# Partnership to Prepare Students for Careers in the Emerging Field of Cybersecurity

**Dr. James K. Nelson Jr. P.E., Texas A&M University**

Dr. James K. Nelson received a Bachelor of Civil Engineering degree from the University of Dayton in 1974. He received the Master of Science and Doctor of Philosophy degrees in civil engineering from the University of Houston. During his graduate study, Dr. Nelson specialized in structural engineering. He is a registered professional engineer in three states, a Chartered Engineer in the United Kingdom, and a fellow of the American Society of Civil Engineers. He is also a member of the American Society for Engineering Education and the SAFE Association. Prior to receiving his Ph.D. in 1983, Dr. Nelson worked as a design engineer in industry and taught as an adjunct professor at the University of Houston and Texas A&M University at Galveston. In industry he was primarily involved in design of floating and fixed structures for the offshore petroleum industry. After receiving his Ph.D., Dr. Nelson joined the civil engineering faculty at Texas A&M University. He joined the civil engineering faculty at Clemson University in 1989 as Program Director and founder of the Clemson University Graduate Engineering Programs at The Citadel and became Chair of Civil Engineering in 1998. In July 2002, Dr. Nelson joined the faculty at Western Michigan University as Chair of Civil and Construction Engineering. At Western Michigan he started the civil engineering undergraduate and graduate degree programs and also chaired the Departments of Materials Science and Engineering and Industrial Design. In summer 2005 he joined the faculty at The University of Texas at Tyler. At UT Tyler he was the founding chair of the Department of Civil Engineering and instituted the bachelor's and master's degree programs. In 2006 he became the Dean of Engineering and Computer Science. Dr. Nelson returned to Texas A&M University in 2016 as the Director of Special Academic Initiatives for the Texas A&M University System. Dr. Nelson's primary technical research interest is the behavior of structural systems. For almost 25 years he has been actively involved in evaluating the behavior of free-fall lifeboats and the development of analytical tools to predict that behavior. His research has formed the basis for many of the regulations of the International Maritime Organization for free-fall lifeboat performance. Since 1988, Dr. Nelson has served as a technical advisor to the United States Delegation to the International Maritime Organization, which is a United Nations Treaty Organization. In that capacity, he is a primary author of the international recommendation for testing free-fall lifeboats and many of the international regulations regarding the launch of free-fall lifeboats. He has authored many technical papers that have been presented in national and international forums and co-authored three textbooks. Dr. Nelson chaired a national committee of the American Society of Civil Engineers for curriculum redesign supporting the civil engineering body of knowledge. He is actively engaged in developing strategies for enhancing the STEM education pipeline in Texas and nationally, and has testified before the Texas Senate and House Higher Education Committees in that regard. He served on a committee of the Texas Higher Education Coordinating Board to develop a statewide articulation compact for mechanical engineering and chaired the councils for developing articulation compacts in other engineering and science disciplines. He also served on the Texas State Board of Education committee preparing the standards for career and technical education.

**Dr. Brent L. Donham, Texas A&M University-Commerce**

Dr. Brent Donham is the Dean of the College of Science & Engineering at Texas A&M University-Commerce. Throughout his academic career, he has been actively involved in engineering / STEM education. He has led the development and implementation of multiple engineering and engineering technology degrees along with award winning career awareness programs. Dr. Donham holds a bachelor's degree in Electrical Engineering from New Mexico State University, a master's degree in Electrical Engineering from Stanford University, and a doctorate in Educational Administration from Texas A&M University-Commerce. In addition to his higher education experience, he has more than twelve years of industry experience with Sandia National Laboratories and E Systems (now L3/Harris).

# Preparing Students for Careers in the Emerging Field of Cybersecurity


## Abstract

Cybersecurity is an emerging field with significant implications as the use of interconnected devices increases. Each device represents a potential entry point for individuals with malicious intentions. A direct result of the growth of the number of Internet connected devices and the inherent security risks is the need for more individuals trained in the field of cybersecurity and related operational technologies. Presented in this paper is the development and implementation of the RELLIS Cybersecurity Alliance and the programs offered. Included is the new bachelor's degree in cybersecurity, which was developed from a "clean sheet." Also presented are the initial professional development courses being offered. The physical laboratory spaces that have been purpose-built enabling students to obtain hands-on experience as part of the academic and professional development programs are also discussed. A strong component in the development of each of these pieces was the active involvement the public and private sector.


## Introduction

Cybersecurity is an emerging field with significant implications as the use of interconnected devices increases. The need for trained cybersecurity professionals is increasing, yet the workforce is not increasing to match the need. Jeff Kaitlin in 2017 reported that:

> *The ISACA, a non-profit information security advocacy group, predicts there will be a global shortage of two million cyber security professionals by 2019. Every year in the U.S., 40,000 jobs for information security analysts go unfilled, and employers are struggling to fill 200,000 other cyber-security related roles, according to cyber security data tool CyberSeek. And for every ten cyber security job ads that appear on careers site Indeed, only seven people even click on one of the ads, let alone apply. [1]*

In 2011 the Cisco Internet Business Solutions Group presented the data shown in Figure 1. They reported that sometime between 2008 and 2009 the number of connected devices exceeded the world population.

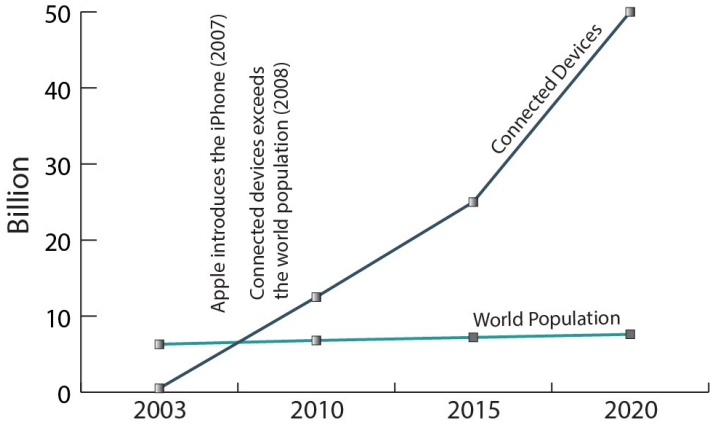
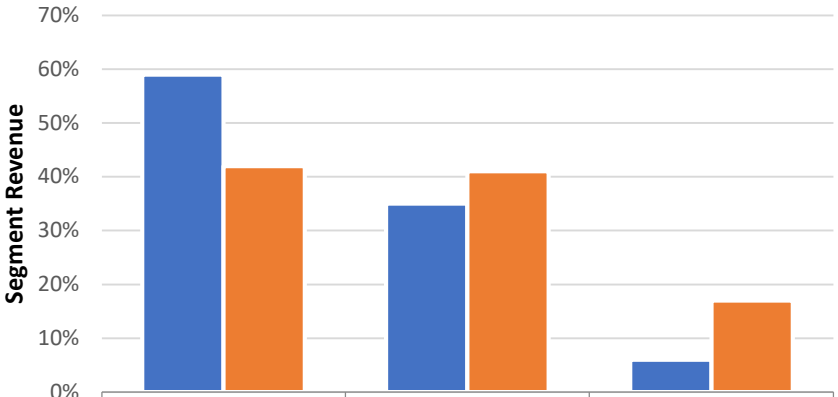



