

A CONDENSED 4-WEEK COURSE ON CYBERSECURITY: A CONNECTIVISM APPROACH WITHIN THE COMMUNITY OF INQUIRY FRAMEWORK

L. Whisenant

University of North Texas (UNITED STATES)

Abstract

This abstract provides an overview of a condensed 4-week course on cybersecurity, which is designed based on the connectivism learning theory and wrapped in the community of inquiry framework. The course aims to present a comprehensive understanding of cybersecurity, emphasizing its significance in safeguarding digital assets and preserving privacy. It covers various aspects, including the identification of common types of threats, vulnerabilities, and attacks in computer systems and networks. Additionally, the course explores the fundamentals of network security and its pivotal role in protecting data and systems. Furthermore, it highlights the importance of security awareness and training in maintaining a secure computing environment.

The course also focuses on developing critical thinking and reflective writing skills through the analysis of readings and the expression of personal insights. Students will have the opportunity to apply risk assessment techniques to identify vulnerabilities, assess the likelihood of threats, and prioritize risk mitigation strategies. Moreover, the course delves into the process of incident response and its importance in mitigating cybersecurity incidents. Students will gain an understanding of the potential impact of emerging technologies on cybersecurity.

By adopting a connectivism approach, the course encourages active participation, collaboration, and knowledge creation among learners. The community of inquiry framework provides a structured environment for meaningful interactions and critical thinking. Overall, this condensed 4-week course offers a concise yet comprehensive learning experience in cybersecurity, equipping learners with essential knowledge and skills to address the challenges of the digital era.

Keywords: Cybersecurity, connectivism, community of inquiry, higher education, learning theory.

1 INTRODUCTION

1.1 Background

In the swiftly evolving digital landscape, the essential role of cybersecurity is undeniable, a realization that has deepened through my extensive exploration in this domain. The digital sphere is akin to a living entity, ceaselessly morphing, ushering in challenges that are unprecedented, thereby calling for a fortified line of defense: cybersecurity. "The capability to detect, analyze, and defend against such threats in near real-time conditions is not possible without employment of threat intelligence, big data, and machine learning techniques" [1, p. 1].

As we steer through the pressing inquiry of what constitutes the foundation of a robust cybersecurity education, we find ourselves traversing the complex pathways of connectivism and the community of inquiry framework. These philosophies, deeply rooted in learner-centric education, collaborative learning environments, and networked learning spaces, unfurl a rich canvas of opportunities, enabling learners to immerse, interact, and evolve. According to Steven Downes, co-creator of the Connectivism learning theory, "earlier generations think of learning as a cognitive process based essentially in logical structures such as language and mathematics, while in the digital era learning is understood as a physical process based on adaptation to concrete experience" [2, p. 149].

Drawing inspiration from these educational philosophies, this article delineates a succinct 4-week course on cybersecurity, while crafting a rich, immersive learning experience grounded in active participation and knowledge creation [3]. Siemens articulated that "learning (defined as actionable knowledge) can reside outside of ourselves (within an organization or a database), is focused on connecting specialized information sets, and the connections that enable us to learn more are more important than our current

state of knowing" [3, p. 6]. This perspective is pivotal in course design, fostering a networked learning environment that encourages connectivity, collaboration, and communal knowledge creation.

Moreover, the community of inquiry framework, expounded on by Apostolidou, fosters "research and course development not only within the online conferencing context in which it evolved but also with new technologies as they have emerged [4, p. 5]. This approach is intricately woven into the course fabric, nurturing a space where learners are encouraged to delve deep, fostering a community where inquiry is not just encouraged but is central to the learning experience.

Furthermore, this course leverages the potential of emerging technologies, encouraging learners to delve deep into the realms of cybersecurity, exploring the nuances and intricacies that define the digital landscape today. "After the development of technologically mediated environments and the wide dissemination of open resources, radically alternative educational models are now thinkable and urgently needed for the reshaping of education in the 21st century away from lecturing and information relaying" [4, p. 2]. This sentiment resonates throughout the course; encouraging learners to approach the subject with a critical, analytical mindset, ready to navigate the complex, ever-evolving landscape of cybersecurity with a fortified understanding and a readiness to adapt to the changing dynamics.

1.2 Purpose

This course is more than a learning expedition; it is a collaborative endeavor, a space where learners are not just encouraged but expected to dive deep, critically engage with the content, and articulate their insights with a depth that mirrors profound understanding. It is a crucible for nurturing critical thinkers; individuals empowered to reflect deeply and articulate their reflections with eloquence, honing skills that break free from the traditional classroom confines.

