Bringing the Industry Partner to the Cybersecurity Education Table as an Active Participant

Randy J. Hinrichs
University of Washington
Seattle, WA
avatar@uw.edu
0000-0002-8636-0319

Viatcheslav M. Popovsky
University of Idaho
Moscow, ID
slava@endicottconsulting.com

Barbara Endicott-Popovsky
Portland State University
Portland, OR
endic@pdx.edu
0000-0002-8700-0358

***Abstract*—The University of Washington (UW) published their pedagogical model for Cybersecurity Education – the Kuzima-Bespalko-Popovsky (KBP) model. In 2005, the National Center for Academic Excellence in Cybersecurity certified the status of NCAE-CR based on the tight pairing to the Knowledge Units (KUs). The KBP model aided in maintaining the quality of the instruction. The original KBP model goals are reviewed here and the changes to those goals are explained. The model provided a solid public – private partnership engagement model. Industry professionals from the field taught the NIST / NICE KSAs and provided real-time experience, contributing to the curriculum's resiliency. We modified our competency assessment from the World of Work Inventory (WOWI) assessment test to the CYBERGenius.IQ, integrated industry-based CERT material for scalability, and created a certified student collaboratory to manage continuing education post-graduation into the job.**

Keywords—KBP Model, Cooperative Learning, CyberGENIUS.IQ, NCAE-C, KSAs, NIST, collaboratory, resiliency, human factors in cybersecurity, ontology. NIST/NICE Framework

I. INTRODUCTION

In Spring 2015, CISSE published a Conceptual Foundation for the University of Washington's Center of Academic Excellence in Information Assurance Education [1]. This present article explores the application and sustainability of the Kuzima-Bespalko-Popovsky (KBP) pedagogy by demonstrating acceleration in cybersecurity education in the Pacific Northwest, including Washington, Oregon, Idaho, Montana, Colorado, and Hawaii through a cooperative learning model.

An NSA National Center in Academic Excellence - Cybersecurity (NCAE-C) education grant funded the original course development for a course based on the KBP Pedagogical Model [2], including a Teacher Training Module and a resiliency model for critical infrastructure. The courses certified UW as a NCAE-C in Cybersecurity Education. Taught today at the University of Washington, Professional Continuing Education, the Certificate in Risk Management is designed for professional development for cybersecurity practitioners. The program combines both technical and human factors, cooperation with industry, cybersecurity competency assessment, and mentor models collaborating with outside partners.

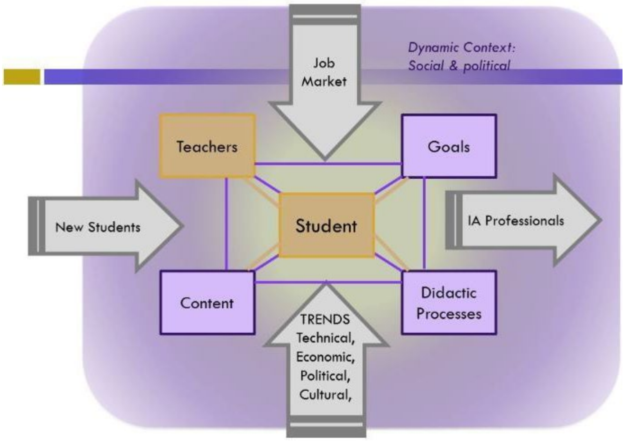
Job Market
Dynamic Context: Social & political
Teachers
Goals
New Students
Student
IA Professionals
Content
Didactic Processes
TRENDS Technical, Economic, Political, Cultural,

Fig. 1. The KBP model as a System

II. PROBLEM STATEMENT

How do we scale the model shown in Fig 1: The KBP model as a system? Teachers, content, trends, and didactic processes need to adapt to student goals and learning pathways while maintaining the baseline requirements for NCAE-C certification. Goals must be aligned to knowledge, skills, and abilities. Assessment must speak the language of cybersecurity competency and pair to an agreed ontology. The NIST/NICE Framework is a connective tool for aligning talent discovery to job placement. Content must adjust to the vocabulary as technical, economic, and political trends affect cybersecurity mastery. Cultural blind spots must also be explored to leverage value sensitive cybersecurity design. Industry needs students to come to the job with repeatable outcomes for attaining proficiency in their system, and their need to come with a passion and system for learning.

III. APPROACH

We will review the 2015 KBP Model and the Certificate in Risk Management for Cybersecurity Professionals at the University of Washington by doing a gap analysis. We will also explore the three modifications made to the course to increase scalability: targeted cybersecurity assessment, pedagogical immersion, and creating an agora for student certificate bearers to increase collaboration and engage in continuous cybersecurity education.

IV. METHODOLOGY: PROVING THE MODEL

The system-activity approach characterized the 2015 pedagogical model as:

A. *Social Learning or Activity-based learning*. The approach involves industry, academia, and government communities.

B. *Professional Development*. Students learn from every resource, narrowing the scope to an area of expertise.

C. *Cybersecurity Knowledge is a Tool*. Standards, compliance, techniques, processes, technology are all tools to critically analyze problems and their solutions. Critical thinking and problem solving determine competency.

