Development of Undergraduate Interdisciplinary Cybersecurity Program: A Literature Survey

Dr. Tamer Omar, California State Polytechnic University, Pomona

Tamer Omar is an Assistant professor at the Electrical and Computer Engineering Department in California State Polytechnic University- Pomona. Dr. Omar earned his Ph.D. from the Electrical Engineering department at Iowa State University, USA. Dr. Omar research interests include broadband wireless networks, cybersecurity in IOT, and big data systems. Dr. Omar has over 15 years of experience in both academia and industry serving in different roles at engineering and technology systems domains.

Dr. Srikanth Venkatesan, California State Polytechnic University, Pomona

Dr. Venkatesan is an assistant professor in Computer Information Systems department at Cal Poly Pomona. He received his doctorate degree from University at Buffalo, The State University of New York. His research interests include cloud computing, information assurance, health informatics, online social networks, social network analytics and e-commerce. His teaching expertise at the graduate level is in the area of cloud computing and internet of things. At the undergraduate level, he has taught object-oriented systems analysis and design, intermediate java programming, management information systems, statistics and project management.

Dr. Abdelfattah Amamra, California State Polytechnic University, Pomona

Dr. Abdelfattah Amamra joins California State Polytechnic University, Pomona as an Assistant Professor in the Department of Computer in the College of Sciences. Prior to coming to CalPoly, Pomona he was an Assistant Professor at the University of Conncticut. Dr. Amamra received his Ph.D. from the University of Quebec, Montreal , Canada. His primary research interests are in the field of cybersecurity and machine learning. Specifically, he is interested in smartphone security, and IoT security.

Development of Undergraduate Interdisciplinary Cybersecurity Program: A Literature Survey.

Abstract

Individual dependency on digital systems is continuously growing. Cybersecurity modeling and operations are deemed mandatory to secure these digital systems. Providing current students and future employees with advanced cybersecurity skills is an urgent requirement. As an initiative to address this expanding demand, this study aims at surveying the current undergraduate interdisciplinary cybersecurity programs adopted by different universities. The survey scope covers three main schools and the interdisciplinary relationships among these programs. The schools include the electrical and computer engineering departments in the school of engineering, the computer science departments in the school of sciences, and the computer information systems departments in the business school. The objectives of the survey are three folds; first identifying the program structures in the surveyed universities. The second objective is to determine the interdisciplinary basis on which the three schools collaborate to boost the student learning experience and to cover cybersecurity basic and advanced concepts from multiple dimensions. The last objective is to determine a roadmap that can be adopted by the cybersecurity cluster team at California State Polytechnic University, Pomona (CPP) based on the outputs of this survey to develop an interdisciplinary program. A broad range of universities from research, teaching universities and community colleges are covered in the survey. An analysis of the data collected from surveying the literature is conducted and the results are tested for significance. Finally, recommendations based on the analysis are summarized to aid other interested universities in developing new programs.

1. Introduction

Cybersecurity is a major concern in today's world. According to Juniper research, the cost of data breaches in 2019 is expected to be $2.1 trillion globally showing an increase of almost four times the cost of breaches in 2015 [1]. This tremendous increase in cybercrimes requires an adequate preparation for future students to acquire the skills needed to deal with these future risks.

The importance of cybersecurity comprises on the information secured. Its' well known that information is secure when it costs more to get it than it's worth. Initiating from this principle, securing vital resources that jeopardize human lives is considered priceless. Latest attacks on important assets like the cyber-attack on the Ukrainian power grid shows the seriousness of securing the control systems for such critical infrastructure [2]. Such incidence and others have tremendously increased the awareness of government, companies, and organizations about the severity of damage that cybercrimes can perform. This awareness is lately translated nationwide into a higher demand for qualified candidates to work on cybersecurity. This result in an increasing demand to create cybersecurity programs.

