Integrating Andragogy Theory into a Multidisciplinary Curriculum to Achieve a Connected Program for a Doctorate in Cybersecurity

Andrew Hall
School of Technology and Innovation
Marymount University
Arlington, Virginia, USA
ahall@marymount.edu

Xiang (Michelle) Liu
School of Technology and Innovation
Marymount University
Arlington, Virginia, USA
xliu@marymount.edu

Diane Murphy
School of Technology and Innovation
Marymount University
Arlington, Virginia, USA
dmurphy@marymount.edu

***Abstract*—This Innovative Practice Full Paper presents a case study on constructing and implementing a connected program in the Doctor of Science (D.Sc.) in Cybersecurity at Marymount University. We adapted a connected curriculum framework to this professional doctorate program based on two overarching pillars: andragogy theory and a multidisciplinary perspective. We use an andragogical instructional methodology that follows a learner-centered teaching philosophy to promote professional and adult learner engagement. Furthermore, the D.Sc. program takes a multidisciplinary approach to bridge and integrate domain-specific silos such as technology and its evolution, risk management, legal compliance, human factors, machine learning, business impact, and more. This integration helps enhance students' knowledge in multiple disciplinary specializations, focusing on problem-solving skills across the various domains important in cybersecurity.**

Building on these two pillars, our connected program model integrates five dimensions of connectivity to connect 1) academic learning and research with the workplace, 2) research activities and research-related curriculum over time, 3) various disciplines related to real-world cybersecurity challenges, 4) students with each other, across phases and with alumni, and 5) students with research and researchers across multiple domains. This paper's primary contribution is to demonstrate an innovative andrological and connected approach to tackle the ever-changing cybersecurity threats by cultivating the next generation of cybersecurity leaders with both advanced technical and refined management skills. We further showcase the potential of externalizing this framework in other settings and discuss future research work.

Keywords—Cybersecurity, Multidisciplinary Design, Doctoral Students, Pedagogy, Adult Learning Theory

I. INTRODUCTION

A. The cybersecurity landscape

There is a steady stream of reports concerning data breaches and cybersecurity failures across various institutions, from the government to financial institutions to hospitals. When there appears to be a lull in reporting these latest cyber incidents, the discussion naturally turns to the skill shortage across the cybersecurity field. One of the latest analyses of the security of the cyber domain was detailed in the U.S. Cyberspace Solarium Commission report in 2020, where the overall conclusion is that we in the U.S. "are dangerously insecure in cyber" [1]. This extensive and high-level review of the state of cybersecurity in the nation documented the continuing need for more skilled workers and different approaches to protecting the nation, in government, and the private sector. Even with such increased attention and government funding, the skills gap or workforce shortage has not lessened.

The cybersecurity profession has continued to evolve. The central concerns of information technology and cybersecurity professionals are quickly becoming essential discussions across the highest levels of management, both for private industry and government. As conversations turn to the enormous challenges of attribution of our many attackers and the motivation of nation-state actors within the cyber realm, cybersecurity teams in government and industry are competing for resources. As risk-based discussions and optimal investment strategies [2] are designed to advise and recommend how much to invest, the fundamental problem remains to find qualified professionals to secure our country's critical cyber resources effectively.

B. Workforce Challenges

With today's multigenerational workforce and the continued evolution of the cyber realm, continuing education is critically important. It is a reality that traditionally educated employees from across the organization may be interested in, or required to explore, the discipline of cybersecurity. Blair et al. [3] describe the breadth of knowledge, skills, and abilities required within the cyber workforce and advocate for a multidisciplinary approach. Yoo et al. [4] explore the team nature of cybersecurity, and Margolis [5] explores multiple team membership providing ideas to consider when believing that we can list cybersecurity as an additional duty for employees across the organization.

Cybersecurity can be viewed as a science, an engineering discipline, or a part of the social sciences and thus may be of interest to a wide variety of the workforce. The education and training needs are pretty varied when considering accessing a workforce, from career changers inside your organization to the continual upskilling of information technology and security professionals to students interested in cybersecurity in the K–12 space. Henry [6] discusses some ideas relevant to creating educational programs designed to meet this skill shortage. Martin and Collier [7] further explore the elements of the domain that necessitate an interdisciplinary approach.

