewpoint aligns with the need to see AI as a crucial component of institutional strategy. He also discussed successfully applying adaptive learning platforms, including Arizona State University's ALEKS platform, to highlight how AI may improve academic results and facilitate individualized learning.

Edward Murphy (UW System Administration): Edward Murphy promoted a comprehensive AI strategy that aligns with ethical norms and educational objectives by providing a system-wide viewpoint. His observations emphasize the necessity of a coordinated strategy to utilize AI's capabilities while adhering to moral norms fully. He emphasized the significance of guaranteeing impartial and equitable AI technologies, particularly in delicate domains such as student admissions, assessments, and performance tracking.

According to Alenezi, the digital transformation of modern higher education institutions entails implementing new technology and changing procedures, business models, and practices (Alenezi, 2021). This change aligns with higher education's goal, which is to produce more sophisticated and efficient procedures and processes. This viewpoint is consistent with what Mark Clements and Michael Bubolz have been saying about strategically incorporating AI into the larger goals of their respective universities.

The previous transition of higher education institutions (HEIs) to digital universities is explained by Fernandez (Fernández et al., 2023). This involves adopting new technology such as artificial intelligence (AI) and an organizational transformation involving information, processes, and human elements. This aligns with the scale of digital transformation initiatives and the path to digital maturity, mirroring Edward Murphy's strategic vision for AI integration and the requirement for an all-encompassing digital strategy.

Q2: AI's Role in Educational Transformation

Topic/Question: From your perspective, how can AI transform education dynamics at your university? What potential does AI have in improving student services, learning experiences, and overall success while maintaining ethical standards and data security?

UW Green Bay's Michael Bubolz: Speaking on AI's revolutionary potential, Michael Bubolz of UW Green Bay emphasized how it may completely change classroom instruction and student services.

> *"Our focus is on harnessing AI's potential while safeguarding ethical standards and data integrity,"* he said, arguing in favor of an ethical and balanced approach to integrating AI into education.

The use of adaptive learning systems in higher education is one of AI's more significant potential uses. These systems can adapt the learning process to each student's individual pace, preferences, and performance by using algorithms.

The use of the adaptive learning platform "ALEKS" (Assessment and Learning in Knowledge Spaces) by Arizona State University (ASU) in their introductory math courses is a notable example. ALEKS's real-time assessment of student knowledge and its dynamic adaptation to individual strengths and weaknesses are prime examples of an efficient, personalized learning process. Increased pass rates and better retention in future courses prove that ASU's implementation of ALEKS greatly improved student results. For example, after ALEKS was implemented, pass rates in a collegiate mathematics course increased from 64% to 75%. This approach showed how AI can change conventional teaching methods by enabling teachers to recognize and assist students with difficulties early in the course (Tyson & Sauers, 2021).

The UW System Administration's Edward Murphy: Edward Murphy explored the profound implications of generative AI technologies, such as Bing Enterprise Chat, on pedagogy and learning approaches. He emphasized that integrating AI requires careful consideration, especially when safeguarding private student data.

Murphy brought up an important issue: "There are instructors on all our campuses wrestling with issues related to generative AI, such as, you know, do I prohibit my students from using generative AI?"

This claim emphasizes the continuous discussions and difficulties surrounding AI's morally and practically acceptable integration in educational environments.

Mark Clements (UW Oshkosh): Mark Clements stated that AI has been essential in changing UW Oshkosh's educational methods. He underlined how educational institutions must adapt their practices and offerings to new developments in AI while upholding the highest moral standards. Clements' viewpoint is consistent with the larger trend in education toward the creative and responsible use of AI.

Q3: Emerging AI Trends in Higher Education

Topic/Question: What emerging trends in AI technology do you find most relevant for higher education? How is your university preparing to embrace these advancements, especially regarding digital literacy and information security?

The UW System Administration's Edward Murphy: Focusing on the promise of generative AI to change student services, Edward Murphy underlined the requirement of painstaking caution in AI integration, especially involving student data.

> He emphasized that *"we must approach AI integration with meticulous care, especially when dealing with student data,"* emphasizing the need for high schools to embrace AI technology while striking a critical balance between innovation and security.