In this endeavor, we heed the insights of Kweon et al., emphasizing the criticality that "past research indicates that implementing information security training and education is an effective method" [6, p. 361]. Thus, this course stands as a beacon, guiding learners to harmonize theoretical knowledge with practical skills, fostering a holistic understanding that encompasses both the tangible and intangible facets of cybersecurity.

Moreover, reflective writing emerges as a linchpin in this educational journey, a practice underscored by Yeh et al., as instrumental in that "reflective writing should be incorporated into the curriculum across disciplines to cultivate students' CT (Critical Thinking). This is a key component for students' academic success and career development" [5, p. 256]. Through assignments steeped in reflective writing, learners are propelled to engage with the content on a deeper plane, fostering a rich environment of critical analysis and reflective practice. This approach not only cultivates critical thinking but nurtures a deeper understanding and appreciation for the intricacies of cybersecurity.

Drawing from Siemens' connectivism theory, we foster a learning environment where "knowledge resides in the diversity of opinions," and learning morphs into a dynamic process of connecting specialized nodes or information sources [3, p. 5]. This theory is intricately woven into the course fabric, encouraging learners to forge connections, collaborate, and construct knowledge through a networked learning environment.

Moving forward, this course aims to sculpt learners who are not just scholars in the theoretical realms of cybersecurity but critical thinkers and reflective writers, adept at navigating the complex, ever-evolving digital landscape with fortified understanding and a critical, analytical mindset. It is a journey of exploration, of discovery, and of growth, where learning is not confined to the classroom, but grows from a community of thinkers.

2 LITERATURE REVIEW

As we navigate this complex subject matter, we anchor our journey in the principles of connectivism, a learning theory that champions the diversity of opinions, fostering a rich tapestry of interconnected knowledge nodes [3]. Siemens, the creator of this theory, emphasized that in the connectivism approach, "decisions are based on rapidly altering foundations. New information is continually being acquired and the ability to draw distinctions between important and unimportant information is vital" [3, p. 5]. It is this philosophy that guides our course structure, facilitating an environment ripe for meaningful interactions and critical discourse, nurturing a community of inquiry where learners change from mere consumers to vibrant creators of knowledge.

Kotzee and Palermos delve deep into the intricate dynamics of collaborative learning environments, shedding light on the transformative potential of networked learning spaces. They underscore the pivotal role of diversity of expertise in enhancing the efficacy of interconnected networks, emphasizing the necessity for a differentiated structure that facilitates autonomous and diversified contributions from members. The discourse resonates with a deep understanding of the collaborative dynamics, highlighting the synergetic cooperation of group members in fostering epistemic reliability and responsibility, a phenomenon they term as "epistemic self-organization and self-regulation" [7, p. 507].

A critical insight emerges as they delve into the concept of "distributed cognition," a phenomenon that encapsulates cognitive processing distributed between individuals, rendering it irreducibly social. The authors vividly illustrate this through the lens of large scientific projects, where collaborative science experiments embody a kind of thinking that transcends the capabilities of a single individual, fostering a space of "distributed cognition" [7, p. 504].

Moreover, they explore the potential of online platforms in facilitating collaborative learning, emphasizing the democratization of learning through Web 2.0 technologies. They note, "Web 2.0 has also democratized learning: traditional educational institutions are being challenged by start-up education providers, and teachers as sources of knowledge are being challenged by new forms of teaching using technology" [7, p. 498].

Li Chen and Yaqian Xu, researchers from China, delve deep into the realms of connectivism, and its burgeoning application in the educational landscape of China. The paper stands as a testament to the pioneering efforts of the MOOC Research Team at the Distance Education Research Centre at Beijing Normal University, who orchestrated China's inaugural cMOOC grounded in the principles of connectivism. It was conceived to navigate the intricate pathways of knowledge overload that characterizes the internet era, championing the continuous forging of connections and the nurturing of networks as the linchpin of learning [8].

As we navigate through the methodology, we find ourselves immersed in the meticulous crafting of China's first cMOOC, a vibrant learning space titled "Internet plus Education: Dialogue between Theory and Practice." The course, a rich repository of knowledge, unfolded over six offerings spanning from October 2018 to August 2021, offering a rich data landscape for exploration. The research leverages a myriad of analytical tools, including the big data paradigm and network analysis, to unravel the complex tapestry of connectivist learning [8]. The paper offers a glimpse into the diverse demographic landscape of the 5,426 participants who embarked on this learning journey, a vibrant community of learners encompassing teachers, educational managers, industry practitioners, and students, all eager to share their insights and experiences.

