Development of Graduate Level Cybersecurity Programs at North Dakota State University

Dr. Jeremy Straub, North Dakota State University

Jeremy Straub is the Associate Director of the NDSU Institute for Cyber Security Education and Research and an Assistant Professor in the Department of Computer Science at the North Dakota State University. He holds a Ph.D. in Scientific Computing, an M.S. and an M.B.A. and has published over 40 journal articles and over 120 full conference papers, in addition to making numerous other conference presentations. Straub's research spans the gauntlet between technology, commercialization and technology policy. In particular, his research has recently focused on cybersecurity topics including intrusion detection and forensics, robotic command and control, aerospace command and 3D printing quality assurance. Straub is a member of Sigma Xi, the AAAS, the AIAA and several other technical societies, he has also served as a track or session chair for numerous conferences.

Development of Graduate Level Cybersecurity Programs at the North Dakota State University

Abstract

There is an acute need for both graduate and undergraduate degree holders in the cybersecurity field. Approximately one out of three cybersecurity positions is currently unfilled, creating significant potential employment opportunities for students with cybersecurity skills. This paper describes how the North Dakota State University (NDSU) has responded to this demand, creating graduate programs in cybersecurity. Specifically, NDSU has created a graduate certificate in the field and added cybersecurity options to its existing masters and doctoral degrees in computer science and software engineering. These degree programs are described, design decisions are discussed and their current status is qualitatively assessed. Identified future directions are also discussed.

1. Introduction

There is significant focus on the need for cybersecurity professionals. However, many focus on the products of primarily undergraduate programs. In the longer term, the current cybersecurity problems will likely be solved by fundamental and applied research, rather than just preparing skilled technicians and developers to serve on the front lines of a war with those that choose to attack and compromise systems.

Because of this long-term need, the development of quality graduate programs with cybersecurity content is critical. This paper discusses the creation of graduate programs with embedded cybersecurity content at the North Dakota State University (NDSU). While a cybersecurity graduate certificate was developed, a choice was made, for other offerings, to integrate the new cybersecurity curriculum into existing degree programs instead of developing a new cybersecurity degree program.

The created and augmented degree programs support and benefit from an effort in North Dakota to incorporate cybersecurity and computing content in the curriculum from kindergarten through to the end of all Ph.D. programs. They were also developed with the idea of satisfying the requirements for the National Security Agency's Center of Academic Excellence in research in mind.

Four degree programs were augmented. These included M.S. programs in Computer Science and Software Engineering and Ph.D. programs in both these areas, as well. Fundamentally, there was a key choice between extending and developing a new program or programs. The choice to extend allowed the heritage of the existing programs to be leveraged. This approach also exposes learners to core topics that they attain skills in as part of the required Computer Science and Software Engineering curriculums. In addition to producing students that have multiple career path options, it also prepares students with an additional skillset, should demand for cybersecurity professional decline in the future or graduate production increase so much such as to have an overabundance of qualified individuals.

In particular, this approach acknowledges that while graduates may wish to start out their career in cybersecurity, over time they may be promoted or seek out other jobs aligned to more general information technology or software development activities. It also recognizes the long-term role of improving software engineering practices to prevent defects and other issues in software that drive the need for cybersecurity professionals to secure this software and systems.

It is also notable that for secure code development, it is highly beneficial to have computer scientists and software engineers with backgrounds in safe coding practices. Thus these extended programs prepare students for careers outside the core cybersecurity area.

The graduate certificate, alternately, is a four course sequence that is well suited to be taken in conjunction with another graduate degree, by on campus students. It is also designed to serve individuals who perhaps have graduated from a computer science, information technology or similar degree program some time ago and who want to gain new skills to seek a job in cybersecurity.

The degree programs and their requirements and course progressions are presented. Qualitative analysis comparing the types of benefits offered by each is also included.

