2024 Summer Team Impact Project: Addressing the International Artificial Intelligence Cyber Question with the United States Cyber Command

Overview of the Project

The United States Cyber Command (US CYBERCOM)'s mission is to "Direct, Synchronize, and Coordinate Cyberspace Planning and Operations - to Defend and Advance National Interests - in Collaboration with Domestic and International Partners." Through working with a US CYBERCOM point of contact (POC), the cyber undergraduate research team (CURT) of eight will be split into two groups to focus on a research question identified by the US CYBERCOM POC: "What countries are leading the development of Artificial Intelligence (AI), particularly the use of AI in malware development and infrastructure deployment for networks security?" From this research question, the two CURTs will be tasked with two separate efforts from the United States of America's (USA) point of view: one focusing on countries who may be considered adversaries and the other focusing on countries who are considered allied partners. The overall goal will be to publish two papers in the Information Systems Audit and Control Association (ISACA) Journal – a premier cyber security and audit practitioner journal.

Timeline

The following schedule lays out the activities for the 10-week program.

Week #	Content & Activities
Week 1	***Introduction to the Research Problem & Welcome Breakfast or Lunch*** US CYBERCOM Point of Contact & Team Building Activities
Week 2	***Initial Research Efforts*** Literature Reviews & Explaining the Question's Challenge or Opportunity
Week 3	
Week 4	***Outlining the Research Paper*** Developing the Solution's Method/Framework/Theory
Week 5	
Week 6	***Drafting the Research Paper*** Detailing the Recommended Solution through a Use Case
Week 7	
Week 8	***Finalizing the Research Paper for Submission to Cyber Practitioner Journal*** Review, Edit, Revise, & Submit!
Week 9	
Week 10	***Final Ice Cream Social & Networking with the Cyber Professionals*** Reflect, Network, & Adjourn

The first week will focus on introducing the CURT to the research problem, the US CYBERCOM POC, and the faculty members. During this week, there will be an in-person meet-and-greet with breakfast or lunch (depending on the time) where the faculty members and US CYBERCOM POC introduce the complex international AI-cyber-focused research problem to the students. This is also when the CURT will be divided into two groups to tackle the research problem and participate in a team building activity.

During weeks two to nine, the CURT will meet with the US CYBERCOM POC and the faculty members to go over progress: What was done since the last meeting, what will be done until the next meeting, and any challenges / questions the team has. These weekly meetings keep

the efforts agile by allowing consistent progress reporting from the project teams, and consistent client feedback to address requirement changes and misunderstandings. Weeks two and three will have the CURTs focus on understanding the research problem and determining the challenges or opportunities through literature review activities. Weeks four and five will then challenge the student teams to develop innovative solutions (methods, frameworks, and or theories) that can address or enhance the research problem's challenges or opportunities. Weeks six and seven will further challenge the students by having them focus on applying their proposed solution through developing a use case to demonstrate its potential impact to the research problem. Finally, weeks eight and nine will focus on editing and revising efforts for submission to the ISACA, the Information Systems Security Association (ISSA) International, or other cyber security practitioner journals.

The summer program will end in week ten with an Ice-Cream Social and Networking event where the CURT participants will get the opportunity to meet other cyber professionals and leaders to discuss their summer team impact projects. The goal here is to share their work with the other student teams, network with industry professionals and leaders in the cyber security field, reflect on their work and its impact to the research problem, and have some fun after a long summer.

Additionally, students participating in this cyber-focused research program will have access to the faculty member's career seminar recorded videos; as well as three cyber security recorded guest lectures presented by industry leaders from AT&T (Cyber Security in the 5G environment), the Institute for Defense Analyses (Cyber Security Operations), and Parsons Corporation (Critical Infrastructure Cyber Security). These additional enrichment activities for the student participants will help them broaden their cyber security knowledge, as well as broaden their interest in the different the different cyber security career paths available – which will hopefully help positively impact the cyber security workforce deficit.

Undergraduate Participation

The eight CURT participants will be divided into two groups to answer the research problem of "What countries are leading the development of AI, particularly the use of AI in malware development and infrastructure deployment for networks security?" The first group will focus on countries who may be considered adversaries to the USA, while the second group will focus on countries who are the USA's allied partners. Through weekly research activities, weekly meetings with the faculty members for guidance, and weekly meetings with the US CYBERCOM POC for feedback – the CURTs will develop a specific challenge or opportunity based on the research question, develop a solution to the challenge or path forward for the opportunity, and detail how the application of the solution can positively impact the challenge or opportunity derived from the research question.

Through the 2024 Summer Team Impact Project, we would like the CURT participants to learn and take away multiple things working with us including:

- Enhancing their research methods and skills

- Have a deeper understanding of AI, cyber security, and the intersection of the two fields of study
- Understand the importance of international affairs from a USA perspective: adversaries versus allied partners and the relationship needed for each of the two categories
- The importance of both the AI and cyber security fields, and why going into these fields are rewarding, important to the workforce and nation, as well as dangerous

Because the topics of cyber security, international affairs, and US CYBERCOM are high-interest topics in the northern Virginia area, the faculty members expect that there will be high demand and high impact for this particular Summer Team Impact Project. This is especially true for students in the School of Business, College of Engineering and Computing, as well as the Schar School of Policy and Government. This has been experienced with similar efforts such as the Commonwealth Cyber Initiative (CCI) where the faculty has received well over 100 applications for a position.

Involvement of Partners

The CURTs will engage with library resources through the university by receiving a short workshop training from Business School liaison about how to use the library resources to write their journal paper for submission to the ISACA Journal. The CURTs and industry participants will also get an opportunity to engage with our research centers on campus by taking a tour of the Arlington Pilot Space as well as the Center of Center of Excellence in Government Cybersecurity Risk Management and Resilience, and learn about the 5G network security and AI intersection from the research ongoing there.

The faculty members are working with US CYBERCOM to frame and answer this research question. The faculty members have worked with US CYBERCOM before on an experiential learning project which has resulted in a student-faculty accepted publication titled *"Enhancing Collaboration to Improve Cybersecurity Practices"* to be published in the January 2024 edition of the ISACA Journal. ***The National Security Innovation Network (NSIN) within the US Department of Defense – who has provided the letter of support for this Summer Team Impact Project with its Mission Partner [US CYBERCOM] – will also be engaging with the CURTs*** to provide support, encouragement, and media highlights on the effort as they have prior with similar projects including: Department of Defense Cyber Crime Center's Vulnerability Disclosure Program Partners With George Mason University and George Mason University Students Improve VDP Onboarding Through Paid Opportunity.