In a 2018 scholarly discourse, Vas, Weber, and Gkoumas offer a deep exploration into the realms of connectivism. The authors emphasize the pivotal role of semantic technologies in implementing connectivism, fostering a space where learners transform from mere consumers to vibrant creators of knowledge. They engage in a dynamic process of connecting specialized nodes or information sources, creating a rich, immersive learning experience grounded in active participation and knowledge creation. The authors note, "Due to the speed of change in today's social and economic environments, the learner cannot experience every situation on his own anymore. Experiences should be borrowed from external sources, and individual learners should find ways of connecting the relevant external experiences and knowledge objects to their own knowledge" [9, p. 1034].

Echoing the sentiments of Siemens, the discourse emphasizes the dynamic process of learning where connections, collaboration, and communal knowledge creation stand paramount. The authors foster a rich narrative, encouraging learners to forge connections, collaborate, and construct knowledge through a networked learning environment, a space vibrant with diversity of opinions and rich with opportunities for self-directed learning. They articulate, "Moreover, learning happens in such environments where core knowledge objects may change over time and are potentially out of the learners' control" [9, p. 1034].

In a forward-thinking piece published in the 2023 issue of the Journal of Curriculum Studies Research (JCSR), B. I. Omodan delves deep into the intricacies of connectivism as a potent tool for sculpting posthuman university classrooms. These include the pivotal role of connections in learning and knowledge acquisition, the symbiotic relationship between humans and technological appliances in the learning ecosystem, the necessity of connectedness and interactivity, and the imperative of constantly updating knowledge through these connections.

Omodan envisions a transformative educational landscape where students change into active nodes in a vibrant network, leveraging technology to foster both collaborative and individualized learning experiences. The author depicts a future where classrooms are not just spaces of learning but hubs of critical inquiry, a vision grounded in the deep integration of technology into learning environments, thereby nurturing a generation adept at navigating the complex, interconnected world of the future [10].

Drawing a parallel between connectivism and posthumanism, Omodan articulates a compelling vision for the future of education, one that transcends traditional boundaries to foster a rich tapestry of ideas and values that shape the learners' lives. The author advocates fervently for a shift towards a more inclusive and democratic educational paradigm, leveraging the rich potential of connectivism to nurture learners for a posthuman era characterized by a seamless integration of technology and education. Omodan calls upon universities to be pioneers in this transformative journey, urging them to foster environments that are not just technologically enabled, but vibrant spaces promoting critical thinking, collaboration, and the acquisition of up-to-date knowledge.

2.1 Cybersecurity

In this seminal work, Leah Zhang-Kennedy, and Sonia Chiasson, hailing from the University of Waterloo Stratford School of Interaction Design and Business and the Carleton University School of Computer Science respectively, embark on a meticulous exploration of the multimedia tools designed for non-expert end-users in the dynamic landscape of cybersecurity education. The authors have curated a rich repository of 119 tools, categorizing them into five broad media categories, offering a deep dive into the current trends, instructional design principles, and the empirical evidence of their effectiveness.

The duo champions the multimedia educational tools, a vibrant landscape where text, images, audio, animation, and interactive content come to life, fostering a rich environment of learning characterized by heightened motivation, engagement, and comprehension. They envision a future where games transcend their current boundaries, evolving into potent tools of learning, a vision that calls for empirical substantiations through robust evaluations. The paper stands as a beacon, guiding the future trajectories of research, calling for a nuanced approach to understanding the trends in multimedia tools, a space brimming with potential yet requiring a structured pathway to navigate.

Zhang-Kennedy and Chiasson articulate a fervent call for the integration of games in formal learning contexts, a space yet untapped to its fullest potential. They emphasize the critical role of cybersecurity awareness, stating, "Cybersecurity is both a technical problem and also one that is significantly impacted by non-expert end-users who interact with online content. Due to the ever-changing and nuanced nature of security, technological countermeasures alone are rarely enough to protect these users from online threats" [11, p. 12]. They further highlight the consolidation of existing research, guiding future research efforts by identifying gaps and open research issues, thereby illuminating a pathway for future endeavors in this vibrant field, noting, "Our review consolidates existing research in the area, includes analysis of 119 cybersecurity educational tools, and guides future research efforts by identifying gaps and open research issues" [11, p. 12].