*Figure 1: Growth of internet-of-things versus population [2]*

Within major telecommunications companies, the mix of services provided is changing. Data for AT&T, as presented by the Wall Street Journal, are presented in Figure 2. Of interest is the decrease in wireline services and the increase in wireless services. Although wireless services segment grew by six percent, the revenue from wireless services grew by 166 percent.




| | Wireline | Wireless | Other |
|---|---|---|---|
| 2007 | 59% | 35% | 6% |
| 2018 | 42% | 41% | 17% |

*Figure 2: Shift in market share of a major provider [3]*

Of further interest in these data is the growth of the "Other" business sector, which includes streaming and online services. That segment nearly tripled in the decade reported. This segment indicates that not only are individuals connecting more devices, they are utilizing more on-line resources.

The spectrum is perhaps best characterized as shown in Figure 3. The internet of things has its complement in the industrial internet-of-things (IIOT), which is characterized as "operational technology" (OT) to distinguish it from information technology (IT). The nation's infrastructure and economy (*e.g.*, transportation, electrical grid, and manufacturing) is increasingly dependent on securing the interface between IT and OT within the broader internet-of-things.

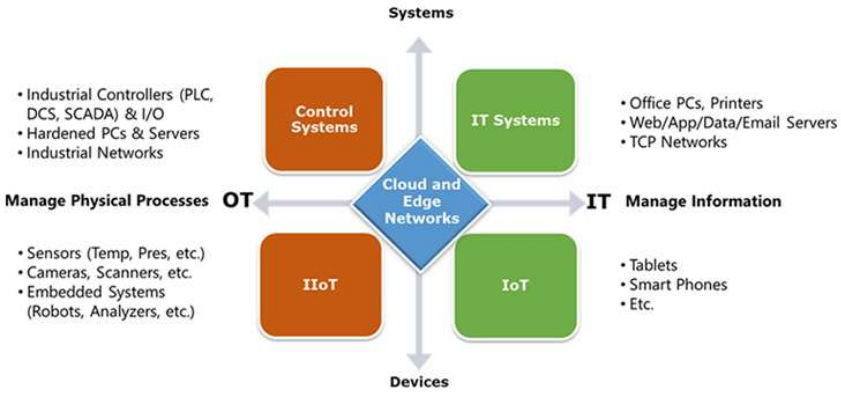



*Figure 3: Industrial IT and OT systems and devices [4]*

The economic impact of the IoT is quite significant. In June 2015, the McKinsey Global Institute evaluated 150 use cases that ranged from individuals with devices that monitor health to manufacturers using the IoT to optimize equipment maintenance and protect worker safety. [5] They found that the IoT has a potential economic impact of $3.9 trillion to $11 trillion a year by 2025. They further stated that the top end of this range is equivalent to 11 percent of the world economy.

Each connected device represents a potential entry point for individuals with malicious intentions. As such, many contend that cybersecurity is national security. A direct result of the growth of the number of Internet connected devices and the inherent security risks is the need for more individuals trained in the field of cybersecurity and related operational technologies.

**Genesis of the Cybersecurity Alliance**

Located in Bryan, Texas, the 2,000-acre Texas A&M System RELLIS campus is a collaborative ecosystem built to foster advanced research, technology development, testing and evaluation, higher education, and hands-on career training. The RELLIS Academic Alliance oversees the educational operation of the campus. The unique partnership brings together ten regional A&M System universities and Blinn College to one location

At its meeting on September 28, 2018, the RELLIS External Academic Advisory Council met with then Texas Secretary of State, Rolando Pablos, and the Workforce Commissioner for Labor, Julian Alvarez, to discuss evolving workforce needs in the region and the state. During the council meeting, multiple individuals from different industry sectors expressed the need for more individuals trained in cybersecurity risk assessment, and threat identification and mitigation. This is an issue not only for the State of Texas, but also the nation.

In response to recommendations made by the External Academic Advisory Council, the RELLIS Academic Alliance developed the RELLIS Cybersecurity Alliance to provide for quality control and coordination of program offerings at RELLIS. The purpose of the RELLIS Cybersecurity Alliance is to:

- Provide a venue through which relevant academic and training programs that satisfy industry needs are offered and that enable the students to develop demonstrable hands-on skills,
- Provide a mechanism by which industry involvement in the offerings can be ensured, and
- Educate the region about career pathways in cybersecurity, and the vast opportunities within those careers.

The thrust areas of the Cybersecurity Alliance are shown in Figure 4. As shown, there are three primary thrusts: Undergraduate and graduate degrees, workforce training and continued professional development, and facilitation of research across institutional and agency boundaries. A knowledgeable and trained workforce are at the heart of the Alliance and the programs offered through it.