D. *Self-Efficacy*. Students need to learn individually and as individuals within groups.

E. *Pedagogical efficiency*. Student success is measured by contributions to science and industry.

V. GAP ANALYSIS

In 2015, the UW-PCE Certificate in Cybersecurity Risk Management launched a three-course certificate program mapping to the NSA KUs. The course focused on WOWI career assessment, career development, using rules and tools in a model to solve competency-based problems, thinking like a CISO, and creating relevant work products. WOWI Career Assessment uses comprehensive scientific techniques to incorporate career interests, work related skills and work styles to find the best career matches.

The KBP Model reinforces the original three values.

1. Learning occurs through productive activities developed in partnership with the community, academic researchers, and industry.
2. Emphasis is on student professional development and motivating students to learn more from every resource.
3. Knowledge is treated, not as the end goal of the educational process, but as a tool to solve practical, complex problems, creatively and independently, unleashing the learner’s potential.

“The WOWI is designed to provide an assessment of three major considerations in vocational counseling, planning, and career decision making: interests (Career Interest Indicators), aptitudes-abilities, and temperaments (Job Satisfaction Indicators). Combining these three types of information into one system is the greatest accomplishment of the system's developers” [3].

Activities and discussions are designed from a contextual view – the student is placed in a problem-solving learning environment with events offered in a linear progression to teach fundamentals. Each student explores individual goals based on the WOWI, and delivers portfolio assets, and a year-end capstone that combines both the baseline KSA knowledge required, and the career development knowledge explored during assessment and application. Students study how professionals apply rules and tools and develop reference architectures and assessments in their organizations. Students engage in collaborative policy development, incident response planning, tabletop exercises in critical infrastructure, and case studies to practice methods and techniques.

The question of how well the students engaged in the materially asynchronously became a concern.

Industry-based materials from EC-Council teach network defender essentials, ethical hacking attacks and countermeasures, and digital forensics essentials to investigate and redress. The EC-Council materials were added in 2020 to allow for relevant content that rounds out the student. Students are expected to develop both the people and technical side to ensure cross fertilization.

Leveraging industry developed content enhances the student experience with strong visualizations that update as the technology changes. Our use of EC Council material engages industry in scaling content development while providing professional quality learning materials setting student expectations for professionalism. The integration creates a nice balance between the Human Factors side of cybersecurity education with the supplement of the technical side.

Students work on this material alone as well, causing us to pause again for whether the students are being made breach ready as originally intended.

The integration addressed the content scalability.

Quarter 1: Information security and risk management in context (CISO Perspective, the law, regulation, policy writing, incident response plan, and defining a project with a customer).

Supplemented with Network Defense Essentials and labs, NIST SP 800-series, the Cybersecurity Capability Maturity Model, introducing access control protocols, network performance controls, physical security controls, technical security, virtualization, wireless fundamentals, IoT devices, cryptography, security concepts (data encryption, data loss prevention, backup concepts), network traffic monitoring.

Quarter 2: Building an information risk management toolkit (assessing risk, quantitative/qualitative models, applying the incident response plan, running, and participating in a tabletop).

Supplemented with EC-Council Ethical Hacking Essentials, and labs for wireless security, BYOD Risks, mobile attacks, IoT attacks, cloud computing attacks and penetration testing strategies and phases.

This model is scalable because it can integrate any industry-based course content. The CyberAlumni student group was instrumental in choosing this material for the yearlong opportunity to finish the content, get evaluated, and receive the Essential Skills series certificate.

Quarter 3: Designing and executing information security strategies (examine case studies to prepare for consultation, digital forensics, and assessments of organizations).

Supplemented with Digital Forensics Essentials, introducing indicators of compromise (IoCs), readiness planning and business continuity, forensic investigation process and anti-forensic techniques.

Students use a mixture of NCAE-C approved course material (videos, exercises, discussions, readings, learning objectives, rubrics) and industry CERT based content for technical deep dives and cyber ranges. The courses use a Massive Open Online Course (MOOC) style asynchronous model to deliver baseline cybersecurity educational instruction. Videos are four to six minutes long. Reading is paired with learning objectives. Discussion groups encourage students to collaborate in problem solving. Faculty is semi present and accessible for extended hours based on night scheduling. Grades are numbered with x out of y points. Students must achieve 80% to pass.

The underlying videos, activities, readings, and project assignments remain the same year after year. We leverage the discussion sections of Canvas to encourage students to identify their special interests. Other students post web pages and papers for students to follow up on. A Class Commons page encourages students to find great articles, news, new rulings, or other relevant, contextual information. Students must comment on postings and give relevant information for other students to trace back to course goals.

Students choose their own projects and may partner with an outside organization to complete a relevant task. Students can work their project through Canvas collaboration technologies, or rely on well-known alternatives: Teams, Discord, Slack. The objective is to lighten the cognitive load by using familiar tools that allow for communication, collaboration, storage, and discovery.