The literature also identifies the pertinence of cybersecurity approaches and their applications across industries. For example, [3] shows that cybersecurity professionals are often required to possess an understanding and skills in both IT and business fields. The triad of people, process and technology need to be integrated into cybersecurity education [4]. While the elements related to people and processes are often emphasized in techno-managerial education, the technical knowledge spans a wide spectrum area of expertise ranging from core engineering concepts like networks, data communication, and infrastructure to computer science concepts like operating systems, programming, computer architecture and database concepts [5].

This need entitled the universities to start new programs with a concentration on teaching basic and advanced cybersecurity aspects. The author in [6] discussed the educational and training activities required for undergraduate majors to improve the conceptual and practical understanding of cybersecurity. A multi-tier approach is proposed to address academic, industrial and assessment requirements to address the lack of awareness and involvement in cybersecurity. Lessons learned from teaching cybersecurity classes in a cross-disciplinary cybersecurity scholarship program is investigated in [7]. The paper discussed the common projects and events performed by the students from all majors involved in the study. The study concludes that supports cross-disciplinary research and teaching is important, and recommend the starting up of new interdisciplinary programs.

This paper aims at investigating the current cybersecurity programs available nationwide and highlight some the successful international programs that show a good reputation. Programs details will be studied and elaborated. Interdisciplinary as an important aspect of cybersecurity will be examined within the surveyed programs. Three main disciplines will be identified in the study, Computer Information Systems (CIS), Computer Science (CS), and electrical and computer engineering (ECE). All three different departments will be surveyed to show the difference between the offered programs in each one of them and if there is common programs or

courses that are being taught jointly within the three departments. Further investigations will involve the nature of offered courses, theoretical versus hands-on approaches, and admission prerequisites. The degree offered, the length of the program.

2. Cybersecurity Programs Survey

The recent increase in cybersecurity challenges and the need for qualified candidates to mitigate the threats of cyber-attacks motivate higher educational institutes to start different programs in cybersecurity. “Cyber degrees", a website which ranks cybersecurity-related programs nationwide is used to identify the universities investigated in this study [8]. For the purposes of this paper, we analyze the top ten ranked universities from the “cyber degrees” website. This website uses the following factors for ranking and evaluation of the programs:

- Degrees offered On-Campus.
- The availability of research labs to provide the required resources for programs.
- The qualification of faculty instructing in the program.
- The relationship of the institution with government & private sector.
- Availability of scholarships & grants to students.
- Location proximity of the institution to tech areas, government defense agencies, and hubs of corporate activity.
- NSA CAE Designation: CAE designations provides indicators to the quality of the program.

Table 1 provides a list of the universities, their available programs, and related information. For purpose of the quantitative analysis in this study, a Boolean variable Y or N is used to indicate the availability or nonexistence respectively of a certain surveyed variable.

The collected data shows that the total enrolment ranges from 15,142 to 46,165 students and that most of the programs are hosted in either the CS or ECE departments. The data also shows that more graduate degrees offered than the undergraduate degrees with more masters’ degrees than Ph.D. The data also indicates that a majority of the universities are providing interdisciplinary degrees that involve more than one department in offering the program courses or include an interdisciplinary research project. Finally, the all the universities have either a cybersecurity center or lab to motivate, advance and manage the different cybersecurity activities performed by the university.

ID	University Name	Total Enrolment	Program Hosting Department[1]				BS Degree Offered	MS Degree offered	Ph.D. Degree offered	Interdisciplinary Degree Offered	Cybersecurity Center/LAB
			CS	ENG	CIS	Other					
1	Perdue University	41,573	Y	Y	Y	N	N	Y	Y	Y	Y
2	Georgia Institute of technology	15,142	Y	Y	N	N	N	Y	N	Y	Y
3	University of Washington	46,165	N	N	Y (INFO)	N	Y	N	N	N	Y
4	University of Maryland	39,083	Y	Y	N	N	Y	Y	Y	Y	Y
5	University of Illinois at Urbana-Champaign	33,932	Y	Y	N	N	Y	Y	Y	Y	Y
6	University of Pittsburgh	34,934	N	N	N	Y (C&I)	Y	Y	Y	N	Y
7	Syracuse University	21,970	Y	Y	N	N	N	Y	N	Y	Y
8	George Mason University	33,925	Y	Y	N	Y	Y	Y	Y	Y	Y
9	University of California-Davis	35,186	Y	N	N	N	N	Y	Y	N	Y
10	University of Texas at San Antonio	28,787	N	N	Y	Y (IS&C)	Y	Y	N	Y	Y
Total		Y	7	6	3	3	6	9	6	7	10
		N	3	4	7	7	4	1	4	3	0