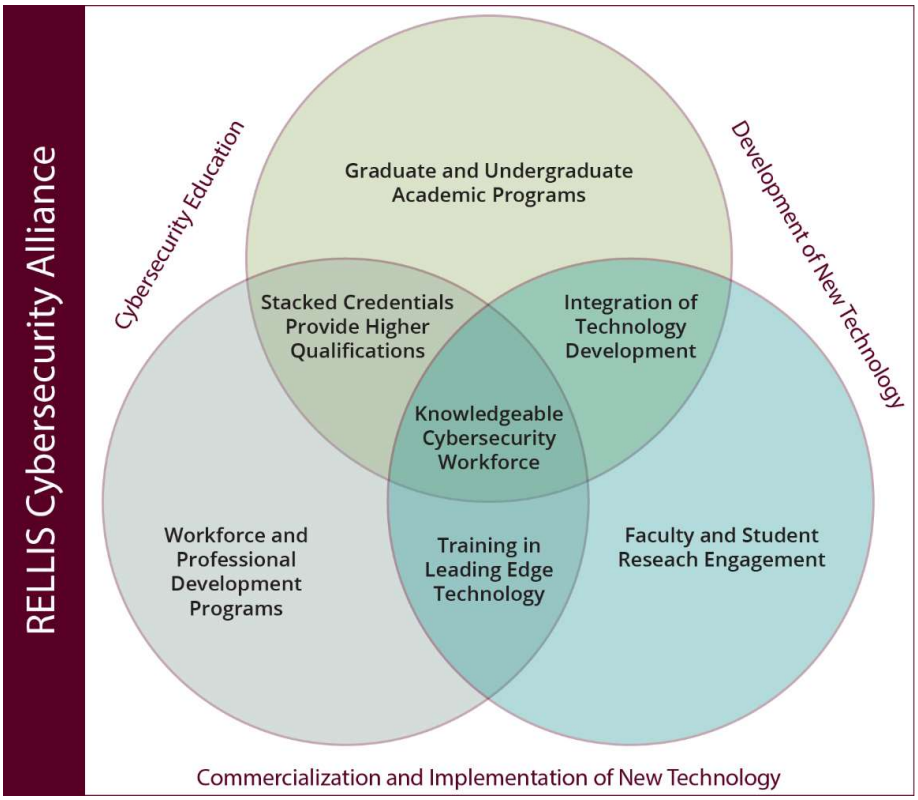



*Figure 4: Interaction within the cybersecurity alliance*

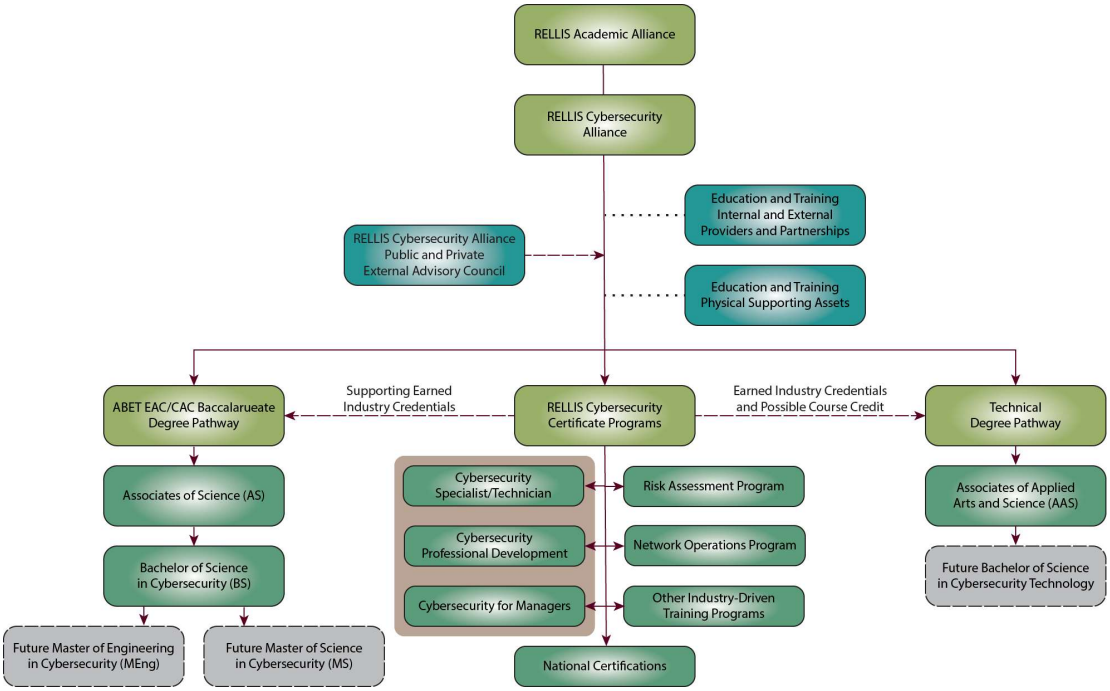



*Figure 5: Programmatic structure of the cybersecurity alliance*

The organizational structure of the offerings is presented in Figure 5. The left side represents the academic undergraduate and graduate degree programs. These programs are offered by the universities within the system. The right side represents the associate and technical degree offerings; typically, these are offered by a community college. The center section represents the training and professional offerings. These offerings can be from multiple institutions, agencies, and public and private entities.

In the sections that follow, these elements are discussed, along with the supporting facilities. Of importance is that all offerings are reviewed for relevance by the RELLIS Cybersecurity External Advisory Council. The flowchart for program review is presented in Figure 6.