UW Green Bay's Michael Bubolz: Michael Bubolz addressed the dualistic character of artificial intelligence and the opportunities and challenges it brings.

> *"AI presents both a challenge and an opportunity - it's about finding the right balance,"* he said, arguing in favor of a calculated strategy prioritizing increased digital literacy and strong information security protocols.

Mark Clements (UW Oshkosh): Addressing issues of digital literacy and security, Mark Clements reiterated the comments about utilizing AI's potential in the administrative and academic spheres.

Further investigation of Data Security and Ethical Considerations resulted from this question. According to Edward Murphy, the ethical implications of AI have received a lot of attention, especially in managing sensitive student data. He discussed how higher education is becoming more conscious of the ethical ramifications of AI, including data security and student privacy. These worries are becoming more and more pertinent as large volumes of student data are analyzed by AI systems in education, which calls for strong privacy protection and data breach prevention methods.

In keeping with a larger educational trend that supports the ethical application of AI, Michael Bubolz underlined the necessity of ethical frameworks and rules that strike a balance between innovation and responsibility. Using Georgia Tech's AI ethics course as an example; he emphasized the significance of educating the ethical design of AI systems.

The talks between Murphy and Bubolz highlight the crucial balance that must be struck when implementing AI: taking advantage of its promise for efficient data-driven decision-making and personalized learning while upholding ethical oversight, openness, and justice.

As noted by Borenstein et al., integrating raises difficult ethical issues in several spheres of human existence, including education (Borenstein & Howard, 2021). They stress the significance of preparing upcoming AI experts to consider how AI affects people's lives and take on responsibilities for maximizing benefits while minimizing possible risks. This aligns with Michael Bubolz's focus on the necessity of ethical frameworks in the use of AI, arguing that ethics should be taught in AI curricula and through interdisciplinary teams.

Q4: University Readiness for AI Adoption

Topic/Question for All Panelists: Based on your insights and experiences, how would you evaluate your university's readiness for adopting AI technologies? What aspects make you most optimistic, and what concerns, if any, do you have, particularly regarding IT security? In navigating the AI landscape, Mark Clements (UW Oshkosh) underlined the significance of strategic planning.

> As he pointed out, *"We're navigating uncharted waters with AI, and strategic planning is key to our successful adoption,"* proactive policy formulation and alignment with institutional objectives are critical.

In his discussion of AI preparedness, Michael Bubolz (UW Green Bay) concentrated on identifying the potential of AI and creating strategic plans for its successful integration.

> *"It's about aligning our AI initiatives with our mission while upholding our commitment to ethical standards,"* said Bubolz, emphasizing the significance of doing so. Bubolz also emphasized the need to maintain high ethical standards.

The importance of creating adaptable AI regulations to control AI's expanding interest and applications in the educational sector was highlighted by Edward Murphy (UW System Administration). He emphasized the necessity of a system-wide strategy and the significance of strategic adoption and cooperation across the educational landscape.

As reported by Crompton's systematic review, the substantial growth in publications on AI in higher education suggests a quickening of interest and advancement in this topic (Crompton & Burke, 2023). The review revealed some trends, including a greater emphasis on language acquisition and undergraduate students and the application of AI in tutoring, assessment, prediction, and assistance. These results demonstrate the variety of uses of AI in higher education and give context to Mark Clements' discussion of adoption readiness.

This question prompted further investigation of the Opportunities and Challenges in AI Integration. The conversation between Michael Bubolz and Mark Clements highlights the challenges of incorporating AI into systems of higher learning. The significance of preparation and strategic planning for the effective integration of AI addresses a range of AI uses, including intelligent tutoring systems, predictive analytics, assessment, evaluation, and student learning management.

These varied applications draw attention to the necessity of all-encompassing approaches that balance institutional preparedness, ethical issues, and technical potential. For instance, predictive analytics in artificial intelligence presents ethical questions about handling sensitive data and is essential for predicting patterns like dropout rates and school performance.

The subject of System-Wide Coordination and Strategy was then brought up. Edward Murphy's observations regarding the need for an all-encompassing strategy when using AI technologies speak to a larger issue facing the industry. This strategy addresses policy, ethical issues, data security, and stakeholder involvement at the university system level while integrating technology.