Table 1: Universities General Information

[1] INF = Informatics C&I = Computing and Information IS&C = Information Systems and Cybersecurity

3. Evaluation and findings

This section presents an overview about the current universities offering interdisciplinary programs and an analysis to the interdisciplinary efforts in the surveyed universities, a comparison between the different offered masters' and bachelor programs, and the roles of cybersecurity centers in advancing cybersecurity in the surveyed universities.

3.1.1. Interdisciplinary programs.

Interdisciplinary cybersecurity programs provide multi-faceted learning to students by providing education in cybersecurity defense and countermeasures on one hand and training them in management, governance, and policy aspects of cybersecurity on the other. From a defense perspective, students acquire skills necessary to protect computer systems, networks, and online data from attack and compromise through courses that focus on computer science, computer engineering and Information technology. Coursework in cybersecurity analysis of vulnerabilities and threats to network environments offers students with skills required in information technology technical project management. Law and criminal justice courses like cybercrime combined with digital forensics and courses from accounting and psychology make students a well- rounded product for the industry to absorb. The holistic perspective gained through such interdisciplinary training enables students to understand cybersecurity from a governance and management standpoint while possessing the necessary technical skills.

Across the ten universities surveyed, courses from varied disciplines were part of the cybersecurity offerings. The names of the disciplines include computer science, electrical engineering, information systems, information science, business statistics, accounting, psychology, criminology, criminal justice, forensic science, communications, and linguistics. In eight of the ten universities surveyed, there was a hosting department such as computer science offering the specialized degree. Only two of them had a specialized department or specialized course numbers unique for their cybersecurity degrees. The benefit of having specialized course numbers is that they are not tied to any department and the interdisciplinary course can be utilized independently, thereby serving students from any educational discipline and background. Also, security emphasis as part of the department name opens itself to security-related courses across the university. As part of our future research, we intend to empirically analyze how interdisciplinary is achieved by performing text mining of course descriptions. Another interesting avenue for research is surveying current cybersecurity-related cluster activities in top universities. Typically, such clusters promote interdisciplinary work through direct collaboration of university-wide faculty.

The data from the survey in Table 1 shows an interesting relationship between the interdisciplinary programs offered and the programs hosting departments. Almost all the interdisciplinary programs have both the ENG and the CS departments as the two majors offering the program jointly. However for all other programs that do not support an interdisciplinary initiative, departments such as Informatics or Computing and Information are the departments offering the program separately.

3.1.2. Masters' and Bachelor Degrees

Table 2 & 3 shows a detailed insight about the bachelor and masters' degrees in the surveyed universities. Ph.D. degrees are excluded from the detailed discussions due to their distinct nature that incurs more research activities. It is decided that bachelor and masters' degrees are more appropriate to the objectives of this survey. The collected data indicates that the specializations offered ranges from cybersecurity, information security, information assurance, networking, telecommunication, and forensics. The survey also shows that more scholarships (60%) are available to students pursuing bachelor level than those offered (20%) to students pursuing a masters' degree.

The top 10 universities offer different cybersecurity programs: bachelor, master, Ph.D. and others such as certificates as illustrated in Table 2 and Table 3. In comparison between master's degree and bachelor's degree, all the top 10 universities offer master degree while only 6 universities offer bachelor degree. This emphasis the results that have been presented in [9]. This study compiles 183 cybersecurity programs from rated institutions. The percentage of master's degree was highest 38%. However, the bachelor's degree percentage was only 10%. This result may be due to many different reasons, such as:

- Cybersecurity is a new field and people who already hold a bachelor's degree and holding down a full-time job may want to apply to a cybersecurity master's degree program rather than re-do a new bachelor's degree.
- Cybersecurity field is the one that requires knowledge in other fields such as electrical engineering, computer science, and information management. Therefore, Master's degree program is more appropriate for people having different backgrounds.
- Getting a bachelor's degree is something to take seriously. It is time-consuming where the average time to get graduated is around 4 years-, it is expensive, and at times frustrating. However, most master's degree programs are concentrated and take only 1-2 years to complete.

