# Rock Paper Scissors:
# Towards Infusing Adversarial Thinking
# Into Computing Education

Christian Servin[1], Nadia V. Karichev[1], and Alejandro Solano[2]
[1]El Paso Community College, cservin1@epcc.edu/nmerzlya@epcc.edu
[2]Department of Computer Science,
University of Texas at El Paso, axsolano@miners.utep.edu

## Abstract

Adversarial Thinking (AT) is recognized as a key cross-cutting concept in cybersecurity education, as highlighted by the *Cybersecurity Curricula 2017 (CSEC 2017)* guidelines and recommendations. Similarly, Computational Thinking (CT) is a critical problem-solving approach that facilitates expressing solutions in ways both humans and computers can execute. It underpins complex problem-solving across computer science and other fields by offering a structured, logical framework.

As cyber threats grow in sophistication, integrating secure coding practices into computer science curricula alone is no longer enough. It is essential to instill a sense of responsibility in developing secure software—beyond functional code—to anticipate and mitigate vulnerabilities. Fostering an adversarial mindset, is crucial for encouraging the next generation of programmers to proactively identify and counter potential security threats in their development work.

Integrating AT into computer science fundamentals is expected to boost software resilience, reducing vulnerability to attacks and strengthening digital infrastructure. The authors view adversarial thinking as the "new computational thinking," a vital mindset for all computer science students. As computing becomes ubiquitous and technologies evolve rapidly, programming must go beyond functionality to include security and risk awareness. Students trained in AT will be better prepared to address the diverse demands of cybersecurity across industries.

The authors' research further shows that students who adopt an adversarial mindset often develop a stronger sense of belonging and purpose within the field. This is fostered by AT's focus on real-world applications and the mentality that programming can, and should, include considerations for risk mitigation. AT becomes a means through which students see the societal impact of their technical skills, making the work more meaningful and enhancing student engagement. To support this transformative approach, the authors are actively developing best practices to incorporate Adversarial Thinking into computer science education in various ways. This includes curriculum integration—where AT concepts are woven into foundational computer science courses, rather than as stand-alone topics—peer-led team learning, which empowers students to collaborate and learn from each other's approaches to problem-solving, and experiential learning activities, such as simulations and hands-on projects that allow students to apply adversarial thinking to real-world scenarios.

This work presents the ongoing project titled *Developing Computational Adversarial Thinking: Bridging Technical Skills Training and Academic Coursework*, which explores methods to instill AT principles in students. By bridging technical skills training with academic coursework, this project offers students a comprehensive approach that emphasizes both technical proficiency and the critical mindset needed for cybersecurity. Additionally, the authors illustrate how adversarial thinking can be applied in fundamental computer science areas, using practical examples that highlight AT's core principles.