Taking care of the digital gap and ensuring that all educational institutions have equal access to cutting-edge AI technologies and resources are important components of this strategy. This is essential to guarantee that the benefits of AI are shared fairly and to avoid escalating the gaps in educational outcomes.

Harry discusses how artificial intelligence (AI) can potentially change higher education. Still, he also highlights some current barriers, including potential bias, expense, lack of trust, and privacy and security issues (Harry, 2023). Focus is placed on the importance of ethical considerations, which include making sure AI-based systems are accessible, transparent, and equitable. This emphasizes the necessity to weigh the advantages and disadvantages of integrating AI into educational settings, consistent with Edward Murphy's focus on the ethical aspects of AI managing sensitive student data.

Conclusion

The panelists' combined experiences presented the higher education industry at a critical point in its embrace of AI. Their observations demonstrate a deep understanding of the significance of ethical issues, strategic alignment, and AI integration readiness. These themes are not isolated; they are a part of a larger story in higher education, where technology is becoming increasingly recognized as essential to operational effectiveness, instructional innovation, and institutional strategy.

The conversation made it evident that although there is hope for AI's potential, there is also a clear understanding of its drawbacks. Because of this, the panelists' perspectives provide a road map for navigating AI's potential in higher education, highlighting the significance of methodical, calculated, and moral methods.

Key Findings

The opinions from our panel of experts have shed light on the dynamic and changing role of AI in higher education. Chief Information Officers (CIOs) must concentrate on a few crucial areas as colleges traverse this crucial time to adequately meet the problems posed by AI and realize its full potential. These domains consist of:

- **Strategic Alignment with Institutional Goals:** AI projects need to be closely aligned with the purpose and goals of universities. This necessitates incorporating AI into institutions' pedagogy and fundamental operations, ensuring that these technologies advance the overarching strategic vision.
- **Ethical Issues with AI Deployment:** Adhering to ethical guidelines is critical when implementing AI, especially concerning data protection, bias, and transparency. CIOs need to take the lead in creating guidelines and regulations that support ethical AI use and educate the academic community for higher education on the moral implications of AI.
- **Readiness for AI Integration:** Investing in infrastructure, promoting innovation, and improving digital literacy are all necessary steps in getting ready for AI adoption. CIOs play a

critical role in equipping the university community to effectively use AI technology by helping to develop AI competencies among staff and students.

- **Reducing the Digital Divide:** It is essential to guarantee equitable access to AI resources. CIOs must work to close the digital gap by supporting policies that give all faculty and students fair access to AI tools.
- **System-Wide Coordination and Collaboration:** Because AI integration is complicated, university divisions must work together in a coordinated manner. CIOs should encourage cooperation and knowledge exchange to maximize AI adoption and impact.

Our research team found that CIOs are critical in helping institutions navigate the AI-driven era in our panel report. They must manage cooperative efforts, ethical deployment, community preparedness, equitable access, and strategic alignment.

Directions for Future Work

Future research should examine faculty and student perspectives on artificial intelligence's impact on higher education, according to our collaborative panel, which includes me (Steve Schilhabel) and the distinguished panel of Chief Information Officers. One can acquire a fuller understanding of the diverse impact of AI. This strategy will make it easier to compare and contrast these viewpoints with those of the IT and administrative leadership, improving our understanding of AI's place in the educational system.

AI's role in higher education will not be limited to transforming teaching and learning. It will entail changing labor markets, rethinking educational models, and restructuring institutional frameworks. Universities can take the lead in educating students for a workforce driven by AI and develop into hubs for innovation in technology and community involvement.

Acknowledgments

This research report results from teamwork and draws from various sources and viewpoints. We thank Tyton Partners and Ellucian for their thorough reports on generative AI in higher education. These papers' conclusions and analyses have been crucial in setting the scene for our conversations and giving us a solid grasp of the situation of AI in academia today.

