Open Access License Notice

Systems Thinking Pedagogical Design: Developing a Veteran-Centric Masters Degree In Cybersecurity and Leadership

Tracy Thompson, Marc Dupuis, Bryan Goda, Yan Bai, Charles Costarella, Morgan Zantua

University of Washington Tacoma

Abstract - Cybersecurity is a promising area because business, military, government, and utilities all desire trained cybersecurity professionals that can lead and effect change. Post-9/11 veterans represent a large untapped pool of talent ideal for addressing the nation's shortage of senior cyber leaders. But veterans often have difficulty transitioning to the civilian workforce. If they are to take advantage of the opportunity to usher military veterans into careers as cybersecurity leaders, universities need to engage in systems thinking pedagogical design. This paper introduces and assesses the utility of one approach for design as suggested by the KBP Pedagogical Model (Endicott-Popovsky & Popovsky, 2014). We use UW Tacoma's experience in mounting a new Master's level degree program in Cybersecurity and Leadership (the MCL) as a test case to evaluate the utility of this model for developing a veteran-centric approach to cyber security education. A retrospective analysis reveals the model to provide a useful frame for how to design the content of the curriculum and how it should be taught, but that it should be extended to address additional elements at the organizational level. Mechanisms to ensure strong and ongoing structural linkages between university schools support the interdisciplinary nature of the curriculum, control systems in the form of ongoing curricular evaluations methods support ongoing learning and the deep incorporation of non-faculty recruiting and advising capabilities into the administrative organization supports the students and ongoing ability of the faculty to adjust and deliver the curriculum. Each of these organizational design elements are critical features that enhance the performance of the pedagogical system and lower the risk of developing a new degree program that serves the needs of the transitioning veteran.

INTRODUCTION

Post-9/11 veterans, especially members of the officer corps who possess four-year or advanced college degrees, represent a large pool of untapped talent ideal for addressing the nation's shortage in the engineering and science workforce (Report of the National Science Foundation Workshop on Enhancing the Post-9/11 Veterans Educational Benefit, 2009). Demand for cybersecurity personnel continues to increase (Gjelton, 2010) and senior cyber leaders who can effectively communicate cyber-related business cases and are able to lead, persuade, and negotiate in a fast-moving business environment are in particularly scarce supply (CSFI, 2014; Roman, 2012). Many of those who serve today and are looking to transition out of the military are experienced in managing technical systems, solving complex problems, and leading teams. But these veterans often have difficulty translating their skills into the civilian work world, adjusting to a more individualistic and unstructured work environment, and engaging in effective job searches (Simpson & Armstrong, 2009; Stone & Stone, 2014). Capitalizing on this opportunity to develop and shape post 9-11 veterans into workforce-ready cybersecurity professionals requires educational institutions to develop specialized degree programs at the Masters level.

However, the startup of any new Master's program can be a risky proposition, especially one that will serve our nation's veterans. Basic questions need to be answered about the local context facing a proposed program, including: "Who will attend this program? What is the demand for this program? What skills should graduates have? Who will hire them after they leave the program? How should the curriculum be designed?"

One way to begin to addressing these questions is to employ a holistic model that can guide design efforts. This paper introduces and assesses the utility of one approach for design as suggested by the KBP Pedagogical Model (Endicott-Popovsky & Popovsky, 2014). We use UW Tacoma's experience in mounting a new Master's level degree program in Cybersecurity and Leadership (the MCL) as a test case to evaluate the utility of this model for developing a new veteran-centric

approach to cyber security education. Our retrospective analysis reveals the model to provide a useful frame for designing the curriculum itself but it also points to the importance of considering the organizational context within which curriculum resides. In particular, curriculum exists inside universities as organizations, and our work highlights the importance of how the curriculum needs to be supported by additional organizational design elements. Mechanisms to ensure strong and ongoing structural linkages between university schools support the interdisciplinary nature of the curriculum, control systems in the form of ongoing curricular evaluations methods support ongoing learning, and the deep incorporation of non-faculty recruiting and advising capabilities into the administrative organization supports the students and ongoing ability of the faculty to adjust and deliver the curriculum. Each of these organizational design elements are critical features that enhance the performance of the pedagogical system and lower the risk of developing a new degree program that serves the needs of the transitioning veteran.