ID	University Name	Specialization	No of Program Credits/Hrs.				Total No. Of Courses Offered	Cybersecurity related Courses in Catalog	prerequisites	No. of Interdisciplinary Areas for Courses	Scholarship
			CS	ENG	CIS	Other					
3	University of Washington	Information Assurance and Cybersecurity			16-20[2]		35	7	CC[3]	3	Y
4	University of Maryland	Cybersecurity	21	15			37	13	CC	8	
5	University of Illinois at Urbana-Champaign	Cybersecurity	21	21			39	9	CC	4	Y
6	University of Pittsburgh	Networks and Security				18	39	13	CC	0	N
8	George Mason University	Cybersecurity Engineering and Information Security				42	42	10	CC+1SE	3	N
9	University of Texas at San Antonio	Cybersecurity	40				48	9	CC+6SE	3	Y

Table 2: BS Programs information

[2] Additional credits to degree core courses
[3] CC = Core Courses SE= Security Elective

ID	University Name	Specialization	No of Program Credits/Hrs.				Total No. Of Courses	Cybersecurity related Courses in Catalog	Prerequisites	No. of Interdisciplinary Areas for Courses	No of Research Credits/Hrs.	Scholarship
			CS	ENG	CIS	Other						
1	Perdue University	Information Security				30	70	19	CC	5	3	N
2	Georgia Institute of technology	Information Security				32	34	11	GPA 3.5	5	5	N
4	University of Maryland	Cybersecurity		30			18	8	GPA 3.0	1	0	N
5	University of Illinois at Urbana-Champaign	Cybersecurity	30	30			21	7	CC	4	0	Y
6	University of Pittsburgh	Tele-Communications & Information Science				30	12	7	CC	0	0	N
7	Syracuse University	Cybersecurity	30				13	7	CC	0	0	N
8	George Mason University	Forensics and Cybersecurity	30	30		36		9	CC	1	3	N
9	University of California-Davis	Information Assurance	23[3]	23[3]				4	CC	0	0	N
10	University of Texas at San Antonio	Cybersecurity			33		24	11	CC	4	0	Y

Table 3: MS. Programs Information

On another side, Figure 1 shows the total number of job postings based education level base on analysis of 68,228 cybersecurity job postings, June 01, 2016 – May 31, 2017 [10]