C. Challenges in Higher Education

The variety of roles within the global cybersecurity field argue for differential preparation as well as a holistic approach to create a cadre of graduates from our educational institutions ready to take the challenge of cybersecurity [8]. This is a global problem. Kim and Beuran [9] describe the considerations in establishing a master's degree program in Japan, and Austin and Lu [10] describe educational reform within China.

Additional challenges arise when looking to educate career changers and workers currently in the field, where there is a heterogeneity of background knowledge and experience. The tension between education and training, between certifications and formal academic credentials, only increases the difficulty for hiring managers to access the capability of those they are assessing to fill available positions [11].

These challenges and the desire for cybersecurity professionals to further develop their expertise have motivated the development of doctorate programs within cybersecurity. When a cybersecurity professional could have come from any of variety of undergraduate programs, and many had earned master's degrees before cybersecurity was recognized as a discipline, the signal of expertise from a terminal degree (doctorate) in cybersecurity is an intriguing opportunity. From the perspective of academia, the opportunity to create scholarly practitioners, prepared to educate, train, and mentor our students while serving as the next generation of guild masters, is equally attractive. Creating scholarly practitioners is our best chance to bootstrap the experience from within the community of practice and finally address the higher levels of the workforce gap.

D. Doctorate of Science in Cybersecurity Case Study

We will describe a case study of our university's Doctor of Science in Cybersecurity program implemented in Fall 2018: our attempt to develop scholarly practitioners for leadership positions in the cybersecurity field. We will address the overall structure of our program and our attempt to leverage the principles of a connected curriculum framework. We discuss our pedagogical approach drawn from adult learning theory, andragogy, and our multidisciplinary mission. We describe five dimensions of our connected approach and provide some lessons learned from the implementation of our program and producing our first cohort of scholarly practitioners.

II. The Primary Framework

A. Overall Approach

Contrary to traditional higher education models tending to focus on segmentations of functional disciplines and rely on a single pedagogical method, in cybersecurity, we need to bridge silos as well as to sustain focus on various missions and goals. One of the primary criteria for an educational institution's success remains to be the volume and impact of the research it produces [12]. Therefore, it is imperative for higher education institutions, especially doctoral programs to seek innovative approaches with their curricula and programs of study to achieve a balance between high-quality education and research. This section outlines the philosophical principles guiding us to create the doctoral program in cybersecurity, followed by an overview of Fung's [13] connected curriculum framework enlightening our educational strategy.

B. Bildung

The philosophical foundation for designing and developing our doctoral program draws on the core values of higher education with reference to the German term *Bildung*. The word means self-formation or development, stemming from the German tradition of self-cultivation and maturation through education [14]. It does not have an exact translation in English; the word implies transformation, emphasizing self-development and self-growth as 'action to create a self that is valuable' [15, p.305].

The primary goal of our doctoral program is informed by and well-aligned with the tenet of *Bildung.* The program emphasizes the intersection of technology, human factors, management, leadership, policy, and data science aspects of cybersecurity, focusing on working practitioners within the field. Since virtually all the students enrolled in our doctoral program are experienced working professionals, the key is to extend their knowledge base in an environment of scholarly inquiry of real-world situations, reflecting the changing nature of the maturing cybersecurity field. This goal embodies the fundamental characteristic of *Bildung,* which regards the nature of learning as 'unsatisfied with what it imagines it knows' [16, p.3] and remaining intellectually curious and open to new evidence and new perspectives.

C. *Pas de Deux*

It is a French term for a dance duet performing steps together. In the case of designing the cybersecurity program of study, research and teaching go hand in hand with synergies between various institutional mission statements, strategies, and consecutive goals such as broadening participation and lifelong learning. Building a sustainable doctoral program in cybersecurity requires the synergy and unity of both teaching and research, orienting towards continuous knowledge transfer and creation. The purposes of education, at its core, lie in that 'the teacher does not exist for the sake of the student; both teacher and student have their common justification in the common pursuit of knowledge' [von Humboldt 1809, cited in 14]. As stakeholders of the doctoral program, teachers, researchers, and students each participate in this endeavor from diverse backgrounds and with diverse expertise and research interests. Therefore, it is essential to foster healthy dialogues among students, faculty, researchers, and industry practitioners for common values, peer mentorship, and collaborative learning. Connecting research and education enables advancements of knowledge through research and empowers students to learn through research inquiry and enhanced practices.

