Conceptual Foundation for UW Center of Academic Excellence in Information Assurance Education[1]

B. Endicott-Popovsky, V. Popovsky, P. Osterli, P. Rosario, S. Nelson

The Center for Information Assurance (IA) and Cybersecurity (CIAC) at the University of Washington, an NSA/DHS Center of Academic Excellence in Information Assurance Education, brings together industry, academia and the Pacific Northwest community to develop cooperative cybersecurity education programs that reflect the region's unique nature: tech-aware, industrially-based, cloud-driven. The programs produce IA professionals at all organizational levels, and across all 31 NICE pathways, who are immediately effective in the work place. A focus of CIAC programs is assisting the 8,000 military a year transitioning through Joint Base Lewis McCord (JBLM), Camp Murray and state-wide Army Reserve Centers, as well as approximately 15,000 veterans that retire annually in Washington State. A large number will enter law enforcement, emergency management and the private sector and can benefit from cybersecrurity education. Their 360 awareness and military training make them ideal homeland defenders; however, they need orientation to industry and a soft skill set that prepares them for the different culture and authorities of the private sector. This paper describes the conceptual models that are the foundation of the CIAC that could be replicated.

[1] Barbara Endicott-Popovsky, Executive Director for the Center of Information Assurance and Cybersecurity and Professor, Institute of Technology, Academic Director Master of Infrastructure Planning and Management Dept. of Urban Planning, University of Washington;
V.M. Popovsky, Affiliate Professor, School of Education, Department of HERD, University of Idaho;
LTC Philip Osterli, Private-Public Partnership Initiative, Army Reserve Cyber Operations Group.
MAJ Pedro Rosario, Cyber P3i Texas, Army Reserve Cyber Operations Group.
LTC Scott Nelson, Deputy Commanding Officer Army Reserve Cyber Operations Group.

INTRODUCTION

Since the late 1990's, NSA and DHS have encouraged universities to create Centers of Academic Excellence in Information Assurance Education and Research (CAE's and CAE-R's) in order to:

- **Meet national demand** for IA professionals
- **Prepare IA professionals** for national information infrastructure protection
- Provide sources for **IA recruitment**
- Provide sources for **IA research**. [1]

In 2002-2003, the University of Washington sought designation as a Center of Academic Excellence in Information Assurance Education in the under-represented (in terms of CAE's) Pacific Northwest (Figure 1). Through a multidisciplinary collaboration of the Information School, the College of Engineering and the Institute of Technology (UWIT) at Tacoma, CAE status was awarded to UW's Center for Information Assurance and Cybersecurity (CIAC) in 2004.

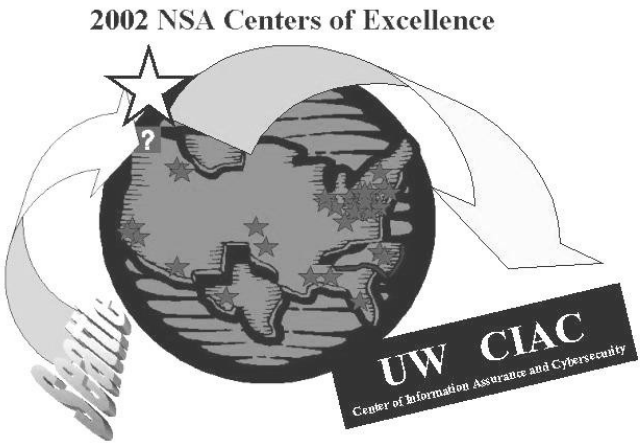

Figure 1 CIAC in Underrepresented Northwest (Stars represent CAE's in 2002)

The motivation came from Northwest business and government stakeholders who had expressed interest in Information Assurance programs, e.g.: Microsoft had launched its Trustworthy initiative [2]; Boeing Defense and Space was seeking students from programs with IA concentrations; local companies, such as IO Active, were explicitly asking for students with IA and secure coding backgrounds.

In addition, undergraduate and graduate students were demanding IA courses knowing that they needed that knowledge to be competitive in the work place. In response, we created our initial educational offering, the Information Assurance and Risk Management (ISRM) certificate, a three course series of graduate classes that earn a certificate from the CIAC, as well as an academic credential from the university.

IA Professional and Continuing Education Certificates

- Information Systems Security
- Information Security and Risk Management (ISRM)
- Network Engineering
- Digital Forensics
- e-Discovery

Degrees/Tracks/Electives

- Master of Science Info Management IA track
- Informatics network courses
- Tri-campus IA undergrad option
- Master of Science Computer Science - (IA focus)
- Master Cyber Leadership
- Master of Science Cybersecurity
- Master Infrastructure Planning and Management

- PhD Computer Science- IA track (U of Hawaii)

ISRM MOOC (Massive Open Online Course) Coursera

Research Program

- Pacific Northwest National Laboratory MOU- Contracts, Internships
- Interpares Trust University of British Columbia (Canada)
- NSF Scholarship for Service Program/grants
- Fraunhofer Darmstadt (Germany) Collaboration

Outreach

- Unintended Consequences of Information Age Lecture Series (UW TV)
- UW Conferences and Workshops: Honeypots Workshop, Intl Conference on Cloud Security and Management
- Honeynet Alliance Chapter

Pacific Rim Collegiate Cyber Defense Competition (PRCCDC)

Figure 2 UW Cybersecurity Offerings

We have since implemented a series of certificates and degree and research programs over the past decade to meet student and employer demand (Figure 2). In addition, faculty in a variety of disciplines have demonstrated interest in IA research and education, incorporating IA topics in courses and pursuing IA research agendas.