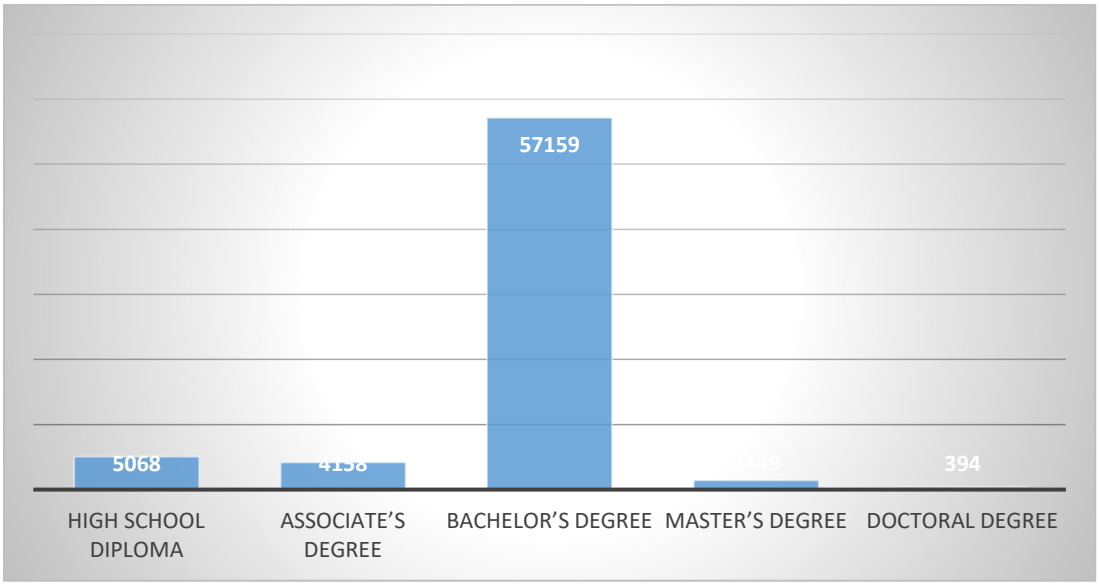

Figure 1: Education level vs jobs posting in cybersecurity

Figure 1 clearly illustrates that the most employers are seeking candidates with a Bachelor's degree. Therefore, earning a bachelor's degree makes students eligible for 39 times as many jobs as a student with master's degree. Thereby, developing a flexible interdisciplinary bachelor's degree program that's going to provide future students with solid computing and engineering skills like programming, statistics, system administration and information assurance is the future trend for cybersecurity education. A good BS degree curriculum should prepare students to better understand, prevent and respond to cybersecurity's threats by considering both practical and theoretical aspects.

3.1.3. Cybersecurity Centers Support

This section will investigate the existence of a cyber-security center in the surveyed universities and evaluate the role of these centers in promoting a cybersecurity culture and advancing the cybersecurity education process in these universities. The output of the survey shows that the following cybersecurity centers are available to support the offered programs in the ten universities:

1. Purdue University; Center for Education and Research in Information Assurance and Security (CERIAS) [11].
2. Georgia institute of technology; Institute for Information Security & Privacy (IISP) [12].
3. University of Washington; Security and Privacy Research Laboratory (SPRL) [13] & Tech Policy Lab (TPL) interdisciplinary lab [14].
4. University of Maryland; Maryland Cybersecurity Center (MC2) [15].

5. University of Illinois at Urbana-Champaign; Center for Information Assurance Education and Research (CIAER) [16].
6. University of Pittsburgh; Laboratory for Education and Research on Security Assured Information Systems (LERSAIS) [17].
7. Syracuse University; Center for Advanced Systems and Engineering (CASE) [18].
8. George Mason University; Center for Secure Information Systems (CSIS) [19], Center for Assurance Research & Engineering (CARE) [20].
9. University of California-Davis; Computer Security Lab (CSL) [21].
10. University of Texas at San Antonio; Center for Education and Research in Information and Infrastructure Security (CERI²S) [22], Center for Security and Privacy Enhanced Cloud Computing (C-SPECC) [23] & Center for Infrastructure Assurance and Security (CIAS) [24].

The survey shows that all the universities have either a cybersecurity center or a lab that support the educational and research activities in these universities. The centers/labs strategies are aligned with the higher education institutions strategies. Generally, the cybersecurity centers/labs focus on delivering either one or more of the following three activities, education, research\funding, and services to each university such as facilitating Co-ops and interns, partnering with industry, partners, events and seminars organization, and handling competitions. However, the scope of delivered activities varies from one center to another.

Nine out of the fourteen cybersecurity centers/labs surveyed offer educational services such as managing interdisciplinary course offerings, marketing, and advertising for the different the programs offered by the university colleges. However, these centers/labs are not an academic department, they are not degree-granting units and the degrees are offered by the different university college departments. However, four of the centers namely CASE, CSIS, CARE, C-SPECC do not offer any educational services. This shows that although teaching and program offerings are one of the major university activities, cybersecurity centers may not have a role in providing instructional services and they only perform activities in the two other areas of research and services to the university. Few of the centers also promote professional education by either offering graduate certificate program or conducting training. In addition to the four centers that do not offer any educational services CERIAS, TPL, LERSAIS, CSL do not offer any professional education or training.