D. *Outline of the Primary Framework*

We developed our D.Sc. in Cybersecurity program based, in part, on a six-dimensional framework created in [13]. The framework aims to promote dialogue and discussion among faculty members, students, and professional staff and to cultivate new ideas and opportunities for enhancing the quality of education and research in parallel. As shown in Fig. 1, the framework highlights the initiative of developing a connected curriculum as a 'research-education ecosystem' [13, p.8] in higher education to interconnect diverse people with different backgrounds and academia broader communities.

The six dimensions of the framework are enumerated as follows:

- **Connection between students and researchers**: this dimension fosters interconnections between researchers and students, introducing students to applied research projects based on real-world problems;
- **Connection between courses and relevant research projects:** this dimension requires a calculated roadmap in a program to enable students to experience a variety of learning activities throughout the program, including an extensive understanding of the process of evidence-based research;

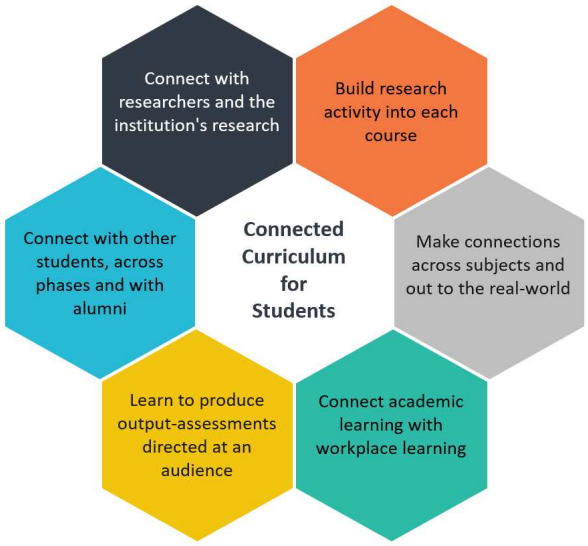

Fig. 1. The Connected Curriculum Framework (Adapted from [13])

- **Connection across subjects and disciplines**: the dimension promotes an inter-disciplinary program with emphases on global perspective and service to society in the protection of the nation and everyday lives in the digital world;
- **Connection between academic learning and workplace learning:** this dimension cultivates students to gain workplace knowledge in an academic environment and empower them to be a lifelong learner;
- **Connection between learning outcomes and targeted audience:** this dimension builds a pathway to reinforce experiential learning and college work experiences through skill-based internships and micro-credentials focusing on skills sought by industries;
- **Connections among students across phases and between students and alumni:** this dimension focuses on inclusive learning, creating a healthy environment for students from different backgrounds to network with one another.

III. Two Pillars

Underpinning the connected curriculum framework are two pillars focusing on adult learning and a multidisciplinary approach. This section discusses the rationale of adopting these two pillars in our D.Sc. program and illustrates the implementation with some use cases.

A. *Andragogy*

The continuum of teaching philosophies ranges from the subject-centric pedagogy to the learner-centric andragogy. The main principles of andragogy represent a shift from focusing on subjects to students [17] and include principles of creating community [18]. The teaching philosophy of andragogy offers a structure for cybersecurity education

combining the benefits of self-directed learners, students with substantial experience within their field, and students that are both ready to learn and explore applied research.

Malcolm S. Knowles revived andragogy in the study of philosophies of adult learning and has written a series of articles and textbooks developing his ideas [19]. The efficacy of the andragogy has been reviewed and debated [20]-[23] and has coalesced on an established set of principles [24]. The principles are the learner's need to know, the learner's self-awareness, the learner's prior experience, readiness to learn, orientation to learning, and motivation to learn [24, p.6].

Our doctoral students understand the importance of cybersecurity, and as for most of them, it is their current profession. However, we must programmatically include the rationale for transforming each of them into a scholarly practitioner. The combination of evolving self-concept as a learner and the variety of prior experiences in our courses align with andragogy concepts.

Most of our students are very ready to learn but must recognize the different learning styles required with a doctoral program. The transition of a student's orientation to learning towards immediate applications of knowledge is aligned well to our applied research methodology, more so than a purer research approach as in a Ph.D. program. We must consider the variety of motivations of our students when they join our program and their personal goals that they anticipate achieving within our program en route to a terminal degree.