With broad, multi-discipline interest, the Provost Office continues to house the Center which promotes collaboration across schools and campuses. The challenge we faced as the Center grew its offerings was to develop conceptual models that

would promote interdisciplinary collaboration and focus on career outcomes for students. Like industry, universities are siloed by discipline.

Working interdisciplinarily, across UW campuses, and across sectors: industry, government, and academia requires governance clarity and collaborative relationships that need continuous nurturing. The balance of this paper describes the conceptual foundation underpinning the Center that includes conceptual and operational models that guide activities. We also discuss operational outcomes as an indication of the value of this approach.

CONCEPTUAL FOUNDATION

By bringing together industry, government, and academia, CIAC:

- Promote regional collaboration,
- Produce interdisciplinary research directions and educational programs, and
- Develop IA professionals at all levels who are well- prepared for the work place.

The CIAC's stated mission is to "identify, address, and promote IA solutions as a catalyst for IA research and education, entrepreneurship, invention, public awareness."

In order to produce and promote integrated interdisciplinary programs, the Center employs a system-activity approach developed by Russian and American pedagogues [3, 4, 5, 6, 7, 8, 9, 10]. Some applications and modifications of this approach have been discussed, extensively, in Endicott-Popovsky's previous publications [11, 12, 13, 14, 15, 16, 17, 18, 19, 20].

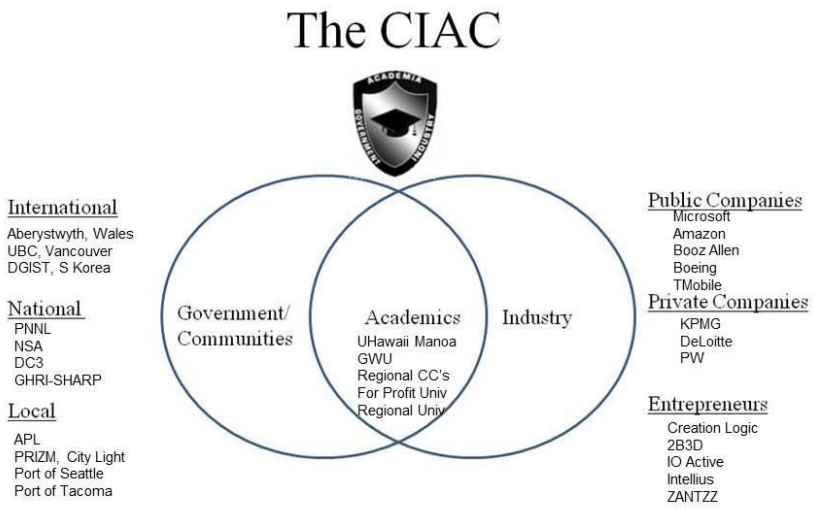

Figure 3 Integrating Academics, the Community and Industry

The system-activity approach is characterized as follows:

1) Learning occurs through productive activities developed in partnership with the community, academic researchers, and industry. The approach involves ***all*** participants - community and industry leaders, university instructors and students, and IA experts - in the learning process. Everyone learns from one another, often creating new knowledge.

2) Emphasis is on student professional development and motivating them to learn more from every possible resource: educational partners throughout the Northwest, certifications, the CIAC's IA network, professional memberships.

3) Knowledge is treated, not as the end goal of the educational process (i.e., learning for a grade), but as a tool to solve practical, complex problems, creatively and independently, unleashing the learner's potential.

4) The end result becomes the personal and professional development of all participants who exhibit creativity, professionalism, and high motivation to

learn continuously and independently which helps researchers, experts, educators, business leaders and students alike stay current in the rapidly evolving field of IA. We encourage reflection on practical experiences, in order to induce generalizations from these experiences and to extend their knowledge.

5) Criteria for measuring the efficiency of this educational approach include contributions to science and industry made by CIAC participants.

This system activity approach is adaptive. The five fundamentals above were implemented as guiding principles for our work, allowing all participants to move rapidly to adjust to evolving learning objectives arising from our fast-paced field.

THE CIAC AS A PEDAGOGICAL SYSTEM

To operationalize the five fundamentals above, the Center is designed, conceptually, as a pedagogical system that produces the following outcomes:

1) Qualified IA professionals who understand current trends, technologies and regulatory policies,,

2) Development of new knowledge and technology,

3) Development of new educational programs, curricula, classroom artifacts (labs, assignments, lectures, etc.)

A major method for achieving these outcomes is integrating recognized IA practitioners into the classroom as guest lecturers and course instructors. This maintains currency of our programs, inspiring students to maintain their knowledge currency. It also makes students triage between the real world and what they learn in books and lectures, which often lags behind what is happening on the 'firing line' in organizations coping with rapidly evolving threats.

The CIAC is conceived as a pedagogical system as depicted in Figure 4 [20]. The Kuzmina-Bespalko-Popovsky (KBP) Pedagogical model is composed of five elements - **students**, **teachers**, **goals**, **content** and **didactic processes** - the first two

are intelligent elements, the teacher and the student; the remaining three are infrastructure elements - the **goals**, **content**, and **didactic processes** of the curriculum. All elements of the model are dynamic, subject to varying rates of change and adaptation. All of the elements of the model function as an interconnected whole and operate within a larger dynamic professional and social context that includes economic and political environments, as well as a constantly evolving set of threats, vulnerabilities and operational systems which are affected by influences such as global competition; technological innovation; legal policies; and the creativity of business leaders, entrepreneurs and IA specialists. The context informs the different elements of the model.

