CASE STUDY: National CYBERSECURITY Centers

PI: Casey O'Brien, National CyberWatch	NSF Award #1204533, 1601150	www.nationalcyberwatch.org
PI: Corrinne Sande, NCyTE	NSF Award # 1800589, 1902329	www.ncyte.net
PI: John Sands, CSSIA	NSF Award #1465163	www.cssia.org

EXECUTIVE SUMMARY

This study identifies the structural conditions that promote collaboration between centers. The Center for Systems Security and Information Assurance (CSSIA), the National Cybersecurity Training & Education Center (NCyTE; formerly CyberWatch West), and the National CyberWatch Center are a consortium of cybersecurity centers funded through the National Science Foundation (NSF) Advanced Technological Education (ATE) program that have a long history of cooperation. Collectively, the three centers address the common problem of preparing the technical cybersecurity workforce by focusing on complementary efforts, resulting in a synergistic approach. Each center has its own areas of focus, including mentoring, faculty development, curriculum, student assessments and cyber competitions, that build upon and complement each center's work. Understanding the conditions that allowed these centers to achieve such deep collaboration may be of use to other centers seeking to expand their reach and spread their innovations.

ACRONYMS:

CAE-2Y	National Centers of Academic Excellence in Cyber Defense Two-Year
CCDC	Collegiate Cyber Defense Competition
CSSIA	Center for Systems Security and Information Assurance
NCC	National CyberWatch Center
NCL	National Cyber League
NCyTE	National Cybersecurity Training & Education Center (formerly CyberWatch West)
WCC	Whatcom Community College

BACKGROUND OF CENTERS

CSSIA

The Center for Systems Security and Information Assurance (CSSIA), headquartered at Moraine Valley Community College, IL, has been an NSF ATE-funded center since 2003. CSSIA provides students with real-world learning experiences in information assurance and network security through several program

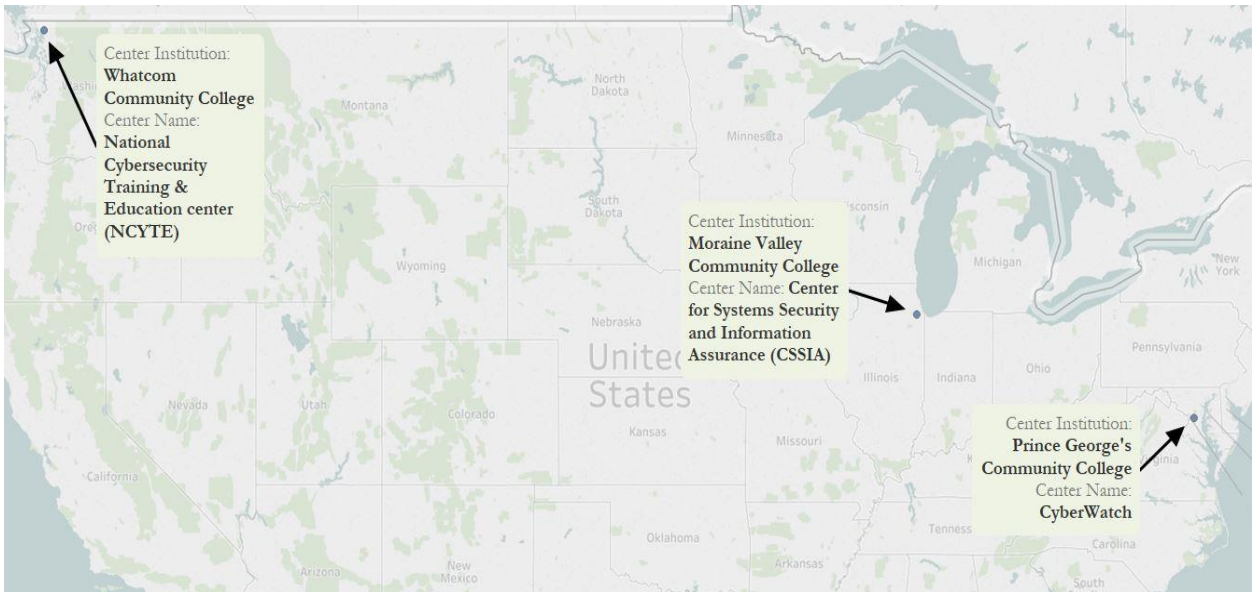
improvement initiatives. CSSIA focuses on curriculum, faculty professional development, and support of certificate and degree programs and internships.

