Multiyear collaboration between the US Army and an ECE program to develop student skills in cybersecurity of cyber-physical systems

Virgilio Gonzalez
Electrical and Computer Engineering
University of Texas at El Paso
El Paso, TX, USA
vgonzalez3@utep.edu

Oscar Perez
Cybersecurity Analyst and Outreach
DEVCOM Analysis Center
WSMR, NM, USA
oscar.a.perez46.civ@army.mil

Rodrigo Romero
Electrical and Computer Engineering
University of Texas at El Paso
El Paso, TX, USA
raromero2@utep.edu

Pilar Gonzalez
Teacher Education
University of Texas at El Paso
El Paso, TX, USA
pgonzalez27@utep.edu

Hector Erives-Contreras
Electrical and Computer Engineering
University of Texas at El Paso
El Paso, TX, USA
herivescon@utep.edu

***Abstract*— This innovative practice full paper describes a collaboration to incorporate cybersecurity into an Electrical Engineering program. It is widely recognized that there is a need to educate the technical workforce to be prepared against cybersecurity threats. There is a growing recognition of the importance of Cybersecurity in various engineering fields, including Electrical Engineering (EE). However, including Cybersecurity in EE curricula may not be as prevalent or emphasized as in fields like Computer Science or Computer Engineering. For three years the ARMY – DEVCOM – Analysis Center at WSMR has collaborated with the Electrical and Computer Engineering Department at The University of Texas at El Paso in a multifaceted series of efforts to increase the number of students capable of working on cybersecurity from the physical perspective. In addition, there is a general increase in awareness about vulnerabilities, attacks, and their countermeasures in system confidentiality, integrity, and availability in each cohort.**

There are four major efforts in the partnership. First, the entire capstone design cohort receives basic training to increase awareness of cybersecurity to be considered as part of the general requirements of all projects. Second, in each cohort, there is at least one team focusing on developing a system solution for a cybersecurity application, such as training devices or demonstration platforms in an unclassified setting. Third, the degree plans of the ECE bachelor's and master's degree programs have evolved to include formal elements of cybersecurity through several courses, including a cybersecurity track within Computer Engineering. Finally, concurrently with other efforts, a group of students is hired by the university to work as interns with the ARMY.

In previous years, we presented initial results regarding the number of students who benefitted from these efforts as well as representative systems developed by students. To complete the assessment, we are working on a two-phased explanatory sequential mixed methods study using quantitative data and then explaining the quantitative results with in-depth qualitative data. The initial phase of the study collected quantitative data through surveys for several student cohorts. This will be followed by some interviews with selected individuals to probe or explain those results in more depth. Our initial hypothesis is that the different efforts should increase the number of students aware of cybersecurity considerations in engineering designs as well as their expertise level. Our next question to answer is which methods produce the best results in preparing the specialized workforce to deal with cybersecurity aspects of cyber-physical systems.

Keywords*— *Cybersecurity; Industry collaboration; Capstone Design

I. INTRODUCTION

Computers and electronics have evolved to smaller sizes and prices, and due to these two factors, they continue to be integrated to support many aspects of our daily lives. Due to the many benefits, humans rely on computers and electronics as systems for communications, banking, sales, directions, and health, among others. Computers and electronics have become a part of our day-to-day operations. This integration of computers and electronics has triggered an increase in hardware and software development to support new innovative devices and applications. Unfortunately, new software and hardware development have security gaps that have opened the door to cybersecurity threats. As new devices and applications arrive to the public, the attack surface for cybercriminals continues to increase. Due to the critical functions computers and electronics perform, cybersecurity threats are growing and impacting our

daily lives. There have been multiple incidents reported in the news. The potential to become more disruptive by affecting vital infrastructure is even more worrisome [1-3]. The trend is that they are becoming more costly to organizations [1, 2] and potentially weaponized as part of global conflicts [2, 3]. Those incidents have prompted different organizations to emphasize the need for a better-trained workforce in cybersecurity [4]. However, the typical approaches only promote the best common-sense practices [5]. Therefore, there is a need to adjust the scope and complexity of skills required by a modern workforce [6, 7].