APPLYING THE KBP MODEL TO UW TACOMA'S MCL PROGRAM

Figure 1 provides an overview of the KBP Pedagogical Model (Endicott-Popovsky & Popovsky, 2014) which offers a systems view of curriculum development. In such a system, resources (potential students), the job market, and trends in the larger societal and economic environment are inputs. New students are transformed via an educational process into outputs, in this case professionals. The internal components related to the model consist of two human elements, students and teachers, and three infrastructure elements, the goals, content, and didactic processes of the curriculum (see Figure 1). Congruence, or the notion of fit, underpins the model – when the elements fit together, the inputs (veteran students) transform into the desired outcomes, in this case, cybersecurity professionals with leadership capability. The model is also dynamic, so as any one element changes over time, other elements need to be adjusted to maintain good fit and hence performance.

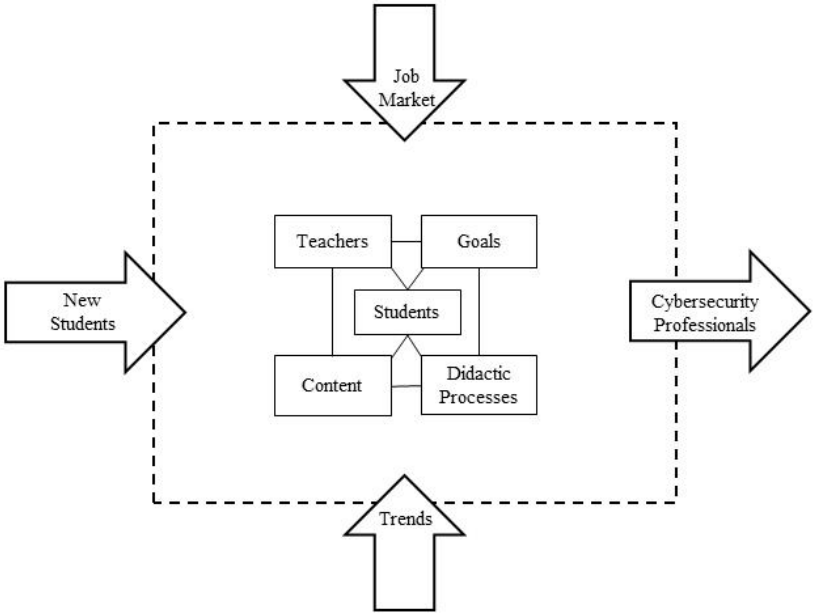

Figure 1. KBP Pedagogical Model for IA Curriculum Development

Students are at the heart of the KBP model; for purposes of our analysis we examine the fits between veterans as students and the other elements of the model. After providing a brief overview of UW Tacoma's MCL degree program, we evaluate the local context and opportunity, focusing on the supply of potential students, the demand for jobs, and the trends in the competitive context. Collectively, these factors shape the curriculum, specifically, the program learning goals, the teachers, the content of the curriculum, and the didactic processes. After explaining how these elements are designed to fit together in order to integrate technical and business concerns and to serve veterans seeking to become future cybersecurity leaders, we highlight additional organizational design factors that supplement the KBP model.

INPUTS: THE STUDENTS, THE JOB MARKET AND TRENDS IN THE MARKETPLACE

Founded in 1990, the University of Washington Tacoma (UWT) campus is located approximately 10 miles from Joint Base Lewis-McChord, one of the premier military installations on the West Coast. The opportunity for a Cybersecurity and Leadership program at the graduate level was supported by a strong local source of students, strong demand by employers, and a lack of competitors in the region. Approached by the Washington National Guard who wanted to have a professional degree program that would support their mission to respond to cybersecurity attacks on our nation's infrastructure, the Institute of Technology and the Milgard School of Business began to explore a joint degree program in 2012 (Goda & Friedman, 2012). The degree program is highly interdisciplinary in nature. It combines a technological education in cybersecurity policy and design with managerial and leadership skills yielding graduates who are well-positioned to lead an organization's cybersecurity functions and to advocate for the role that cybersecurity plays in furthering an organization's performance and effectiveness.