In another article, Lori Sussman delves deep into the non-technical knowledge, skills, and abilities (KSAs) that are pivotal in the cybersecurity field, drawing from a rich pool of insights garnered from semi-structured interviews with professionals in the sector. The research, grounded in qualitative methodology, leverages the NICE Cybersecurity Workforce Framework as a foundational tool to derive the KSAs for the interviews, albeit acknowledging the initial list as a starting point for further inclusive research [12].

Sussman meticulously categorizes the insights into three significant themes that resonate uniformly across different roles, ages, and educational backgrounds. These themes underscore the criticality of utilizing information judiciously, honing communication skills, and fostering collaboration to ensure customer or client success in the cybersecurity landscape. The research highlights the pronounced emphasis professionals place on problem-solving, critical thinking, and communication abilities, with a substantial clustering around these elements in the discussions [12].

Sussman's research stands as a seminal work, offering a rich repository of insights into the non-technical KSAs that are pivotal in the cybersecurity landscape. It is a compelling call to action, urging future research to build upon this foundational work, to explore the intricate tapestry of non-technical KSAs, and to craft a future that is grounded in knowledge, collaboration, and critical thinking, steering the cybersecurity field towards a promising horizon.

In the December 2022 issue of the "International Journal of Electrical and Computer Engineering (IJECE)," Alturkistani and El-Affendi present a groundbreaking study titled "Optimizing cybersecurity incident response decisions using deep reinforcement learning." The authors, affiliated with the College of Computer and Information Sciences at Prince Sultan University in Riyadh, Kingdom of Saudi Arabia, embark on a meticulous exploration of the potentials of Deep Reinforcement Learning (DRL) in enhancing the decision-making process in Security Information and Event Management (SIEM) incident response systems.

The researchers utilized a Deep Q-Network (DQN) model to delve into this realm, leveraging standard public datasets to emulate data streams akin to those encountered in real-life SIEM systems. The results are promising, showcasing higher accuracies compared to those produced by trained supervised models, thereby indicating the substantial potential of DRL models in the post-alert and post-exploitation decision phases where traditional model training is not feasible. The authors note, "The results show that DRL models can be effectively used in the post-alert and post-exploitation decision phases where model training is not feasible" [13, p. 6774].

In the research article "Values and Value Conflicts in the Context of OSINT Technologies for Cybersecurity Incident Response: A Value Sensitive Design Perspective," Thea Riebe examines the use of Open-Source Intelligence (OSINT) technologies in cybersecurity incident response. This study, part of the CYWARN project, enriches the CSCW-discourse by presenting a detailed analysis based on a systematic literature review and empirical data, focusing on stakeholder values and value conflicts in the application of ML-based OSINT technologies.

Riebe utilizes a methodological triangulation, incorporating both empirical case studies and a literature review to explore the emerging values and conflicts in the development and application of these technologies. The goal is to outline essential design and research implications for the future development of OSINT systems, aiming for societal acceptance and stakeholder cooperation. Riebe states, "In this paper, we employed a triangulation of methods to investigate which values and value conflicts are relevant to the application and development of ML-based OSINT technologies in the context of cybersecurity incident response" [14, p. 30].

The study identifies three key implications for fostering multi-actor collaboration in the CSCW perspective. It emphasizes the need for trustworthy OSINT systems that support the reasoning and autonomy of operators while adhering to legal and social norms. It also advocates for bias-free communication in system design, promoting collaboration among CERTs and stakeholders to enhance situational awareness and develop risk mitigation strategies. Riebe notes the importance of understanding value conflicts as a means to facilitate value-sensitive technology design in complex socio-political systems.

Lastly, Riebe discusses the study's limitations and suggests directions for future research, encouraging further technical investigations to address value conflicts and support stakeholder values more effectively. The paper calls for more detailed research to find technical solutions that would foster a collaborative cybersecurity incident response environment grounded in value-sensitive design.

3 INSTRUCTIONAL DESIGN

3.1 Week 1: Introduction to Cybersecurity and Foundations

- LO1: Understand the importance of cybersecurity in protecting digital assets and maintaining privacy.
- LO2: Describe the key principles of computer security and their application in safeguarding information systems.
- LO3: Develop critical thinking and reflective writing skills by analyzing readings and expressing personal insights.

Lesson Outline:

1. Introduction to Cybersecurity (Cognitive Presence):

- Present an overview of cybersecurity, explaining its importance in protecting digital assets and maintaining privacy. Use resources like the Cybersecurity Basics guide from the U.S. Cybersecurity & Infrastructure Security Agency to supplement the lecture.