National CyberWatch Center

Headquartered at Prince George's Community College, MD, National CyberWatch formed in 2005 with five community colleges, five four-year colleges, five Cisco Academy high schools, and the Metropolitan Washington Council of Governments with the express goal of increasing the quantity and quality of the Information Security workforce in the D.C. metropolitan region. The Center's approach includes:

- Developing curriculum for a range of Information Technology (IT) and security-based courses
- Conducting defense and forensic competitions
- Connecting students with internships
- Developing educational pathways
- Creating technology to assist with interactive teaching and learning

National CyberWatch is a member organization with over 400 two- and four-year schools in the network. In 2003, the PI of CSSIA was a member of the Center's NSF National Visiting Committee (NVC), tasked with assessing the plans and progress of the project and reporting to NSF and the project leadership. National CyberWatch will remain funded through 2021 as a National ATE center. After this grant phase, National CyberWatch will apply for additional NSF funds to serve as a resource center.



NCyTE

The National Cybersecurity Training & Education Center (NCyTE; formerly CyberWatch West) was initially funded in 2011 at Mount San Antonio College as a regional center, building off the work of CSSIA and CyberWatch to increase the quantity and quality of the cybersecurity workforce throughout the western United States. NCyTE is now funded as a national resource center based at Whatcom Community College in Bellingham, WA (moving from Mount San Antonio College in California in 2013). Prior to the establishment of the center, there were minimal cybersecurity education degree opportunities on the west coast. In fact, WCC was the only community college on the west coast that had the CAE-2Y designation. (CAE-2Y Program designation is evidence of having met the rigorous requirements established by the National Security Administration and the Department of Homeland Security.) As part of its mission, NCyTE mentors other colleges and universities to achieve the CAE designation nationwide.

A SHARED MISSION: MOTIVATION FOR COLLABORATION

Each of the PIs spoke about the shared mission of improving cybersecurity education opportunities in service of a strong technical workforce. CSSIA PI Sands noted that collaboration starts with shared goals. He noted that "we're all solving the same problems, but have different approaches." NCyTE has a greater emphasis on mentoring, establishing veteran, high school, community college and university pathways and in supporting other colleges in earning the CAE-2Y designation. National CyberWatch has an emphasis on curriculum development, dissemination, and assessments. CSSIA focuses on faculty development and has a strong research arm. The centers rely on each other's expertise in both their respective specialty content areas and for administrative tasks, or functions such as marketing. The centers sometimes share the development of projects, such as building a national contact library for all the community colleges reached through the ATE centers. **PI Sands recognizes that, "the [workforce] problem is so big we need each other. We're stronger as a group than if we're operating individually."** Each center is represented on the NVC of the other, allowing for higher levels of strategic coordination of center efforts.

"we're all solving the same problems, but have different approaches"

Through the collaborative efforts of the ATE cybersecurity centers, the opportunity for community colleges to offer robust programs has expanded.

Cyber Competitions

Running cyber competitions is a unifying and signature feature of the centers. Each center serves as a regional hub for the National Collegiate Cyber Defense Competitions. Participants from the community colleges are well represented and frequently outperform university students. The centers have since developed the National Cyber League, a competition that is more accessible to community college students and leverages curriculum and labs developed through the ATE centers (see page # for more information).

Shared Activities: Examples of Collaboration

2005-2012: CSSIA and National CyberWatch

CSSIA and National CyberWatch have a long history of collaboration, working for half a decade before NCyTE was funded. A 2012 impact report prepared by the centers' evaluators found a significant impact from the joint efforts of the two centers. Fruits of this collaboration include:

- Curriculum development including degree programs and stackable credentialing.
- Professional development for over 3,000 faculty as of 2012.
- Program capacity building at other colleges through consultation and the sharing of materials.
- Increasing student participation (see Figure 1 for a graph of cybersecurity enrollments through CCSIA and National CyberWatch).