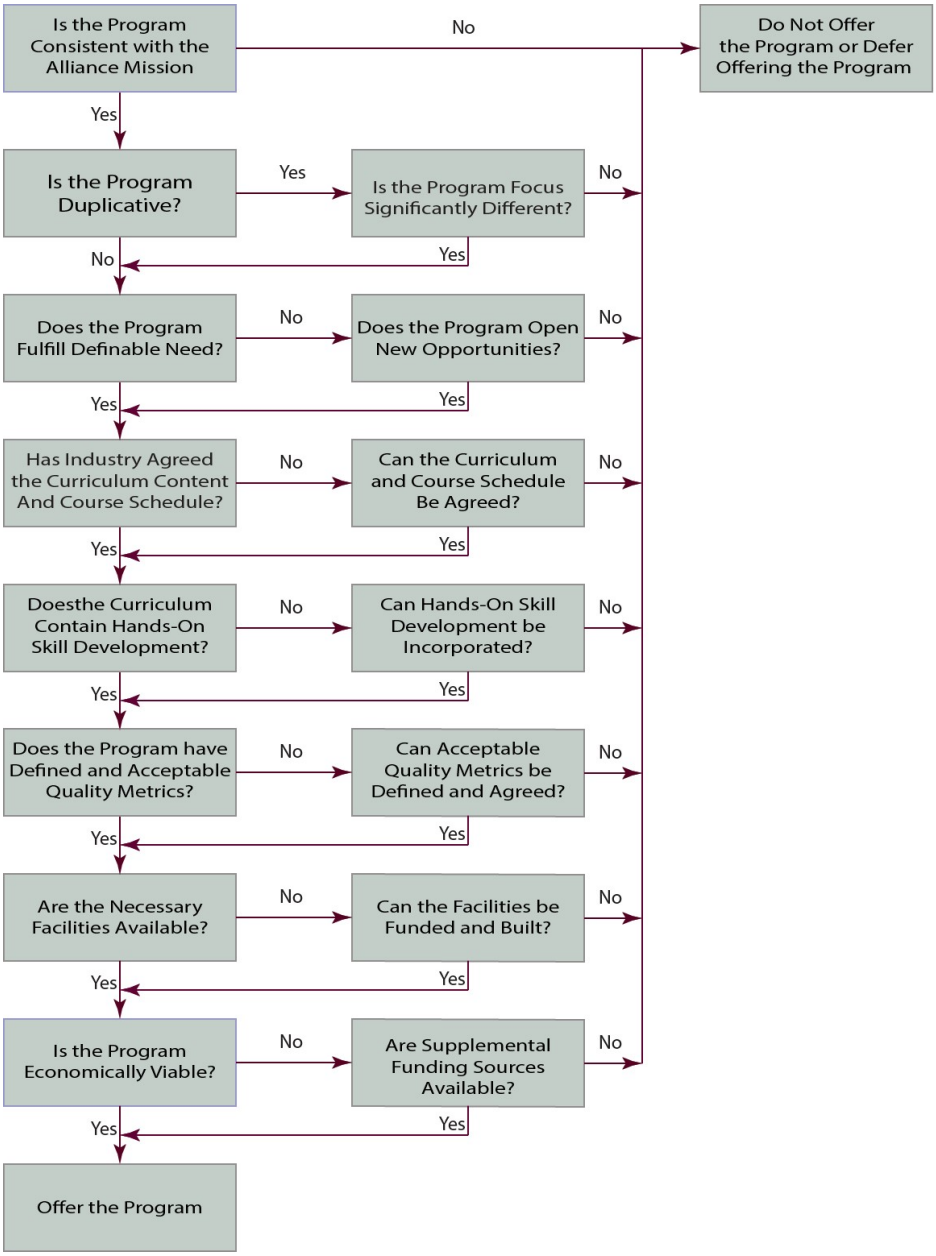



*Figure 6: Flowchart for program review*

**Bachelor of Science in Cybersecurity Curriculum**

Driving Influences

There were three dominant influences in the development of the Bachelor of Science degree program. These influences were:

- Advice from industry must be sought for the degree program to be relevant looking into the future.

  The public and private sectors are the employers of our students, Nevertheless, degree programs are often developed from an academic perspective, with review and comment from industry afterwards. As the cybersecurity field is so rapidly evolving, and the problems faced are those in the public and private sectors, the expectations of industry were considered essential, including their expectations of what will be needed five to ten years in the future.

- Development of the degree program must begin with a "clean page" rather than starting with an existing degree and modifying the curriculum.

  When a degree program is developed from an existing degree program, unnecessary artifacts may remain and needed instruction may be left out. Often when developed from an existing degree, the new "degree" is often little more than a track in the existing program rather than a new degree.

- The degree program must be structured so that students can study only at a four-year institution or can study at a community college earning an appropriate associates degree and then transfer to a four-year institution to complete the baccalaureate degree program.

  Regional universities continue to have a high number of transfer students. As such, the lower division program of study needs to contain courses that the community colleges are offered, that lead to award of an associate degree at a community college, that positively support the upper division coursework, and that do not "lock" students into a single baccalaureate degree program.

Industry Expectations: Baccalaureate Degree Program

Recommendations and considerations for the development of the baccalaureate degree program from external advisory council include:

- Development of the degree should begin with a "clean page," i.e., an existing degree program should not be morphed or augmented initially.
- The degree program will be able to seek accreditation under one of the commissions of ABET, Inc.
- Providing a pathway for graduating students to migrate to the Master of Engineering degree program at Texas A&M University if they so choose and are admitted, or to another graduate degree program.
- Include DHS expectations that the degree would provide for CAE certifications from NSA as a result of its content.

- The curriculum should be structured so that an associate degree can be conferred if the first two years of the degree program are completed at a community college and the student will have marketable skills. (Note: This expectation implies that the Texas Common Core Curriculum is completed in the first two years).
- The student should have the opportunity to obtain industry certifications either as a part of the degree program or as an "add-on" to the degree program.

In broad terms, the recommended curricular content should include:

- Calculus through Calculus II,
- Statistics, and discrete mathematics,
- Laboratory science with University Physics preferred,
- Technical writing in addition to composition,
- Macro or microeconomics,
- Logic and ethics,
- Public speaking,
- Programming,
- Data Structures and Algorithms,
- Networks,
- Database, and
- Cybersecurity and supporting computer science core cores.

The final curricular composition was at the discretion of the faculty at the offering institution and had to satisfy all institutional requirements for admission and graduation.

Lower Division Curriculum

Th lower-division curriculum was structured with three guiding principles:

- Ensure that students who complete the first two years at a community college within the region can transfer to the upper division program to complete the baccalaureate degree and be on par with students who start the degree program as a freshman at the university;
- Ensure that the Texas Common Core Curriculum is completed in the first years so students transferring from a community college can be awarded an associates degree without reverse articulation of courses; and
- Ensure that students who begin as freshmen in cybersecurity could change to a different major in the computing area (i.e., computer science or computer information systems) during the first two years seamlessly.

The resulting lower-division curriculum is presented in Table 1. The sequencing of courses over the two years is the recommended sequence enabling students to complete the entire baccalaureate curriculum in eight semesters. Consideration was given to prerequisite courses and when those courses could be completed.

Consideration was also given to the reality that the degree will be available at an off-campus site. At the off-campus site, only the upper-division would be available from the offering university, the lower-division curriculum would be from a community college. This consideration meant that no specialized lower-division courses could be included in the lower division curriculum unless they were included in the State's "Lower-Division Academic Course Guide Manual" (ACGM). [6], which has specific and relatively restrictive criteria for adding courses.

Each semester contains at least four courses, which is a reasonable load for most full-time students. However, because of the number of credit hours associated with each course, the second semester of the first year contains 17 semester credit hours because of the number of 4 credit hour courses. If this load is considered too heavy for a second semester student, the second history course or creative arts elective could be completed during the third semester or during a summer semester. Also, many students enter with dual credit or AP credit, which can alter when courses are taken. As such, this is a recommended sequence only.