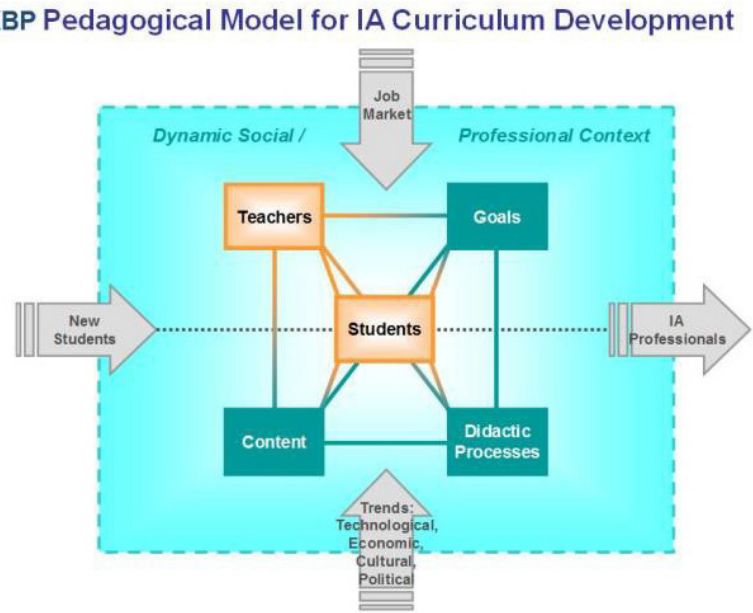

Figure 4 The KBP Pedagogical Model: CIAC as a pedagogical system [20]

In any given context, a specific instructor with their own specific slice of IA knowledge and expertise is responsible for developing a specific set of infrastructure components designed to address the needs of a specific type of student.

Students are central to the model - entering the system as potential IA employees; exiting as IA professionals. By describing each component of the model in relation to learning objectives drawn from the environment and an integration of trends and the condition of the job market, an educational program is developed iteratively. According to Bespalko and Kuzmina, the more precisely the five components are characterized - along with the connections among them - the more repeatable and predictable the learning results [3, 4].

The five elements interact and are changing constantly. Over time, as each of the elements is changed, it affects the other four, requiring each of them to be re-defined, and so on, until all five elements are specified in relation to one another. By continuously updating descriptions of these elements, curriculum is kept current ensuring that students remain competitive. Curriculum is on an annual review cycle, using the model to help think through curricular changes. This process has been described in depth in previous publications [13, 15, 16, 17, 18, 20].

Further the Center relies on the NICE (National Initiative for Cybersecurity Education) to align programs and courses with the 31 pathways defined therein that describe career path required skills and knowledge units. Students are familiarized with NICE to encourage them to drive their own self-study to equip them for the careers they choose [21].

INTERDISCIPLINARY ACADEMIC COOPERATION

Figure 5, is an organizational model for academic interdisciplinary cooperation. Current CIAC members include ten disciplines, administrative functions and partners: the Information School; Tacoma Institute of Technology; University of Washington Bothell; Computer Science and Engineering Department; Electrical Engineering Department, the Daniel J. Evans School of Public Affairs; the Center for Arts, Technology and the Law; the Provost's Office; the Chief Information Security Officer; Professional and Continuing Education; and the Pacific Northwest National Laboratory.

The Center provides an umbrella for current IA research activities of its members, while research is conducted undisturbed within member departments. Collaboration through the Center allows for sharing of information and research results and the development of multi-disciplined research programs. Research is classified within four areas of Information Assurance - Policy, Procedures, Technology and Education/Awareness. The Center provides an umbrella for the current IA research activities of its members, while research is conducted undisturbed within the member departments. Collaboration through the Center allows for sharing of information and research results and the development of multi-disciplined research programs. Research is classified within four areas of Information Assurance - Policy, Procedures, Technology and Education/Awareness.

The Center also serves as a clearinghouse for dissemination of IA research to industry and the local community and for integrating research into the classroom through lectures, workshops, seminars and lab exercises. Ad hoc, solution-oriented committees act as "Rapid-Research-Response teams" to solve emerging problems introduced through member initiatives or by government and industry sponsors (Figure 5).

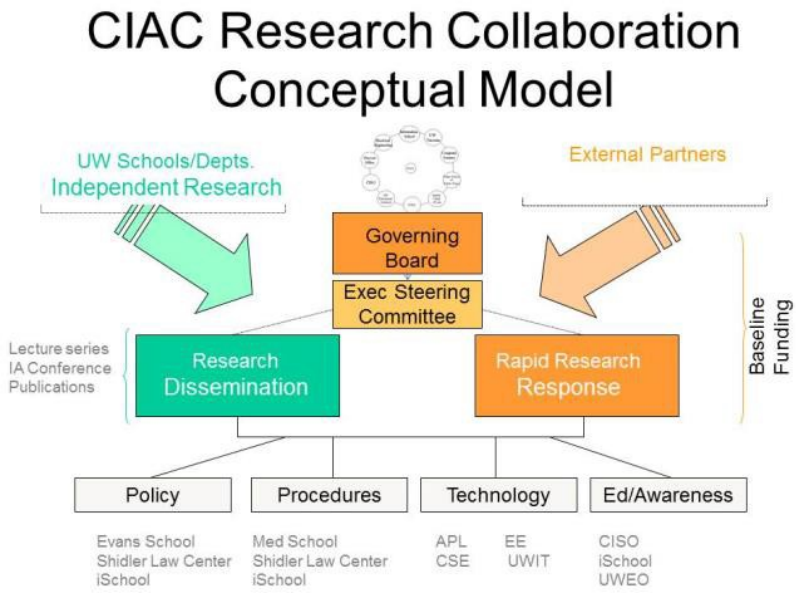

Figure 5 Organizational Model for Research Collaboration through the CIAC

The Center is led by a Governing Board consisting of the leadership from participating faculty and representatives from the Provost's office, the CISO, Pacific Northwest National Labs and other industry and government partners (Figure 6). Board membership grows as the Center expands. The Board provides strategic guidance to the Center and convenes annually with more frequent meetings of an Executive Steering Committee empowered to develop plans and projects for the Center.