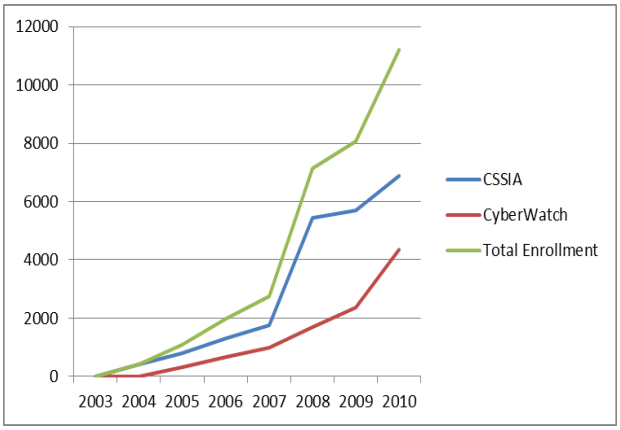


Figure 1: Growth in early enrollment in cybersecurity programs through CSSIA and National CyberWatch

The three centers together have collaborated on endeavors such as:

- The Community College Cybersecurity Summit (3CS), an annual conference produced by the three centers (starting in 2014) and other ATE centers[1] to focus on cybersecurity education at two-year schools. The summit includes showcasing innovative practices, workshops for skills development, and topical sessions. Approximately 500 people attend the annual event, at times maxing out the available physical space (colleges donate space to host the conference, and most don't have facilities for more participants). The conference is self-sustaining through sponsorships and nominal registration fees, relying on volunteers to staff many of the event's functions.
- The regional competitions of the National Collegiate Cyber Defense Competitions (CCDC), in which up to eight full-time students per school participate, with the winners going to the national event. Though the competition wasn't started by the centers, the centers coordinate in hosting it, and have had a significant role in its expansion. Historically, the Mid-Atlantic regional CCDC (run by National CyberWatch) and the Midwest regional CCDC, run by CSSIA, have the largest numbers of schools participating each year. Between these two centers, five national CCDC champions have been crowned in the past 14 years. NCyTE has provided extensive support to the Pacific Rim Regional Competition, and the PI served on the operations and planning team from its founding, along with providing support for students to participate.

2012-current: National Cyber League

The National Cyber League (NCL) is a non-profit organization founded by four ATE centers and one university partner[2] that supports learning through cybersecurity competitions. The NCL provides "an ongoing virtual training ground for participants to develop, practice, and validate their cybersecurity knowledge and skills using next-generation, high-fidelity simulation environments."

[1] Broadening Advanced Technological Education Connections (BATEC), Mid-Pacific Information and Communication Technologies (MPICT)

[2] The George Washington University Cybersecurity & Privacy Research Institute and the Mid-Pacific Information and Communication Technologies (MPICT) Center, an NSF ATE funded center.

Through involvement in the CCDC, it became clear to the centers that cybersecurity competitions favored four-year schools in the way that they were structured. The CCDC events were often expensive, requiring year-long involvement and limiting participation to full-time students, which limited community college student involvement. National CyberWatch, CSSIA, and their partners identified the opportunity to create a semester-based competition that would be more inclusive of community college students. In 2012 a supplement was awarded to CSSIA to pilot a new competition, open to all students, that leveraged the educational resources (curricular materials, labs and professional development) and technology (virtual "training" and "competition" venues) that CCSIA, National CyberWatch and partners had developed. The NCL provides a training ground for collegiate students to develop and practice their cybersecurity skills through combined individual and team exercise by removing the requirement for full-time student status and moving to a completely virtual platform. This allows an unlimited number of students from each school to participate and reduces the cost for participation.

There are now 5,000 students representing hundreds of two- and four-year schools participating in the event each fall and spring (see Figure 2). The virtual nature of the NCL has allowed the competition to scale effectively by accommodating any number of students interested in participation, from any location. Many of the schools integrate the competition into their classrooms as a way to develop their students' knowledge and skills. PI O'Brien notes that "embedding learning objectives and content into the classroom has been what helped make it grow and make it an integral part of higher education curricula."