UWT's proximity to the Army and Air Force at JBLM and the Washington Air and Army National Guard provide an excellent source of students, the first contextual element in the KBP Model. Moreover, JBLM is surrounded by a veteran rich population (1 out of every 11 citizens in Washington State is a veteran). The U.S. Military's continued drawdown from its Iraq War peak strength has and will continue to strongly affect the South Puget Sound region, with some estimating JBLM to lose as many as 11,000 positions (Ashton, 2014, 2015). Outside of the military, the South Puget Sound and the I-5 corridor around UWT is home to such tech savvy companies as Microsoft, Amazon, Boeing, Liberty Mutual, Pacific Medical Centers, KPMG, and the Port of Tacoma, all of whom are likely to supply students to the program. Thus, market conditions suggest a strong supply of new students to feed the program.

A second contextual input into the KBP Pedagogical Model is the job market. This contextual element drives demand and shapes the desired goals and content of a program. In case of cybersecurity professionals, healthy demand exists at the national level for middle- to senior-level leaders of cybersecurity (CSFI, 2014; Gjelten, 2010; Roman, 2012). At the local level, the aforementioned tech savvy and large employers suggest a similar condition. In addition, when asked to go on record to support the development of the MCL program, several UW Tacoma constituents such as the Institute of Technology Advisory Board, the Milgard School of Business Advisory Board, local business leaders, and government agencies all indicated great enthusiasm and interest for the program, saying they would hire these graduates.

An additional input that was considered at the time the program was being proposed relates to the trends in the external marketplace. In addition to the clear demand for cybersecurity professionals with managerial and leadership expertise, the economics and competitive landscape facing UWT revealed a clear market opportunity for this type of program, particularly on the West Coast. An informal benchmarking exercise in 2012-2013 revealed a number of online and resident master degrees in cybersecurity housed in computer science departments. Of note, the exercise found only a few programs that combined business leadership courses with cybersecurity courses, and none located on the West coast.[1]

These efforts to understand the supply of potential students in the local area, particularly those coming from the military, and the demand conditions in terms of the job market and the competitive landscape, mitigate the risk this new program. But more importantly, per the KBP model, they also shape the curricular design. After identifying the specific needs of veterans transitioning to the civilian workplace, we describe the MCL program in terms of its goals, teachers, curriculum

[1] Example of graduate programs that combine technical skills with leadership skills include the National Defense University's Government Information Leadership Masters Degree, George Mason University's Masters in Management of Secure Information Systems, George Washington University's World Executive MBA in Cybersecurity, and Washington University's Cybersecurity Management (c.f., CSFI, 2014).

content, and didactic processes and explain how each of these elements integrates cybersecurity with business in a way that uniquely serves transitioning military personnel. We also highlight how additional organizational and administrative elements also enable and improve the program's interdisciplinary content and it's responsiveness to the veteran student population.

VETERANS AND MCL CURRICULUM DESIGN

Veterans have difficulty translating their skills into the civilian work world, adjusting to a different workplace culture, and engaging in effective job searches (Simpson & Armstrong, 2009; Stone & Stone, 2014). Identifying relevant skills learned in the military and translating them in ways that are meaningful in civilian organizations can be overwhelming to veterans (Biggs, 2014). In addition, veterans report culture shock and the shift from regimented, hierarchical, and a more group oriented environment to a more unstructured environment that focuses on individuality is a big concern (Simpson & Armstrong, 2009). Frequent relocation means that veterans are typically not well connected or networked in the civilian world (Clemens & Milson, 2008), and the skill and processes associated with meeting others, looking for and interviewing for jobs also presents challenges (Biggs, 2014; Simpson & Armstrong, 2009). The main elements of the MCL program, including the mix of students accepted into the program, the learning goals of the program, the content of the curriculum, the mix of teachers, and the didactic processes used in the classes all help the military veteran overcome these challenges and transition successfully into cybersecurity careers in the civilian workplace.

Students

The mix of incoming students is one factor that helps veterans transition. Rather than being just for veterans, the MCL is designed for both military and non-military students. The program also selects individuals with both a technical background in network design and substantial work experience (military work counts as work experience). Although it is a full time program, the MCL program accommodates students who are normally working during the day. Full-time status enables MCL

students to qualify for Veteran's and active duty funding. This combined with an evening delivery model allows the program to meet the needs of military personnel anticipating a transition to the private sector, veterans, retirees as well as others from the private and government sectors. Students attend classes two nights a week, with only small parts of some courses being offered online. Nearly 60% of the first two cohorts of MCL students are military-related, including Active Duty, Reserves, National Guard, veterans, and retirees, with the remaining coming from the governmental and private sectors.