*Table 1: Lower division curriculum*

| Year 1 | | | |
|---|---|---|---|
| Course | SCH | Course | SCH |
| English Composition I | 3 | English Composition II | 3 |
| Calculus I | 4 | Creative Arts Elective | 3 |
| US History | 3 | Calculus II | 4 |
| Programming Fundamentals I | 4 | US History or Texas History | 3 |
| | | Programming Fundamentals II | 4 |
| Semester Total | 14 | Semester Total | 17 |
| **Year 2** | | | |
| Course | SCH | Course | SCH |
| University Physics I with Laboratory | 4 | Data Structures and Algorithms | 3 |
| US Govermnent | 3 | Economics (Macro or Micro) | 3 |
| Machine Language/Computer Org. | 3 | Texas Government | 3 |
| Discrete Mathematics | 3 | Logic | 3 |
| | | University Physics II with Laboratory | 4 |
| Semester Total | 13 | Semester Total | 16 |

Upper Division Curriculum

The upper-division curriculum is presented in Table 2. During development of the upper-division curriculum there was an implicit hierarchy in selection of courses and course content, namely:

1. Identify the courses that must be contained in a comprehensive cybersecurity core curriculum,
2. Identify the necessary computer science that support the core cybersecurity courses, and
3. Develop cybersecurity electives that will enable the student to develop a more specialized expertise in an area of cybersecurity, such as Cybersecurity Operations or Enterprise Security.

*Table 2: Upper-division curriculum*

| Year 3 | | | |
|---|---|---|---|
| Course | SCH | Course | SCH |
| Cybersecurity | 3 | Big Data Security | 3 |
| Introduction to Databases | 3 | Network Security and Management | 3 |
| Introduction to Operating Systems | 3 | Cryptography | 3 |
| Introduction to Networks | 3 | Advanced Cybersecurity Elective | 3 |
| Technical Communication | 3 | Junior Cybersecurity Design Project | 3 |
| Semester Total | 15 | Semester Total | 15 |

| Year 4 | | | |
|---|---|---|---|
| Course | SCH | Course | SCH |
| Statistics | 3 | Ethics, Law and Cybersecurity | 3 |
| AI Enhanced Security | 3 | Wireless and Mobile Security | 3 |
| System Security and Trusted Computers | 3 | Malware Analysis | 3 |
| Smart Things Security | 3 | Advanced Cybersecurity Elective | 3 |
| Advanced Cybersecurity Elective | 3 | Senior Cybersecurity Design Project | 3 |
| Semester Total | 15 | Semester Total | 15 |

*Table 3: Elective Courses in the Upper-Division Curriculum*

| Elective Courses | SCH |
|---|---|
| Secure Programming | 3 |
| Software Engineering | 3 |
| Digital Forensics | 3 |
| Vulnerability Analysis | 3 |
| Secure Software Development | 3 |
| Intrusion Detection & Prevention | 3 |
| Cloud Computing and Security | 3 |
| Server Security and Maintenance | 3 |

As with the lower-division curriculum, the indicated course sequence is a recommendation of when to complete a course to provide as much synergy between course content as possible. Except that prerequisite requirements must be satisfied before taking a course, the semester in which a student completes a course will be dependent upon their personal situation and needs. At the conclusion of the program of study, the students will be prepared to take several industry certification examinations, including Security+, Network+, CySA and CEA.

There are several elective courses in the upper-division curriculum. The courses from which the student can select to satisfy these electives are shown in Table 3

Two significant courses in the upper-division curriculum are the cybersecurity design projects. In these courses the students are expected to be working in a hands-on environment addressing cybersecurity issues brought forward by the industry partners.

The baccalaureate degree program fully satisfies the curricular content recommended by the industry advisory group. Presented in Annex 1 is a mapping of the lower-division and upper-division coursework to the expectations of the industry group.

ABET Accreditation and CAE Knowledge Units

In addition to the curricular recommendations, the industry advisory council recommended that:

- The curriculum must comply with the general and program specific requirements for cybersecurity baccalaureate programs of ABET, Inc., and
- The curriculum must contain the National Centers of Academic Excellence (CAE) in Cyber Defense Education Program Knowledge Units

The recommendations of the advisory council represented a superset of the CAE Knowledge Units [7] and the criteria of ABET [8]. Mappings of courses to the ABET general and program criteria and to the CAE cyber defense knowledge units are presented in Annex 2 and Annex 3, respectively. As evidenced by the mappings presented, the expectations of both are satisfied. These mappings represent a snapshot of the curriculum as of the writing of this paper, and there are multiple ways in which courses can be mapped depending upon the content as implemented. As the field of cybersecurity evolves, and as the CAE knowledge units and ABET criteria change, the curricular content and course mappings will likely change.

**Technical and Non-Technical Cybersecurity Minors**

To support the need for individuals who are not directly employed in the cybersecurity industry, but who need to be knowledgeable about cybersecurity, minors can be developed that can be incorporated into other degree programs. Pursuing such a minor will provide students with additional marketable credentials upon graduation. The minors offered can be of two forms, namely:

- A technical minor that can be pursued by students completing a degree program in engineering or computer science, but not in cybersecurity. A design goal would be that some of the courses required for the minor could be a part of the student's degree program. A further expectation is that these courses for minor, coupled with the courses in the technical major, would enable the student to pursue a Master of Engineering degree in cybersecurity.
- A non-technical minor that can be pursued by students not completing a technical degree program. A design goal would be that some of the courses required for the minor could be a part of the student's degree program. Students pursuing this minor could be business or criminal justice students, for example.

The minor will contain 15 to 18 credit hours regardless of whether it is a technical or non-technical minor. The course content for the minors will vary depending upon the students major and interests. Nevertheless, two courses to be contained in both types of minor are "Ethics, Law

and Cybersecurity" and a cybersecurity design project for non-majors. The purpose of the design project will be to apply the principles of cybersecurity to their major and career interests.

**Non-Degree Programs**

The types of non-degree programs offered can be widely varying and have different entry points, including:

- Short duration certificate programs intended to provide a set of skills necessary for an entry level position,
- Longer duration industry certification programs that prepare the high school graduates for employment and the ability to advance more quickly,
- Advanced and continuing professional development programs, and
- On-demand programs that address specific skills needed by an individual employer, or that satisfy manufacturer's need for training on evolving systems.

These programs are those contained in the middle group in Figure 5. These programs likely result in a certificate of completion. Some can lead to recognized certifications, such as those of the National Security Agency (NSA). There is no preconceived way these certificate programs are offered or their duration.

Non-Degree Program Review

The RELLIS Cybersecurity Industry Advisory Council will review each program of study proposed to be offered through the RELLIS Cybersecurity Alliance. The decision tree for deciding if a program will be offered through the RELLIS Cybersecurity Alliance was presented in Figure 6. The review of the non-degree programs will be based on the syllabus submitted with the request to offer a program through the Cybersecurity Alliance. After reviewing the program, the Industry Advisory Council can make one of four recommendations:

- The program should be offered as proposed,
- The program should be offered as proposed with suggested additions or deletions,
- The program should not be offered as proposed as some elements need to be improved, recommendations for change to make it an acceptable program are provided, and the program is to be submitted for review after the changes are made, or
- The program requires significant change and should not be offered as proposed.