A. Gaps Identified

Like the OpenCourseWare project at MIT, content availability was a great concept for scaling on-line learning. However, after several years of deployment, the general conclusion was that effective asynchronous models needed human interaction for transferable learning to happen. Social learning must be deployed [5].

Although we increased stakeholder contact with the students, both faculty and industry relationships are restricted to short meetings. Students partner with industry for projects, but once the project is viewed in the capstone, the content stalls and the mentors often return only for the final presentation. Trying to figure out how to increase face time with luminaries is not an easy task for a student.

Even though we built professionalism into the course through the assignments, feedback is limited and does not connect to usable job placement. The need to create an environment of employability needs to flow from student selection to employer modeling, into relevant work product that is defensible in real cybersecurity work experience.

Treating content as a tool remains a strong competency for this risk assessment certificate, however increasing the content for individual students is a challenge. Self-efficacy [6] is a value for the course and a well-remembered one in moving forward into industry. But students need models to become truly self-efficacious. So, scaling mentors has been identified as a key gap area that we could work on. Students need to be guided by their mentors to link concepts and make intuitive applications. Yet, our faculty members are working faculty and the ratio of time to student is reduced.

Looking for or creating a mentor network, or Mentor.NET is an appreciable outcome. Scaling apprenticeships and internships into an algorithm that follows from in-course work can produce a menu driven experience for the students, so they learn what they need to learn based on their competencies and attitudes.

Measuring course effectiveness with industry and science contributions remains unaddressed. The pedagogical values established by the KBP model are sound, but the follow through the pipeline is not realized. Communication with the students drops off. In a world of connected social media, LinkedIn, Slack, Zoom, we can address these gaps directly with technological and pedagogical interventions.

VI. GROWING THE MODEL

A. Targeted competency assessment

The five KBP elements introduced in 2015 remain the same, but integrating various programs and learning environments on the cloud may accelerate outcomes and shorten workforce gaps. Using private public partnerships that align learning goals with employability goals is leverageable today. The KBP model is organic and represents how to manage the ambiguity and rate of change in industry. In the model, when one item changes in the model, all other items systemically adjust. Endicott suggests that “By continuously updating descriptions of these elements, curriculum is kept current ensuring that students remain competitive [4]”.

Since 2015, we changed from the WOWI competency assessment to a full Haystack assessment known as CyberGENIUS.IQ [7]. The WOWI assessment was too general, testing public service, science, engineering, business relations, managerial roles, the arts, media design and administrative support. The Haystack CyberGENIUS.IQ uses NIST/NICE workgroup roles and reports them against a backdrop of cognitive capabilities in critical thinking, initiating creatively solving problems, responding to anomalies, performing real-time scans and interpretation of quick events, and examining exhaustive thinking for system processing.

Since the NCAE-C materials and the EC-Council Essentials materials are designed for NIST/NICE workgroup roles, a nice flow between elements prevails. And, because the employer models are beginning to leverage NICE standards, strong AI software integration shows promise in making a cloud-based curriculum to perform a variety of functions, eventually teaching itself to solve new problems. This flow enables the ability to snap other modules, or other content specialists in and out of the model.

Using the CyberGENIUS.IQ with NICE based and SCORM based content allows us to develop an algorithm for creating learning pathways. Test scores initially fall within quadrants. Quadrants are aligned with work roles. Quadrants include Offensive and Defense Operations, critical for cybersecurity placement. As cyber requires both human factors and technical expertise, the quadrants place for Design + Development and Analysis + Forensics. The cognitive classifications parse to a NICE Framework Category. The student's learning management team, then guides the student to select a NICE Framework Category.

The NICE Framework offers the student categories with overarching qualifiers. The Categories include action-oriented context. Analyze, Collect and Operate, Investigate, Operate and Maintain, Oversee and Govern, Protect and Defend, Securely Provision. Learning objectives are written based on these specialty area definitions. The customized learning objectives centered specifically on individual students represent their personalized learning pathway.

An example category is Protect and Defend: identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks. [8]. These categories further divide into specialty areas. one being Cyber Defense Analysis. Use of common language, active listening, and reflective statements are the techniques used by the learning management team to zero in on specialty areas. The student commits to one or two work roles. Here, there is only one Cyber Defense Analyst.

Working with the learning management team (the faculty, mentors, TAs, and others), students then choose the Knowledge, Skills, Abilities, Tasks and Capabilities into a learning pathway. The student finds discrete Knowledge line items and matches them to EC-Council Material that is aligned to specific curriculum blocks, and cyber range activities.

If any industry-based CERT organizations have completed the pairing of their content modules to NIST / NICE categories and has completed the mapping at a granular level, the model of integrating academic content with industry-based content becomes procedural. So other CERT programs can integrate with academic programs, creating regional programs.