B. Multidisciplinary Approach

We developed our D.Sc. in Cybersecurity program based on the multidisciplinary and ever-growing nature of the cybersecurity field. Within cybersecurity, individuals have a variety of work roles, academic backgrounds, and interests. Like the creation of operations research to address the issues of a world at war, the pervasive nature of the internet and our world's increasing reliance on digital connectivity has created multidisciplinary opportunities across multiple disciplines.

Cybersecurity is now recognized as much more than just an information technology problem. The critical issues of the field range from cryptography to human factors, from creating secure code to creating user interfaces that are both intuitive and secure, and from cyber awareness for everyone to law enforcement of cybercriminals. Papers addressing cybersecurity range from political science, international relations, and law to technical engineering papers from across the IEEE and ACM journals suite.

In addition, leaders within the cybersecurity field are increasingly required to interface with their CEOs and boards to advocate for the resources necessary to secure their organizations. As the tenants of cybersecurity impact the firm from finance to marketing to operations, specialists from across the organization must work together and develop teams whose expertise is well beyond what is possible to create in a single interdisciplinary educational program.

Network engineers creating the secure architecture upon which data will travel work alongside mathematicians and computer scientists employing methods as diverse as zero trust architectures, formal methods proofs of security, and post-quantum cryptography. Each of the disciplines fills a vital role on our cybersecurity team, and the inclusiveness of talent needs to be a cornerstone of the cybersecurity field. With this recognition of the diverse teammates needed, we aimed to create a multidisciplinary program that would be separate from a specialization in cybersecurity within another parent discipline. We aimed to develop scholarly partitioners that are prepared to work on and lead the cybersecurity teams of the future to protect our nation.

One of the critical elements of our successful multidisciplinary approach is the diversity of our students. We wanted to leverage the strengths of the adult learning models previously discussed to increase each student's exposure to the field's breadth and future roles. We also designed and developed our curriculum to address research methodologies and tools and the work roles across the National Institute of Standards and Technology (NIST) framework [25]. This exposure to both the new skills of the academic researcher and the variety of work roles that will be expected to supervise and lead provides a robust framework and scaffolding for the student to explore the multidisciplinary and evolving nature of the field.

IV. Constructing a Connected Program in Cybersecurity

We needed to reflect on opportunities as well as risks, and examine what an 'authentic' program of study requires within the intricate ecology of emerging challenges in technology, culture, and economy [26]. Unfortunately, many higher education programs are not able to keep abreast with this everchanging landscape in order to bridge gaps and disconnections across fragmented islands of functional disciplines [27]. We believe that curriculum renovation or innovation should not be only based on individual learning and narrowly formulated objectives [28]. Instead, the focus should center on building connected learning and research communities that empower both students and faculty members to extend their knowledge horizons and 'speak' through their scholarship.

We adapted the framework developed in [13] to construct a connected doctoral program in cybersecurity at a smaller, comprehensive teaching institution, focusing on addressing a critical skill gap, the management and leadership shortage in the current cybersecurity workforce. This section showcases the model we created as a multi-dimension, connected program supported by the two pillars: andragogy and multidisciplinary. The following section will demonstrate how we implemented such a connected program with more details.

Fig. 2 illustrates the framework underpinning the D.Sc. in Cybersecurity program. The core educational principle is that learning should be through research and critical inquiry, surrounded by five interconnected dimensions of practice. The two pillars of andragogical instructional methodology and

multidisciplinary approach further strengthen the connections and drive the organic growth of the program.

A. *Dimension 1: Connect academic learning and research with the workplace*

This dimension asserts that our D.Sc. program should enable doctoral students to integrate academic learning with the subject matter knowledge and skills needed for their professional work and the wider community. Three significant focuses are included here. First, the program focused on developing capabilities and dispositions to adapt to a changing world. Second, we focused on enabling the students to practice articulating the knowledge and understandings gained from the program to others in the workplace and students in the pipeline. Another focus was to engage students in professional and constructive conversations with others about the ethical application of cybersecurity problems and challenges to the community and society.