The final decision to offer or not to offer a program resides with the leadership of the RELLIS Cybersecurity Alliance. Such decisions could be based on facilities or economics of demand, rather than program content. If the action of the leadership team regarding the program is different from the recommendation of the Industry Advisory Council, the leadership team will notify the Industry Advisory Council in writing of its decision and the basis for that decision. The Advisory Council will have the opportunity to respond to that notification, and potentially influence the decision.

Initial Planned Offerings

Initially three certificate and professional development courses are planned to be offered. These programs are those indicated in the brown shaded box on Figure 5. The programs, which are

contained in the white paper entitled “Public-Private Training for Cybersecurity Professionals” [9] are:

- Cybersecurity Specialist/Technician

  Upon successful completion of this program, the student will have demonstrated skills necessary to immediately enter the workplace and perform in an entry level cybersecurity specialist/technician position. During the program students will earn appropriate national certifications.

  This program is anticipated to be a one year long in-residence program combining classroom instruction and hands on experience leading to a certificate of completion. Anticipated offering is once annually. Prior to entering the program, students are expected to have knowledge of a high-level programming language and network operations. They must also pass a competency examination on these topics. The expected prerequisite knowledge can be obtained through relevant high school CTE courses or work experience.

  This program includes 1,800 hours (45 weeks) of study, including approximately 900 hours of hands-on experience in the Security Operations Center (SOC) and as a trainee on the Computer Incident Response Team (CIRT). The basic elements of the training program are:

  - Cybersecurity for State Officials
  - Foundations of Cybersecurity
  - Cybersecurity Law, Policy, and Risk Management
  - Privacy/CIPT Certification Class
  - CompTIA Certifications Class
  - Intro to Python
  - Hardware/Software Security
  - SIEM Management
  - Intro to Digital Forensics
  - Intro to Network Defense
- Cybersecurity Professional Development

  Upon successful completion, the student will have the necessary technical and organizational knowledge to successfully lead cybersecurity operations within an organization. The intended audience is individuals who have been working in the IT arena but need to develop enhanced skills in the area of cybersecurity. This program is anticipated to be a 12-week long program combining classroom instruction and hands on experience leading to a certificate of completion. Parts of the program will be on-line to facilitate participation. The primary learning modules and the breakdown of on-line and on-campus components are:

  - 5 weeks of on-line instruction on cybersecurity fundamentals,
  - 1 week on campus working on the cyber-range working with simulated threats,

    - 5 weeks of on-line instruction requiring one weekend on campus related to operations, and
    - 1 week on campus working on the Texas Cyber-Range and in the SOC working with real-time system monitoring and threats.
- Cybersecurity for Managers

  Upon successful completion, the student will have the necessary technical and organizational knowledge to mitigate cybersecurity risks within their organization through a better understanding of the risks and necessary organizational and operational structures to identify and report attacks. The intended audience for this program is individuals responsible for cybersecurity at the managerial level but are not necessarily the individuals providing the operational and technical support.

  This program is anticipated to be a weeklong on-campus program combining classroom instruction and hands on experience leading to a certificate of completion. The basic topics to be addressed are as follows:

    - The issues relating to cybersecurity
    - The potential risks and vulnerabilities
    - The questions to be asked about your organization
    - Organizational structures for reporting and mitigating risk

**Supporting Facilities**

On the RELLIS Campus and the Texas A&M University Campus are several facilities that directly support the cybersecurity training discussed herein. These facilities include:

- IoT Apartment Laboratory: Within the Academic Complex Building 1 an apartment was constructed with a plenum providing access to the outer walls. The apartment was constructed in the same manner as typical residential construction, including the electrical and plumbing infrastructure. This apartment provides the ability to conduct research and student design projects dealing with the consumer Internet-of-Things.
- SCADA Laboratory: Currently in construction is a SCADA laboratory in the second building in the second building in the academic complex, which is currently under constructions. This laboratory will be a working industry sponsored laboratory that will provide for student projects, coursework assignments, and internships for students. It contains approximately 900 sf of space.
- SOC: The Texas A&M University System SOC is available for student training and internships. It will be used extensively in some of the professional development programs.
- Cybersecurity Center: The Center seeks to advance the collective cybersecurity knowledge, capabilities, and practices, doing so through ground-breaking research, novel and innovative cybersecurity education, and mutually beneficial academic governmental and commercial partnerships. Working with researchers, faculty, and

industry leaders, the Center stands committed to make outsized contributions to social good through the development of transformational cybersecurity capabilities.

- Texas Cyber-Range: The Cyber-Range enables faculty to develop specific scenarios and types of attacks that students using the range need to mitigate. As the range is a simulated environment, attacks can be simulated that a student may never see in practice but could see. It provides a training environment similar to the SOC, but there is greater control over what the students sees while on the range; training is not dependent upon the occurrence of an actual attack.

## Conclusions

As technologies advance and the world becomes more interconnected, the ability of government, industry, and the private sector to secure its cyberspace, from both physical and cyber threats, will continue to be a growing concern, which must be addressed. Alliances and/or partnerships between the public, private, and education sectors are needed to close the skills gap and produce a highly qualified cyber defense workforce, according to the national Chief Information Officers and Chief Information Security Officers [10] [11]. In a 2018 article, which addressed needed improvements in cybersecurity education, Zurkus stated "To change this (skills gap), higher education has to address the theoretical and hands-on skills students need to do their jobs post-graduation." [12]

Recognizing these needs the RELLIS External Academic Advisory Council authorized the creation of the RELLIS Cybersecurity Alliance. RELLIS is an innovative campus with resources to facilitate a collaborative research, technology development, education, and training partnerships between public, private, and educational entities. With an Industry Advisory Board and strategic partners, the Alliance can meet the portion of its mission to provide a mechanism for industry involvement in educational/training offerings and support career awareness initiatives. The other part of the mission to establish applied research and demonstrable hands-on skills, including internships, is afforded to faculty and students as a result of the resources available through the Alliance. These include but are not limited to an IoT Apartment Laboratory, Texas Cyber-Range, SCADA Laboratory, Cybersecurity Center, and Security Operations Center. The RELLIS Cybersecurity Alliance and its partners are uniquely positioned to address the critical needs in the evolving cybersecurity field.