I (Steve Schilhabel) extend my heartfelt gratitude to the panel of Chief Information Officers, which includes Edward Murphy from UW System Administration, Michael Bubolz from UW Green Bay, and Mark Clements from UW Oshkosh. Particular emphasis on their unique perspectives and ideas regarding AI integration, educational reform, upcoming AI trends, and university readiness for AI adoption in the Panel Discussion part (part 4), which resulted from their expert contributions.

Using sophisticated language tools was quite helpful in writing this piece. Grammarly was used to guarantee clarity and grammatical accuracy throughout the paper. Additionally, ChatGPT from OpenAI was helpful in several areas, such as improving the language, making the arguments more coherent, and recommending changes for better articulation, especially in the Introduction, Motivation, and Conclusion sections. This use of generative AI shows how it can improve academic writing and research by providing a useful application for combining and presenting complex data. Finally, Mendeley Cite was used for reference management.

This paper's quality has been enhanced by the combined efforts of these eminent specialists and cutting-edge technical tools, which have also shown how easily AI may be incorporated into academic panel report. I (Steve Schilhabel) would like to express my sincere gratitude for all of the help and contributions that have enabled this thorough investigation of AI in higher education.

Finally, I'd like acknowledge and thank Gaurav Bansal, Ph.D. from the University of Wisconsin Green Bay who suggested I conduct this research.

References

AlDhaen, F. (2022). The Use of Artificial Intelligence in Higher Education - Systematic Review. In COVID-19 Challenges to University Information Technology Governance. https://doi.org/10.1007/978-3-031-13351-0_13

Aldosari, S. A. M. (2020). The future of higher education in the light of artificial intelligence transformations. International Journal of Higher Education, 9(3). https://doi.org/10.5430/ijhe.v9n3p145

Alenezi, M. (2021). Deep dive into digital transformation in higher education institutions. Education Sciences, 11(12). https://doi.org/10.3390/educsci11120770

Beltran, K. (2023). Higher Education Leaders Eager to Embrace AI and Transform Campus Operations. https://www.ellucian.com/assets/en/article/higher-education-leaders-eager-embrace-ai-transform-campus-operations.pdf

Borenstein, J., & Howard, A. (2021). Emerging challenges in AI and the need for AI ethics education. AI and Ethics, 1(1). https://doi.org/10.1007/s43681-020-00002-7

Crompton, H., & Burke, D. (2023). Artificial intelligence in higher education: the state of the field. International Journal of Educational Technology in Higher Education, 20(1). https://doi.org/10.1186/s41239-023-00392-8

Fernández, A., Gómez, B., Binjaku, K., & Meçe, E. K. (2023). Digital transformation initiatives in higher education institutions: A multivocal literature review. Education and Information Technologies, 28(10). https://doi.org/10.1007/s10639-022-11544-0

Harry, A. (2023). Role of AI in Education. Interdiciplinary Journal and Hummanity (INJURITY), 2(3). https://doi.org/10.58631/injurity.v2i3.52

Michel-Villarreal, R., Vilalta-Perdomo, E., Salinas-Navarro, D. E., Thierry-Aguilera, R., & Gerardou, F. S. (2023). Challenges and Opportunities of Generative AI for Higher Education as Explained by ChatGPT. Education Sciences, 13(9). https://doi.org/10.3390/educsci13090856

NeJame, L., Bharadwa, Dr. R., Shaw, C., & Fox, K. (2023, April 25). Generative AI in Higher Education: From Fear to Experimentation, Embracing AI's Potential. Tyton Partners, Blog Post.

Tyson, M. M., & Sauers, N. J. (2021). School leaders' adoption and implementation of artificial intelligence. Journal of Educational Administration, 59(3). https://doi.org/10.1108/JEA-10-2020-0221

OLD WINE IN NEW BOTTLES? AN ANALYSIS OF AI IN CYBERSECURITY

Paul D. Nugent, Ph.D., Western Connecticut State University, nugentp@wcsu.edu

ABSTRACT

This paper is a preliminary analysis of the various uses of Artificial Intelligence (AI) in the field of cybersecurity. AI plays roles in threat detection and prevention, malware creation, security, and access control. The research question is whether these roles represent something revolutionary and unique or whether they simply advance existing concepts and practices in an incremental fashion. Although still preliminary, the results of the analysis indicate that while AI is primarily making existing cybersecurity processes and practices more effective and efficient, it is doing so in a revolutionary manner.