Computer science programs have taken the lead in introducing cybersecurity into their curriculum. However, Blair et al. [8] propose that cybersecurity teams must be composed of different specialties to be more effective. Interdisciplinary teams can provide a cybersecurity analysis from different perspectives, addressing the cybersecurity gaps at the different layers of the technology development cycle, allowing the reduction of the attack surface. NIST has published the National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework (NCWF) [9], which decomposes the significant functionalities and skills needed in this field. Consequently, several professional organizations (ACM, IEEE, AIS, and IFIP) have jointly developed the CSEC 2017 curriculum guidelines for cybersecurity degrees [10]. This framework proposes to structure the curriculum around several knowledge areas:

- 4.1 Knowledge Area: Data Security
- 4.2 Knowledge Area: Software Security
- 4.3 Knowledge Area: Component Security
- 4.4 Knowledge Area: Connection Security
- 4.5 Knowledge Area: System Security
- 4.6 Knowledge Area: Human Security
- 4.7 Knowledge Area: Organizational Security
- 4.8 Knowledge Area: Societal Security

Electrical engineering programs might benefit from introducing general cybersecurity concepts through their curriculum, as they are better prepared to focus on the Component Security and Connection Security knowledge areas. This layered approach to security provides different tiers of protection to the systems being developed. Similarly, providing cybersecurity touchpoints across the academic curriculum allows students to understand and focus on the security requirements for different technologies such as sensors, antennas, processors, memory, etc. This approach implements security from the design stage on systems and not as an afterthought in the final stages of the development cycle. Some preliminary efforts to introduce cybersecurity concepts at different levels of the ECE curriculum have been reported [14-15]. The literature suggests that while initiatives and discussions about integrating Cybersecurity into EE programs exist, it is not yet a standard or widespread component [16,17].

A. Partnerships with the Department of Defense

The US Army DEVCOM Analysis Center (DAC) [13], delivers future readiness as the Army's premier organization for the modernization cornerstones of science, technology, and engineering. DAC's - Cyber Experimentation & Analysis Division (CEAD) needs skilled personnel to perform cyber analysis, experimentation and development of state-of-art cyber analytical tools and methodologies, as well as study, analyze, and experiment with various cybersecurity threats and their corresponding remediation solutions.

The Department of Defense (DoD) needs a well-prepared multidisciplinary STEM workforce to support the development and integration of modern tools used by the defense sector. In addition, DAC needs a workforce that can design, develop, and integrate emerging technologies to secure data communications, data processing, and other functions. DAC has several initiatives that have created a pipeline of students to fill positions in different cybersecurity-focused DoD entities or related industries [11]. These activities motivate students to pursue careers within the STEM fields. DAC provides outreach activities that range from K-12 education involvement [12] to graduate level in university research collaborations.

DAC's at White Sands Missile Range (WSMR) has collaborated with the Computer Science Department at The University of Texas at El Paso (UTEP) for several years to analyze software vulnerabilities and develop a complete analysis of the software and hardware of different systems. In 2019, DAC started collaborating with the Electrical and Computer Engineering (ECE) department, sponsoring a capstone design project for Electrical Engineer (EE) majors each semester. With this initiative, research and development at the hardware level started in the last year of a student's college education. The capstone design collaboration successfully promoted undergraduate research and development and advanced students' skills and abilities within complex cybersecurity topics. In 2020, academic and government institutions developed and proposed a comprehensive collaboration to include cybersecurity holistically across the undergraduate academic curriculum and the student academic journey. The proposed approach expanded collaboration activities and impacted more students.

Working with CS and ECE cohorts allows cybersecurity skills development at the software and hardware levels. Curriculum intervention for the whole cohort can quickly be done by focusing on cybersecurity skills on emerging technologies within the labs, even before these technologies are widely implemented within the consumer domain.

II. STUDY METHODOLOGY.

The explanatory sequential mixed methods research process starts with acquiring quantitative data to identify general trends of the intervention. This will be followed by a second phase, in which a qualitative method study will validate the initial observations and obtain more profound insights into the project results. The explanatory portion interprets the qualitative results to verify or expand the insights obtained during the quantitative phase.

The preliminary work started with quantitative information about the participants and the effect of the interventions. We obtained cohort statistics for the course enrollment and other cohorts' exposure to cybersecurity. Later, we applied surveys to get student perceptions on the level of skills acquired in different stages of the academic program, culminating with capstone design.

We plan to continue next semester by applying the qualitative phase of the methodology through focus groups and individual interviews to better understand the project's elements that contribute to the success and those that have a null or negative impact.

