Virginia Cyber Navigator Internship Program (VA-CNIP): Service Learning in Local Election Security

Angela Orebaugh
Computer Science
University of Virginia
Charlottesville, Virginia, USA
angelao@virginia.edu
0000-0001-7676-681X

Jack Davidson
Computer Science
University of Virginia
Charlottesville, Virginia, USA
jwd@virginia.edu
0000-0002-5883-8274

Deborah Johnson
Engineering and Society
University of Virginia
Charlottesville, Virginia, USA
dgj7p@virginia.edu
0000-0002-4783-8279

Daniel Graham
Computer Science
University of Virginia
Charlottesville, Virginia, USA
dgg6b@virginia.edu
0000-0002-0518-0333

Worthy Martin
Computer Science
University of Virginia
Charlottesville, Virginia, USA
martin@virginia.edu
0000-0002-5385-5163

***Abstract*—A coalition of Virginia universities, in partnership with the Virginia Department of Elections (ELECT), launched the Virginia Cyber Navigator Internship Program (VA-CNIP) – an innovative educational program to develop future cybersecurity professionals to protect the election infrastructure. The program addresses the need for more skilled cybersecurity professionals, and those who are supporting public services such as elections. This paper provides an overview of the key components of the program: a full semester gateway course covering sociotechnical election topics, a two-day kickoff bootcamp to prepare students for their internship, an internship with an election office, and a one-day debrief and assessment at the end of the internship.**

Keywords—cybersecurity, elections, security education, experiential learning, service learning

I. INTRODUCTION

Fair and secure elections are essential to democracy. Our nation's voting systems are as much a part of our nation's critical infrastructure as are transportation, energy, financial, communications, and water systems. In January 2017, the United States Department of Homeland Security designated election systems as part of the nation's critical infrastructure [1]. Thus, the importance of securing state and local voting systems that support both national and local elections cannot be understated. Yet, while the federal government has designated election infrastructure as critical, the administration of elections is largely decentralized. The U.S. Constitution grants states the right to regulate and administer elections and this means that voting laws and procedures vary from state to state. While this gives states a good deal of autonomy to administer elections, elections are generally implemented at the county or city/town level. Thus, just as there is variability from state to state in the administration of elections, there is variability in infrastructure and implementation at the local level.

II. THE CONTRIBUTION

A coalition of Virginia universities, in partnership with the Virginia Department of Elections (ELECT), have launched the Virginia Cyber Navigator Internship Program (VA-CNIP) to create an innovative educational program to train future cybersecurity professionals to protect election infrastructure [2]. ELECT's mission is to promote and support secure, accurate, fair and open elections for the citizens of the Commonwealth. To support the mission, ELECT created the Cyber Navigator Program (CNP) involving universities and colleges in Virginia and the VA-CNIP project builds on and expands the CNP.

The University of Virginia is leading the VA-CNIP effort along with other university and industry partners including George Mason University, Norfolk State University, Old Dominion University, Virginia Commonwealth University, and Virginia Tech. The VA-CNIP is supported by a multi-year National Security Agency grant for National Centers of Academic Excellence in Cybersecurity. The VA-CNIP course curriculum and supplemental materials will be shared and open source, so that other states' can adopt the program and offer it to their students.

To help enhance the security posture of local election infrastructures in Virginia, the VA-CNIP built a regional cybersecurity coalition of Commonwealth of Virginia Universities and Colleges partnering with ELECT and industry. Several external industry organizations have agreed to participate. These organizations include the Greater Washington Partnership, Leidos, Veracode, Ernst & Young LLP, Capital One, Accenture Federal Services, General Dynamics Information Technology (GDIT), Praxis Engineering Fortinet, and LMI. Coalition members are involved in the overall goal of improving the cybersecurity of local registrar offices across the Commonwealth while simultaneously providing a valuable educational experience for students.

ELECT provides the following program support:

- Establishing cyber security needs of the local government units concerned with elections.
- Facilitating the selection of the local government units.
- Ongoing coordination of communication between the local government units and the academic groups.
- Making presentations to the interns, as a group, about the governmental aspects of security with regard to the overall voting process, e.g., voter registration as well as the voting process.
- Being a resource for an assessment process with regard to the attained cyber security levels in the local government units.
- Being a resource for an assessment of the internship program, e.g., the process to attract qualified students and supervise their activities with the local government units.