- Discuss the key principles of computer security, such as confidentiality, integrity, and availability.
 - Engage learners in a brief discussion or reflection on the significance of cybersecurity in their personal and professional lives.
 - **Formative Assessment:** After the lecture, include a short quiz on Moodle to assess students' understanding of the key principles of cybersecurity.
2. **Case Study 1: Analyzing a Real-World Cybersecurity Incident (Cognitive Presence and Social Presence):**
- Provide a case study of a real-world cybersecurity incident, such as the SolarWinds attack or the Equifax data breach, highlighting the impact on an organization and lessons learned.
 - Instruct learners to analyze the case study, identify the key factors contributing to the incident, and propose mitigation strategies.
 - Encourage learners to collaborate in small groups or engage in online discussions on Moodle to share their analyses and insights.
 - Formative Assessment: Ask students to write a brief report summarizing their findings and proposed mitigation strategies. This report can be submitted and graded on Moodle.
3. **Discussion: Sharing Personal Experiences and Observations (Social Presence):**
- Create an asynchronous discussion forum on Moodle where learners can share their personal experiences or observations related to cybersecurity breaches or threats.
 - Prompt learners to reflect on the impact of these incidents and discuss the measures they have taken to protect their own digital assets.
 - Encourage learners to engage in meaningful discussions and provide constructive feedback to their peers.
4. **Cybersecurity Tool: Exploring a Relevant Cybersecurity Tool (Cognitive Presence and Teaching Presence):**
- Introduce a relevant cybersecurity tool, such as a network vulnerability scanner or a password manager.
 - Provide an overview of the tool's features, functionality, and benefits in enhancing cybersecurity.
 - Demonstrate how to use the tool and encourage learners to explore its capabilities on their own.

3.2 Week 2: Threats, Vulnerabilities, and Risk Management

- LO1: Identify common types of threats, vulnerabilities, and attacks in computer systems and networks.
- LO2: Assess the potential impact of threats and attacks on the confidentiality, integrity, and availability of information.
- LO3: Explain the concept of risk management and its role in proactive cybersecurity practices.
- LO4: Apply risk assessment techniques to identify vulnerabilities, assess the likelihood of threats, and prioritize risk mitigation strategies.
- LO5: Develop critical thinking and reflective writing skills by analyzing readings and expressing personal insights.

Lesson Outline:

1. **Introduction to Threats, Vulnerabilities, and Risk Management (Cognitive Presence):**
- Present an overview of common types of threats, vulnerabilities, and attacks in computer systems and networks. Use resources like the Understanding Cyber Threats, Vulnerabilities, and Risk Management guide from the U.S. Cybersecurity & Infrastructure Security Agency to supplement the lecture.
 - Discuss the potential impact of these threats on the confidentiality, integrity, and availability of information.

- Explain the concept of risk management and its role in proactive cybersecurity practices.
 - **Formative Assessment:** After the lecture, include a short quiz on Moodle to assess students' understanding of threats, vulnerabilities, and risk management.
2. **Case Study 2: Analyzing a Specific Cybersecurity Threat or Vulnerability (Cognitive Presence and Social Presence):**
 - Provide a case study of a real-world cybersecurity incident, such as the WannaCry ransomware attack or the Heartbleed bug, focusing on a specific cybersecurity threat or vulnerability.
 - Instruct learners to analyze the case study, evaluate the potential impact of the threat or vulnerability, and propose risk mitigation strategies.
 - Encourage learners to collaborate in small groups or engage in online discussions on Moodle to share their analyses, insights, and proposed mitigation strategies.
 - Formative Assessment: Ask students to write a brief report summarizing their findings and on the proposed cybersecurity threat or vulnerability. This report can be submitted and graded on Moodle.
 3. **Discussion: Exploring Risk Management Best Practices (Social Presence):**
 - Conduct a synchronous or asynchronous discussion on Moodle on risk management in cybersecurity.
 - Prompt learners to share their experiences or observations related to risk assessment and mitigation.
 - Discuss best practices and challenges associated with implementing effective risk management strategies.
 4. **Major Writing Assignment: Reflective Essay on Risk Management (Cognitive Presence and Teaching Presence):**
 - Assign a major writing assignment where learners write a reflective essay on the significance of risk management in maintaining a secure computing environment.
 - Instruct learners to analyze the challenges and best practices in implementing risk management strategies.
 - Provide clear guidelines and assessment criteria on Moodle to ensure the assignment aligns with the intended learning outcomes.
 5. **Cybersecurity Tool: Exploring a Relevant Cybersecurity Tool (Cognitive Presence and Teaching Presence):**
 - Introduce a relevant cybersecurity tool, such as a firewall or an intrusion detection system.
 - Explain the functionalities of the tool and its role in mitigating threats.
 - Demonstrate how to use the tool and encourage learners to explore its functionalities and applications.

