Collaborative Research SaTC-EDU: EAGER –
Creating Concept and Curriculum Assessment Tools for Cybersecurity

To help universities better prepare the substantial number of cybersecurity professionals needed in America, this project will provide infrastructure for a rigorous evidence-based improvement of cybersecurity education by developing the first *Cybersecurity Assessment Tools (CATs)* targeted at measuring the quality of instruction. The first CAT will be a *Cybersecurity Concept Inventory (CCI)* that measures how well students understand basic concepts in cybersecurity after a first course in the field. The second CAT will be a *Cybersecurity Curriculum Assessment (CCA)* that measures how well curricula prepared students graduating from college on fundamentals needed for careers in cybersecurity. Each CAT will be a multiple-choice test with approximately thirty questions. Finally, the project will perform psychometric evaluations of these two CATs to demonstrate their quality and value.

The first essential step is to build consensus among respected cybersecurity experts and educators about the core concepts and skills that should be assessed in the CATs. This consensus will be built through a Delphi method and structured dialogues at relevant conferences. Modeled after the development of concept inventories in many other areas (e.g., physics, digital logic), the CCI will be based on a minimal common subset of fundamental cybersecurity concepts that initial courses in any cybersecurity domain should cover. The CCA will measure broadly-based skills that are fundamental for future success, such as how to develop an adversarial model for a cybersecurity challenge, and how to design and analyze a security system for solving this challenge in the context of the model.

Despite a growing and significant demand for cybersecurity professionals, there is a lack of rigorous evidence-based methods to advise educators of how best to engage, inform, educate, nurture, and retain cybersecurity students and of how best to structure cybersecurity curricula to prepare new professionals for careers in this field. The CCI will permit comparisons among the effectiveness of different instructional methods in reinforcing the core concepts of the field, where instructional methods focus on how material is taught (e.g., lab-based, case-studies, collaborative, competitions, gaming.) The CCA will permit comparisons among the knowledge and skills gained from different curricula, where curriculum focuses on the overarching skill sets and abilities that students possess upon graduation.

Intellectual Merit. The value of high-quality assessment tools is demonstrated by the impact of the *Force Concept Inventory* on physics education, which helped motivate the adoption of active learning pedagogies in physics. The project team provides a diversity of expertise to tackle this project. With several experts in cybersecurity knowledge and two education researchers, the team has the skill set necessary to articulate the core content of each CAT, uncover common student misconceptions, devise questions, and evaluate the quality of the CATs that are developed.

Broader Impacts. This project will help our country meet the huge demand for cybersecurity professionals by creating tools that identify effective approaches to teaching cybersecurity. The CCI will measure college student understanding of fundamental cybersecurity concepts. The CCA will identify college curricula that are effective at preparing students for cybersecurity careers. These CATs will provide useful feedback to educators in improving cybersecurity teaching and learning. In addition, the project team will promote collaboration among CAEs, beginning with the three CAEs of the core team, and extending to all CAEs who will be invited to participate in the Delphi method.[1]

[1] National Center of Academic Excellence in Information Assurance Research and Education (CAE-R, CAE-IAE).