Program Goals

The overarching goal of the MCL program is to produce students who will understand the design and policy issues surrounding cybersecurity and be able to solve problems, manage people, information, and processes to accomplish broader organizational and business goals related to cybersecurity. Table 2 lists the four specific learning objectives of the MCL Program. These learning objectives serve both veterans who are not fluent in the language and practices of business as well as technical types who may not be attuned to the organizational and behavioral sides of management.

1) **Communication Skills:** Our graduates are fluent interdisciplinary communicators who can integrate the technical aspects of cybersecurity with the strategic and managerial concerns of their organization.

2) **Risk Management Skills:** Our graduates are diagnostic problem-solvers who can evaluate the information security needs and design strong cybersecurity capabilities into their organization. Our students are able to use risk assessment concepts and methodologies to determine proactive measures in protecting their organization from critical data exposure, and they are able to evaluate a major cybersecurity event, evaluate the business impact, determine a risk posture, and develop effective responses.

3)	**Leadership and Interpersonal Skills:** Our graduates are change-savvy managers who can effectively coordinate activities and lead individuals and teams. They know how to launch and assess organizational change initiatives, understand how to effectively lead and manage teams, and they can work effectively within an interdependent group to achieve common goals.

Table 1. Program Learning Objectives for the MCL

Content and Teachers

The content of the MCL curriculum is delivered as a traditional program with resident instruction and is structured on a cohort basis where students take a locked sequence of courses together. The cohort design with lock-step classes helps to develop a strong culture and supportive network among students in the program. Connections that form between those with a military and those without a military background help the transitioning veteran connect his experience to the outside business world. In terms of the class content itself, on the technical side, the MCL program exposes students to the principles of data protection, network security, counter cyber-terrorist techniques, and risk management. And on the managerial side, the MCL program gives students the perspective and understanding of an organizational leader that extends beyond the IT function so that they can effectively advocate for cybersecurity issues at the highest levels of the organization.

The curriculum content consists of eight 5-credit courses which are designed and taught by faculty from the Institute of Technology and the Milgard School of Business. Two classes are offered each quarter for a total of 40 credits, and in any given quarter, students have one class taught by a professor from the Milgard School and the other taught by a professor from the Institute of Technology. The content and flow of the classes listed below have been designed to expose the transitioning veteran (and the technical employee who may be siloed in the IT function) to see

the bigger picture of business. All of the courses focus on preparing the student to work on a team solving a capstone cybersecurity project in a real organization.

Autumn Quarter (Introduction)	*Principles of Cybersecurity* provides an overview of the ten domains of cybersecurity.
	Business Essentials provides an overview of key concepts in business including business communication, marketing, ethics, accounting, and financial analysis.
Winter Quarter	*Information Assurance, Risk Management, and Security Strategies* exposes students to key risk assessment and management frameworks, which enables them to assess and prioritize risk in an organizational setting and communicate these risks to high level decision makers.
	Individual and Group Dynamics prepares students to establish, manage, and lead high-performing, successful teams and to lead their own careers effectively.
Spring Quarter	*Network and Internet Security* ensures that students are exposed to current industry best practices, such as white listing, intrusion detection systems, and other technical and policy concepts. Additionally, students are exposed to concepts in high demand by governmental organizations, such as defense in depth, constant monitoring, and incident response preparedness.

	Strategic Organizational Change explores the repertoire of concepts, tools, and techniques for understanding the strategic management of organizations and how successful leaders and change agents can create, implement, and manage change.
Summer Quarter (Capstone)	*Cybersecurity Management* provides a framework to support the Cybersecurity Challenge with consultants and periodic updates.
	Project Management supports the Cybersecurity Challenge project from a business administration point of view.

Table 2. Sequencing of Courses in the Masters of Cybersecurity and Leadership Program

Didactic Processes: Innovations in the MCL Classes

Several innovations in how these courses are taught represent the fifth internal element in the KBP Pedagogical Model. Specifically, these pedagogical innovations create a rich and meaningful experience for students that help veterans transition. Below we summarize the major activities and the kinds of experiences that help veterans learn about cybersecurity and about the business world outside of the military.