An Advisory Board consisting of external leader-collaborators from industry and government engages the community in assisting with resource acquisition and access to funding and internships/jobs for students. The Board draws from a rich set of collaborative relationships forged for various purposes and formalized in memoranda of understanding.

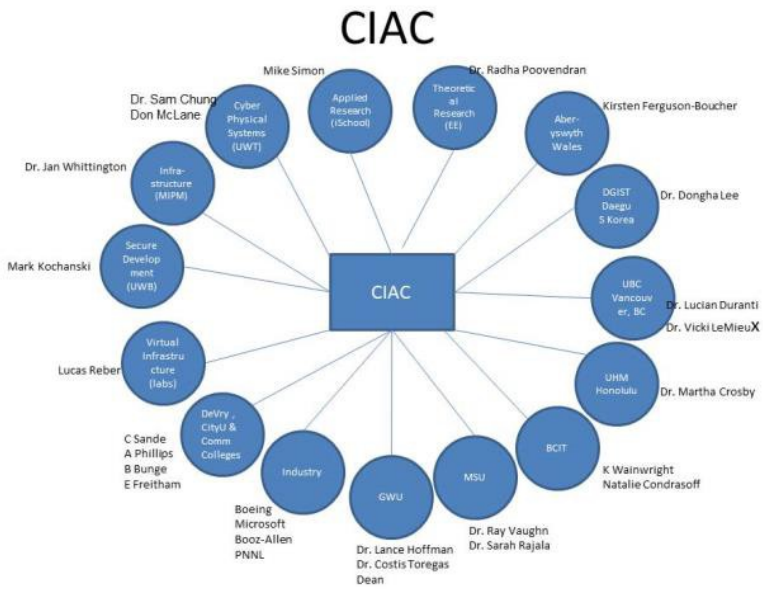

Figure 6 Network of CIAC Collaborators

Since the Center is also a designated CAE-R (Center of Academic Excellence in IA Research), students at all levels of study are involved with Center research offering students unique opportunities to learn from cutting-edge IA leaders. Students learn research methodologies that immerse them in the scientific method, contributing to their development as 'out-of-the-box' IA problem solvers who have situational awareness.

CENTER OPERATIONS

The Center has been chartered at the University Provost level, facilitating interdisciplinary and cross-campus collaboration. Plans have been developed for continued growth and expansion. The following principles are incorporated into the Center to ensure there is maximum learning for students that will prepare them to be successful in their chosen career pathway once graduated.

Multidisciplinary Approach

The Center actively exercises a multi-disciplinary approach to educational and research programs offered across all three campuses to both technical and non-technical students alike. An example of an educational program is our recently created Tri-Campus IA Option that leverages the strengths of all three campuses' IA course inventory. Students are allowed to choose different electives at any campus to build curriculum corresponding to any of the specialties defined by NICE [21].

All three campuses working together on a unified concentration provide a greater opportunity for students attending one campus to learn from faculty across all three campuses. This flexibility gives students the ability to customize their learning in line with their career goals. It also is much more efficient than each campus building its own program. Some courses may be offered online or in a hybrid format to encourage enrollment from distant campuses.

The Center's research agenda has evolved within the context of the ARC initiative at the Pacific Northwest National Laboratory with faculty exchanges, internship and financial support to the Center, as well as joint grants. Similar collaborative partnerships are evolving with other institutions: University of Hawaii Manoa, Aberyswyth University Wales, Interpares IV funded by the Canadian government at University of British Columbia, and Fraunhofer SIT at Darmstadt, Germany.

Participation in the Practice of IA

The University's Chief Information Security Officer, Kirk Bailey[2] presides over information assurance policies and practices across the institution and also collaborates with the academic and research programs of the Center. As an example,

[2] Mr. Bailey has been featured frequently in *Information Security* magazine, which reaches 68,000 security practitioners around the world [22].

students annually perform penetration tests on the campus network as part of classroom assignments.

Mr. Bailey's extensive network of IA professionals, the Agora, convenes quarterly at the Seattle campus, providing educational and networking opportunities for students. Incorporating these meetings into course schedules and having members of his network make guest lecture appearances in the classroom are ways the Center integrates IA industry expertise into curricula.

Students also participate in PRISEM, our Public Regional Information Security Event Management system. This is a regional alert system that integrates and analyzes netflow data from local municipalities, ports, hospitals and local businesses to give us a sense of the regional threat patterns which inform security professionals and provide an escalation path to national and regional authorities.

Partnerships in IA Education

The CIAC is partnering on projects with several institutions of higher learning which exposes students to other universities and institutions and expands their understanding of the field. Some examples:

1) The United States Military Academy at West Point collaboration led to development of the Pacific Rim Collegiate Cyber Defense Competition (PRCCDC). This event gives students live-fire hands-on experience that simulates real world management of actual networks. The project received regional and national funding from local business and the National Collegiate Cyber Defense Competition.

2) George Washington University and University of Hawaii Manoa collaboration on an NSF grant, Sea to Shining Sea [DUE - 1128989], provided access to Washington DC IA experts through guest lecture videos and live chat.

3) Whatcom Community College-led NSF grant [*NSF Proposal #7252472*] that is developing articulation agreements with Washington State universities. At UW, it includes articulation to a Tri-Campus IA degree program.

4) Highline Community College, Seattle University and University of Washington collaboration [DUE0341356] developed Computer Forensics curriculum that has been implemented throughout the CIAC network.

