

# EAGER: SaTC-EDU: Learning Platform and Education Curriculum for Artificial Intelligence-Driven Socially-Relevant Cybersecurity



## Challenge:

- Few educational materials have been designed to engage students by integrating AI and socially-relevant cybersecurity through an interdisciplinary approach.

## Solution:

- Develop AI-driven socially-relevant cybersecurity curricular modules and hands-on labs to engage students with diverse backgrounds

### AI for Text-based Cyberbully Detection

This lab teaches students how AI models can be used to distinguish between a cyberbully and non-cyberbully text-based content. Students will learn data preprocessing, training, and the evaluation metrics of AI-based classifiers.

### AI for Multimodal (Image and Text) Cyberbully Detection

Cyberbullying can occur in images, and it can also occur in both image and text. Students will extract visual features from images and combine these features with textual features to detect cyberbullying in this lab.

### Adversarial Attacks in Cyberbully Detection

AI models are vulnerable to adversarial attacks. In this lab, students will use different algorithms to generate images that can fool models trained to detect cyberbullying, causing the model to produce incorrect output.

## Scientific Impact:

- Advance the knowledge of AI-cybersecurity education by creating curriculum and hands-on labs based on cutting edge research on AI-driven cyberharassment detection, related attacks against the AI models, and social issues in AI models for cyberharassment detection

## Broader Impact and Broader Participation:

- Strengthen the cybersecurity and AI research at CU, NC A&T, and UB.
- Develop course materials for CS students and non-CS students
- The proposed curriculum materials in this project will be taught in GenCyber summer camp