3.3 Week 3: Network Security and Incident Response

- LO1: Understand the fundamentals of network security and its role in protecting data and systems.
- LO2: Analyze common network security threats and vulnerabilities.
- LO3: Understand the process of incident response and its importance in mitigating cybersecurity incidents.
- LO4: Analyze incident response frameworks and procedures.
- LO5: Develop critical thinking and reflective writing skills by analyzing readings and expressing personal insights.

Lesson Outline:

1. **Introduction to Network Security (Cognitive Presence):**

- Provide an overview of network security and its importance in protecting data and systems. Use resources like the Network Security Basics guide from the U.S. Cybersecurity & Infrastructure Security Agency to supplement the lecture.
 - Discuss fundamental network security concepts, such as network segmentation, access controls, and encryption.
 - Explain the role of network security in safeguarding against common threats and vulnerabilities.
 - Formative Assessment: After the lecture, include a short quiz on Moodle to assess students' understanding of network security fundamentals.
2. **Case Study 3: Investigating a Network Security Incident (Cognitive Presence and Social Presence):**
- Present a case study of a real-world network security incident, such as the Target data breach or the Sony Pictures hack.
 - Instruct learners to analyze the case study, identify the root cause of the incident, and propose appropriate incident response actions.
 - Encourage learners to collaborate in small groups or engage in online discussions on Moodle to share their analyses, insights, and recommended incident response strategies.
 - Formative Assessment: Ask students to write a brief report summarizing their findings and proposed incident response actions. This report can be submitted and graded on Moodle.
3. **Discussion: Best Practices in Network Security and Incident Response (Social Presence):**
- Facilitate a synchronous or asynchronous discussion on Moodle on network security best practices and incident response strategies.
 - Prompt learners to share their experiences or observations related to network security incidents and their resolution.
 - Discuss the importance of incident response planning, incident containment, and post-incident analysis in mitigating cybersecurity incidents.
4. **Cybersecurity Tool: Exploring a Relevant Network Security Tool (Cognitive Presence and Teaching Presence):**
- Introduce a relevant network security tool, such as a firewall or an intrusion detection system.
 - Explain the functionalities of the tool and its role in enhancing network security.
 - Demonstrate how to use the tool and encourage learners to explore its functionalities and applications.

3.4 Week 4: Security Awareness, Legal Considerations, and Emerging Trends

- LO1: Recognize the importance of security awareness and training in maintaining a secure computing environment.
- LO2: Analyze different approaches and strategies for security awareness and training programs.
- LO3: Understand the legal and ethical considerations in cybersecurity.
- LO4: Analyze the impact of laws, regulations, and industry standards on cybersecurity practices.
- LO5: Explore emerging trends in the field of cybersecurity.
- LO6: Analyze the potential impact of emerging technologies on cybersecurity.
- LO7: Develop critical thinking and reflective writing skills by analyzing readings and expressing personal insights.

Lesson Outline:

1. **Introduction to Security Awareness and Training (Cognitive Presence):**
- Discuss the importance of security awareness and training in maintaining a secure computing environment. Use resources like the Security Awareness Guide from the U.S. Cybersecurity & Infrastructure Security Agency to supplement the lecture.

- Explore different approaches and strategies for security awareness and training programs.
 - Explain the benefits of ongoing security education and training to address evolving threats.
 - Formative Assessment: After the lecture, include a short quiz on Moodle to assess students' understanding of security awareness and training.
2. **Case Study 4: Evaluating a Security Awareness and Training Program (Cognitive Presence and Social Presence):**
- Provide a case study that focuses on evaluating a security awareness and training program within a real-world organization.
 - Instruct learners to analyze the case study, assess the effectiveness of the program, and propose enhancements based on identified gaps.
 - Encourage learners to collaborate in small groups or engage in online discussions on Moodle to share their analyses, insights, and proposed program enhancements.
 - Formative Assessment: Ask students to write a brief report summarizing their findings and proposed program enhancements. This report can be submitted and graded on Moodle.
3. **Discussion: Legal and Ethical Considerations in Cybersecurity (Social Presence):**
- Conduct a synchronous or asynchronous discussion on Moodle on legal and ethical considerations in cybersecurity.
 - Prompt learners to share their perspectives on the impact of laws, regulations, and industry standards on cybersecurity practices.
 - Discuss the ethical dilemmas faced by cybersecurity professionals and the importance of ethical decision-making.
4. **Discussion: Exploring Emerging Trends in Cybersecurity (Social Presence):**
- Engage in an asynchronous discussion forum on Moodle to explore emerging trends in the field of cybersecurity.
 - Discuss the potential impact of emerging technologies on cybersecurity practices.
 - Encourage learners to share their insights, opinions, and predictions regarding the future of cybersecurity.
5. **Cybersecurity Tool: Exploring a Relevant Cybersecurity Tool or Emerging Technology (Cognitive Presence and Teaching Presence):**
- Introduce a relevant cybersecurity tool or emerging technology, such as multi-factor authentication or blockchain.
 - Discuss its implications for cybersecurity and its potential benefits and challenges.
 - Demonstrate how the tool or technology can be applied in real-world scenarios.