2. Background

While graduate programs in cybersecurity may not be the "defense against the dark arts (of cyberspace)" proposed by Patel [1], they are an area of significant need (along with undergraduate degrees in cybersecurity). Patel notes that there is a significant need for these graduates, which is resulting in most graduates from graduate level cybersecurity programs getting multiple job offers with higher-than-average starting salaries [1]. The workforce need has translated into expecting graduates to have specific skills, directly from cybersecurity graduate programs, instead of just having general skills [2]. Bocak, Liu and Murphy [2] propose that cybersecurity graduate programs should incorporate specializations to provide these key skills to students. Kumar [3] presents one such example: a graduate program in information security and analytics developed at Coastal Carolina University. Ardis and Mead [4], similarly, discuss the creation of a software assurance-focused graduate program.

A wide variety of techniques have been proposed for cybersecurity education. Competitions [5], [6] are an area that has received significant attention. These include competitions where students configure and defend or defend pre-configured networks [7] as well as in-person [8] and online [9] 'capture the flag' style offensive competitions, the use of peer instruction [10] and mentoring [11] have also been proposed. Other approaches include professional certification-driven curriculum development [12], challenge based learning [13] and systems [14] and multi-disciplinary based approaches [15]. To help determine what approaches are best for this challenge, Mirkovic, et al. [16] propose a protocol for evaluating cybersecurity education interventions that is outcome driven and combines skill assessment, self-assessment and longitudinal follow-up. Harris and Patten [17] suggest the use of Bloom's and Webb's Taxonomies as another approach for driving curriculum development.

The use of a variety of learning technologies has also been proposed. These have included virtual machines [18], [19], augmented reality glasses [20] and cloud-based learning environments [21]. Special focus has also been placed on supporting the growth of women [22] and military service members [23] in cybersecurity education activities. Others have proposed incorporating cybersecurity directly into computer science education [24] and low budget program development [25].

3. Need for Graduate Programs in Cybersecurity

Patel [1] says that the need for graduates from cybersecurity graduate programs is demonstrated in several ways. The first is the consistent hiring of graduates. Purdue's cybersecurity program's masters-level graduates get "five-plus" offers, while Ph.D. graduates will receive two or three. Second, the U.S. bureau of labor statistics projects 37% growth in this need by 2022 [1]. Others have described the need, more immediately, as the field having negative unemployment [26] and the industry experiencing a "crisis" [27].

The demand outpacing supply has resulted in jobs going unfilled or being performed by individuals with less than the desired level of qualifications [26]. It has also resulted in starting salaries that exceed even the higher-than-average salaries for computing graduates, with a starting salary of $116,000 per year for cybersecurity professionals in the Washington D.C. area, for example. At the time of this writing, approximately 30% of cybersecurity positions in the United States are unfiled: with 313,735 open positions, 715,715 filled positions for a total desired workforce size of 1,029,450 [28]. While not all of these positions require graduate education – many don't – graduates with masters and doctoral degrees are needed to educate, lead, review and manage in many areas.

4. Graduate Certificate

The Graduate Certificate in Cybersecurity was initially proposed as a university system wide program. Because of this, it can be completed at NDSU. Alternately, it can be completed by taking courses from other institutions in the North Dakota University System.

The program requires completion of 12 credits of cybersecurity coursework. It was developed to serve a variety of educational goals. For example, it can be taken by students directly after completing their undergraduate degree (in computer science or another discipline). This could, potentially, allow a student to showcase his or her additional competence in cybersecurity, beyond taking relevant coursework at the undergraduate level. The certificate provides an additional credential, attesting to this additional knowledge and experience.

The certificate can also be taken concurrently with a graduate degree, such as a M.S. or Ph.D. in computer science, software engineering or another field. The certificate provides a way to demonstrate graduate-level cybersecurity competence, beyond the standard degree requirement or in conjunction with a degree in an alternate area.

Additionally, the certificate program was designed to serve those already in the workforce. The certificate could serve as a way for someone with a career in information technology to develop

additional cybersecurity skills to use in their current position or to prepare them for advancement into a new position. Alternately, it could serve as a way to demonstrate the knowledge and experience required to allow someone to switch from a career in a completely different field into information technology and cybersecurity.