Keywords: artificial intelligence, cybersecurity, access controls, risk management framework, malware creation

INTRODUCTION

There is no doubt that in all technically oriented spheres of life, Artificial Intelligence (AI) is having important impacts. AI chatbots are revolutionizing fiction and non-fiction and creating/correcting computer code. AI engines are creating music and art that rival those produced by human beings. AI can collect, analyze, and interpret vast amounts of data from around the globe to answer important technical and scientific questions.

However, the worlds of technology, business, and science have a long history of birthing new concepts that are the latest “shiny” thing; the latest “buzzword” that promise a revolution in theory and practices. However, often these new shiny ideas only address old questions but from slightly different angles and fail to be the revolutions they proclaim to be. The analogy “old wine in new bottles” is often used, especially in academia, to capture this phenomenon.

Clearly AI has succeeded in being a distinct new varietal of wine in many of the spheres discussed above. However, with the proliferation of AI into more specialized fields, such as cybersecurity, is it having the revolutionary impacts its proponents claim? This an important question as the global price tag of AI-powered cybersecurity products exceeds $135 billion (Morgan, 2023). Given this flurry of excitement and investment, this paper explores to what extent it is truly introducing something novel, versus simply tweaking existing theory and practice

ANALYSIS

Threat detection and prevention

AI algorithms are used to detect threats to the confidentiality, integrity, and availability of information by analyzing threat-level data and comparing them against baseline levels or patterns (Cyber, 2024; Lundgren & Padyab, 2022). However, long before AI was a shiny new gem, Intrusion Detection Systems (IDPs) and Intrusion Detection and Prevention Systems (IDPSs) were widely used in organizations. Therefore, conceptually, AI does nothing *functionally* new. Rather, it makes these systems more efficient and effective through machine learning and predictive analysis to ascertain the likelihood of certain attacks, detect attacks, respond to attacks, and modify trigger levels (Shuba et. al., 2019; Siddiqi, 2020; Cyber, 2023; Frackiwicz, 2023; Jain et al., 2016). Therefore, they greatly automate and improve some of the processes that were previously performed by IDPs, IDPSs, and human beings (Watkins, 2024; Shutenko, 2024).

Malware creation

Cybersecurity is a cat and mouse game. Through white hat hacking and penetration testing, organizations are able to discover vulnerabilities at the same time that black hat hackers are feverishly trying to stay one step ahead. This dynamic continues with the introduction of AI. AI is able to write computer code and will be a weapon to produce increasingly sophisticated malware (Cyber, 2024; De Angelo, 2024). As mentioned in the previous section, AI is very effective in characterizing threat actors and performing white hat functions. This provides a basis from which AI can generate malware that equals or exceeds existing threats. An example of this is the Bumble Bee Web Shell – a threat agent that AI was able to approximate with great accuracy (De Angelo, 2024; Falcone, 2021). AI, then, takes the cat and mouse game to the next level, using machine learning and code generation to aid both the attackers and the defenders.

Security of AI systems

Cybersecurity Risk Management (RM) is a cost-benefit business approach to reducing cyber risk in organizations. Traditionally it attempts to use quantitative measures of asset value, probability of threats being successful, and effectiveness of controls to derive a level of risk that becomes the basis for deciding how to invest in risk reduction.

The AI Risk Management Framework (NIST, 2024) playbook applies these RM activities to reduce risk associated with AI systems. This framework provides guidance on governance structures and policies, maps to better model AI systems, effective metrics and ongoing management processes (NIST, 2024). Therefore, in line with other types of technical systems, NIST and other policy makers have expanded their guidance to include AI systems (Comiter, 2019). This means that the cybersecurity community deems AI to be a significant new form of technology requiring novel methodologies and risk management approaches.

Access control

Authentication and access control are fundamental facets of cybersecurity. They involve user identification, ensuring that the user is who they claim to be (authentication), and what the user will be able to do within the system (authorization). AI is now beginning to play a role in enhancing these critical components. AI-based access controls transcend traditional username/password implementations. Some of the major elements in which AI is making contributions include data tracking and analytics, access accuracy, decision-making, visitor monitoring, task automation, system integration, and AI alarm systems (LenelS.2, 2024).