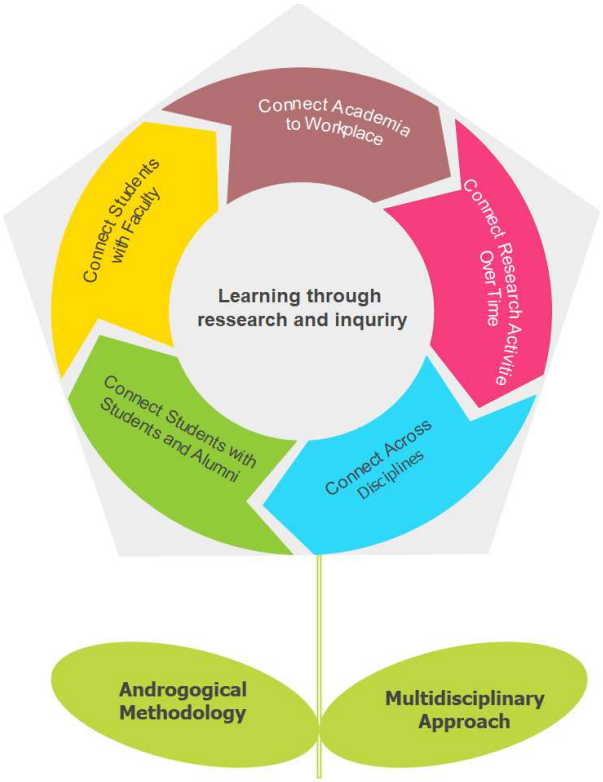

Fig. 2. A Connected Program Model

B. *Dimension 2: Connect research activities and research-related curriculum over time*

This dimension highlights the need to design the doctoral program curriculum so that students experience a connected sequence of research-related courses, projects, and learning activities that prepare them with the substantial expertise needed to undertake critical inquiries. The applied research nature of our program allows students to bring their cybersecurity expertise to the program and take their research results back to the workplace.

C. *Dimension 3: Connect various disciplines and the real-world cybersecurity challenges*

Even though specialized expertise remains vital, it becomes more and more critical for our students to be equipped with capabilities to adapt in a world full of uncertainties and complexities [29]-[31]. Further, cybersecurity is a multidisciplinary subject spanning across the bounds of a wide range of disciplines and domains such as management, information technology, human behavior, and law. We took the inherently multidisciplinary nature of cybersecurity into account when we structured the program to create opportunities for students to make conceptual connections between cybersecurity and other disciplines. By creating channels for inquiries about more than one discipline, our D.Sc. program empowers doctoral students with the breadth and adaptability [13].

D. *Dimension 4: Connect students with each other and with alumni*

This dimension aims to facilitate the collaborations between students and their diverse peers and promote a supportive community through various channels, including faculty advisor schemes or connecting with alumni. According to [13], the rationale behind this dimension of connection lies in that it promotes students' learning and particularly their critical thinking skills, creates a sense of belonging to a community, and fulfills the goals of education. The decision was made not to make the program "cohort-based" but to enable students across the program to take the knowledge-based courses together

E. *Dimension 5: Connect students with research and faculty within and across multiple domains*

As discussed in Dimension 3, cybersecurity research requires multidisciplinary knowledge and expertise. Therefore, it is essential to connect students with faculty within the program as well as from other disciplines. The program constructed a scalable mechanism for students to meet individual faculty researchers as their subject matter experts, mentors, or dissertation committee members. The program also provides numerous opportunities for students to gain better understandings of Marymount University's research focuses and other research relevant to their study. The students must also communicate their research findings to diverse audiences in subject-related, professional conferences or peer-reviewed publications.

V. IMPLEMENTING THE CONNECTED PROGRAM

The university has a long history of providing innovative cybersecurity education at the undergraduate and graduate levels, going back to 2008 [32]. Thoughts about instituting a terminal degree in cybersecurity began around 2015, resulting from feedback from students and alumni looking for a post-master's program in cybersecurity, explicitly focusing on qualifying for leadership positions in the field.

A. Selecting the Type of Degree

The first decision for the university to make was the type of terminal degree, given the target was working professionals, mostly already with a master's degree. Research showed that cybersecurity is generally considered an applied science, based on concepts in "computer science, mathematics, economics, law, psychology and engineering" [33]. This led us to the D.Sc. rather than the Ph.D. with the additional focus on the multidisciplinary nature of the field. Furthermore, applied research would enable our students to research real-world problems to solve practical problems, generate new knowledge, and foster improvements in current practices.

B. Program Design

We began by going back to students and alumni, now working cybersecurity professionals in industry and government. We focused on learning from individuals who had started other doctoral programs and who had not completed them. Most were ABD, all but dissertation, in Ph.D. programs. These individuals stressed their general dissatisfaction with all the coursework before beginning their research and courses not being connected to the research itself. They felt a lack of community between the students in their programs and between faculty and students. Most importantly, they thought that the research faculty lacked respect for the cybersecurity knowledge they had learned from years of experience in the front lines of cybersecurity in government and the private sector, even though many of them were now long-term adjuncts in community colleges and universities.