The suggested completion plan for the certificate is:

- CSCI 603 – Defensive Network Security
- CSCI 604 – Ethical Hacking
- CSCI 609 – Cybersecurity Law and Policy
- One additional course

There are a number of options for the final course. These include, at NDSU:

- CSCI 610 – Computer Crime and Forensics
- CSCI 669 – Network Security
- A computer science special topics or directed / independent study course with a cybersecurity focus.
- MATH 673 – Cryptology

Applicable partner school courses include:

- EE 590 – Emerging Threats and Defenses
- CSCI 558 – Applied Cryptography
- EE 590 – Information Security and Security Practices

Students apply to enter the certificate program and file an additional form upon the completion of their coursework. Students who successfully complete the coursework receive a certificate from the NDSU Graduate School.

5. Graduate Degree Programs

The cybersecurity certificate as well as the cybersecurity degree program components are designed to be able to be completed online. All of the courses recommended for the cybersecurity graduate certificate and degree options are available online and on campus. Many of the optional courses are also available through both methods

The M.S. and Ph.D. degrees are not specifically designed for online completion; however, they can largely be completed online. Attendance on campus is typically required to take the comprehensive examination and for the thesis or dissertation defense (for non-coursework option students). Previously, the department has waived the in-person completion requirement for students that are demonstrably unable to make it to campus.

6. Master's Degree in Computer Science with Option in Cybersecurity

The NDSU M.S. in Computer Science [29] is widely respected within the upper great plains region and beyond. Table 1 presents the course requirements for the M.S. in Computer Science.

Table 1. M.S. in Computer Science Degree Requirements [29].

Course #	Description	Credits
CSCI 713	Software Development Processes	3
CSCI 724	Survey of Artificial Intelligence	3
CSCI 741	Algorithm Analysis	3
CSCI 765	Introduction To Database Systems	3
	Other Credits	Var
	Total required – thesis or paper	32
	Total required – coursework	36

As part of completion of the degree, students can elect to take a nine-credit option in cybersecurity. Because of the flexibility of the degree program, this option can be completed without increasing the total number of credits required to complete the M.S. in computer science degree.

The recommended fulfillment of the option is:

- CSCI 603 – Defensive Network Security
- CSCI 604 – Ethical Hacking
- one additional course

Options for the additional course include:

- CSCI 609 – Cybersecurity Law and Policy
- CSCI 610 – Computer Crime and Forensics
- CSCI 669 – Network Security
- A special topics course focused on cybersecurity
- MATH 673 – Cryptology

Students can elect to complete a thesis, masters' paper or pursue the coursework option (requiring 36 credits instead of 33). Completion of the cybersecurity option is noted, along with degree conferral, on the student's transcript.

7. Master's Degree in Software Engineering with Option in Cybersecurity

The NDSU M.S. in Software Engineering [30] builds on NDSU's legacy of computer science graduate education. It has been recognized as being among the lowest cost software engineering programs by Best Value Schools [31]. Table 2 presents the course requirements for the M.S. in Software Engineering.

Table 2. M.S. in Software Engineering Degree Requirements [30].

Course #	Description	Credits
CSCI 713	Software Development Processes	3

CSCI 715	Software Requirements Definition and Analysis	3
or CSCI 718	Software Testing and Debugging	3
CSCI 716	Software Design	3
CSCI 765	Introduction To Database Systems	3
CSCI 790	Graduate Seminar	3
Six credits from:		
CSCI 714	Software Project Planning and Estimation	3
CSCI 715	Software Requirements Definition and Analysis	3
CSCI 717	Software Construction	3
CSCI 718	Software Testing and Debugging	3
CSCI 845	Formal Methods for Software Development	3
CSCI 846	Development of Distributed Systems	3
CSCI 847	Software Complexity Metrics	3
CSCI 848	Empirical Methods in Software Engineering	3
	Other Courses	Var
	Total credits	33

Like with the computer science M.S., as part of completion of the degree, students can elect to take a nine-credit option in cybersecurity. Depending on the specific plan suggested, it is possible to complete the option without increasing the total number of credits required to complete the M.S. in software engineering degree.