Deriving a pathway currently is an analog process, students apply for programs, they begin an area of study, they are evaluated through activities and experts. In this model in Fig. 2, we use NIST/NICE standards to identify competency. The student is the object we choose to protect in our model, in other words, we minimize the content pathway and match their passion and ability to achieve their goal using the Cybersecurity Framework and supportive. NIST/NICE tools: Workforce Framework for Cybersecurity and the Cyber Career Pathways Tool for understanding the complex relationships between roles.

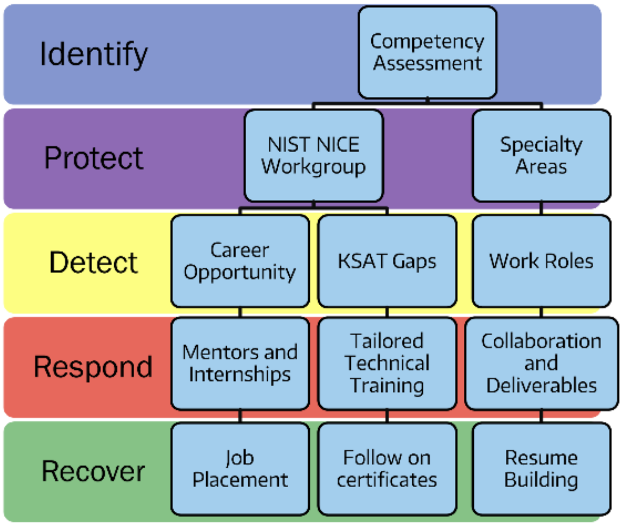

Fig. 2. Deriving a learning pathway

Using the Cybersecurity Workforce Framework to drive a pathway is useful. In serving a learning pathway, the CyberGenius.IQ assessment test places the student in a quadrant: Defense or Offensive Operations, with other quadrants Design and Development, or Analysis and Forensics. The determination allows the learning management team to work with the student in choosing a workgroup, and a specialty area and different pathways. The goal setting process helps place the student in a NICE Framework category, a work role, and then a list of knowledge (K: 0301, 0339), skills (0025), abilities (0128, 1059), tasks (0023) and capabilities (CL/I - continuous learning, intermediate), allowing the student to customize their learning specifically. In discrete goal setting, the learning management team can identify specific, customized learning objectives and pair them to content that has been tagged with KSA metadata as well.

Automating this algorithm and workflow is a viable direction for this research.

Storing grades, competencies, cyber range pathways, webinars, certifications, and experience into a cloud-based learning employment record (LER) is a missing link. Certain organizations are creating LER wallets that are based on NIST / NICE classifications. Integrating such a tool could represent the student in a cybersecurity specialty score and allow AI based employment software to pick up the student pathway and align it with discrete content and outcomes.

B. *Immersion*

The pandemic worked as a forcing function to energize the KBP pedagogy to thrive over the cloud. Since students had to stay home, they had to rely on video and on-line learning to communicate. They also had to figure out how to replace the dynamism of the classroom, the library, and the labs. Students had to do more than read documents, ruminate in discussion groups, and work on projects in collaboration sites, like Google Docs. Students needed to build strategies for increasing their interaction models. We refer to that experience as immersion. How do you augment an environment like Canvas to increase immersion?

Immersion is a state in which the user is engaged in an on-line learning environment that results in an increase in the state of flow. Instructional designers engage students with activities that capture their attention, and maintain their attention, increasing concentration on a task. When the student is in a state of flow, their goals and learning outcomes are clear to them, and they speed up and slow down to keep the pace of their flow.

Language learning in a foreign country demonstrates the flow state well. When a person is in a country learning a language, there are many implicit cues in the environment. Students see signs, hear people talking, watch people in context as they point and bring meaning into conversation through body gestures.

The longer a student remains in a country, the effortlessness and ease of communication begins to grow exponentially. The student learns intrinsically satisfying their individual needs and balancing between the challenge of everyday interactions with an increased language proficiency in tackling the challenges. The students' actions and awareness are merged, and they lose the state of self-conscious translating. The student feels control over the communication and language tasks they need to leverage to get things done.

Almost every learning task requires vocabulary acquisition and context for using the right words in the right place at the right time. Thinking of how students get immersed in cybersecurity can be done by creating an immersive learning environment that reproduces working in a cybersecurity environment. This can be done through environments like Canvas, Zoom, Teams, or even virtual reality environments.

In Fig. 3 we present a model for immersive cybersecurity education. Increasing one's presence in an on-line learning environment requires techniques that make the participants sense they are in the same place. Synchronous Zoom events create the sense of presence. Sharing the screen, and seeing where another user is working in a spreadsheet, or a doc, or showing a video editing session increases presence.