III. RELATED WORKS

The U.S. Cyber Navigator Program is a nationwide effort that created "state liaisons that can help under-resourced local jurisdictions manage their cyber risks, help sort through the onslaught of risk information, advice, and available services, and help fast-track mitigation efforts" [3]. In recent years, at least seven states including Florida, Illinois, Iowa, Massachusetts, Michigan, Minnesota, and Ohio have launched cyber navigator programs [4]. These programs offer local election officials state-backed contracts for cybersecurity support [4].

Illinois was the first state to create a cyber navigator program, in response to the 2016 voter registration system attack, by hiring nine cyber navigators to assist the state's 108 election offices [4, 7]. The program, costing over $5 million annually, has a line item in the state's budget and is funded through federal Health America Vote Act (HAVA) grants [4]. Illinois Cyber Navigators provide several services to local election offices including risk assessments, best practices and guidance, and incident response [5]. Similarly in Massachusetts, one cyber navigator is assigned to each of the areas five regions, each consisting of about 70 towns [4].

While several states have created Cyber Navigator Programs for fulltime and contract support, to the best of our knowledge VA-CNIP is the first internship program designed to support a state's election security needs with student interns while fostering career and cybersecurity workforce development.

IV. VIRGINIA CYBER NAVIGATOR INTERNSHIP PROGRAM GOALS

The goals of the VA-CNIP are:

1. **To assess the security of Virginia's election system, a system that includes 133 local election offices (95 in counties and 38 in independent cities)**.
2. **To provide students with cybersecurity education focused on election systems and an experiential, service learning opportunity as interns in election districts working on their cyberinfrastructure**. This goal responds to the urgent need for a labor force of excellently trained cybersecurity experts.
3. **To have the internship program serve as the focal point for coalition collaboration**. The internship program consists of a course offered at universities that are part of the coalition; a bootcamp preparing interns for their internship experience; the internship supporting the cybersecurity of an election district; and a debrief meeting to reinforce what students learn during their internships, assess the effectiveness of the internships, and learn how to improve for the next year's program. Members of the coalition from the universities, ELECT, and industry representatives are involved in various ways in planning for these components of the internship program. Industry partners are engaged during course design and delivery and they participate in career development activities organized for the VA-CNIP interns to discuss what qualities and skills they seek in interns.
4. **To posture the coalition for future and sustainable collaboration**. Potential forms of collaboration facilitated by the VA-CNIP especially between universities and colleges include joint course development and enhancement, cross-listing courses across schools, co-teaching, student activities that involve students from different schools, and a speaker series that features activities at coalition schools. Potential forms of collaboration with industry partners include company site visits, career fairs, guest speakers, and funding support for the program.

Equally important to securing our nation's election processes, securing other vital government infrastructures is also important. We believe the VA-CNIP can serve as an inspiration and model for other public interest cyber security internship programs.

V. PROGRAM DESIGN AND IMPLEMENTATION

A. Pedagogical Approach

Interns are working in the service of public good. Service learning is a teaching method that enriches education by engaging students in meaningful service to their schools and communities. Previous research has shown that service learning can substantially enhance coursework by involving students in relevant, real-world activities [8, 9, 10]. Creating opportunities for students to provide a valuable service to their community and society increases student motivation and interest in the subject field. It provides a real-world setting for students to develop skills and personal growth relevant to their career path. The VA-CNIP engages with the career development offices at our schools and with our

industry partners to ensure that students have a rewarding internship experience and to create awareness of the many employment opportunities in the field of cybersecurity.

B. Gateway Course

The program includes a full semester gateway course called "Cybersecurity and Elections" that introduces students to the major sociotechnical aspects of election security and provides knowledge, skills, and abilities in areas that are essential to prepare the students for a productive internship with a local election office. The gateway course was developed by a team of coalition faculty members. The goals of the gateway course are to:

- Discuss the historical, cultural, and political significance of voting.
- Provide students with an understanding of the technical issues of securing election processes.
- Introduce students to careers in service for public good.