III. Interventions

DAC, in collaboration with the Computer Science (CS) department, helped introduced a cybersecurity course and has been the software engineering capstone design customer for CS students for over ten years. This collaboration proposed interventions in three significant areas for the ECE program, including capstone design projects, dissemination of cybersecurity awareness, and curriculum changes. The expansion to the Electrical Engineering program started in the spring of 2019 with a single capstone project each semester and a team of 4 students. In 2020, ECE supported an expansion of cybersecurity awareness for the entire EE student cohort, which was working on capstone design projects. Cybersecurity awareness was accomplished by hiring a graduate teaching assistant who provided cybersecurity awareness presentations. The presentations focused on different cybersecurity vulnerabilities affecting the technologies the EE capstone design class constructed. We also proposed curriculum changes, including new courses and a specialized concentration for ECE students on special cybersecurity topics.

Figure 1, Mobile Cybersecurity Trainer System

Capstone design projects in cybersecurity. The EE program has a two-semester capstone sequence called Senior Projects I and II (EE4220 and EE4230) offered every semester; thus, there are always simultaneous courses in parallel. EE4220 focuses on engineering design and requirement gathering, while EE4230 focuses on developing and integrating a working prototype. Students must participate in a team of three or four students, and all the topics differ among the student cohort. During the academic years 2019 and 2020, only two groups participated in cybersecurity projects each semester in the corresponding EE4220/4230. Their designs targeted the creation of portable cyber-trainer systems (Figure 1) that had an embedded demonstration of the three pillars of cybersecurity concepts: Confidentiality, Integrity, and Availability. The intended audience for this cyber training system was soldiers and entry-level cybersecurity analysts who needed to learn about cybersecurity applied to hardware systems and the cyberphysical effects of each sensor being compromised. Student project prototypes were chosen to present familiar contexts for the target audience. In each context, explorations of confidentiality, integrity, and/or availability were introduced through scenarios combining a related concept, vulnerability, attack, and countermeasure to illustrate each aspect for users. Some examples of students' work include demonstrating a computer-controlled factory and the different attack vectors that affect each communication protocol, network, and sensor. Other projects showcased compromising the confidentiality of human-to-machine and machine-to-machine communications between unencrypted and encrypted channels.

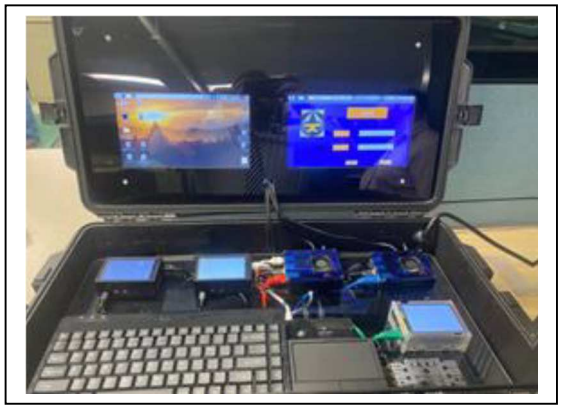

Figure 2, Biomedical micro cyber-range

Furthermore, these first-year prototypes included a Denial-of-Service cyber-attack to compromise availability by turning off services within the computer-controlled factory. The intended purpose of these capstone projects was to create a micro cyber range that isolates the technologies in a sandbox for repeated experimentation with the ultimate goal of educating the audience about cybersecurity and mitigation strategies to be incorporated within these types of systems. The second-generation project assigned to the capstone students was a biomedical prototype (Figure 2) with several biometric sensors within this system using wireless technologies for machine-to-machine communications. The biomedical prototype provided a sandbox to illustrate cyber threats to biomedical instrumentation and mitigation strategies for these devices. Most recently, the capstone design projects included an augmented reality tool using the Microsoft® HoloLens system. (Figure 3). The augmented reality capstone project included cyber threats to an AI/ML algorithm in charge of doing image detection. All the capstone design prototypes up to Spring 2023 have been

delivered to DAC, where these prototypes have been used to train and showcase different cybersecurity attack vectors, illustrating the cyberphysical effects on the operations and functionality of the different elements within the system.