PRELIMINARY CONCLUSIONS

While the analysis is not an exhaustive treatment of all instances of AI's role in cybersecurity, it nonetheless reflects the most important areas. In answering the research question, the analysis is somewhat divided. On the one hand, AI has not changed the basic tenets of cybersecurity. Threats to the confidentiality, integrity, and availability of information continue to be the main focus and risk management techniques continue to monopolize a business-centered approach to reducing risk. Therefore the "old bottles" haven't changed in theory. On the other hand, AI is such a powerful analytic tool that it acts like a steroid for existing techniques/practices. In this respect, the "new wine" is potent enough to warrant the claim that AI represents a revolutionary turning point in cybersecurity.

REFERENCES

Comiter, M. (2019). Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It | Belfer Center for Science and International Affairs. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/AttackingA

Cyber (2024) *Risks of AI & Cybersecurity: Risks of artificial intelligence*. Malwarebytes. https://www.malwarebytes.com/cybersecurity/basics/risks-of-ai-in-cyber-security

De Angelo, D. (2024). *The Dark Side of AI in Cybersecurity — AI-Generated Malware.* https://www.paloaltonetworks.com/blog/2024/05/ai-generated-malware/#:~:text=The%20Shifting%20Landscape%20of%20Cybersecurity&text=He%20further%20predicts%2C%20%22AI%20will,and%20be%20much%20more%20effective.%22

Falcone, R. (2021). *xHunt Campaign: New BumbleBee Webshell and SSH Tunnels Used for Lateral Movement.* https://unit42.paloaltonetworks.com/bumblebee-webshell-xhunt-campaign/

Frąckiewicz, M. (2023, June 6). *The ethics of OpenAI's AI integration in the workplace: Addressing human labor rights and dignity*. TS2 SPACE. https://ts2.space/en/the-ethics-of-openais-ai-integration-in-the-workplace-addressing-human-labor-rights-and-dignity/

Jain, P., Gyanchandani, M., & Khare, N. (2016). Big Data Privacy: A Technological Perspective and Review. *Journal of Big Data, 3*(1). https://doi.org/10.1186/s40537-016-0059-y

LenelS.2. (2024). 7 Ways AI is Changing Access Control & Security https://www.lenels2.com/en/news/insights/7_ways_ai_is_changing_access_control.html

Lundgren, M., & Padyab, A. (2022). A review of Cyber Threat (artificial) intelligence in security management. *Artificial Intelligence and Cybersecurity*, 29–45. https://doi.org/10.1007/978-3-031-15030-2_2

Morgan, S. (2023, September). *AI and Cybersecurity: A New Era*. Morgan Stanley. https://www.morganstanley.com/articles/ai-cybersecurity-new-era

NIST. (2024). NIST AI RMF Playbook. https://airc.nist.gov/AI_RMF_Knowledge_Base/Playbook#:~:text=NIST%20AI%20RMF%20Playbook&text=Suggestions%20are%20aligned%20to%20each,Map%2C%20Measure%2C%20Manage)

Siddiqi, S. (2020). Leveraging Artificial Intelligence for Cybersecurity: Trends, Opportunities, and Challenges. International Journal of Network Security & Its Applications (IJNSA), 12(5). https://doi.org/10.5121/ijnsa.2020.12503

Shuba, C. A., et al. (2019). Application of Artificial Intelligence for Cyber Security: A Comprehensive Review. IEEE Access, 7, 10151-10176. https://doi.org/10.1109/ACCESS.2018.2886377

Shutenko, V. (2024, March 15). *AI in cyber security: Top 6 use cases*. TechMagic. https://www.techmagic.co/blog/ai-in-cybersecurity/

Stanham, L. (2023, November 3). *Machine Learning in Cybersecurity: Benefits and Use Cases | CrowdStrike*. Crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/machine-learning-cybersecurity

Watkins, O. (2024, April 19). 4 use cases for AI in cyber security. https://www.redhat.com/en/blog/4-use-cases-ai-cyber-security