5) The University of Hawaii at Manoa collaboration for IA curriculum dissemination, teaching exchange and research collaboration was funded by NSA [H98230-07-1-0244].

Each of these collaborations has leveraged and extended IA programs at the University of Washington, promoting a rich exchange of ideas and further collaborative opportunities with other university partners.

Academic Concentrations in IA

Academic concentrations in Information Assurance have been developed in multiple programs, creating a curriculum database that facilitates the ability to develop new curricula for different disciplines, as requested. Most recently, these artifacts contributed to a Master in Cyber Leadership (MCL) degree that integrates both the computer science/cybersecurity and business departments in a jointly offered degree directed toward transitioning military personnel. Approximately 8,000 veterans a year for the foreseeable future are expected to pass through military installations near the UW Tacoma campus as they transition into civilian careers.

The University is committed to accommodate the academic needs of transitioning and active military by not only offering specific programs designed for military personnel, but also by developing a database of all local cybersecurity program offerings throughout the State so service people are able to find academic programs most aligned with their needs, capabilities and interests. Called CREATES, Cybersecurity Rapid Education Apprenticeship Training Employment System, this is a pipeline from military through academia to civilian jobs. Work

began on CREATES (Figure 7) during a 2010 NSF grant called *VetsEngr* [EEC 1037814].

In addition, special topics courses are developed as needed. For example, Dr. Edward Lazowska, the Bill and Melinda Gates Endowed Chair in Computer Science and Engineering, developed and delivered a course, "Homeland Security / Cyber Security," that was a 4-site, distance-learning collaboration among the University of Washington Dept. Engineering), and Dr. Geoff Voelker (UCSD Computer Science & Engineering), UC Berkeley, UC San Diego, and Microsoft [23]. Lead instructors included Dr. Lazowska, Dr, Christine Hartmann-Siantar, Dr. Steve Maurer (UCB Goldman School of Public Policy), Dr. Stefan Savage (UCSD Computer Science).

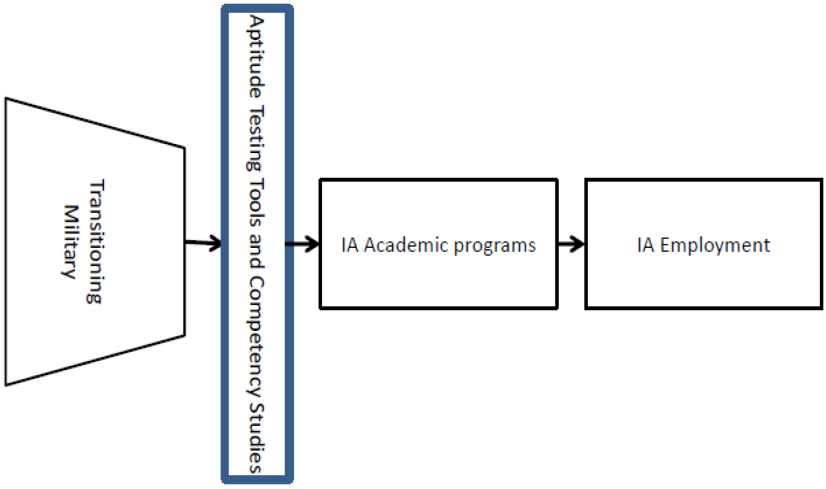

Figure 7 CREATES Pipeline

Faculty members have received national and international recognition for their research in information assurance. For example: Dr. Tadayoshi Kohno, Dr. Radha Poovendran and Dr. Barbara Endicott-Popovsky are internationally recognized leaders in computer science, electrical engineering, forensic readiness, respectively.

Neal Koblitz, co-inventor of elliptic curve cryptography, offers courses in number theory and other topics and guest lectures in our IA classes.

Student Participation in Research and Publications

Our researchers expose students to the most recent developments in IA. Students are expected to publish and participate in research, regardless of level (bachelor, master, or doctorate). Student capstone projects, in partnership with industry, are reviewed in a day of research presentations at each campus for each program where students share the results of their work with faculty and peers. Some examples:

Dr. Poovendran, Professor and Chair of Electrical Engineering, is Director of Research for the Center. He embodies the Center's principle of bringing research into the classroom. He publishes extensively in wireless security and applied cryptography, and was named a Presidential Early Career Awards recipient.[3]

Dr. Tadayoshi Kohno, Associate Professor of Computer Science and Engineering, is known for his riveting research experiments that attract students, such as hacking into traveling cars, that has gained world attention.

Dr. Barbara Endicott-Popovsky, Professor UW Institute of Technology, Tacoma, who explores forensic readiness, has attracted broad interest from the international community as evidenced by her leadership at a Dagstuhl conference, Germany, attended by researchers from four continents and eleven countries, resulting in a research manifesto for forensic readiness and digit evidence. She brings students into her international collaborations.

[3] The highest honor bestowed by the Federal government to young researchers at the outset of their careers in technical fields.