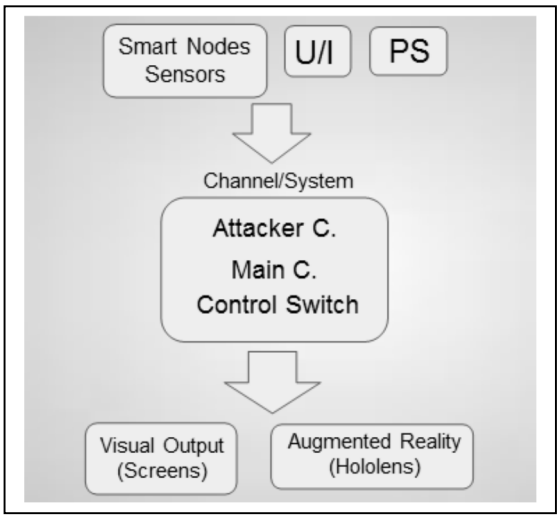

Figure 3, Augmented Reality Project

Entire ECE cohort awareness. In spring 2020, after successful first-year implementation feedback from DAC, a new proposal was created between the university and the government agency to expand the work within this collaboration. The positive feedback the university received from the government agency was based on the number of students graduating with cybersecurity skills and abilities. Specifically, the EE capstone project students were hired as full-time employees. Additional funding was provided to support more initiatives through DAC's Cyber Center for Analysis and Assessment (CCAA). The capstone design has continued with more advanced projects requiring higher technical complexity. The third-generation system incorporates ideas using Augmented Reality (Figure 3) devices and an Artificial Intelligence (AI) system to identify objects. The students working on the Augmented Reality prototype could identify adversarial AI attack vectors and introduce basic data poisoning mitigation strategies to make the AI system resilient to these attacks. Besides the teams developing a cyber-trainer prototype each semester, ECE incorporated a Graduate Teaching Assistant (TA) into the capstone course. The TA specializes in cybersecurity topics and creates training materials to raise awareness among all the senior project students in each cohort. The training provided by the TA intervention included concepts in preserving the confidentiality of information in the system, maintaining data integrity, and keeping the system services available. The capstone teams with different projects each had to make a vulnerability analysis of their system design. This student analysis of their own system addressed simple cybersecurity attacks on confidentiality, integrity, and availability. With the analysis assigned, the TA-led training allowed students to integrate cybersecurity concepts into their design.

Additionally, students created a list of cybersecurity risks, allowing the team members to brainstorm potential solutions before the prototype was built. The student analysis triggered a change in the student's mindset. Students focused on design for functionality without overlooking the cybersecurity aspects of their design.

The cost for each senior project ranges from $1k to $5k, depending on the technology requirements from DAC. The senior project prototypes focusing on Augmented Reality were more expensive and required specific hardware. This part of the budget changes every semester as it is adjusted to the selected technology to be implemented on the prototypes, and the budget changes according to the supply and demand on the market. ECE has about $20k per year budgeted for the teaching assistant. There are other indirect institution costs added.

Curriculum changes. The ECE department and DAC constantly communicate, reviewing emerging technologies and their associated cybersecurity threats. Based on these discussions and technology trends, the ECE department created two formal courses in cybersecurity geared toward embedded systems. These two courses look at cybersecurity vulnerabilities and mitigation strategies from the hardware perspective of embedded systems, focusing on the lower layers of the Open Systems Interconnection (OSI) model. In addition, these classes provide EE students with foundational knowledge of cybersecurity concepts and emerging threats to electrical and electronic systems. One class is for undergraduates, and the other is for graduates. Other courses, such as Software Design II, Introduction to Communication Networks, and Data Communications, added cybersecurity awareness topics in security. These courses emphasize the knowledge areas of Component Security and Connection Security, which focus on hardware [9].

The ECE department initiated the process to offer a new BS degree in Computer Engineering, which was approved in the summer of 2022. The collaboration with DAC and the gap in cybersecurity experts to fill available positions supported the need to provide this new degree and to include a cybersecurity specialization track. The process was already underway, and the collaboration influenced the decision to include a concentration track in cybersecurity. The ECE department has approximately 20 students who switched from the EE program to the new Computer Engineering program and 30 newly enrolled students in 2023.

IV. Results

The proposal for additional funding was awarded in the Fall of 2020, and six advanced capstone projects have been supported directly by this grant. There were 20 students involved (as students participating in capstone projects). These students benefited from the direct application of cybersecurity knowledge in their senior projects. The ECE department intentionally added cybersecurity topics in four concentration courses and two graduate classes. Before Fall 2019, there was no formal course offering or cybersecurity awareness in the EE program.