Industry Professionals. Throughout the program, faculty members invite guest speakers that are experts in their field, in particular leaders in business with the responsibility of protecting an organization's information security assets, such as Chief Information Security Officers (CISOs) from major corporations. The incorporation of industry professionals helps ensure that students both see the big picture, develop an appreciation for the type of careers available, and have an opportunity to ask these leading experts relevant questions related to cybersecurity

and management. Students are encouraged to add these industry experts to their growing network of professional contacts. This is particularly important for veterans who may not have many contacts in the civilian world. In the cybersecurity domain, individuals work most effectively through collaboration and partnerships - not isolation. Thus, the inclusion of guest speakers that are experts in their field and offer varying viewpoints is of paramount importance to a career that demands an interdisciplinary and holistic approach to security (Endicott-Popovsky & Popovsky, 2014). Having students add these experts to their own professional network helps ensure this is carried forward from the classroom to their eventual careers in cybersecurity management.

Real-World Information Assurance Strategies. A major theme of the program is the development of student expertise in the area of information security and risk management. Students examine real world cases studies in information assurance and this provides the background for students to become future managers. These future mangers will be charged with responsibility for making decisions about the security of information systems. Since there is no 100% secure system and since there are not unlimited budgets to spend on securing systems, choices must be made about how, where, and when to invest in security. Students practice methods and techniques for applying industry methodology to problems in information assurance. Mastering this material will make the information assurance professional a better executive. Students develop an understanding of information assurance applied research, executive presentation of topics, and financial drivers for budgets and decision making. Students also practice developing and maintaining risk assessments, risk management plans, auditing, and enforcing policies and procedures. Parts of the program are based on the education and training standards of the Committee on National Security Systems certifications CNSS 4012, Senior System Manager (National Security Agency 2013).

Hands' on Experiences through Virtual Labs. Proprietary virtual lab environments have been developed by program faculty, which give students hands-on experience. One set of labs used in the network and internet security class helps students learn security policy design, incident response, and techniques to defend

against, react to, and recover from a cyber-attack. Students conduct comprehensive laboratory exercises on internet protocols, reconnaissance, scanning, vulnerability assessment, and system hardening in a virtual network. These labs are designed with natural relationships among common phases of the attacks and defense technologies, providing students the opportunity to design and implement their own systems that meet a given security policy. Virtual Box is used to emulate the hardware of a computer and different operating systems (e.g., Windows XP and Windows 7 virtual machines). These virtual labs enrich students' experiences in operating and managing various network systems and applications with minimal operating and maintenance costs.

Engagement with the Non-Technical Business World. In addition to a curriculum that links students' coursework to problems in the business world and pays explicit attention to exposing students to the language and concepts involved in business and management, the students benefit from the affiliation with the Milgard School of Business in a variety of other ways. In particular, they are able to engage in activities and events that connect them to Milgard Master in Business Administration students and to local private sector employers. For example, students in the MCL program are invited to the annual Milgard Professional Networking Event where they learn useful tips on how to build their professional network and engage in several rounds of speed networking. They also are invited to the quarterly Executive Speaker Series where they can benefit from hearing regional business leaders talk about their organizations and experiences. These experiences help to forge informal relationships between students in both programs as well as with private sector employers.

Engagement in the Technical Business World. Students in the MCL program attend the annual South Sound Technology Conference (SST), which is hosted annually by the Institute of Technology at UWT. The SST is a technology showcase for the South Puget Sound (Cooper 2013), and since 2000 it has brought together leaders from industry, education, and government from around the state to discuss and demonstrate technological innovations and their ongoing applications. Panel and keynote presentations - including networking opportunities - provide a

venue to discuss, explore, understand, and deploy technology as a solution, an opportunity, and as an advantage. Sessions planned for the South Sound Technology Conference have included discussions on mobile application development, energy and sustainability, information technology, and cybersecurity. Throughout the conference, graduate and undergraduate students from the Institute of Technology showcase their work through poster sessions and demonstrations in the gallery area. Students get to interact with members of industry and industry participants can observe potential employees in a relaxed atmosphere.

Cybersecurity Capstone Challenge. A capstone course is a culminating experience for students in the program which gives them an opportunity to apply what they have learned in the classroom and gain valuable experience. Regional business leaders collaborate with program faculty to pose a relevant and interesting problem for a team of graduate students to solve in a three-month period. Past cybersecurity challenges are presented in Table 3. The benefits of the Cybersecurity Capstone Challenge include: 1) giving students the opportunity to apply their cybersecurity studies to real world issues and to receive valuable experience; 2) giving companies a motivated team at no cost; 3) enabling both students and company employees to expand their professional networks, thus increasing the opportunities to future employment, and 4) increasing the companies' engagement with UWT and the broader security community.