Access to Leading Practitioners

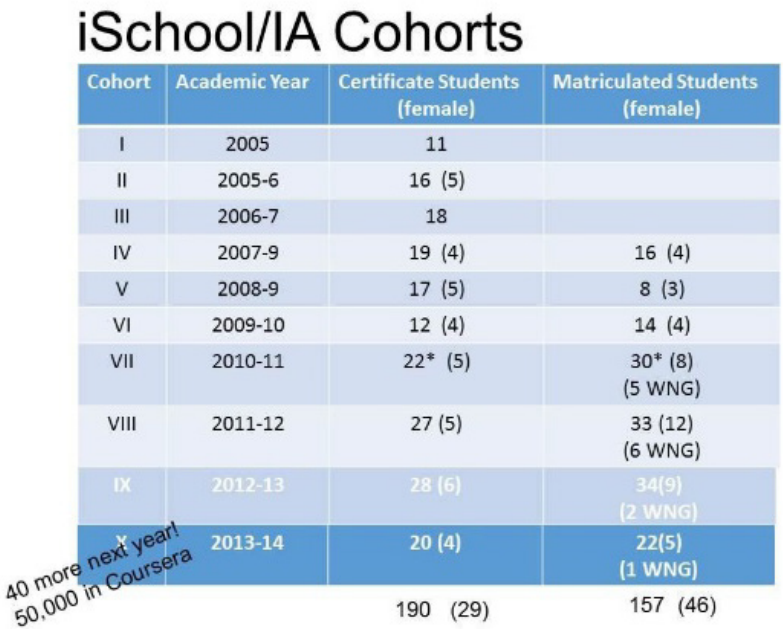

Figure 8 Cohorts of ISRM Certificate Graduates

An example of our use of practitioners in academic programs is our Information Security and Risk Management (ISRM) certificate program developed by Dr. Endicott-Popovsky in collaboration with members of the regional IA community. The program teaches an interdisciplinary systems approach to establishing, managing, and operating a comprehensive IA program in organizations and makes ample use of practitioner guest lecturers who provide a practical perspective on topics covered in the program. The ISRM certificate is now in its 11th year and is offered in either asynchronous hybrid mode or through a MOOC (Massively Open Online Course). Over 300 students have gone through the classroom version of this program to date and many are now in leadership roles in cybersecurity.

Participants from industry who guest lecture in the program include such luminaries as:

1) Kirk Bailey, VP and CISO of the University of Washington,

2) Mike Hamilton, former CISO City of Seattle, founder of both MK Hamilton and Associates and PRISEM, and policy advisor to the CIO of the State of Washington,

3) Michael Simon, nationally-known network design engineer, entrepreneur and author, and now adjunct instructor in our IA programs,

4) Ilanko Subramaniam, VP Global Business Associates and national/international expert in GRC (Governance, Risk Management and Compliance), and adjunct instructor in our IA programs,

5) Seth Shapiro, VP and risk management consultant, Kibble and Prentice, who pioneered development of products that insure against cyber intrusion, also an adjunct instructor in risk management,

6) Steven Schroeder, JD, retired Federal Prosecutor who successfully prosecuted the Gorschkov case, [24]

7) William Nelson, author, teacher and Senior Digital Forensic investigator for The Boeing Company.

Involving the IA community in the program ensures that students are exposed not only to the theoretical foundation of IA and recent research in the field, but also to practitioners who are solving complex problems. The certificate culminates in a practicum that includes actual case experiences drawn from industry, a hands-on attack-defend laboratory with PRISEM and the PRCCDC, and a practical problem that students are invited to solve in collaboration with IA experts from industry. In 2014, University of Washington was ranked the 10th best place for studying cybersecurity in the country by Ponemon Institute for its outcomes-based programs [25].

USAR Cyber Public Private Initiative (P3i) Pilot Program at UW CIAC

US Army Reserve future Cyber initiatives partner directly with UW CIAC in a public-private partnership that increases advanced cyber and IA educational opportunities for Cyber Security soldiers. These educational offerings directly relate to their Cyber positions, duties and KSA development. An example of the urgent need is the Army Reserve Cyber Operations Group transition to 10 Cyber Protection Teams (390 soldiers). This transition enhances and builds a new Army cyber force structure; of which the transition of the ARGOG from 308 soldiers to around 561 soldiers is an instance.

The USAR needed a way to provide continuous education, development and advancement of apprentice and master cyber defense soldiers. The CIAC program with its broad cyber academic and technical program offerings, for resident and distance learning students at three different UW campuses links directly to 3-5 year Army Force Cyber Generation model for skills development. A UW CIAC program, such as UW Tacoma's Master in Cyber Leader (MCL), are matched to USAR Cyber leader skill development and KSAs.

Advanced USAR cyber technical positions, likewise, are matched with more technical cyber degrees such as UW Bothell's software and hardware security engineering programs.

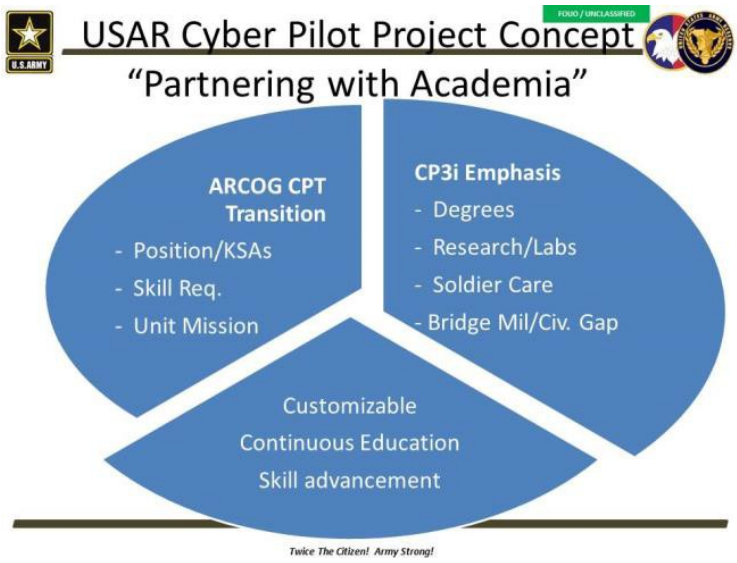

Figure 9 USAR Partnering with Academia

In other words, in the context of our partnership, a CIAC program is directly matched with a USAR Cyber soldier's position and required skill development. After a 3-4 year academic commitment, that soldier will be available for mobilization, having earned a Cyber/IA bachelors, masters or PhD. The CIAC partnership also addresses a gap in methods, tools, TTP (tactics techniques and procedures) and applied research for USAR cyber security units. Our broad partnership includes developing laboratories that provide opportunities for soldiers and students to exercise and research a broad area of cyber security and defense issues impacting industry, government and military operations.