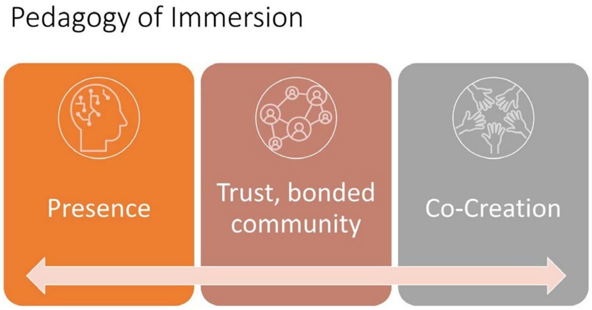

Fig. 3. Pedagogy of Immersion

Seeing each other in video is more perceptual than cognitive, as the video images help the user to imagine a classroom, with the ability to watch other people's reactions. Learning how to set up the screen is critical in these environments. Students have to put their chat on one side of the screen, and maintain the video in a panel format to watch facial expressions. Students can move around the video faces to position talkers together. Students must learn to effortlessly share screens, and get the users's attention with their cursor, or other graphic components.

Working with mentors and apprentices increases a sense of presence for students [10]. Students focus on creating a keen sense of presence in the virtual environment and build their identities and reputations by demonstrating increased attention and keeping in flow. Communication cues such as answering questions immediately, recognizing hand raising, creating comprehensive chat entries that create a narrative are key to increasing presence.

Students build a trusted, bonded community by sharing components of the work to form a greater whole. Students work together in shared writing docs, real time. They manage timelines, Gantt charts, and other visualizations connecting them in teams. Multiple projects allow teams to thrive in distinct groups, bringing their interests to the fore with Q&A, other times, completing a real-time task like inserting a graphic in a document. Students working together in collaborative environments increases their trust to get things done simultaneously, and take accountability for the final outcomes. Positive social interactions that depend on trust and accountability engender bonding.

Immersion requires co-creation. If students lurk in immersive environments, they lose their relevance to the groups. We co-create projects purposefully so students must work together to finish a product and share accountability for its quality and timeliness.

Each quarter the students have a quarter end deliverable; first quarter, students produce a 3–4-minute video on the area of cybersecurity identified through the competency assessment; second quarter, students participate in a live tabletop exercise, with after action reporting and mitigation strategies to improve their incident response plans. Third quarter is a forensic analysis of cases experienced by the teaching professionals or Q&A consultants during live webinars. Co-creation in context locks in trusted bonding.

If students do not build up models of interaction in an immersive environment, understanding what creates presence, community and accountability, they may find that being in highly productive environments that rely on collaboration to be exhausting. When students learn the techniques of immersion, they accelerate their outcomes.

In the 2023 KBP model, we took our immersion model even deeper. We used the NIST/NICE standards to create a shared common vocabulary. We improved our student selection through cybersecurity competency assessment, and shared the results with each other to identify our strengths and weaknesses to pair up more effectively. We integrated academic and industry content to create discrete learning pathways to accelerate KSAT acquisition. We brought in mentors to simulate working real-time in an office environment. And, we rolled up results in a cloud-based LER software to extend the results of our immersive experience to employers.

The cloud based learning model in Fig. 4 serves as a living laboratory, or a collaboratory for learning in practice. We model this pipeline in Figure 4, so we can classify which immersive learning techniques belong in each step of the model.

The step discussed here is the Cooperative learning student. THe analysis of student results places the student in a quadrant that maps to the NIST/NICE Workgroup Work Roles [8]. Students examine the knowledge, skills, and abilities and reset their goals, accordingly, discussing changes with mentors and faculty. Students annotate their posted career goals and map the pathways to the goals over the three quarters. They repeat the process for the EC-Council materials, skipping to the modules that support their specialties. The career goal final assignment summarizes their plan. The University instructional designers integrate these pedagogical inputs and align activities and discussions to balance baseline curriculum with goal-based curriculum.

Students then explore the affinities they have with other work roles, so they can familiarize themselves with roles and responsibilities, thus increasing communication flow and threat assessment with most common pairs.

A Cyber Defense Forensics works directly with a Vulnerability Assessment Analyst and a Cyber Defense Incident Response within their own category. They have career pathways with cyber policy and strategy planners, law enforcement and counterintelligence forensics analysts, and cybercrime investigators. Knowing the affinities between cyber roles is essential for incident response planning or other interrelated roles. The CyberGENIUS.IQ assessment helps to identify which cognitive skills might be useful in matching team members.

The content, the goal setting, the faculty and mentors, and the pedagogical practices change to match the student. The student experience is captured in a cloud based visualizer that is accessible by employers. Cloud based internships and apprenticeships provide the breach ready environment, and the students arrive on the job, having already been there virtually for a year or two.

C. *CyberAlumni*

Underlining this process is the student run social community known as the CyberAlumni. The group meets to advance their learning. They work together to complete the EC-Council certificates. They function as a peer group to advance learning in different forms – mentoring, collaborating, and often work on projects together. Students plan to advance CyberAlumni to find jobs. The group plans to invite the 1600 students that have moved through this program into a centralized organization that can attract other cybersecurity clubs across the multiple NCAE Schools. The students like having a peer-to-peer networking group that allows them to continue their education and serve as a forum for staying connected and leveraging each other's careers.