Learning outcomes help students anticipate what they will gain from an educational experience, track their progress, and know in advance how they will be assessed. The gateway course learning outcomes include:

- Understand election system and legislative history of voting in the U.S.
- Understand the cultural significance of voting in American democracy and the important role of trust.
- Identify threats, vulnerabilities, and attacks in election infrastructures.
- Understand election system security standards and regulations including the Virginia Department of Elections Voting Systems Security Policies, Standards, Guidelines, and Locality Election Security Standards (LESS).
- Assess security controls for voting systems, voter registration databases, and associated IT infrastructure and systems used to manage elections.
- Explore cybersecurity careers in the public sector.

The gateway course is designed as a flexible set of modules that build upon an introductory cybersecurity foundation. The recommended prerequisite cybersecurity knowledge includes: CIA triad, defense-in-depth, access control, cryptography, network security, risk assessment, security testing and monitoring, security policies and procedures, incident management, and security awareness training. Fig. 1 shows the gateway course modules. The two required modules for any Cybersecurity and Elections gateway course include *U.S. Election Systems History & Background and Voting Systems Security Background & Standards*.

A brief description of each module is as follows:

- **U.S. Election Systems History & Background** – This module addresses the history of election systems; social context of voting; legislative history including the Voting Rights Act (VRA) and HAVA; state and jurisdiction variations; and Virginia elections and organizational structure including the State Board of Elections (SBE), ELECT, locality Election Boards (EB) and General Registrars (GRs).
- **Voting Systems Security Background & Standards** – This module focuses on the people, processes, & technology in elections; standards; regulations; policies; election infrastructures; election operations; and an intro to security requirements such as the Voting Systems Security Guidelines (VSSG) and LESS.