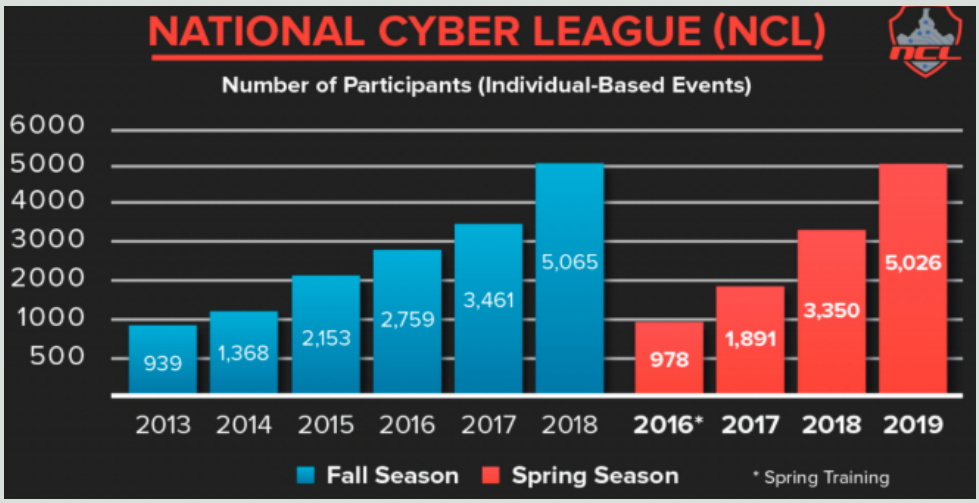


Figure 2: Participation in the National Cyber League (taken from 2019 National CyberWatch Center Annual Report)

Although developed through grant funding, the NCL no longer relies on grants. NCL is now an independent non-profit 501(c)(3) organization supported through nominal student competition fees ($25), which schools often subsidize. The NCL board is made up of representatives from CSSIA, National CyberWatch and NCyTE, and all of the incorporated labs are developed by the ATE centers.

CONDITIONS FOR COLLABORATION

Leadership

When trying to parse what conditions needed to be in place to facilitate collaboration, PI O'Brien identified four attributes of the centers' host college leadership that created a culture of partnership:

1. The willingness to collaborate came from the top. All three centers reside on campuses where the college presidents understand and embrace that the conditions of the grant funding of the centers require a national perspective, going beyond the local service area of the institution.

Cybersecurity graduates have employment opportunities nationally, thus the individual college programs are not necessarily developed to meet local workforce needs. Taking a national perspective, however, does not preclude the need to invest in local relationships.

2. The presidents of Moraine Valley and Prince George's community colleges knew and trusted each other prior to the grant awards. They have worked closely with the president of Whatcom Community College as she has emerged as a leader in this space. PI O'Brien has noted a "concerted effort [among the presidents] to lift each other up."

3. Beyond the grant, the presidents of Moraine Valley Community College, Prince George's Community College and Whatcom Community College have all been participants in the national conversation around cybersecurity workforce development and the role of community colleges. Each of these presidents has had leadership positions on the board of the American Association of Community Colleges (including two who have served as president of AACC). As PI O'Brien noted, "It's one thing to have a president that supports your project, and another to support a national initiative."

4. The presidents of all three colleges are champions of cybersecurity education/workforce development outside their respective service areas. Each center PI has facilitated their president's success in advocating for cybersecurity education by keeping their administration abreast of center accomplishments. PI Sande reports that the president of Whatcom was particularly interested in hosting the grant, expecting the grant to bring resources to help improve and expand the college's existing program, along with increasing the number of programs at other colleges, thus contributing to easing the national workforce crisis.

Personal Connection and Philosophy

The PIs of the three centers enjoy working together. Founding CSSIA PI Erich Spengler[3] helped PI O'Brien think through how to operationalize the National CyberWatch Center. The two PIs, who had enormous respect for each other professionally and shared similar technical interests, developed a personal friendship.

Both PIs Sands and Sande spoke about a philosophy of sharing. PI Sande noted that "if your goal is to help others grow programs and graduate students into the workforce, you can't accomplish that if you're unwilling to work with anyone else. If your goal is to build up yourself or your school, then you'd be less likely to collaborate with others because you feel like your work is being diluted in doing that."[4] PI Sands said that CSSIA has worked with other centers beyond cybersecurity. "What makes it work or not is when you're willing to share anything. If you're willing to share, it works. Some centers are reluctant to share, thinking that people will 'steal our idea.' PI Sands goes on to explain that when you evolve an idea and apply it to something new, its impact is increased. Plus, "other people copying our ideas means it's a great idea."

[3] The untimely death of PI Spengler was a blow to the cybersecurity and ATE community. John Sands took over as PI of CSSIA, having been part of the CSSIA team since the beginning. Although the priorities of the centers ebb and flow in terms of alignment, the PIs continue to enjoy a collaborative relationship.

[4] PI Sande further noted that through collaboration the college has benefitted from increased enrollments (about 17% per year), increased faculty, expanding the physical space from one lab to an entire building and the prominence of the college's name. In addition, the college president has become involved in a National Initiative for Cybersecurity Education (NICE) Academic Working Group and is involved in leadership roles in cybersecurity as a college president.