Only one (CIAS) of the surveyed centers/labs do not provide research activities. All the other centers provide different research activities such as research projects management, support grant proposal initiatives, publicize research publications, encourage interdisciplinary and industry collaboration, commercializing research products to the marketplace, and promote undergraduate and graduate research. Samples of the research areas focus on the surveyed universities include the following:

1. Information assurance, assured identity and privacy, cloud privacy, wireless information assurance.
2. Cryptography.
3. Systems, networks and sensors security, systems attribution, software security.

4. Attack tolerance, threat attribution.
5. Side channel attacks, backscattering, distributed denial of service (DDOS) attacks.
6. Human-centric security, Security awareness, behavioral aspects.
7. Intel and security analytics in machine learning.
8. Detection and prevention response, surveillance, web tracking.
9. Industrial control systems security, embedded applications, Infrastructure resiliency.
10. Pen testing, BOTNETS, the economics of cybersecurity.

The last activity provided by the centers/labs in university services. There is a wide range of services provided by the surveyed universities that include facilitating Co-ops and internship opportunities by partnering with industry, mandate or encourage students to perform one of the professional Co-ops/internship before graduation. The centers partner with industry to promote research by collaborating on cybersecurity projects that interest industrial partners. The centers/labs organize educational events and seminars to increase their students' awareness about cybersecurity and its importance in the different domains, updating their research community with the latest topics in cybersecurity and present the research findings produced due to the efforts of their faculty and research teams. The centers/labs also improve the quality and level of interaction with other institutions by handling competitions. Competitions and gaming such as National Collegiate Cyber Defense Competition (CCDC), CyberPatriot, and Panoply are used as a method to encourage students to get involved in cybersecurity domain by applying their skills in an attractive structured setting.

4. Recommendations for CPP

Our recommendations for CPP is manifold. One of the ways in which a university can harness its collective strengths is by developing cybersecurity centers which integrate multiple departments. Such centers also pave way for industry and governmental collaborations. Second, providing dedicated cybersecurity undergraduate degrees would create avenues for truly interdisciplinary contributions by combining the selective courses from multiple departments into a single stream. Creation of cybersecurity clusters provides opportunities for lateral collaborations among faculty across departments. For example, students from computer science background may not get exposure to criminal law and justice, thereby not appreciate the value of digital forensics when they are merely exposed to forensic tools and techniques. Interdisciplinary degree programs provide a holistic view of the cybersecurity space and also provide opportunities for students to pursue niche career paths due to the exposure to such breadth and depth of topics. The knowledge provided by faculty from varied disciplines also help students gain insights through the lens of each discipline.

5. Observations and Conclusions

This paper surveyed cybersecurity programs for both graduate and undergraduate degrees. The aim of the paper is to provide recommendations for the cybersecurity team hired within the

cybersecurity cluster in University-name of the current trends in cybersecurity programs and the interdisciplinary nature of these programs. Also, the current structure, similarities, and differences between masters' and bachelor offered degrees. The roles of cybersecurity centers and security labs are also investigated to highlight the importance of these university units in promoting cybersecurity awareness and research initiatives.

The survey shows that most universities offer and focus on graduated cybersecurity program. However, cybersecurity labor market needs bachelor's degree more than master's degree. Therefore, developing bachelor's degree with cybersecurity concentration is the future trend of cybersecurity education.

Cybersecurity science is not only related to computer and engineering science. However, it is related to many different domains, such as information science, business and management, psychology, criminal justice and forensic science. Therefore, cybersecurity programs should be interdisciplinary to provide students with strong skills and knowledge in different areas.

Cybersecurity is science and this science requires the application of mathematics to solve problems, design processes, measures, and tools; therefore, cybersecurity research centers/labs have a positive impact on cybersecurity program.

The authors are planning to extend this study in future work to include more universities especially those interested in offering interdisciplinary programs and study the technical content of the cybersecurity-related courses offered by their respective departments.