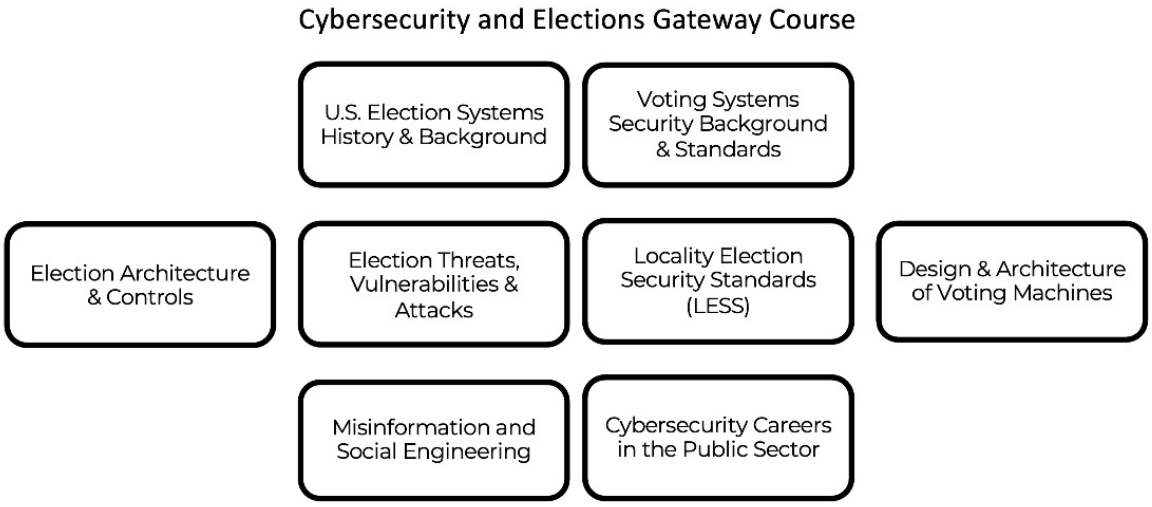

Fig. 1. Cybersecurity and Elections Gateway Course Modules

- **Election Architecture & Controls** – This module provides an overview of each of the election architecture components and security controls including the voter registration database, data transfer, Election Management Systems (EMS), Electronic Poll Books (EPBs), communications controls, network controls, access management, system management, recovery, and continuity of operations.
- **Election Threats, Vulnerabilities & Attacks** – This module addresses topics such as fraud, tampering, the Democratic National Committee a (DNC) attack, vulnerabilities, and election security research.
- **Locality Election Security Standards** – This module covers the twenty one areas of LESS and methods and tools to assess for compliance with LESS.
- **Design and Architecture of Voting Machines** – This module covers the hardware and software of voting systems; encryption; security vulnerabilities; and Internet and mobile voting.
- **Misinformation and Social Engineering** – This module introduces the concepts of misinformation, disinformation, and malinformation and how they are used to disrupt elections.
- **Cybersecurity Careers in the Public Sector** – This module includes the opportunity to explore a variety of cybersecurity careers in the public sector through videos, career searches, and guest speakers.

Course learning assessments include seven homework assignments, four quizzes, class participation, written midterm exam, and written final exam. The course also features a variety of government, industry, and alumni guest speakers, as well as a career development panel. In Spring 2022, an inaugural version of the course was offered by all schools participating in VA-CNIP. The course was offered in both in-person and online formats.

C. Bootcamp

As part of the internship, students participate in a two-day kickoff bootcamp designed to prepare students for their internship assignments. These activities include all interns, faculty mentors, local registrars and support staff, industry representatives, and representatives from ELECT. The kickoff bootcamp is designed as a career development activity. The University of Virginia's School of Engineering's Center for Engineering Career Development participates in the kickoff bootcamp to help prepare the interns so they make the most of, what for many, is their first professional experience. The bootcamp also hosted many guest speakers including speakers from ELECT, CISA, NSA, industry, and alumni.

The bootcamp is also an important event for building community. It provides opportunities for interactions between faculty at multiple universities; faculty and industry; and between interns and their election locality representatives as well as with industry. The bootcamp is an opportunity for students at different universities to meet one another and form a network that they can draw on during their internships, communicating with one another to share their experiences. In bringing all the members of the community together, the bootcamp builds a sense of unity, commitment, and purpose among all the VA-CNIP participants.

D. Internship

After the gateway course and kickoff bootcamp, interns put knowledge into practice and gain real-world experience supporting information systems at Virginia election localities. Interns work in teams of two or three to support an assigned election locality in Virginia. Each intern team is supported by a faculty mentor from the coalition who helps answer questions and provides support throughout the internship. During the summer of 2022 thirty four interns from six participating universities participated in a ten-week paid internship at one of seventeen Virginia election localities, shown in Fig. 2.

Fig. 2. Participating Virginia localities 2022

Interns participate in a variety of cybersecurity activities depending on the locality needs. The Department of Homeland Security (DHS), through its Cybersecurity and Infrastructure Security Agency (CISA), describes election infrastructure as including the following [10]:

- Voter registration databases and associated IT systems.
- IT infrastructure and systems used to manage elections (such as the counting, auditing, and displaying of election results, and post-election reporting to certify and validate results).
- Voting systems and associated infrastructure.
- Facilities for election and voting system infrastructure.
- Polling places to include early voting locations.

The list highlights the complexity of the infrastructure that each locality must manage to secure its elections. Information technology is now a central part, arguably the backbone, of election processes. While offering numerous opportunities for improving and streamlining election processes, information technologies (IT) also open the door to new threats from increasingly adept bad actors. Given the large scope of election infrastructure components, interns may work on a variety of security efforts for their assigned election locality including but not limited to: risk assessment of registrar information systems, analysis of system and network documentation for accuracy, guidance and assistance regarding software patches, systems updates, help configuring and deploying appropriate security software, ensuring compliance with best practices in securing systems, policy review and development, and helping share relevant information with other registrars.