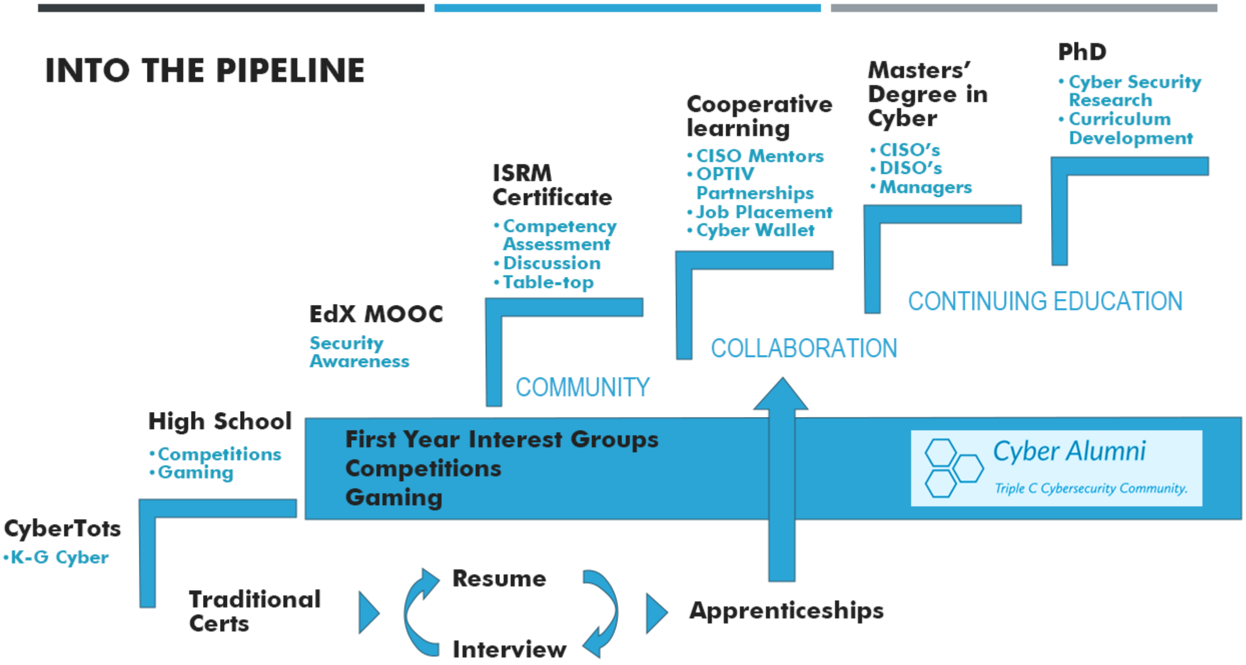

Fig. 4. Cybersecurity Entrepreneurship in Education

VII. RESULTS: PUTTING IT ALL TOGETHER

The NCAE-C funded SmartGrid project is centered at Portland State University. The seeding of the students from the University of Washington into the project enabled our two schools to explore each other's cybersecurity content and pedagogical practices. Chemeketa Community College and Portland Community College CyberFellow students participated in webinars and the MOOC materials created from the KBP process. The full course materials were set up on PSU's Canvas site so anyone could take the MOOC on Canvas.

In a new NCAE-C Initiative for FY2022-23, Norwich University will work with the University of Washington and other stakeholders in NCAE-C education in the Pacific Region, including Hawaii and Oceania to agree on the curriculum, the rubric and the certificate. We will then disseminate it across all the NCAE regions in the following year. A Cooperative Education model will formalize the KBP model and baseline cybersecurity content in compliance with Educational Standards established by the NIST / DHS / CAE-CDE Program Office. A system for talent identification, goal setting, course mentoring, job assignment, course development and job placement will extend the model. This is CyberEd in a Box, designed to fill the Cybersecurity pipeline.

We will deliver a Cooperative Education model to the NCAE-C Careers Preparation National Center collaborating on NCAE-C student professional development, credit transfer, and career matching. course development and job placement. Incorporating entrepreneurship in the model allows meaningful partnerships in industry and emboldens the creativity in advancing cybersecurity education. Industry thinks in terms of products and services. Students can focus on various levels of developing relevant solutions, from building cybersecurity toys to energizing K-12 curriculum. Students in community colleges and universities can evolve high school curriculum to include games and simulations, participate in competitions and build collaboratories and work with mentors in industry to gain in-service experience. The KBP model enables academia to work easily with industry, simulating the work place through highly immersive cybersecurity educational models. The adaptability of the model makes industry a valuable partner to meet students' needs, broaden faculty options and meet customers' expectations.

Meaningful partnerships in academia open the pathway for industry to communicate their jobs requirements into academic programs. Academia scales up their content development with certification materials and consulting services inside the virtual classroom. Testing can be replaced with work product and 360 feedback loops from full teams. Students can model working in teams, not individually, and create industry like work groups. Through apprenticeships, the students can product relevant, useful material for an organization.