The recommended fulfillment of the option is:

- CSCI 603 – Defensive Network Security
- CSCI 604 – Ethical Hacking
- one additional course

Options for the additional course include:

- CSCI 609 – Cybersecurity Law and Policy
- CSCI 610 – Computer Crime and Forensics
- CSCI 669 – Network Security
- A special topics course focused on cybersecurity
- MATH 673 – Cryptology

Students can elect to complete a thesis or masters' paper option. Both require a total of 33 credits. Completion of the cybersecurity option is noted, along with degree conferral, on the student's transcript.

8. Ph.D. Degree in Computer Science with Option in Cybersecurity

The NDSU Ph.D. in Computer Science [29] is widely respected within the upper great plains region and beyond. The former graduates of the NDSU Ph.D. program hold faculty positions

throughout the region and beyond, in addition to positions in industry and government. Table 3 presents the course requirements for the Ph.D. in Computer Science.

Table 3. Ph.D. in Computer Science Degree Requirements [29].

Course #	Description	Credits
CSCI 713	Software Development Processes	3
CSCI 724	Survey of Artificial Intelligence	3
CSCI 741	Algorithm Analysis	3
CSCI 765	Introduction To Database Systems	3
	Other courses	Var
	Total with prior M.S.	60
	Total without prior M.S.	90

Like with the computer science and software engineering M.S., as part of completion of the degree, students can elect to take a nine-credit option in cybersecurity. Because of the flexibility of the degree program, this option can be completed without increasing the total number of credits required to complete the Ph.D. in computer science degree.

The recommended fulfillment of the option is:

- CSCI 603 – Defensive Network Security
- CSCI 604 – Ethical Hacking
- one additional course

Options for the additional course include:

- A special topics course focused on cybersecurity – Research Methods for Cybersecurity is strongly suggested
- CSCI 609 – Cybersecurity Law and Policy
- CSCI 610 – Computer Crime and Forensics
- CSCI 669 – Network Security
- MATH 673 – Cryptology

Students must also complete a dissertation. The degree requires a total of 90 credits, up to 30 credits from a completed masters' degree can be applied to this requirement. Completion of the cybersecurity option is noted, along with degree conferral, on the student's transcript.

9. Ph.D. Degree in Software Engineering with Option in Cybersecurity

The NDSU Ph.D. in Software Engineering [30] builds on NDSU's legacy of computer science graduate education. Table 4 presents the course requirements for the Ph.D. in Software Engineering.

Table 4. Ph.D. in Software Engineering Degree Requirements [30].

Course #	Description	Credits
Five courses from:		

CSCI 713	Software Development Processes	3
CSCI 714	Software Project Planning and Estimation	3
CSCI 715	Software Requirements Definition and Analysis	3
CSCI 716	Software Design	3
CSCI 717	Software Construction	3
CSCI 718	Software Testing and Debugging	3
CSCI 845	Formal Methods for Software Development	3
CSCI 846	Development of Distributed Systems	3
CSCI 847	Software Complexity Metrics	3
CSCI 848	Empirical Methods in Software Engineering	3
	Other courses	Var
	Dissertation	15
	Total credits with existing M.S.	60
	Total credits without M.S.	90

Like with the computer science and software engineering M.S. and the computer science Ph.D., as part of completion of the degree, students can elect to take a nine-credit option in cybersecurity. Because of the flexibility of the degree program, this option can be completed without increasing the total number of credits required to complete the Ph.D. in software engineering degree.

The recommended fulfillment of the option is:

- CSCI 603 – Defensive Network Security
- CSCI 604 – Ethical Hacking
- one additional course

Options for the additional course include:

- A special topics course focused on cybersecurity – Research Methods for Cybersecurity is strongly suggested
- CSCI 609 – Cybersecurity Law and Policy
- CSCI 610 – Computer Crime and Forensics
- CSCI 669 – Network Security
- MATH 673 – Cryptology

Students must also complete a dissertation. The degree requires a total of 90 credits, up to 30 credits from a completed masters' degree can be applied to this requirement. Completion of the cybersecurity option is noted, along with degree conferral, on the student's transcript.