Following the discussions, our faculty conducted extensive research on teaching styles, particularly andragogical techniques that would maximize the educational strategy for adult learners with extensive work experience and background knowledge. As a result of this research, the program design included recognition that collaboration was essential to the andragogical paradigm. Students' research should begin in a collaborative environment until the students and their Committee Chairs were confident in their research design and could successfully conduct the research.

We also recognized that our students were entering the program with an existing cybersecurity knowledge base and often wanted to extend that valuable expertise through research. Consequently, we had to ensure that we had faculty to handle their topic area during the admissions process.

The connected program framework allows students to begin their research earlier in the program, maybe from day one. They take topic courses in parallel with research courses based on a degree plan supported by the multi-dimensional connectivity of the program. The goal is to enable a seamless integration of subject-matter-related knowledge with the students' research topic and research methodology.

C. Post-Master's Program Design

These design principles, focusing on andragogy, multidisciplinary, and connectedness, led to the following three-pronged structure where each prong was taken in parallel.

Students must take six knowledge-based courses selected by the student to extend their current knowledge and support their research or workplace in the first prong. Courses might include machine learning, risk management, malware analysis, emerging technology security, cyber threat intelligence, law and policy development, cloud computing, and others. The inquiry-based courses can be taken in any order, including group work and smaller research projects, often leading to conference presentations and publication. Students get exposed to students in all phases of the doctoral program, assisting with the sense of community and an essential part of the andragogical approach. A student in their first semester may be learning alongside a student in their fourth semester who is much further along in their research process and can provide advice and guidance to the new student.

In the second prong, students take six research courses. The first four scaffold the students collaboratively through the research process – higher-order thinking, literature reviews, research method, and proposal preparation – and can begin as early in the program as the student feels comfortable. As students build their research strategy, they get feedback from other students, some of whom may be very familiar with the applied research topic. The remainder two courses are self-study under the auspices of their selected committee chair.

In the third prong, we emphasize collaboration and community. Students must achieve candidacy before taking the last two one-on-one research courses. They must have contributed at least 18-hours of community service to the cybersecurity profession. This can be achieved in any number of ways, including organizing events for the campus community, such as a cybersecurity competition for undergraduates, or mentorship for students at the undergraduate and master's level, or organizing a professional event for a professional organization. This requirement increases the connectedness with the university and the upcoming cybersecurity workers that they will manage in the future. The second requirement is for at least one external-facing presentation or publication, beginning the credentialing process for the student.

D. Initiating the Program

After approval by the university's multi-tiered curriculum approval process and by our accrediting body, SACSCOC, the program began in Fall 2018 with a class of 24 students. It has grown to over 100 students as of Spring 2021. In general, the program is very diverse, with about 60% from underrepresented minorities, around 30% female, and representatives from a broad age group with students in their twenties to students in their sixties. Interest in the program has been high with students applying from across the country with various backgrounds, including military, intelligence agencies, civilian agencies, and a whole array of businesses from cloud service providers, social media companies, manufacturers, insurance companies, and academia.

Most importantly, the research topics selected by the students have been very diverse, from the very technical to the social aspects of cybersecurity. Completed dissertations include research on intrusion detection and prevention, cyber diplomacy, election security, metrics to measure security effectiveness, cybersecurity in non-for-profits, the dark web, and the cybersecurity workforce, to name a few. These dissertations are published in Pro*Quest.

E. Lessons Learned

The program has proved exciting for both faculty and students but a significant workload for the faculty. We are very connected with the students and have created a culture of collaboration between faculty and students and students with other students in the doctoral program. Maintaining this high level of connection and the increased teaching load has resulted in the need to add more faculty to the school.

The transition from the cybersecurity workplace to evidence-based research requires a significant amount of instruction in the first research course. We have used a number of strategies to emphasize the tenets of academic research early in the sequence of research courses. A detailed handbook has also been developed.

Academic writing, in contrast to business writing, has proven to be an unexpected issue. To reduce the load on faculty, a writing specialist joined the team and was able to give one-on-one assistance to doctoral candidates, particularly in the final stages of the dissertation process. She was also instrumental in providing additional encouragement to the students as they neared completion.