## Acknowledgement

The authors gratefully acknowledge the support, encouragement and wisdom of Dr. Stephen Cambone in the development of the RELLIS Cybersecurity Alliance and the programs of study offered through the Alliance. Without question, his insights and knowledge have made the Cybersecurity Alliance stronger and more complete.

**References**


[1] J. Kauflin, "The Fastest Growing Job with a Huge Skills Gap: Cyber Security," Forbes Media LLC, March 2017. [Online]. Available: Forbes.com.

[2] J. Manyika, "Unlocking the Potential of the Internet of Things," McKinsey and Company, 2015.

[3] D. FitzGerald, "Activist Investor Challenges AT&T Over Strategy, Board," *Wall Street Journal,* 9 September 2019.

[4] Universaltech News, "IT-OT Cybersecurity Convergence-ARC Viewpoints (Blog)," 2020. [Online]. Available: https://universaltechnews.com/it-ot-cybersecurity-convergence-arc-viewpoints-blog/.

[5] J. Manyika and et. al., "Unlocking the Potential of the Internet of Things," McKinsey Global Institute, McKinsey and Company, June 2015.

[6] THECB, "Lower-Division Academic Course Guide Manual," Texas Higher Education Coordinating Board, Austin, TX, 2019.

[7] Center for Academic Cyber Defense, "2019 Knowedge Units," [Online]. Available: http://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf. [Accessed 2020].

[8] ABET, "Criteria for Accrediting Computing Programs, Effective for Reviews During the 2020-2021 Accreditation Cycle," ABET, Inc., Baltimore, 2019.

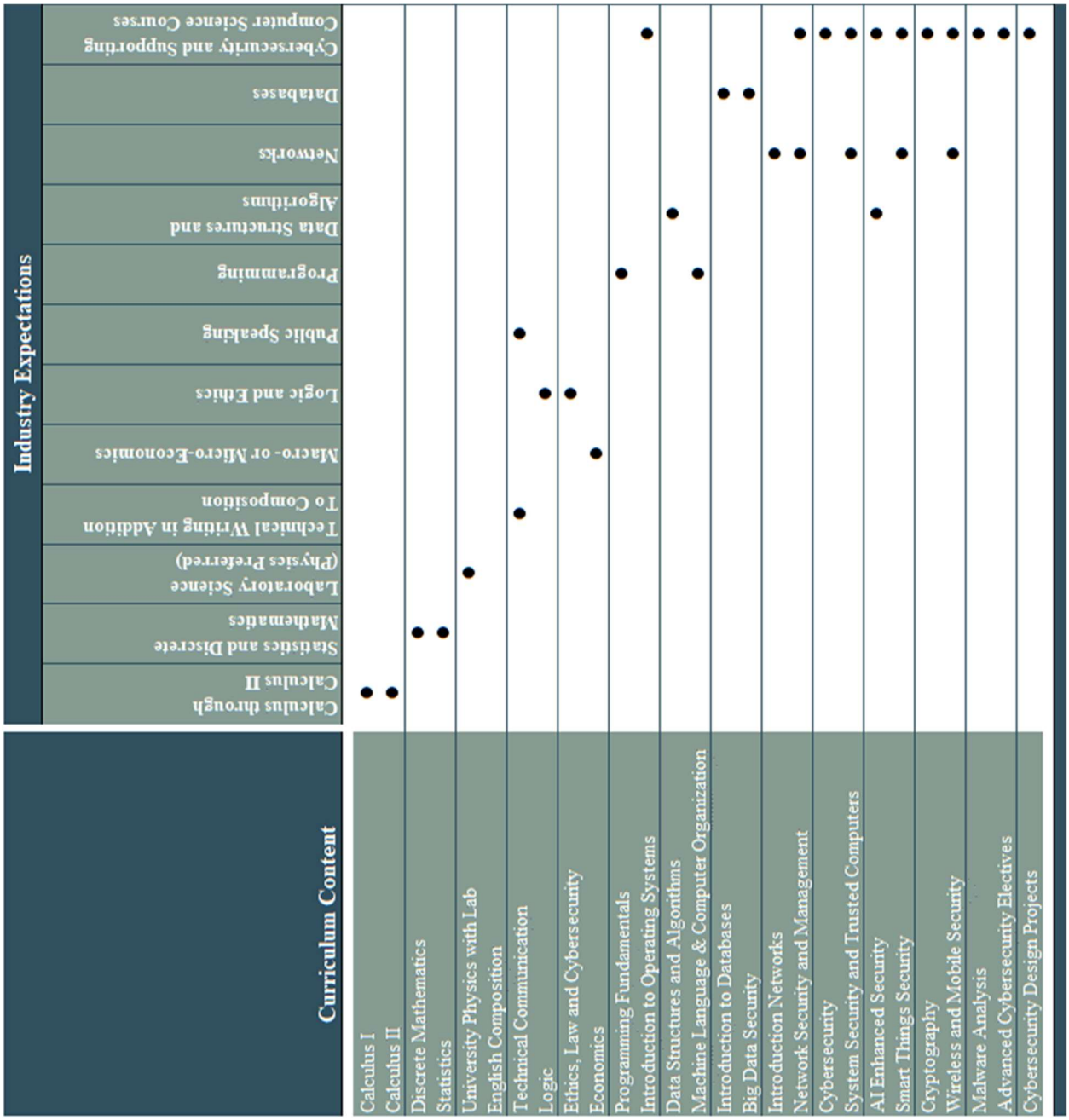
[9] J. K. Nelson, D. Davis, S. Smith and M. Stone, "Public-Private Training for Cybersecurity Professionals, A RELLIS Cybersecurity Alliance White Paper," Texas A&M University System, College Station, 2019.

[10] Office of the Chief Security Information Officer, "Texas Cybersecurity Strategic Plan: Fiscal Year 2018-2023," Texas Department of Information Resources, Austin, 2018.