Finally, the CIAC and USAR partnership indirectly bridges a military, industry and public sector gap as citizen soldiers' interact and are employed in civilian positions that directly apply the skills and education from UW degrees in full-time civilian and part-time military careers. At the same time, the Army and DoD gain highly skilled soldiers in support of operational military missions when on annual

training, exercises or mobilized for active duty cyber defense deployments CONUS or OCONUS.

Outreach and Online Offerings

The Center has an active outreach program and has developed online educational offerings to reach students anywhere in the world. This is especially helpful for military students subject to deployment. In the last few years, we have had students participate from the mountains of Afghanistan, on navy vessels and in undisclosed areas that still have network access. We offer complete degree programs in this mode, such as our Master of Infrastructure Planning and Management (MIPM) developed, in partnership with the Washington State National Guard, the Department of Urban Design and Planning and Professional and Continuing Education at the University.

Additionally our flagship education offering, the ISRM certificate, is offered in a hybrid mode, in class and online simultaneously. In addition, the Center, in advisory collaboration with the Pacific Northwest National Labs and Battelle, has presented a public televised lecture series in Information Assurance.

CIAC continues to pursue online offerings like its MOOC being offered through Coursera:

https://www.coursera.org/course/inforiskman.

In the last three years, over 50,000 students worldwide have finished our MOOC offerings. Several have gone on to take certificate or degree programs through the university.

CONCLUSIONS AND FUTURE WORK OF THE CIAC

Through its collaborations, the Center provides significant mutual benefits for industry, the community and other academic institutions. Additionally, our leading, multidisciplinary, IA experts are available to industry and government to develop and implement advanced solutions to complex, real-world IA problems. This

creates a unique environment for rich IA educational and research offerings that attract top talent, including leading faculty and highly motivated students with career and research interests in IA and cybersecurity. This has a stimulating effect on entrepreneurial efforts and innovation that attracts industry and jobs to the region, provides support to regional government for disaster preparedness related to a catastrophic cyber event, and keeps IA professionals on the cutting edge of the discipline, ensuring their competitiveness and the competitiveness of the State.

Over the next three years, the Center will continue to expand its research agenda and its academic programs, bringing together the rich individual and organizational IA talent in the Pacific Northwest. The intent is to facilitate solutions to difficult IA and cybersecurity problems.

Phase 1 -

Expand partnerships: 1) with Pacific Northwest National Laboratory (PNNL) to integrate research programs, building a wider bridge between the two institutions. The Executive Director of the Center is currently partially funded by PNNL which is enhancing the development of the partnership; 2) with Fraunhofer which unites CIAC and Fraunhofer SIT in solving forensic readiness and digital evidence issues; 3) with USAR and the State's National Guard that extends our offerings to current and transitioning military students and assists with ramp up in cybersecurity preparedness of our military and the translation to the civilian world for those leaving military service; 4) with its array of academic, industry and government partners who will provide increased opportunities for learning and careers in IA.

Phase 2 -

During the second phase, the Center will evolve from as an increasingly significant presence nationally with its industry/private sector focus that makes the Center uniquely posed to provide a critical infrastructure perspective on IA that includes the cloud which is forming in the Northwest. This is an orientation that is an important presence in the formation of IA policy and approaches to protecting the homeland.

Phase 3 -

During the third phase, the Center will consolidate its gains and continue to expand in influence and impact. Near term projects include (1) creation of an interdisciplinary, policy-focused, research agenda to integrate the contributions of key researchers involved with the Center, 2) developing a governance model for an expanded Center that has grown and matured in the last decade (3) formalization of CREATES that includes offering cooperative opportunities to learn in the real world, (4) development of technical academic programs with increasing depth, integrated with PRISEM [26] and (5) holding more community security and awareness events as part of our outreach mission [27]

The spectrum of these efforts is directed at public and private organizations/agencies, military, different government levels (local, state, regional and Federal), across a range of other sectors: law and law enforcement, industry, academia, etc. Cyber by its nature is the connective tissue of organizations and the backbone for the flow of information and good decisions. Without identification, detection, protection, response, and recovery it will fail. This connective tissue will only become more dense, complex and critical as the internet of things provides demand, convenience and vulnerability.

REFERENCES

[1] National Security Agency. (No Date) IA Academic Outreach: NIETP. Retrieved July 12, 2014 from the World Wide Web: http://www.nsa.gov/ia/academic_outreach/index.shtml

[2] Gates, W. "Trustworthy Computing," Memo published January 15, 2002. Microsoft Corporation, Seattle, WA.

[3] Kuzmina, U. *Fundamentals of Pedagogy of Higher Education.* (Leningrad, RU: Lenizdat, 1972).

[4] Bespalko, V. *Fundamentals of Theory of Pedagogical Systems.* (Vorenege, RU: Voronege State University Press, 1977).

[5] Talizina, N.F. (1975). Management of the Learning Process. Moscow, Russia.

[6] Roginsky, V.M. (1990). Alphabet of Pedagogical Work. Moscow, Russia: School of Higher Education.

[7] Hutton, G. "Backward curriculum Design Process" Retrieved May 1, 2003 from the World Wide Web: http://www.g4v.com/~glen.hutton/ED3601/BackwardDesi gnFeb11_03.pdf

[8] Bloom, B.S., Mesia, B.B. and Krathwohl, D.R. (1964). Taxonomy of Educational Objectives. New York: David McKay.