E. Debrief

At the end of the internship, interns participate in a one-day debrief to share their experiences with the coalition faculty and representatives from ELECT. This provides an opportunity to reinforce and frame what they learned. Intern teams present an overview of the work they did for their locality, including outcomes and deliverables. Interns also participate in two focus group discussions that enable them to provide feedback on the rewards and challenges of the internship. Many interns found immense value in supporting election infrastructure and our nation's democracy. They reported an increase in their knowledge of security policies and processes and performing within the bounds of state and local standards and regulations. In addition to the intern debrief, coalition faculty gather feedback from ELECT, the local registrars that hosted interns, and the mentors of the interns. Local registrars reported on the high value of having interns support their locality's cybersecurity. They stressed the importance of incorporating writing and communication along with technical content in curriculum. They all said they would participate in the program again and welcome intern support. The debrief meeting and associated feedback is an opportunity to perform an assessment of the intern learning experience and obtain feedback for improving the internship program for all stakeholders and participants in the next year's program.

VI. CONCLUSION

The VA-CNIP has demonstrated several significant impacts. First, the program helped to ensure the security of the Commonwealth of Virginia's election information infrastructure. Second, VA-CNIP provides a rich, relevant, educational and experiential learning opportunity for students in a critical area of public interest election security. VA-CNIP is a unique approach to cybersecurity education that includes the sociotechnical aspect of cybersecurity, providing students with an understanding of the history and cultural context of voting. The program also enables students to engage with relevant industry companies, especially those interested in supporting work in the public interest. Lastly, and most importantly, VA-CNIP can serve as a model for other universities and states interested in implementing a cyber navigator internship program. Equally important to securing our nation's election processes, is securing other vital government infrastructures. We believe the VA-CNIP can serve as an inspiration and model for other public interest cyber security internship programs.

We expect VA-CNIP to scale as long as resources are available to administer the program at the state and local level. The inaugural summer 2022 internship included seventeen localities who had a need for internship support and were able to administratively support interns. We expect the number of interested localities to increase as the value and results of the inaugural internship are shared. We also expect the number of students interested in the internship to increase as the program is marketed and discussed among peers.

We are preparing the VA-CNIP course, bootcamp, and debrief material to be shared open source through the CLARK repository and the Virginia Cyber Range to enable more educational institutions to participate.

The internships are paid via grant for summer 2022 and 2023 so there was no cost to the state or localities. We are working with the Virginia Department of Elections to explore methods of future funding to ensure program sustainability.

ACKNOWLEDGEMENT

Project sponsored by the National Security Agency under Grant/Cooperative Agreement 2021 NCAE-C-001-2021 Contract Number H98230-21-1-026. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation herein.

REFERENCES

[1] Department of Homeland Security. Election security. https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical, April 2021.

[2] Audra Book. UVA, State Department of Elections Join Forces to Boost Cybersecurity. UVAToday. https://news.virginia.edu/content/uva-state-department-elections-join-forces-boost-cybersecurity, December 2021.

[3] Cybersecurity & Infrastructure Security Agency. CISA Hosts Election Cybersecurity Navigators Forum for State and Local Election Officials. December 2021. https://www.cisa.gov/news/2021/12/21/cisa-hosts-election-cybersecurity-navigators-forum-state-and-local-election

[4] Vasilogambros, Matt. Facing Foreign Election Foes, States Hire 'Cyber Navigators'. August 2021. https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/08/25/facing-foreign-election-foes-states-hire-cyber-navigators

[5] National Institute for Standards and Technology. NICE eNewsletter Spring 2021 Government Spotlight. April 2021. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-enewsletter-spring-2021-government-spotlight

[6] Praetz, N. (2019). Election Security and Large Counties. In: Brown, M., Hale, K., King, B. (eds) The Future of Election Administration. Elections, Voting, Technology. Palgrave Pivot, Cham. https://doi.org/10.1007/978-3-030-18541-1_23

[7] Robert G. Bringle and Julie A. Hatcher. Implementing service learning in higher education. The Journal of Higher Education, 67(2):221–239, 1996.

[8] Janet Eyler and Dwight E. Giles J. *Where's the Learning in Service-Learning? Jossey-Bass Higher and Adult Education Series*. Institution of Education Sciences, 1999.

[9] Jeffrey PF Howard. Academic service learning: a counternormative pedagogy. *New directions for teaching and learning*, 73:21–29, 1998.

[10] Cybersecurity & Infrastructure Security Agency. Election infrastructure security. April 2021. https://www.cisa.gov/election-security