4 DISCUSSION

In the evolving landscape of artificial intelligence (AI), we find ourselves at a crossroads where the rich tapestry of perspectives intertwines with the intricate pathways of subconscious processes, fostering a vibrant discourse that navigates through the realms of education, technology, and the human mind. As we delve deeper into this narrative journey, we encounter the meticulous explorations of seasoned researchers and scholars, each offering a unique lens through which to view the complex world of AI.

Roger C. Schank, a luminary in the field, embarks on a deep exploration of the subconscious mechanisms that govern both human and computer decision-making processes. Schank challenges the conventional narratives in AI research that emphasize logical planning, advocating for a more realistic approach grounded in the richness and complexity of subconscious processes. He urges us to embrace the derivative nature of planning, where "new strategies are but variations of existing ones," offering a fresh perspective that encourages a shift from rational to a more realistic, subconscious approach to AI's approach to planning and decision-making [15].

Peter Stone, another renowned figure in the AI landscape, navigates through the intricacies of defining AI, advocating for a more expansive perspective that accommodates a rich tapestry of viewpoints and agendas. Stone resonates with a definition that paints AI as a discipline drawing inspiration from human

cognitive processes yet operating on a fundamentally different paradigm, fostering a vibrant and inclusive AI research landscape [16].

Looking deeper, we find ourselves oscillating between the deep subconscious landscapes explored by Schank, rich with analytical insights and vivid everyday examples, and the critical, grounded perspectives presented in the reflective critique, nurturing hopes for a future where fruitful collaboration between humans and technology is a reality. It is a discourse that encourages us to rethink established notions, to foster a learning environment grounded in critical thinking and authenticity, and to envision a future where the subconscious processes are not just understood but embraced in the rich landscape of AI research and education. This stands as a rich reservoir of insights, offering a detailed roadmap to foster a learning environment that is not just collaborative but globally connected and culturally inclusive. It is an ideal guiding towards a curriculum that is internationalized through the lens of connectivism, nurturing learners who are not just knowledgeable but are global citizens, ready to navigate the complex landscape of the interconnected world with a deep-seated understanding and a critical, analytical mindset.

As we stand on the cusp of a new era in AI, this discourse offers both a deep reflection on the current state of AI and a hopeful gaze towards a future of symbiotic relationships, grounded yet nurturing the seeds of potential. It is a trial-and-error journey that offers both a deep reflection on the current state of AI and a hopeful gaze towards a future of symbiotic relationships, grounded yet nurturing the seeds of potential, paving the way for a more promising future in AI through case-based reasoning [16].

5 CONCLUSION

As we establish the final remarks on this exploration of a 4-week course grounded in the philosophies of connectivism and the community of inquiry framework, it is pivotal to underscore the harmonious blend of theoretical knowledge and practical skills that it seeks to foster. This course is not merely a pedagogical construct; it is a well-spring of opportunities, a vessel for nurturing critical thinkers who are adept at navigating the complex, ever-evolving digital landscape with fortified understanding and a critical, analytical mindset.

This course encourages learners to delve deep into the realms of cybersecurity, fostering a rich environment of critical analysis and reflective practice. Through a meticulous merger of case studies, discussions, and hands-on experiences with relevant cybersecurity tools, the course provides a rich tapestry of learning experiences, encouraging learners to forge connections, collaborate, and construct knowledge through a networked learning environment.

Concerning mainstream artificial intelligence, it is imperative to foster a learning environment that is not just collaborative but also globally connected and culturally inclusive. This course hopes to serve as that example, steering learners towards a future where they are not just scholars in the theoretical realms of cybersecurity but critical thinkers and reflective writers, adept at articulating their reflections with eloquence and depth.