6. References

[1] Juniper Research©, "Cybercrime will Cost Businesses Over $2 Trillion by 2019," 2015. [Online]. Available: https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.

[2] SANS ICS, "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case," 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[3] J. B.-S. H. R. R. a. U. Lee, "Anatomy of the Information Security Workforce," *IEEE IT Professional,* vol. 12, no. 1, pp. 14-23, 2010.

[4] A. Andress, Surviving Security: How to Integrate People, Process, and Technology, Boca Raton, FL: Auerbach Publications, 2003.

[5] S. A. a. L. S. Jane LeClair, "An Interdisciplinary Approach to Educating an Effective Cyber Security Workforce," in *InfoSecCD '13: Information Security Curriculum Development Conference (InfoSecCD '13),* New York, NY, USA, 2013.

[6] N. Swain, "A Multi-Tier Approach to Cyber Security Education, Training, and Awareness in the Undergraduate Curriculum (CSETA)," in *American Society for Engineering Education*, 2014.

[7] L. H. R. H. Costis Toregas, "Exploring Ways to Give Engineering Cyber Security Students a Stronger Policy and Management Perspective," in *Spring 2016 Mid-Atlantic ASEE Conference*, 2016.

[8] Cyber Degrees, "Top Cyber Security Schools," 2018. [Online]. Available: http://www.cyberdegrees.org/listings/top-schools/#Best_Cyber_Security.

[9] P. Institute, "2014 Best Schools for Cybersecurity," Online, North Traverse City, Michigan, 2014.

[10] C. Malvik, "http://www.rasmussen.edu/degrees/technology/blog/cyber-security-degree-worth-it/," Rasmussen College, 27 07 2017. [Online]. [Accessed 04 02 2018].

[11] Purdue University, "Center for Education and Research in Information Assurance and Security (CERIAS)," Feb 2018. [Online]. Available: https://www.cerias.purdue.edu/.

[12] Georgia Institute of Technology, "Institute for Information Security and Privacy (IISP)," Feb. 2018. [Online]. Available: https://cyber.gatech.edu/.

[13] University of Washington, "Security and Privacy Research Laboratory (SPRL)," Feb. 2018. [Online]. Available: https://seclab.cs.washington.edu/.

[14] University of Washington, "Tech Policy Lab (TPL) interdisciplinary lab.," Feb. 2018. [Online]. Available: http://techpolicylab.org/.

[15] University of Maryland, "Maryland Cybersecurity Center (MC2)," Feb. 2018. [Online]. Available: http://www.cyber.umd.edu/.

[16] University of Illinois, "Center for Information Assurance Education and Research," Feb. 2018. [Online]. Available: https://iti.illinois.edu/education/nsa-center-information-assurance-education-and-research.

[17] University of Pittsburgh, "Laboratory for Education and Research on Security Assured Information Systems (LERSAIS)," Feb. 2018. [Online]. Available: http://www.sis.pitt.edu/lersais/index.php.

[18] Syracuse University, "Center for Advanced Systems and Engineering (CASE)," Feb. 2018. [Online]. Available: http://case.syr.edu/.

[19] George Mason University, "Center for Secure Information Systems (CSIS)," Feb. 2018. [Online]. Available: http://csis.gmu.edu/.

[20] George Mason University, "Center for Assurance Research and Engineering," [Online]. Available: https://care.vse.gmu.edu/.

[21] University of California-Davis, "Computer Security Lab (CSL)," Feb. 2018. [Online]. Available: http://seclab.cs.ucdavis.edu/.

[22] University of Texas at San Antonio, "Center for Education and Research in Information and Infrastructure Security (CERI²S)," Feb. 2018. [Online]. Available: http://business.utsa.edu/ceris/.

[23] University of Texas at San Antonio, "Center for Security and Privacy Enhanced Cloud Computing (C-SPECC)," Feb. 2018. [Online]. Available: http://cspecc.ics.utsa.edu/.

[24] University of Texas at San Antonio, "Center for Infrastructure Assurance and Security (CIAS)," Feb. 2018. [Online]. Available: http://cias.utsa.edu/.