10. Enhanced Course Format

Several new courses have been developed to support the previously discussed options and certificate program. These courses include:

- CSCI 603 – Defensive Network Security

- CSCI 604 – Ethical Hacking
- CSCI 609 – Cybersecurity Law and Policy
- CSCI 610 – Computer Crime and Forensics

Additionally, several other courses have been developed and run as special topics courses. These include:

- Microsoft Windows Security
- Linux Security
- Intrusion Detection Systems

A number of additional courses are under development. These include courses on:

- Malware Analysis
- Social Engineering
- Reverse Engineering
- Steganography

The newly developed courses as well as the courses being developed have a number of specific features. These features are adapted, slightly, to particular course topics. However, the key features shared by the aforementioned courses include:

- ***Technology enabled for both distance and on-campus students*** – the newly developed courses meet in a television studio enabled classroom. This facilitates synchronous participation by distance students as well as high quality capture of lectures and interactive content. Students (including distance students and on-campus who are unable to attend class) can also watch the recorded videos (and everyone can review the videos) at any time, online.
- ***Outside experts*** – the newly developed courses incorporate content from outside experts, to the extent possible. The CSCI 604 – Ethical Hacking course has benefited from significant participation from a military officer with cyber operations experience. The CSCI 610 – Computer Crime and Forensics course has incorporated campus cybersecurity staff, a forensics consultant and North Dakota Bureau of Criminal Investigation officers. In most cases, these presentations are recorded and available for future use.
- ***Recorded lectures*** – The use of pre-recorded lecture content is key to program scalability as well as saving students time and allowing them to proceed at their preferred pace. In some cases, lectures are recorded live for reuse. In other cases, lectures are recorded in a studio environment. The lectures are posted online and closed-captioned, for students with hearing disabilities. The content can be viewed (multiple times, if necessary) at the students choice of pace and stopped and started, as desired.
- ***Integrated research and development*** – the newly developed courses incorporate hands-on projects such as software development projects and other topic exploration group and individual projects. The projects serve to develop students' computing and cybersecurity skills. They also give students tangible products to show to prospective employers when seeking internships and permanent positions, for after graduation.
- ***Discussion boards*** – the newly developed courses incorporate weekly or biweekly discussion boards within the course management system. These discussion boards allow on-campus and

distance students to communicate with each other and have demonstrable participation in the course. The discussion boards also facilitate allowing students to learn from other students' experiences and knowledge.

11. Qualitative Assessment

The implemented new graduate certificate program and graduate degree options have been gaining in popularity since they were introduced at NDSU. They have drawn interest from existing students as well as individuals working for campus information technology and in industry. The courses for these programs have had significant increases in enrolment each time they have been run. The Ethical Hacking course is the most notable example, going from having 24 students (albeit limited by a room size limitation) the first time it was run to over 80 (in three cohorts within a common class) in its second year (including both graduate and undergraduate courses in the 4xx/6xx course).

Another key indication of program success is the retention of undergraduate students into the graduate programs. NDSU has a 4+1 option, where high-performing undergraduate students can study for an additional year and complete a masters' degree. Several students are already taking advantage of this program, with a focus on cybersecurity.

Cybersecurity graduate students are also engaging undergraduate students who are working with them in support of projects of common interest. These have included projects to recognize deliberately misleading news items, develop user interface technologies for cyber-attacks and defense, automatically score cybersecurity lab assignments and competitions and cybersecurity instructional technologies.

A key feature of the approach NDSU has taken to program development is that the degrees combine cybersecurity coursework and research with traditional computer science and/or software engineering coursework and research. This prepares students not just for the immediate cybersecurity challenges and demand of today, but also for professional growth into other areas of the computing disciplines. Additionally, the computer science knowledge that students receive in the masters and doctoral degrees in computer science with the cybersecurity option better prepares them for complex analysis of challenging cybersecurity, networking and malware problems. The software engineering knowledge that the masters and doctoral students in software engineering gain prepares them to be development managers and project leaders as well as to train future generations of leaders in these areas.

There are also a number of areas of desirable or planned future enhancement. These will now be discussed.