Meaningful partnerships in government mean integrating standards that inform curriculum to meet Federal needs and form a baseline for international standards. Working on projects that deliver policy, governance models, incident response plans, and after-action reports generates a real-time experience to the students and matches the expectations of industry. Pairing the human factor side closely with the technical side produces a full-bodied workforce.

The objective of evolving the KBP model into a cooperative learning model is to create an immersive system that enables innovation in cybersecurity education, leverages the reputation of accreditation and scales cybersecurity readiness. Students need to be prepared with frameworks and real-world activities to enhance their ability to assess and mitigate risk, and to deal with active threats and vulnerabilities.

VIII. RESULTS

In the 2015 version, the KBP architects claimed they would 1) expand partnerships; 2) create presence to provide a critical infrastructure perspective on the cloud; 3) create an interdisciplinary, policy-focused, research agenda to integrate the contributions of key researchers involved with the Center; 4) develop a governance model; 5) offer opportunities to learn in the real world; 6) hold more community security and awareness events as part of outreach.

In *the Investment in Expansion of CAE-C Education Report* for this project, Dr. Endicott-Popovsky reported [20], "The high number of students deemed worthy of employment was significant (80+% average between the two cohorts" of Cooperative Learning students".

To prepare to support the Cooperative Education program, the University of Washington transferred the certificate to an online format. "The first cohort was challenged with adding classroom meetings for Information Security Risk Management (ISRM) once a week to their already busy schedule: regular classes, 0,5% FTE employment, seminar/mentoring appointments at the employer.

The course was offered as an asynchronous online delivery to accommodate for time management. During the pandemic, the model worked well for the students. Converting the format to an asynchronous modality and staying connected remained the biggest challenge. Students were asked to bring a client or a problem to their learning environment, and students met with the faculty in 1:1 office hour, and in one-to-many Zoom Groups to deliver results.

Students were asked to create videos of their capstones to provide a finished product for reusability. They participated in a real-time tabletop exercise led by an outside tabletop organization. Students were asked to write up after action reports, which were evaluated by faculty and peer groups.

Converting to asynchronous online has implications to course design that have informed our continued work at curriculum development. We brought in an immersion and interactivity specialist to increase features for deeper augmented cognition.

This project created cybersecurity career opportunities for twenty-two students in the first two cohorts with another twelve in the third cohort. Between 2019-2022, approximately twenty more students have gone through the course. No formal evaluation of the outcomes has been assessed, but the students continue to interact within the student founded and managed CyberAlumni organization and report the benefits of the course. They identify the key impacts were the focus on critical thinking, understanding the systemic approach to cybersecurity education and benefitting from the experiential learning focus. The course is designed to produce breach ready specialists.

The current work with the NCAE's Career Preparation National Center is a testimony to the Cooperative Learning model's potential. We will conduct another cohort in 2022-2023 in the Pacific Northwest and move the model with modifications from academic and industry throughout the other CAE regions in 2024-2025. We have 27 students in the course today, with 12 identified as the Cyber 12, and 5 heading for Optiv for 6 month integration into three departments in the CISO's office - Architecture, the Security Operations Center, the GRC (Governance, Risk Assessment and Compliance) organization.

In view of the original deliverables of the Cooperative Learning model, partnerships are expanding and a presence on the cloud with those partners has grown significantly. The Certificate and its newest incarnation with assessment, industry content, mentors, and job placement software development prove promising. The project is a collaboration between Portland State University's (PSU) Hatfield Cyber Defense and Cybersecurity Policy Center and the University of Washington's Professional Continuing Education organization, and our six state Pacific Northwest Collaboratory (WA, OR, ID, CO, MT, HI). Under supervision from Norwich University leading the efforts in the Career Preparation National Center, the next three years will produce measurable results and achieve the policy-focused research agenda promised.

We have formed a learning management team from the Pacific Northwest Collaboratory to continue development of a governance model. Our partnerships with iQ4 and Optiv allow us the opportunity to gain experience in the real world, through our online seminar series, town halls, and presentations in the CAE Community. These efforts drive awareness as part of outreach.

IX. FUTURE WORK

Future work includes advancing the analysis of the CyberGENIUS.IQ competency battery in terms of applying it to the NICE work roles and evaluating the potential to predict student selection. Further, the competency model emerging from the NCAE's Career Preparation National Center could be applied to the shared curriculum to determine efficacy in writing meaningful competency statements. The model that examines the Actor, their Behavior, the Conditions under which the behavior is being performed, the Degree to which it is performed, and the Employability of the student need to be expanded into an application of practice.

Engaging with industry partners in assessment, content scalability, cyber range interactivity, mentoring and career placement are promising directions for further research as well. Using the systemic KBP model, flexibility is needed to allow for a menu driven approach to skills-based learning. Cooperative learning is a model that can be explored to grow more research insights in this area.