[9] Michailova, A.F. (1985). *Establishing a system of professional–practical activity*. Moscow, Russia: Messenger of Higher Education, No. 11, pp. 31-33.

[10] Talizina, N. F. (1986). *Activity Approach to the Development of the Model Specialist*. Moscow, Russia: Messenger of Higher Education, No 3, pp. 10-14.

[11] Endicott-Popovsky, B.E. and Frincke, D., (2003, June). *A Case Study In Rapid Introduction of Computer Security Curricula*, in Proceedings from the Seventh Colloquium for Information Systems Security Education 7-10, June 2004, Washington, D.C.

[12] 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 Education and Training 1-3 March 2004, Norfolk, VA, pp. 118- 123.

[13] Endicott-Popovsky, B.E., Frincke, D., Popovsky, V.M. *Designing a Computer Forensics Course for an Information Assurance Track*, in Proceedings from the Eighth Colloquium

for Information Systems Security Education 7-10, June 2004, United States Military Academy, West Point, NY, pp.59-64.

[14] Endicott-Popovsky, B.E., Taylor, C., Popovsky, V.M., (2005, February). *International Curriculum Design for Undergraduate Computer Science*, in Proceedings of SIGCSE Technical Symposium on Computer Science Education.

[15] Endicott-Popovsky, B.E., Frincke, D., Popovsky, V.M., (2005, June). *Secure Code: The Capstone Class in an IA Track*, in Proceedings from the Ninth Colloquium for Information Systems Security Education 6-9, June 2005, Georgia Institute of Technology, Atlanta, GA, pp.100-108.

[16] Popovsky, V.M., Endicott-Popovsky, B.E., *Physical Culture Pedagogy: Coaching by Design*, V.E. Grigoriev (Ed.). (2005) Methods for Modernizing Physical Culture: Selection of Scientific and Methodological Works, St. Petersburg, Russia, pp. 176-187.

[17] Endicott-Popovsky, B.E., Seifert, C. Frincke, D. *Adopting Extreme Programming on a Graduate Student Project*, in Proceedings from the Sixth IEEE Systems, Man and Cybernetics Information Assurance Workshop 15-17 June 2005, United States Military Academy, West Point, NY, pp.454-455.

[18] Popovsky, V.M. (1988) *The System of Continuous Pedagogical Practice in IPC*. S.P Evseev and V.M. Popovsky(Ed.) Organization and Methodology of Continuous Pedagogical Practicums in the Institute of Physical Culture: Academic Methodological Benefits, Leningrad: Lesgaft Institute of Physical Culture.

[19] Ageevec, V.U., Popovsky, V.M., Filippov, S.S. (1984) *The Mini–Department of the Institute of Physical Culture–A New Form Of Student Work*. Theory and Practice of Physical Culture, Moscow: Russia, No 11.

[20] *Networks: A Post Mortem*, in Proceedings of the Safety and Security in a Networked World: Balancing Cyber- Rights & Responsibilities Conference at the Oxford Internet Institute, The University of Oxford, Oxford, England. Retrieved September 9, 2005 from the World Wide Web: http://www.oii.ox.ac.uk/research/cybersafety/?view=papers

[21] National Academies of Science. Rising above the Gathering Storm: *Energizing and Employing America for a Brighter Economic Future*. (Washington, D.C.: The National Academies Press, 2005).

[22] Endicott-Popovsky, B.E., Orton, I., Bailey, K. Frincke, D. *Community Security Awareness Training*, in Proceedings from the Sixth IEEE Systems, Man and Cybernetics Information Assurance Workshop 15-17 June 2005, United States Military Academy, West Point, NY, pp.373-379.

[23] Endicott-Popovsky, B. and Popovsky, V. (2013). Application of pedagogical fundamentals for the holistic development of cybersecurity professionals. *ACM Inroads, Cybersecurity Edition, March 2014.*

[24] NIST/NICE framework http://csrc.nist.gov/nice/framework/

[25] Sherman, E. *Peer to Peer.* (2005, January) In Information Security, Retrieved March 18, 2006 from the World Wide Web: http://informationsecurity.techtarget.com/magItem/0,291266,sid42_gci1042652,00.html

[26] Hartmann-Siantar, C, Lazowska, E., Maurer, S., Savage, S., and Voelker G. (2005, Autumn). CSE P 590TU: Homeland Security / Cyber Security. Retrieved March 18, 2006 from the World Wide Web: http://www.cs.washington.edu/education/courses/csep590/05au/

[27] Endicott-Popovsky, B.E., Ryan, D., Frincke, D. (2005, September). *The New Zealand Hacker Case: Tracking Down a Vengeful Hacker Through Public Networks: A Post Mortem*, in Proceedings of the Safety and Security in a Networked World: Balancing Cyber-Rights & Responsibilities Conference at the Oxford Internet Institute, The University of Oxford, Oxford, England. Retrieved September 9, 2005 from the World Wide Web: http://www.oii.ox.ac.uk/research/cybersafety/?view=papers

[28] Ponemon Institute, 2014 Best Schools for Cybersecurity Report. Retrieved at: http://www.ponemon.org/library/2014-best-schools-for-cybersecurity

[29] National Academies of Science. *Rising above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future.* (Washington, D.C.: The National Academies Press, 2005).

[30] Endicott-Popovsky, B.E., Orton, I., Bailey, K. Frincke, D. *Community Security Awareness Training*, in Proceedings from the Sixth IEEE Systems, Man and Cybernetics Information Assurance Workshop 15-17 June 2005, United States Military Academy, West Point, NY, pp.373-379.