1) Communications Company wants their Unified Communications environment tested against a National Vulnerability Database.
2) An Internet security company desires a team to do a controlled assessment inside their Threat Intelligence Lab and link the results to the network defense team.
3) A software company wants to create an approach to embed security in applications development. A second project requests the student team create industry security guidance by assisting a team of developers in writing a protocol for emerging technologies.

4) A local county IT department wants a Critical Security Control Audit to evaluate how the county is adhering to Critical Security Controls. The student team will be working with the full-time county team.
5) A local port wants to harden its cybersecurity position based on the NIST Framework. The student team will work in tandem with the port IT staff and other stakeholders.
6) A local utility company desires the establishment of a policy to support the Cybersecurity Framework for Critical Infrastructure.
7) cybersecurity consulting firm will have a student team work alongside seasoned professionals and be guided in the use of assessment tools, risk analysis, and multiple commercial technologies used with cybersecurity consulting sessions.

Table 3. Cybersecurity Challenges

EXTENDING THE KBP MODEL TO INCORPORATE ORGANIZATIONAL DESIGN

Above, we have used the KBP model to describe three external contextual elements (new students, job market, and trends) that together shape the five internal elements of the MCL program (students, teachers, content, goals, and didactic processes) and have explained how this pedagogical system helps the veteran transition to the civilian workplace. Classes are taught at night on a full-time basis so the transitioning veteran can use their educational benefits to attend and can still work full time if need be. The cohort structure of the program design helps to develop a supportive learning community, one in which veterans are directly interacting and learning from their fellow students, many of whom come from business organizations outside the military. Class content is designed in a way to expose veterans to the cultures and practices of the business world and to connect their leadership and managerial experience to this business world. Innovations in

course design enable the veteran to learn about careers in cybersecurity and to network with cybersecurity professionals.

Using the KBP Model has allowed us to identify broad environmental contextual elements as well as very specific curricular elements that shape pedagogical design of a program that uniquely serves the transitioning veteran. However, our experience with the MCL reveals three additional considerations relating the organizational and administrative context that are important to the program's ongoing ability to effectively integrate broad environmental inputs to the curriculum and pedagogy. We have identified three examples of organizational design elements: 1) the need for formal structural linkages that institutionalize the ongoing engagement and involvement between two separate campus units; 2) the creation of control processes that include the monitoring and collection of data on students and their learning outcomes over time, and 3) the integration of a recruiter and advisor with military expertise. This third organizational design element is particularly critical in terms of recruiting the right kind of veteran student, helping that student to adjust and connect to other services on campus that might benefit them, and providing real-time information to faculty who are responsible for the content of the curriculum.

Institutionalizing Linkages between Programs. Because this is a joint program between two different departments of a university, ongoing administration and governance processes had to be established that support and maintain the interdisciplinary content of the curriculum. A joint venture between two programs on a campus requires faculty and administration to move beyond their own siloed perspectives and to discover shared areas of interest. A key element for success is the establishment of forums for regular dialogue between faculty from the Institute of Technology and the Milgard School of Business. Quarterly program meetings were established to coordinate and improve the linkages between courses and to discuss students' progress towards program learning outcomes. New governance vehicles and procedures for managing the curriculum were also established. A committee comprised of faculty teaching in the MCL program from both schools

is charged with overseeing admissions and developing the curriculum; however, votes among each respective faculty are still taken when required by faculty code.

Creation of Control Systems for Continuous Improvement. Assessment and monitoring of the program and the students' experience enables faculty to be responsive to student needs, especially in the early days. Formally, students are given a survey at the end of every course to assess how to improve each course. Informally, periodic discussion groups are used to gauge student morale and to assess what they are getting out of the classes. Such data collected in the first year revealed a serious deficiency in students' incoming knowledge of basic business concepts, and resulted in the alteration of one of the first classes into what is now the Business Essentials class, a survey oriented class to acclimate students to the world of business. As the program matures and prompted in part by accreditation requirements for the Milgard School of Business, the MCL faculty committee is developing an outcomes assessment process that identifies instruments and measures to assess student learning (the program learning goals and objectives); collects, analyzes, and disseminates the assessment information, and uses that information for continuous improvement of the program (c.f., AACSB Assurance of Learning Standards: An Interpretation, 2013).