Finding industry partners to integrate academic and industry content and processes shows promise. The business models for accelerating the partnership need to be explored and best practices defined. The model for accelerating the partnership is the key to responding to the workforce shortage and the relevancy of the solutions to increase reliability and harden the soft underbelly of the critical infrastructure threat and vulnerability landscape.

Research directions include the study of public / private collaboratories, on-line immersion and interactivity, augmented cognition, predicting cybersecurity talent through competency assessment and managing the Learning and Employment Record for a skills-based economy.

REFERENCES

[1] Endicott-Popovsky, B., and Popovsky, V. (2015). Conceptual Foundation for UW Center of Academic Excellence in Information Assurance Education. In The Colloquium for Information System Security Education (CISSE). Special Edition. Educational Approaches to Transition Former Military Personnel into the Cybersecurity Field. Spring 2015.

[2] Endicott-Popovsky, B., and Popovsky, V. (2014). *Application of pedagogical fundamentals for the holistic development of cybersecurity professionals*. In ACM Inroads, Volume 5, Issue 1, March 2014, pp 57–68. https://dl.acm.org/doi/10.1145/2568195.2568214, last accessed 9/14/2022

[3] Kapes, JT, and others. 1994. A Counselor's Guide to Career Assessment Instruments. 3rd ed. Alexandria VA: National Career Development Association in cooperation with the Association for Assessment in Counseling.

[4] Endicott-Popovsky, B.E. and Frincke, D., (2004, March). *A Case Study in Rapid Introduction of a Computer Security Track into a Software Engineering Curriculum*. In Proceedings of IEEE Computer Society Press 17th Conference on Software Engineering and Training 1-3 March 2004. Norfolk, VA, pp. 118-123. 10.1109/CSEE.2004.1276520

[5] Bandura, A. (1977). Social learning theory. United Kingdom: Prentice Hall.

[6] Tice, L. (2004). Personal coaching for results: How to mentor and inspire others to amazing growth. HarperCollins Leadership.

[7] Campbell, S., O'Rourke, P., and Bunting, M. (2015). *Identifying Dimensions of Cyber Aptitude: The Design of the Cyber Aptitude and Talent Assessment*. In Proceedings of the Human Factors and Ergonomics Society. 59th Annual Meeting. Volume 59, Issue 1. https://doi.org/10.1177/1541931215591170

[8] National Initiative for Cybersecurity Careers and Studies (2022). Workforce Framework for Cybersecurity (NICE Framework). Last accessed 9/12/2022. https://niccs.cisa.gov/workforce-development/nice-framework

[9] National Initiative for Cybersecurity Careers and Studies (2022). Cyber Career Pathways Tool. Last accessed 9/12/2022. https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool?selected-role=IN-FOR-002.

[10] Damer, B., & Hinrichs, R. (2014). *The virtuality and reality of avatar cyberspace*. The Oxford Handbook of Virtuality, 17-41.

[11] Hinrichs, R., and Wankel, C. Eds. (2011). Transforming Virtual World Learning. In Cutting-Edge Technologies in Higher Education. Volume 4. Emerald Publishing, United Kingdom.

[12] Chow, Yang-Wai, and others. (2017). *Cooperative Learning in Information Security Education: Teaching Secret Sharing Concepts*. In International Conference on Cooperative Design, Visualization and Engineering. Pp. 6572. DOI: 10.1007/978-3-319-66805-5_8.

[13] Hinrichs, Randy. (2004). *A vision for lifelong learning: year 2020*. European Journal of Engineering Education, 29(1), 5–16. https://doi.org/10.1080/03043790310001608492

[14] Kranch, M. (2019). *Why You Should Start with the Offense: How to Best Teach Cybersecurity's Core Concepts*. In Colloquium for Information Systems Security Education. CISSE, Las Vegas, USA, 2019.

[15] McLain, V., (2020). *Cybersecurity in Action*. In Innovations in Cybersecurity Education, Springer, 2020, p. 325.

[16] *Networks: A Postmortem*. In Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities (2005: Oxford Internet Institute) et al. 2005. Conference on Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities Held on 8-10 September 2005 at the Oxford University.

[17] Reeves, B., and Leighton Reed, J. (2009). Total Engagement: How Games and Virtual Worlds are Changing the Way People Work and Businesses Compete. Harvard Business Press. Boston, MA.

[18] Vailliou, M. and others (April 2022). Strategy for Cybersecurity Education in Smart Grids. In Cybersecurity Curricula Recommendations for Smart Grids. Erasmus+ Strategic Partnership Project. Intellectual Output 2. European Union. Grant Agreement No. 2020-1-F101-KA203066624.

[19] United States. (2002)/ Visions 2020: Transforming Education and Training through Advanced Technologies. Washington D.C: U.S. Dept. of Commerce Technology Administration Office of Public Affairs. https://purl.fdlp.gov/GPO/LPS34165.

[20] Endicott, B., (2017). *Investment in Expansion of CAE-C Education Program S-004-2017. Grant No. H98230-17-1-0357 Final Report*.