Many of our students are managers in the cybersecurity field. As such, their studies have been interrupted because of the nature of their positions and the increasing number of cyber incidents. As a result, we have added 1-credit extension courses to the last three research classes to allow them extra time to meet the program requirements.

Finally, through a grant from the National Science Foundation (Award number 1927550), an optional teaching component was added to transition students into academia. Doctoral students obtain formal teaching instructions from our education faculty and are incentivized by tuition reimbursement to teach at any level. While many of our doctoral students teach as adjuncts, they have never received any academic teacher training such as developing an effective syllabus, writing good assessments, etc. Several candidates look to full-time faculty positions upon graduation or in the future, such as on retirement from government service.

VI. Conclusion

The cybersecurity workforce needs additional skilled personnel, from the technician to the cybersecurity leader to the teacher. This program is successfully developing a cadre of scholarly professionals to become leaders and teachers in this expanding field. We have a diverse set of students, and as of Spring 2021, alumni who have extended their knowledge and expertise. We have engaged the students by combining two strategies: andragogy and multidisciplinary with a connectedness strategy.

The authors acknowledged the limitation of this study as it is based on anecdotal data due to the fledgling stage of the program. As the program becomes more mature, a summative evaluation will be conducted to collect and analyze data more systematically and rigorously. Another research direction is to examine the generalizability of our connected program framework in a different department or discipline. For example, can this connected program model work in other doctoral programs? In Fall 2021, the university will use the same strategies to implement a Doctor of Business Administration (DBA) in Business Intelligence, which provides an ideal setting to examine the external validity of the connected program.

References

[1] United States Cyberspace Solarium Commission, "The Cyberspace Solarium Commission Report," 2020. [Online]. Available: https://www.solarium.gov/report

[2] L. A. Gordon, M. P. Loeb, and L. Zhou, "Investing in cybersecurity: Insights from the Gordon-Loeb model," *Journal of Information Security,* vol. 7, no. 02, pp. 49-59, 2016, doi: 10.4236/jis.2016.72004.

[3] J. R. S. Blair, A. O. Hall, and E. Sobiesk, "Educating Future Multidisciplinary Cybersecurity Teams," *Computer,* vol. 52, no. 3, pp. 58-66, 2019, doi: 10.1109/MC.2018.2884190.

[4] C. W. Yoo, J. Goo, and H. R. Rao, "Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness," *MIS Quarterly,* vol. 44, no. 2, pp. 907-931, 2020, doi: 10.25300/MISQ/2020/15477.

[5] J. Margolis, "Multiple Team Membership: An Integrative Review," *Small Group Research,* vol. 51, no. 1, pp. 48-86, 2020, doi: 10.1177/1046496419883702.

[6] A. P. Henry, "Mastering the cyber security skills crisis" in *Cyber Security Education: Principles and Policies*, G. Austin Ed., 1st ed.: Routledge, 2020, ch. 2, pp. 29-55.

[7] A. Martin and J. Collier, "Beyond Awareness: Reflections on Meeting the Inter-Disciplinary Cyber Skills Demand," in *Cyber Security Education:Principles and Policies*, G. Austin Ed., 1st ed.: Routledge, 2020, ch. 3.

[8] J. R. S. Blair, A. O. Hall, and E. Sobiesk, "Holistic Cyber Education," in *Cyber Security Education: Principles and Policies*, G. Austin Ed., 1st ed.: Routledge, 2020, ch. 10.

[9] E. Kim and R. Beuran, "On designing a cybersecurity educational program for higher education," presented at the Proceedings of the 10th International Conference on Education Technology and Computers, Tokyo, Japan, 2018. [Online]. Available: https://doi.org/10.1145/3290511.3290524.

[10] G. Austin and W. Lu, "Five years of cyber security education reform in China," in *Cyber Security Education: Principles and Policies*, G. Austin Ed., 1st ed.: Routledge, 2020, pp. 173-193.

[11] CISA, "Cybersecurity Talent Identification and Assessment "Cybersecurity and Infrastructure Security Agency 2019. [Online]. Available: https://niccs.cisa.gov/sites/default/files/documents/pdf/cybersecurity%20talent%20identification%20and%20assessment.pdf?trackDocs=cybersecurity%20talent%20identification%20and%20assessment.pdf

[12] M. Healey, A. Jenkins, and J. Lea, *Developing Research- Based Curricula in College- Based Higher Education*, York, UK: The Higher Education Academy, 2014. [Online]. Available: https://www.advance-he.ac.uk/knowledge-hub/developing-research-based-curricula-college-based-higher-education.