TABLE I. , ENROLLMENT AND PARTICIPATION

Acad. Year	Cyber Courses	Graduates
18-19	8	98
19-20	35	110
20-21	51	98
21-22	62	65
22-23	65	85
23-24	68	71

Since the spring 2021 semester, 274 students have completed the Senior Projects sequence, all of whom have been exposed to cybersecurity concepts through the training provided by the TA in the senior project class and gaining awareness of its application to other problems/systems. However, the cohort of Spring 2023 had 47 students in two sections, and 13 did not receive the training because there was a new instructor for that class who was not involved in the intervention. The 13-student section will be used to compare the results of the survey instrument.

In addition, the following courses started offering some topics in cybersecurity:

- • EE3372 Software Design 2.
- • EE3354 Intro to Communication Networks.
- • EE4395 / 5390 Special Topics in cybersecurity.
- • EE5330 Data Communications.

Table I shows the enrollment in different courses from fall 2018 until spring 2024. Before Fall 2019, there was no formal course offering or cybersecurity awareness in the EE program. Between the Spring of 2019 and the Fall of 2020, 4 students per capstone project were involved in a specific cybersecurity project (8 total per semester). Also, we started offering an elective course that included about half senior and half graduate students. The "Cyber Courses" column indicates the number of students involved in some explicit cybersecurity topics during the semester, and the "Graduates" column is the total number of students graduating during the same semester. The grant from DAC in the Spring 2021 enabled the expansion of course offerings and promoted the broader participation of students (complete graduating cohort).

The EE program graduated 110 students during the AY19-20 (Fall 2019 – Summer 2020); however, according to the data gathered, only 35 obtained cybersecurity knowledge through projects or the new course (which started in the Fall of 2020), and the rest of the cohort did not have any exposure. In comparison, in subsequent academic years, more than 75% of the graduates were involved in some security course or supplementary activity. Some took specific courses in networking, software, and security, while almost the majority of the cohort obtained some essential awareness through the TA intervention during the capstone class. The quantitative data shows that more students participated in cybersecurity efforts every semester. Notice that the recent decrease in cohort enrollment was due to the COVID impact; the decrease in enrollment happened across all colleges within the University.

A recent change is the approval in the summer of 2022 to offer a new degree in Computer Engineering. A critical component of the new degree proposal requires industry and external partnership support. The backing from DAC and the inclusion of the cybersecurity concentration motivated other companies and government organizations to offer support letters indicating their interest in the new program. Support organizations were convinced that the newly offered degree would positively change the landscape concerning students graduating with cybersecurity expertise starting in Spring 2022. The State Higher Education Coordinating Board approved this proposal during the summer of 2022.

As a secondary effect, these efforts have increased the interaction between the University faculty and engineers from DAC in the research areas of communications, robotics, antennas, and cybersecurity. Consequently, the ECE department has obtained new grants and/or contracts to support studies on the future generation of wireless technologies and using AI to train Intrusion Detection Systems within computer networks. Finally, these interactions have increased student research positions. Fourteen semester-long positions have been created at the master's and PhD levels to support the collaborative research efforts up to Spring of 2023.

In addition to the quantitative analysis of students graduating from the ECE program, a qualitative study started in Spring 2023. A survey instrument was developed to measure and understand the students' perspectives on the cybersecurity education they received. The qualitative survey was applied for the first time to the 47 students who graduated in Spring 2023, and to 21 students in Spring 2024, and the questions are listed in Table II. The survey used a Likert scale with the following coding: 1 - disagree, 3 - neutral, and 5 - agree. Most questions were grouped to identify the awareness, importance of cybersecurity, ability to apply principles, and when students received training within cybersecurity. The cybersecurity awareness, importance, and application questions were also expanded to identify the perception before entering the ECE program, before entering the capstone project, and after completing the yearlong capstone project. For the analysis of this survey, the questions have been divided into five groups according to the different colors in Table II. This grouping of questions allows us to visualize the impact of the different intervention methods and the weight of the impact on student perception.