The three PIs are in regular phone communication around different initiatives, and PI Sands notes that he sometimes speaks with PIs O'Brien and Sande more frequently than his own staff. Also, with 10-12 events per year that each of the PIs attend, there is ample opportunity for face-to-face collaboration.

PI O'Brien noted that "there is no real incentive for centers to work together. There is often competition amongst the centers. There are lots more disincentives than incentives to collaborate. It takes people who buy into collaboration for the sake of collaboration, believing we can do more collectively than independently."

Funding Considerations

The ATE funding that launched these centers has created an environment of both collaboration and competition. When CSSIA, National CyberWatch and NCyTE were founded, the ATE program was supporting a national center with regionally-based resource centers for technical education in each discipline (e.g., Biotechnology, IT, Photonics). Each of these centers was responsible for a region of the United States, and those involved felt that there was more than enough work to go around.

Over time, NSF funding has become a bit more competitive, and the cyber centers have taken a broader, national perspective, which has led to feelings of competition as each carves out their unique space in the marketplace. Acquiring other sources of funding, however, mitigates the existential risk of the centers. For example, National CyberWatch has funding from the Department of Education, the Department of Defense, and some revenue generating activities. CSSIA similarly has a diversified funding portfolio and will continue its faculty development academy without NSF funding. NCyTE has benefited from other NSF directorate funding, as well as NSA and DoE funding. The expectation is that the centers will continue even after ATE funds expire. As PI O'Brien reports, "We can collaborate as needed and be competitors in other areas. It's healthy for our institutions and our constituents. We want the best products and solutions for our schools to be successful."

The curricula and labs that provide the base of the NCL experience were all developed through CSSIA and National CyberWatch using federal dollars. Thus, the PIs felt strongly that these materials are part of the public domain, minimizing any issues associated with intellectual property ownership.

> **Finally, PI Sands indicated that the relationships each center has with their local industry partners facilitate private fundraising. He noted that many of the donors are "local companies, and want to invest locally" so there isn't significant overlap in the donor base among centers.**

Though the centers have benefited from a significant investment of funds from NSF, the resources are still limited, and the cybersecurity technical education needs are vast. John Sener, National CyberWatch (and for a period, NCyTE) external evaluator reports he often has to say "remember, they gave you $4 million, they didn't give you $30 million" in an effort to support projects in staying focused. As the program matures, staying focused on what the Center does well will increase efficiencies, allowing it to take on additional work.

Organizational Structure

The organizational structure in which the centers operate and the structures in which they scale are both important. The depth of support for the centers within their community college institutions is critical.

For elements of the centers that have the potential to be self-sustaining, establishing independent entities remains a consideration. Just as the NCL formed to support the competition components, National CyberWatch considers creating independent non-profits for its programs that benefit from the flexibility of a legal entity. This separate entity will be able to respond to market needs at the speed of business.

Impact on the Institutions

When there is quality programming and the value of the center is supported by the administration, the resulting feedback loop reinforces the prominence of the center at the college. At Whatcom, NCyTE promotes its work through ongoing updates to the Board of Trustees and through the press. CSSIA presented an impact report to the board showing that the center has brought nearly $30 million dollars to the college. The college has since institutionalized several center positions.

Planning for Sustainability

Though the centers each operate with a national focus, CSSIA, National CyberWatch and NcyTE have supported each other as they each followed the ATE funding trajectory: regional center → national center → resource center. The timing of their awards has created a sibling-like relationship, with each center learning from their older sibling. Mr. Sener recalls, for example, “that there was a decision that although it could have been competitive, it was more like CSSIA ceded the national center to National CyberWatch.”

In another instance, when planning to transition to a national center, NCyTE heeded advice from the other centers and didn’t wait until they had funding to take a national approach. In advance of the proposal preparation, they began to provide resources developed through previous grants and to recruit national members, which allowed them to identify their potential national impact as part of the grant proposal.

CONCLUSION

The cybersecurity centers have collectively addressed a complex educational domain. The centers have operated in close alignment to one another, each with a unique identity but a shared vision for how they relate. In doing so, they have advanced cybersecurity technical education at two-year colleges more quickly and robustly than any one center would have been able to do independently. As the national cybersecurity workforce crisis deepens, their combined efforts are needed now more than ever.