Integrating Recruiting and Advising Functions. An additional program level organizational consideration relates to the structure of administering the program and how those administrative roles are integrated with ongoing curricular design and modification. The MCL program employs a full-time recruiter and advisor who markets the program and serves the local pool of potential students coming from a military background. While there are active duty officers and senior enlisted seeking a master's degree for promotional purposes, many service members are preparing for retirement or forced transition to civilian careers as a result of the drawdown cycle. Thus, the presence of a dedicated recruiter and advisor who understands these dynamics is critical to the program's success. Encouraging these mid-career professionals through the application process, guiding them through the Graduate Record Exam (GRE), and supporting them as they face a transition from military to academic culture builds rapport, trust, and goodwill in the community. During

the application process, the advisor identifies immediate and long-term career goals. While they are in the program, students receive individualized coaching sessions and workshops enabling them to achieve their goals. Such individual attention increases enrollment as well as retention, two key factors in determining the success of a program. In addition, through relationships with the existing students, the recruiter also provides important feedback to faculty on how the program is serving veterans that feed forward into additional adjustments to the curriculum and to individual faculty's pedagogical practices.

Curriculum design does not occur independent of the organizational structures in which it operates, and these three elements have a direct bearing on the degree to which the pedagogical system can take new veteran students and process them into cybersecurity leaders over time. This level of elements influencing pedagogical design connects the broad environment to the students, faculty, curriculum, and the organization, leading us to suggest revisions to the KBP Model. Our experience at UWT provides three concrete examples of organizational design considerations that link the broad environmental inputs to the specific internal components of the pedagogical system. However, depending on the program and university, other structural organizational design elements might exist that similarly shape and provide feedback to the pedagogical system, including student mental health centers, learning centers, and other centralized student services that exist on a university campus. Figure 2 incorporates the concept of organizational level design elements in the existing KBP Model and shows how this level feeds into and receives feedback from the central internal elements of pedagogical design.

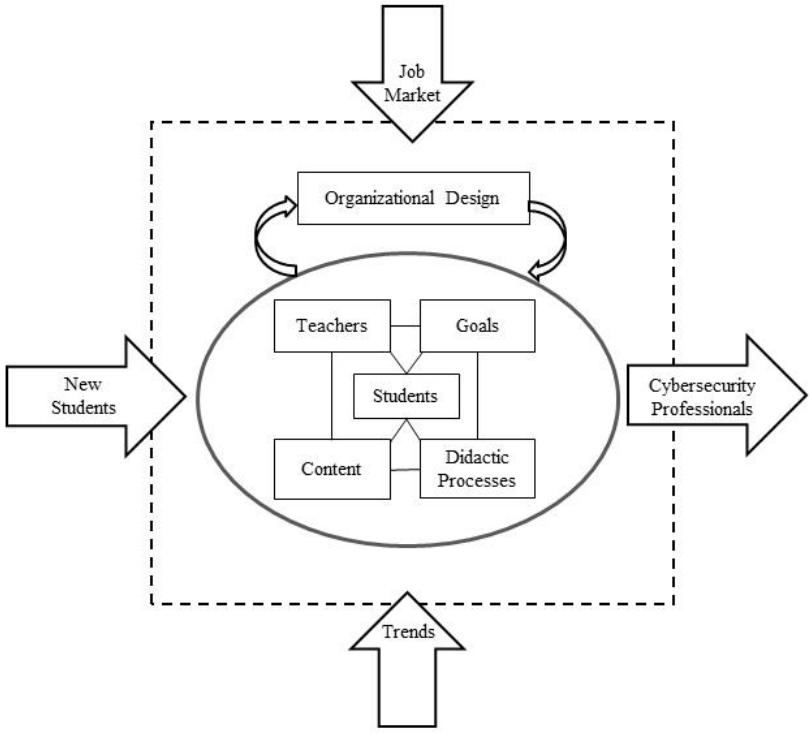

Figure 2. Revised KBP Pedagogical Model for Curriculum Development

In summary, the MCL is a dynamic and vibrant graduate degree program that serves a local and regional community by bringing together academia, community leaders, military, and public and private organizations. The KBP Model is a useful tool for integrating both external contextual considerations relating to inputs of such a program as well as the internal factors that directly relate to the pedagogy and curriculum of a program. For transitioning military personnel in particular, the design of this program enables transitioning veterans to combine the knowledge, skills, and abilities from their military careers with the business and technical acumen so that they may successfully transition into civilian careers that are in high demand. Our test case reveals the importance of including explicit reference to organizational design considerations that further shape the pedagogical system. Institutionalizing the relationships between two separate academic units on campus, creating formal