TABLE II. , SURVEY QUESTIONS

Q1	BEFORE entering the ECE program, I was AWARE of the cybersecurity importance
Q2	BEFORE entering the Senior Projects course, I was AWARE of the cybersecurity importance
Q3	AFTER completing senior projects, I am AWARE of the cybersecurity importance
Q4	BEFORE entering the ECE program, I considered cybersecurity to be critical.
Q5	BEFORE entering the Senior Projects course, I considered cybersecurity to be critical.

Q6	AFTER completing senior projects, I consider cybersecurity to be important.
Q7	BEFORE entering the ECE program, I was able to apply technical cybersecurity methods
Q8	BEFORE entering the Senior Projects course, I was able to apply technical cybersecurity methods
Q9	AFTER completing senior projects, I can apply technical cybersecurity methods
Q10	I had training in cybersecurity methods BEFORE entering the ECE program.
Q11	I had training in cybersecurity methods in courses from the ECE program besides senior projects.
Q12	I have training in cybersecurity methods through the course of senior projects.
Q13	I CONSIDERED cybersecurity requirements for my senior project.
Q14	I APPLIED cybersecurity requirements to my senior project.
Q15	I CONSIDERED following a career to develop and apply cybersecurity methods.

In Table III, we show the results. Answer values of 1-2 were grouped as unfavorable, 3 as neutral, and 4-5 as positive. We observed similar gain levels in both Spring 2023 and Spring 2024.

TABLE III. SURVEY RESPONSES (2023:N=47, 2024: N-21)

Quest	Spring 2023					Spring 2024				
	Avg	Gain	% Neg	%Ntrl	%Pos	Avg	Gain	% Neg	%Ntrl	%Pos
Q1	3		34%	32%	34%	3.4		24%	19%	57%
Q2	3.4	0.39	26%	21%	51%	3.5	0.05	24%	24%	52%
Q3	4.6	1.18	2%	13%	85%	4.3	0.81	5%	5%	90%
Q4	3.6		13%	32%	53%	3.9		14%	14%	71%
Q5	3.9	0.31	6%	23%	70%	4	0.1	14%	5%	81%
Q6	4.6	0.7	2%	9%	89%	4.3	0.29	5%	10%	86%
Q7	2.3		55%	32%	13%	3		33%	24%	43%
Q8	2.8	0.55	34%	36%	28%	3.3	0.24	24%	29%	48%
Q9	3.7	0.85	13%	32%	55%	3.9	0.62	10%	24%	67%
Q10	1.9		70%	17%	11%	2.8		48%	14%	38%
Q11	2.3		57%	23%	19%	2.8		48%	19%	33%
Q12	3.2		28%	34%	38%	3.4		24%	29%	48%
Q13	3.3		32%	17%	51%	3.3		29%	19%	52%
Q14	3.3		32%	15%	53%	2.8		43%	14%	43%
Q15	2.8		43%	28%	30%	2.7		43%	19%	38%

Questions 1, 2, and 3 ask about cybersecurity awareness, which are referred to as Q1, Q2, and Q3. Q1 is before entering the ECE program, Q2 is the level of awareness before entering senior project capstone classes, and Q3 is after completing the senior project capstone classes. The "Gain" column shows the differential compared to the previous instance and intends to show the progression of the skill. We observed that the courses outside the senior project have a lesser impact (measured as 0.39 and shown in the Gain column of Q2), but the senior project classes effect is the increase close to one level (measured as 1.18 , and 0.81 and shown in the Gain column of Q3).

Questions 4, 5, and 6 focus on measuring the progression of cybersecurity importance and how critical cybersecurity has become. In this set of questions, the gain seems almost one level overall. This set of questions also shows how students increase the critical weight given to cybersecurity after the senior project classes. Again, the main factor in these questions is the capstone project classes, in the gain column of Q6. Q5 shows the impact that the ECE curriculum is having on student's perception, Gain column of Q5.

Questions 7, 8, and 9 are related to the ability to apply cybersecurity principles and methodologies, and the main change is that only 55% of students felt unable to do so before entering the program, versus the 13% who expressed they could apply such knowledge after the course. Again, the main factor in these questions is the capstone project (Gain column of Q9). Interestingly, Q8 shows that the most significant impact of the ECE curriculum, according to the students, is on the application of technical cybersecurity methods (measured as 0.55 and shown in the Gain column of Q8).

Questions 10, 11, and 12 show where they received some cybersecurity training, and we noticed the 13 students that did not participate in capstone training in spring 2023 had an impact on the perception. Question 13 shows if they considered cybersecurity as part of the constraints of their project, and 14 of them applied requirements, half of the students did not. Question 15 is about the possibility of continuing a career in cybersecurity, and 14 students positively considered the option.