As we forge ahead, it is my hopeful aspiration that this course will sculpt learners who are not just consumers of knowledge but creators, ready to navigate the vibrant landscape of the 21st century with a critical mind and a hopeful heart; grounded in understanding and critical analysis.

REFERENCES

- [1] K. Cabaj, Z. Kotulski, B. Księżopolski, and W. Mazurczyk, "Cybersecurity: Trends, Issues, and Challenges," *Eurasip Journal on Information Security*, vol. 2018, no. 1, 2018. <https://doi.org/10.1186/s13635-018-0080-0>.
- [2] O. Zawacki-Richter and I. Jung, Eds., *Handbook of Open, Distance and Digital Education*. 1st ed. Singapore: Springer Singapore, 2023. [Online] Available: <https://doi.org/10.1007/978-981-19-2080-6>.
- [3] G. Siemens, "Connectivism: A learning theory for the digital age," in *International Journal of Instructional Technology & Distance Learning*, vol. 2, no. 1, pp. 1-9, 2005.
- [4] A. Apostolidou, "Digitally situated knowledge: Connectivism, anthropology and epistemological pluralism," **International Journal of Educational Research**, vol. 115, 2022. [Online] Available: <https://doi.org/10.1016/j.ijer.2022.102047>.

- [5] H. C. Yeh, S. Yang, J. S. Fu, and Y. C. Shih, "Developing college students' critical thinking through reflective writing," **Higher Education Research and Development**, vol. 42, no. 1, pp. 244–259, 2023. [Online] Available: <https://doi.org/10.1080/07294360.2022.2043247>.
- [6] E. Kweon, H. Lee, S. Chai, and K. Yoo, "The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence," *Information Systems Frontiers*, vol. 23, no. 2, pp. 361–373, 2021. [Online] Available: <https://doi.org/10.1007/s10796-019-09977-z>.
- [7] B. Kotzee and S. O. Palermos, "The teacher bandwidth problem: Moocs, connectivism, and collaborative knowledge," in *Educational Theory*, vol. 71, no. 4, pp. 497-518, 2021.
- [8] L. Chen and Y. Xu, "Theoretical Development of Connectivism through Innovative Application in China," in *Canadian Journal of Learning and Technology*, vol. 48, no. 4, 2022.
- [9] R. Vas, C. Weber, and D. Gkoumas, "Implementing connectivism by semantic technologies for self-directed learning," in *International Journal of Manpower*, vol. 39, no. 8, pp. 1032-1046, 2018. [Online] Available: <https://doi.org/10.1108/IJM-10-2018-0330>
- [10] B. I. Omodan, "Analysis of Connectivism as a Tool for Posthuman University Classrooms," in *Journal of Curriculum Studies Research*, vol. 5, no. 1, pp. 1-12, 2023. [Online] Available: <https://doi.org/10.46303/jcsr.2023.2>
- [11] L. Zhang-Kennedy and S. Chiasson, "A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education," in *ACM Computing Surveys*, vol. 54, no. 1, 2021. [Online] Available: <https://doi.org/10.1145/3427920>
- [12] L. Sussman, "Exploring the value of non-technical knowledge, skills, and abilities (KSAs) to cybersecurity hiring managers," in *Journal of Higher Education Theory and Practice*, vol. 21, no. 6, pp. 99-117, 2021.
- [13] H. Alturkistani and M. A. El-Affendi, "Optimizing cybersecurity incident response decisions using deep reinforcement learning," in *International Journal of Electrical and Computer Engineering*, vol. 12, no. 6, pp. 6768-6776, 2022. [Online] Available: <https://doi.org/10.11591/ijece.v12i6.pp6768-6776>
- [14] T. Riebe, J. Bäumler, M. A. Kaufhold, and C. Reuter, "Values and Value Conflicts in the Context of OSINT Technologies for Cybersecurity Incident Response: A Value Sensitive Design Perspective," in *Computer Supported Cooperative Work: CSCW: An International Journal*, 2023. [Online] Available: <https://doi.org/10.1007/s10606-022-09453-4>
- [15] R. C. Schank, "The computer's subconscious," in *Applied Artificial Intelligence*, vol. 23, no. 3, pp. 186-203, 2009. [Online] Available: <https://doi.org/10.1080/08839510802700219>
- [16] D. Monett et al., "Special Issue "On Defining Artificial Intelligence"—Commentaries and Author's Response," in *Journal of Artificial General Intelligence*, vol. 11, no. 2, pp. 1-100, 2020. [Online] Available: <https://doi.org/10.2478/jagi-2020-0003>