First, it is highly desirable to create additional graduate-only courses. The first of these has been created: an intrusion detection systems course. Additional courses surrounding key topics are planned. For example, courses on side-channel attacks and automated vulnerability discovery are planned. Cybersecurity focused graduate seminars are also planned in the future.

Second, it is desirable to create a course specifically related to cybersecurity research methods to aid graduate students in gaining an understanding of the appropriate tools and techniques to use in this subfield. This development of this course is also planned, in the future.

Third, because of the significant need for instructors (in 2-year, 4-year comprehensive and research universities) in the cybersecurity field, it is highly desirable to create a pipeline of skilled instructors, as part of both the M.S. and Ph.D. degree programs in computer science.

Finally, as the new courses complete multiple offerings, it is desirable to streamline them to the greatest extent possible to facilitate program growth and scalability. The courses have been designed with this in mind; however, final steps must be taken after the course has stabilized after several runs to achieve this goal.

12. Conclusions and Ongoing Work

This paper has described the development of a new cybersecurity graduate certificate and degree options in M.S. and Ph.D. degrees in computer science and software engineering at NDSU. It has described the need for these programs as well as the design of them and the implementation of the courses that support them. Further, it has evaluated them qualitatively and identified areas for further enhancement. The programs and courses are demonstrably growing in popularity and enrolment, at both the undergraduate and graduate levels. Additionally, they are generating significant interest within the State of North Dakota and the local region, among state government, industry and military recruiters.

On an ongoing basis, future work will focus on additional course development and building specializations within the various programs (which may be informal and serve as models for graduate students creating programs of study). Developing models of assessment for program growth and efficacy is also a key area of identified future work.

References

[1] P. Patel, "Defense against the dark arts (of Cyberspace) universities are offering graduate degrees in cybersecurity," *IEEE Spectr.*, vol. 51, no. 6, pp. 26–26, Jun. 2014.

[2] A. Bicak, X. (Michelle) Liu, and D. Murphy, "Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program," *Inf. Syst. Educ. J.*, vol. 13, no. 3, p. 2015.

[3] S. A. Kumar and S. Alampalayam, "Designing a graduate program in information security and analytics," in *Proceedings of the 15th Annual Conference on Information technology education - SIGITE '14*, 2014, pp. 141–146.

[4] M. Ardis and N. R. Mead, "The Development of a Graduate Curriculum for Software Assurance," in *Proceedings of the Seventeenth Americas Conference on Information Systems*, 2011.

[5] M. Bashir, C. Wee, N. Memon, and B. Guo, "Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool," *Comput. Secur.*, vol. 65, pp. 153–165, Mar. 2017.

[6] R. S. Cheung, J. P. Cohen, H. Z. Lo, F. Elia, and V. Carrillo-Marquez, "Effectiveness of Cybersecurity Competitions," in *Proceedings of the International Conference on Security*