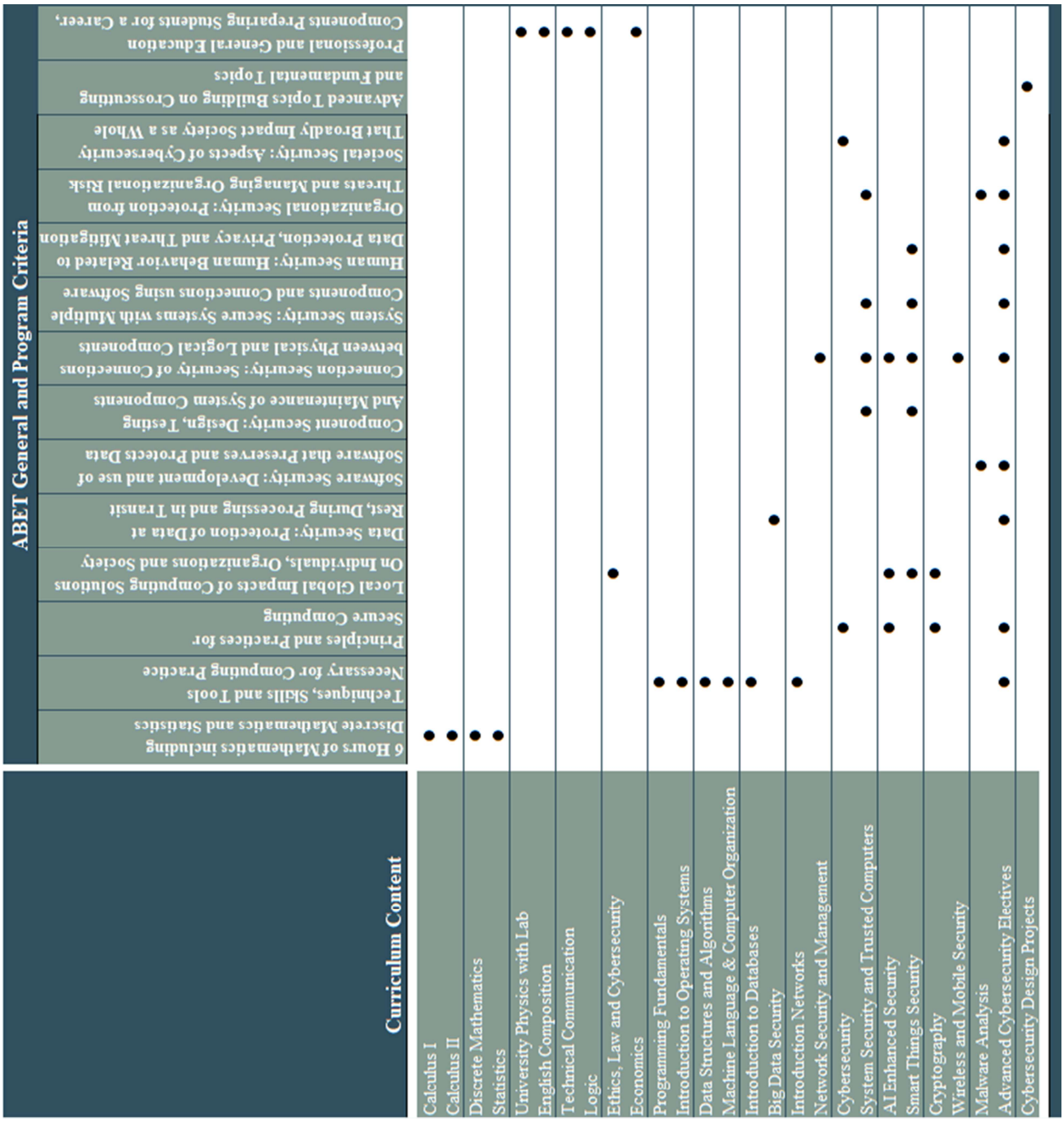
[11] S. Subramanian and D. Robinson, "2018 Deloitte-NASCIO Cybersecurity Study, States at Risk: Bold Plays for Change," 2018. [Online]. Available: https://www2.deloitte.com/us/en/insights/industry/public-sector/nascio-survey-government-government-cybersecurity-strategies.html.

[12] K. Zurkus, "How Can Industry Leaders and Academic Help Improve Cybersecurity Education?," Available online at https://securityintellicence.com, 2018.

## Annex 1: Mapping of Undergraduate Curriculum to Advisory Council Recommendations



## Annex 2: Mapping of Courses to ABET General and Program Criteria



## Annex 3: Mapping of Courses to CAE Cyber Defense Education Program Knowledge Units

| Curriculum Content | Cyber Defense Education Knowledge Units | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Cybersecurity Foundations | Cybersecurity Principles | IT Systems Components | Basic Cryptography | Basic Networking | Basic Scripting and Programming | Network Defense | Operating Systems Concepts | Cybersecurity Ethics | Data Administration | Data Structures | Databases | Digital Forensics | Mobile Technologies | Network Security Administration | Operating System Administration | Privacy | Vulnerability Analysis | System Security Engineering | Supply Chain Security | Software Security Analysis | Secure Programming Practice |
| Ethics, Law and Cybersecurity | ● | | | | | | | | ● | | | | | | | | ● | | | | | |
| Programming Fundamentals | | | | | | ● | | | | | | | | | | | | | | | | |
| Introduction to Operating Systems | | | ● | | | | | ● | | | | | | | | ● | | | | | | |
| Data Structures and Algorithms | | | | | | ● | | | | | ● | | | | | | | | | | | |
| Machine Language & Computer Organization | | | | | | ● | | | | | | ● | | | | | | | | | | |
| Introduction to Databases | | | | | | ● | | | | | ● | ● | | | | | | | | | | |
| Big Data Security | ● | | | | | | | | | ● | | | | | | | ● | | | ● | | |
| Introduction Networks | | | ● | | ● | | ● | | | | | | | | ● | | | | | | | |
| Network Security and Management | | | | | ● | | ● | | | | | | | | ● | | | | | | | |
| Cybersecurity | ● | | | | | | | | ● | | | | | | | | ● | | | ● | | |
| System Security and Trusted Computers | | | | | | | | ● | | | | | | | | ● | ● | | ● | ● | | |
| AI Enhanced Security | | ● | | | | | | | | ● | | | | | | | ● | | ● | | | |
| Smart Things Security | | | | | | | ● | | | | | | ● | | ● | | ● | | ● | ● | | |
| Cryptography | ● | | | ● | | | | | | ● | | | | | ● | | | | | ● | | |
| Wireless and Mobile Security | | | | | ● | | | | | | | | ● | ● | | | | | | | | |
| Malware Analysis | ● | | ● | | | | | | | | | | | | ● | | ● | | | | | |
| Digital Forensics | | ● | ● | | | | | | | | | | ● | | | | | | | | | |
| Cybersecurity Design Projects | | ● | ● | | | ● | ● | | | | | | | | | ● | | | | | | ● |
| Cybersecurity Electives | ● | ● | ● | | | ● | | | | | | | ● | | ● | ● | | ● | | | ● | ● |