control systems that regularly assess and provide feedback on learning outcomes, and integrating dedicated in-house advisors with military expertise to inform faculty on issues related to this population ensures that the pedagogical system functions effectively over time and is responsive to the needs of the cybersecurity field and to our veteran students.

REFERENCES

[1] AACSB Assurance of Learning Standards: An Interpretation. (2013.) Retrieved from http://www.aacsb.edu/~/media/AACSB/Publications/white-papers/wp-assurance-of-learning-standards.ashx.

[2] Ashton, A. (2015). JBLM Airmen Share Memories as They Prep for Squadron's Shutdown, The Olympian, Jan 12. Retrieved from http://www.theolympian.com/2015/01/12/3522436/this-is-what-the-drawdown-looks.html

[3] Ashton, A. (2014). Community Leaders Rally to Protect JBLM Workforce. The News Tribune, Dec. 29. Retrieved from http://www.military.com/daily-news/2014/12/29/community-leaders-rally-to-protect-jblm-workforce.html

[4] Clemens, E. V., & Milsom, A. S. (2008). Enlisted Service Members' Transition Into the Civilian World of Work: A Cognitive Information Processing Approach. Career Development Quarterly, 56(3), 246-256.

[5] Cooper K. (2013). Hundreds Discuss Mobile Web, Data Security at University of Washington Tacoma's South Sound Technology Conference (2013). Retrieved from http://www.tacoma.uw.edu/events/south-sound-technology-conference

[6] Cybersecurity Forum Initiative - CSFI (2014). Senior Cyber Leadership – Why a Technically Competent Cyber Workforce is Not Enough. Retrieved from http://www.csfi.us/?page=reports

[7] Endicott-Popovsky, B., Popovsky, V. (2014). Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals. ACM Inroads. Vol. 5, No. 1.

[8] George Washington University (2013). Program Requirements of the Master of Cybersecurity in Computer Science. Retrieved from http://www.cs.gwu.edu/academics/graduate_programs/master/cybersecurity/program-requirements

[9] Goda, B., Friedman R. (2012). Designing a Masters Program in Cybersecurity and Leadership.

[10] Retrieved from http://sigite2012.sigite.org/wp-content/uploads/2012/08/session01-paper02.pdf

[11] Gjelten, T. (2013). Cyber Warrior Shortage Threatens U.S. Security. Retrieved from National Public Radio http://www.npr.org/templates/story/story.php?storyId=128574055s

[12] Harris, S. (2012) *Certified Information Systems Security Professional Exam Guide, 6th Edition*. New York. McGraw Hill Professional.

[13] International Information Systems Security Certification Consortium (2014). Certified Information Systems Security Professional. Retrieved from https://www.isc2.org/CISSP/Default.aspx

[14] Ma, M. (2015). Mark Pagano Selected as Chancellor of UW Tacoma. UW Today, Jan 6. http://www.washington.edu/news/2015/01/06/mark-pagano-selected-as-chancellor-of-uw-tacoma/

[15] Obama, B. (2009).Obama at the Academy IV: Speech Text. Retrieved from http://news.sciencemag.org/2009/04/obama-academy-iv-speech-text.

[16] Roman, J. (2012). The New IT Security Skills Set. Retrieved from http://www.bankinfosecurity.com/new-security-skills-set-a-5022/op-1

[17] Simpson, A. s., & Armstrong, S. s. (2009). From the Military to the Civilian Work Force: Addressing Veteran Career Development Concerns. Career Planning & Adult Development Journal, 25(1), 177-187.

[18] Stone, C. and Stone, D. (2014). Factors affecting hiring decisions about veterans, Human Resource Management Review, Volume 25, Issue 1, March 2015, Pages 68-79, ISSN 1053-4822, http://dx.doi.org/10.1016/j.hrmr.2014.06.003.