and Management, 2012.
[7] L. J. Hoffman, T. Rosenberg, R. Dodge, and D. Ragsdale, "Exploring a National Cybersecurity Exercise for Universities," *IEEE Secur. Priv. Mag.*, vol. 3, no. 5, pp. 27–33, Sep. 2005.
[8] M. Bashir, A. Lambert, B. Guo, N. Memon, and T. Halevi, "Cybersecurity Competitions: The Human Angle," *IEEE Secur. Priv.*, vol. 13, no. 5, pp. 74–79, Sep. 2015.
[9] D. H. Tobey, P. Pusey, and D. L. Burley, "Engaging learners in cybersecurity careers," *ACM Inroads*, vol. 5, no. 1, pp. 53–56, Mar. 2014.
[10] P. Deshpande, C. B. Lee, and I. Ahmed, "Evaluation of Peer Instruction for Cybersecurity Education," in *Proceedings of the SIGCSE Conference*, 2019.
[11] V. P. Janeja, C. Seaman, K. Kephart, A. Gangopadhyay, and A. Everhart, "Cybersecurity workforce development: A peer mentoring approach," in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 2016, pp. 267–272.
[12] K. J. Knapp, C. Maurer, and M. Plachkinova, "Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance," *J. Inf. Syst. Educ.*, vol. 28, no. 2, pp. 101–114, 2017.
[13] R. S. Cheung, J. P. Cohen, H. Z. Lo, and F. Elia, "Challenge Based Learning in Cybersecurity Education," in *Proceedings of the International Conference on Security and Management*, 2011.
[14] T. R. Andel and J. T. McDonald, "A Systems Approach to Cyber Assurance Education," in *Proceedings of the 2013 on InfoSecCD '13 Information Security Curriculum Development Conference - InfoSecCD '13*, 2013, pp. 13–19.
[15] W. A. Lawrence-Fowler, "Multi-disciplinary Approach to Cyber Security Education," in *Proceedings of the International Conference on Security and Management*, 2013.
[16] J. Mirkovic, M. Dark, W. Du, G. Vigna, and T. Denning, "Evaluating Cybersecurity Education Interventions: Three Case Studies," *IEEE Secur. Priv.*, vol. 13, no. 3, pp. 63–69, May 2015.
[17] M. A. . Harris and K. P. Patten, "Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity Topics into a Computing Curriculum," *J. Inf. Syst. Educ.*, vol. 26, no. 3, pp. 219–234, 2015.
[18] T. Chothia and C. Novakovic, "An Offline Capture The Flag-Style Virtual Machine and an Assessment of Its Value for Cybersecurity Education." 2015.
[19] D. Fenton, T. Traylor, G. Hokanson, and J. Straub, "Integrating Cyber Range Technologies And Certification Programs To Improve Cybersecurity Training Programs," in *Proceedings of the 21st International Conference on Interactive Collaborative Learning and 47th International Conference on Engineering Pedagogy*, 2018.
[20] N. Kommera, F. Kaleem, and S. M. S. Harooni, "Smart augmented reality glasses in cybersecurity and forensic education," in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 2016, pp. 279–281.
[21] K. Salah, M. Hammoud, and S. Zeadally, "Teaching Cybersecurity Using the Cloud," *IEEE Trans. Learn. Technol.*, vol. 8, no. 4, pp. 383–392, Oct. 2015.
[22] X. Liu and D. Murphy, "Engaging females in cybersecurity: K through Gray," in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 2016, pp. 255–260.
[23] F. Spidalieri and J. McArdle, "Transforming the Next Generation of Military Leaders into Cyber-Strategic Leaders: The role of cybersecurity education in US service academies," *Cyber Def. Rev.*, vol. 1, no. 1, pp. 141–164, 2016.

[24] C. Yue, “Teaching Computer Science With Cybersecurity Education Built-in.” 2016.
[25] H. Dhillon and M. Hentea, “Getting a cybersecurity program started on low budget,” in *Proceedings of the 43rd annual southeast regional conference on - ACM-SE 43*, 2005, vol. 1, p. 294.
[26] M. Lloyd, “Negative Unemployment: That Giant Sucking Sound In Security,” *Forbes*, 21-Mar-2017.
[27] B. NeSmith, “The Cybersecurity Talent Gap Is An Industry Crisis,” *Forbes*, 09-Aug-2018.
[28] Cyber Seek, “Cybersecurity Supply/Demand Heat Map,” *Cyber Seek Website*, 2019. [Online]. Available: https://www.cyberseek.org/heatmap.html. [Accessed: 03-Feb-2019].
[29] North Dakota State University, “Computer Science,” *NDSU Catalog*, 2018. [Online]. Available: https://bulletin.ndsu.edu/programs-study/graduate/computer-science/. [Accessed: 30-Apr-2019].
[30] North Dakota State University, “Software Engineering,” *NDSU Catalog*, 2018. [Online]. Available: https://bulletin.ndsu.edu/programs-study/graduate/software-engineering/. [Accessed: 30-Apr-2019].
[31] Best Value Schools, “Best Cheap Master’s in Software Engineering Online Programs 2019,” *Best Value Schools*, 2019. [Online]. Available: https://www.bestvalueschools.com/cheap/online/masters-in-software-engineering-degree-programs/. [Accessed: 30-Apr-2019].