These efforts have increased the interaction between faculty and engineers from DAC as a secondary effect. Consequently, we have obtained new grants or contracts to support studies on wireless security and Artificial Intelligence (AI) and Machine Learning (ML) applied to Intrusion Detection Systems (IDS). As a result, two more graduate students were hired to support the collaborative efforts.

In the qualitative phase of this study, we asked the participants three open-ended questions: 1) What would you say was the most important thing you learned about cybersecurity? 2) How do you suggest we could improve teaching about

cybersecurity? 3) What would you say you learned through this course?

The responses to the first question developed the following results: 61% of the participants expressed that the most essential learning about cybersecurity they learned was safety [Figure 4]. Safety regarding information such as privacy, integrity, and hacking of passwords and systems. One of the participants stated, "The most important thing I learned about cybersecurity is that it is continuously changing." Another one realized the importance of it, as they mentioned: "Including cybersecurity in my project allows for the safety of our system and the country." At the same time, 28% saw the connection between understanding how systems work to protect them from attacks.

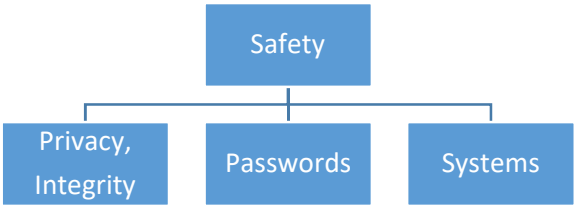

Figure 1, Main ideas related to the question about the most essential learning about cybersecurity

As for the second question, how do you suggest we could improve teaching about cybersecurity? 66% of the participants stated the need for courses about cybersecurity; the "lectures" they have do not seem enough for them to learn what is needed. A participant mentioned: "I think it can be [taught] once a week in a class similar to Junior Professional Orientation. Or it can be taught during the Senior lecture period." In this context, junior professional orientation is a 1-hour per week taken in a previous semester, while the Senior lecture period is a 1-hour per week. The rest of the participants did not respond to this question, which means that 100% of respondents asked for more cybersecurity training.

On the other hand, it is apparent that for some participants, the intervention was not necessarily a class or course in cybersecurity. A couple of participants expressed, "I did not have any teaching by a professor about cybersecurity," and another: "Have a class about it." Therefore, we must be explicit when teaching this topic.

Regarding the last question: What did you learn through this course? We found the following topics, with some examples mentioned in parentheses (Table IV).

Finally, we must restate that this was a laboratory course where the students select their teams and projects. The professors and TAs are a resource the students use to gain guidance. Although the students receive tutorial modules, they do not receive lectures.

TABLE IV. CODIFIED TOPICS

Knowledge	Number of times mentioned
Communications Networks (antenna theory, interference in signals) Devices (telemetry frequency)	4
Cybersecurity (encryption algorithms)	7
Project management (coordinate based on budget and time constraints, multiple testing, system integration, standardization)	5
Control systems (signal processing, control signals)	2
Hands-on approach (building hardware, drones, GPS, security	5
Teamwork (attitudes, feelings, social influence, group dynamics, relationships	2

V. CONCLUSIONS AND FUTURE WORK

The formal collaboration resulting from the funded proposal occurred during the COVID-19 pandemic. For this "Work in Progress," we focused only on implementing the activities required by the proposal and the total number of participants. We observed that before the interventions, at most, 12 out of 110 students obtained some cybersecurity experience. After the intervention, 51 out of 149 students gained a deeper understanding of cybersecurity, and the entire cohort gained awareness. We also noticed that the students who were enrolled in a section without explicit cybersecurity training did not attain the same level of awareness and skills compared to other cohorts. The survey shows that the laboratories should be explicit when teaching cybersecurity, given that some students mentioned that they have never received such instruction. Therefore, we recommend that cybersecurity training be a mandatory component in all future senior project offerings.

Many of the curriculum changes were possible thanks to the support from DAC. Their letters and constant communication describing their needs helped shape the new curriculum.