[13] D. Fung, *Connected Curriculum for Higher Education* 1st ed. London, England: UCL press, 2017.

[14] K. J. Morgan, "Where is von Humboldt's University now?," *Research in Higher Education-Daigaku Ronshu,* vol. 42, March 2011, pp. 325-344, 2011. [Online]. Available: https://ir.lib.hiroshima-u.ac.jp/files/public/3/31450/20141016181556308145/DaigakuRonshu_42_325.pdf.

[15] K. Schneider, "The Subject- Object Transformations and Bildung," *Educational Philosophy and Theory,* vol. 44, no. 3, pp. 302– 311, 2012.

[16] P. Fairfield, Ed. *Education, Dialogue and Hermeneutics*. London: Continuum, 2012.

[17] I. Stephen Paul Forrest and T. O. Peterson, "It's Called Andragogy," *Academy of Management Learning & Education,* vol. 5, no. 1, pp. 113-122, 2006, doi: 10.5465/amle.2006.20388390.

[18] N. Note, F. De Backer, and L. D. Donder, "A Novel Viewpoint on Andragogy: Enabling Moments of Community," *Adult Education Quarterly,* vol. 71, no. 1, pp. 3-19, 2021, doi: 10.1177/0741713620921361.

[19] M. S. Knowles, E. F. Holton, R. A. Swanson, and P. A. Robinson, *The Adult Learner: The Definitive Classic in Adult Education and Human Resource Development*, 9th ed. Routledge, 2020.

[20] J. A. Henschke, "Considerations Regarding the Future of Andragogy," *Adult Learning,* vol. 22, no. 1, pp. 34-37, 2011, doi: 10.1177/104515951102200109.

[21] M. Tennant, "An evaluation of Knowles' theory of adult learning," *International Journal of Lifelong Education,* vol. 5, no. 2, pp. 113-122, 1986/04/01 1986, doi: 10.1080/0260137860050203.

[22] V. McGrath, "Reviewing the Evidence on How Adult Students Learn: An Examination of Knowles' Model of Andragogy," Adult Learner: The Irish Journal of Adult and Community Education, pp. 99-110, 2009.

[23] A. Hartree, "Malcolm Knowles' Theory of Andragogy: A Critique," *International Journal of Lifelong Education,* vol. 3, no. 3, pp. 203-210, 1984.

[24] J. Mews, "Leading through andragogy," *College and University,* vol. 95, no. 1, pp. 65-68, 2020.

[25] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," 2018. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.04162018

[26] M. Van der Steege, "Introduction," in *Visionary leadership in a turbulent world: Thriving in the new VUCA context* M. Van der Steege *et al.* Eds. Bingley, United Kingdom: Emerald Publishing, 2017, pp. 7–24.

[27] H. Demirkan and J. C. Spohrer, "Cultivating T-Shaped Professionals in the Era of Digital Transformation," *Service Science,* vol. 10, no. 1, pp. 88-109, 2018. [Online]. Available: https://doi.org/10.1287/serv.2017.0204.

[28] W. F. Pinar, *What is Curriculum Theory?*, 2nd ed. New York: Routledge, 2012.

[29] A. K. Killion *et al.*, "Preparing the next generation of sustainability scientists," *Ecology and Society,* vol. 23, no. 4, 2018.

[30] R. Klaassen, "Disentangling the different layers of interdisciplinarity," *Journal of Science Communication,* vol. 19, no. 4, p. C03, 2020.

[31] C. Lyall, L. Meagher, J. Bandola, and A. Kettle, "Interdisciplinary provision in higher education: current and future challenges," Higher Education Academy, York, UK., 2015. [Online]. Available: https://www.advance-he.ac.uk/knowledge-hub/interdisciplinary-provision-higher-education-current-and-future-challenges

[32] A. Bicak, X. Liu, and D. Murphy, "Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program," *Information Systems Education Journal,* vol. 13, no. 3, pp. 99-110, 2015. [Online]. Available: http://isedj.org/2015-13/

[33] J. Dawson and R. Thomson, "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance," *Frontiers in Psychology,* vol. 9, 744, 2018, doi: 10.3389/fpsyg.2018.00744.