The straightforward program changes provided all the students in a cohort with awareness of cybersecurity concepts. Such changes can be implemented at any institution without needing an external sponsor. However, adding specialized cybersecurity projects benefits us from having external customers. We believe this type of collaboration can be replicated in other institutions with different levels of involvement from the DoD agencies. Some of the changes are generic and only require focusing on the capstone design and some existing courses in the curriculum. Some projects might require external sponsors, but cybersecurity is in high demand, and many private organizations could be interested in sponsoring specific projects.

ACKNOWLEDGMENT

The research was sponsored by the Army DEVCOM Analysis Center and was accomplished under Grant Number W911QX20D0002. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied,

VI. References

[1] [1] S. Furnell, H. Heyburn, A. Whitehead, and J. N. Shah, "Understanding the full cost of cyber security breaches," Computer fraud & security, vol. 2020, no. 12, pp. 6-12, 2020, doi: 10.1016/S1361-3723(20)30127-5.

[2] [2] D. Woods and P. Hirsch. "Cracking the code on cyber insurance." NPR. https://www.npr.org/transcripts/1093656544 (accessed 04/22/2022, 2022).

[3] [3] Chang. "The role cyberattacks and information campaigns have played in the war in Ukraine." NPR. https://www.npr.org/transcripts/1089774585 (accessed 04/22/2022, 2022).

[4] [4] J. Blazic, "Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?" Education and information technologies, vol. 27, no. 3, pp. 3011-3036, 2021, doi: 10.1007/s10639-021-10704-y.

[5] [5] K. Daimi and G. Francia, III, Innovations in Cybersecurity Education, 1st 2020. ed. Cham, Switzerland: Springer, 2020.

[6] [6] Steven Furnell and M. Bishop. "Addressing cyber security skills: the spectrum, not the silo." https://www.magonlinelibrary.com/doi/abs/10.1016/S1361-3723%2820%2930017-8 (accessed 04/22/2022, 2022).

[7] [7] S. Furnell, "The cybersecurity workforce and skills," Computers & Security, vol. 100, p. 102080, 01/01/2021, doi: https://doi.org/10.1016/j.cose.2020.102080.

[8] [8] J. R. S. Blair, A. O. Hall, and E. Sobiesk, "Educating future multidisciplinary cybersecurity teams," Computer, vol. 52, no. 3, pp. 58-66, 2019, doi: 10.1109/MC.2018.2884190.

[9] [9] W. Newhouse, S. Keith, B. Scribner, and G. Witte, "National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework," NIST special publication, vol. 800, no. 2017, p. 181, 2017.

[10] [10] Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Association for Computing Machinery Joint Task Force on Cybersecurity Education, 2018.

[11] [11] N. Lim, A. Haddad, D. M. Butler, and K. Giglio, "First steps toward improving DoD STEM workforce diversity: response to the 2012 Department of Defense STEM diversity summit," Rand National Defense Research Inst Santa Monica CA, 2013.

[12] [12] "DoD STEM." Department of Defense. https://dodstem.us/ (accessed 04/22/2022, 2022).

[13] [13] "ARMY DEVCOM Analysis Center" https://www.army.mil/DAC (accessed 08/13/2024).

[14] [14] V. Gonzalez, O. Perez, and R. Romero, "Collaboration program to disseminate cybersecurity in the ECE curriculum," in 2022 IEEE Frontiers in Education Conference, FIE 2022, October 8, 2022 - October 11, 2022, Uppsala, Sweden, 2022, vol. 2022-October: Institute of Electrical and Electronics Engineers Inc., in Proceedings - Frontiers in Education Conference, FIE, doi: 10.1109/FIE56618.2022.9962613. [Online]. Available: http://dx.doi.org/10.1109/FIE56618.2022.9962613

[15] [15] Gonzalez, V., O. Perez and R. Romero (2023). Cybersecurity in ECE Curriculum, an Expanded Collaboration Program to Disseminate Real Security Experiences in Cyber-Physical Systems. 53rd IEEE ASEE Frontiers in Education International Conference, FIE 2023, October 18, 2023 - October 21, 2023, College Station, TX, United States, Institute of Electrical and Electronics Engineers Inc.

[16] W. S. University. "Cybersecurity education varies widely in US." www.sciencedaily.com/releases/2024/05/240506194522.htm (accessed 05/06/2024, 2024).

[17] J. Dawson and R. Thomson, "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance," Frontiers in Psychology, vol. 9, pp. 744-744, 2018, doi: 10.3389/fpsyg.2018.00744.