Teaching Adversarial Thinking for Cybersecurity

Seth Hamman, PhD | CISSP | GPEN | CEH-M | GLEG

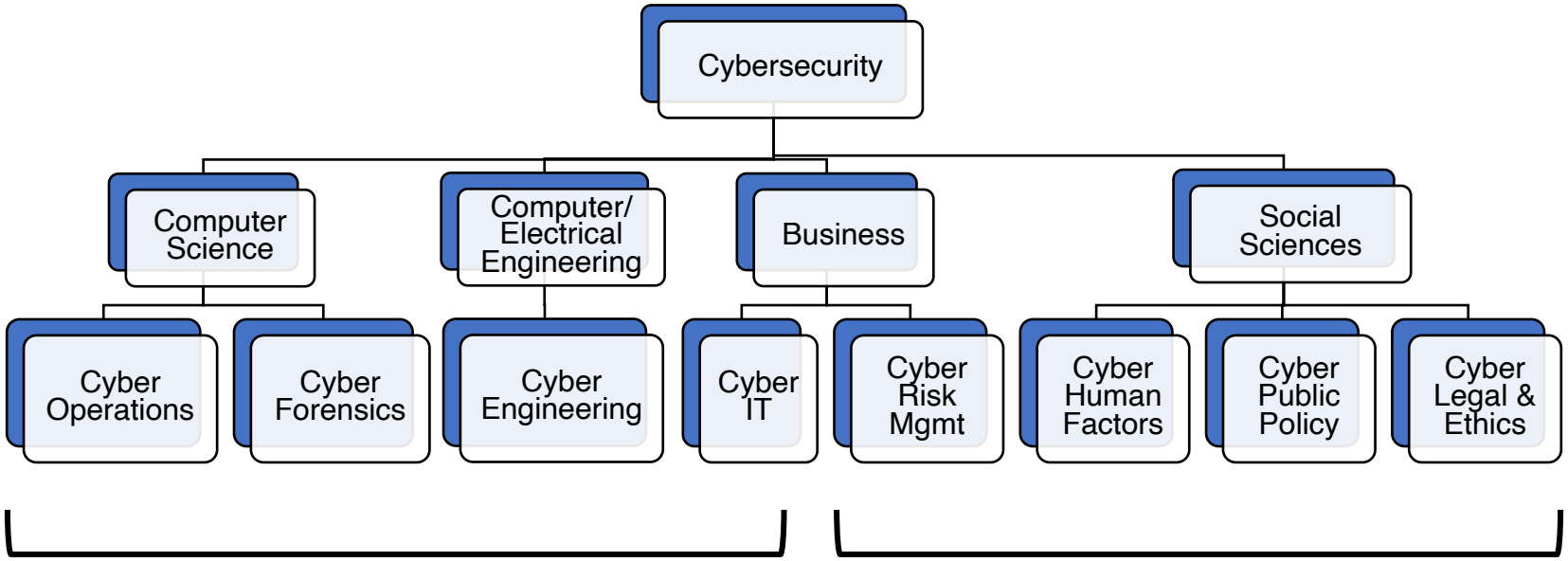
Director & Assoc Professor, Cedarville University

CAE Forum

September 7, 2022

Cybersecurity is IMPORTANT!

Cybersecurity is INCLUSIVE!



CENTER FOR THE ADVANCEMENT OF CYBERSECURITY
PR 22:29
CEDARVILLE UNIVERSITY

CEDARVILLE UNIVERSITY

Cybersecurity is INTERESTING!

A new academic discipline is coming of age in our time, and we are right in the thick of it!

This lesson focuses on what makes cybersecurity unique and interesting.

CEDARVILLE UNIVERSITY

What is the essence of Cybersecurity?

CEDARVILLE UNIVERSITY

Cybersecurity is…

"Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure."

— US Department of Homeland Security

CEDARVILLE UNIVERSITY

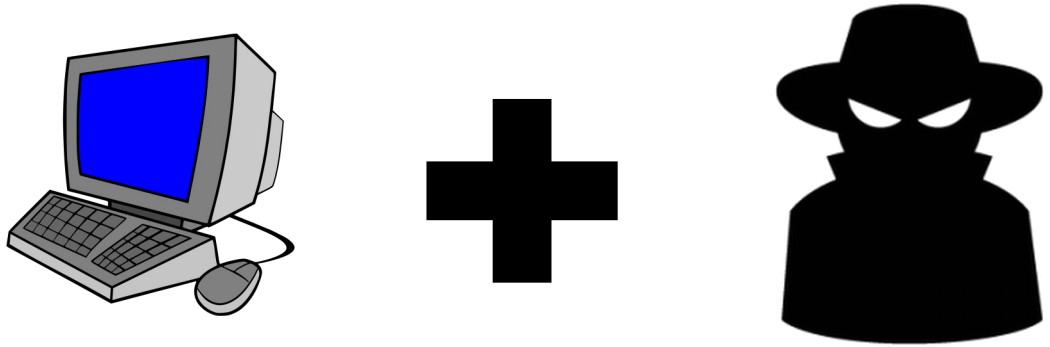
Cybersecurity is...

"Strategy, poli… regarding th…
operations in cy… ompas… of threat
reduction, vulnera… …ional
engagement, incide… …overy policies and
activities, including co… …ons, information
assurance, law enforce… …, and intelligence
missions as they re… …f the global
information a…

— US D… …and Security

CEDARVILLE UNIVERSITY

The Essence of Cybersecurity:

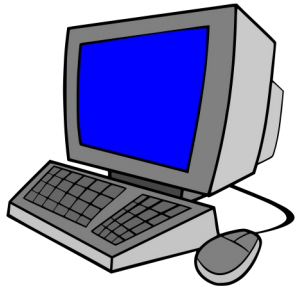


CEDARVILLE UNIVERSITY

Take Away the Computer…

- Criminal Justice
- Criminology
- Public Policy
- Military Studies
- etc.

Take Away the Attacker…

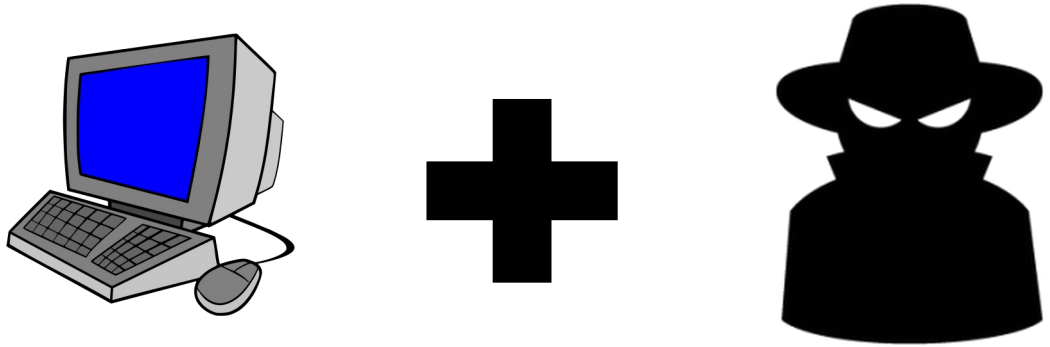


- Computer Science
- Computer Engineering
- Software Engineering
- Information Technology
- etc.

CENTER FOR THE ADVANCEMENT OF CYBERSECURITY
PR 22:29
CEDARVILLE UNIVERSITY

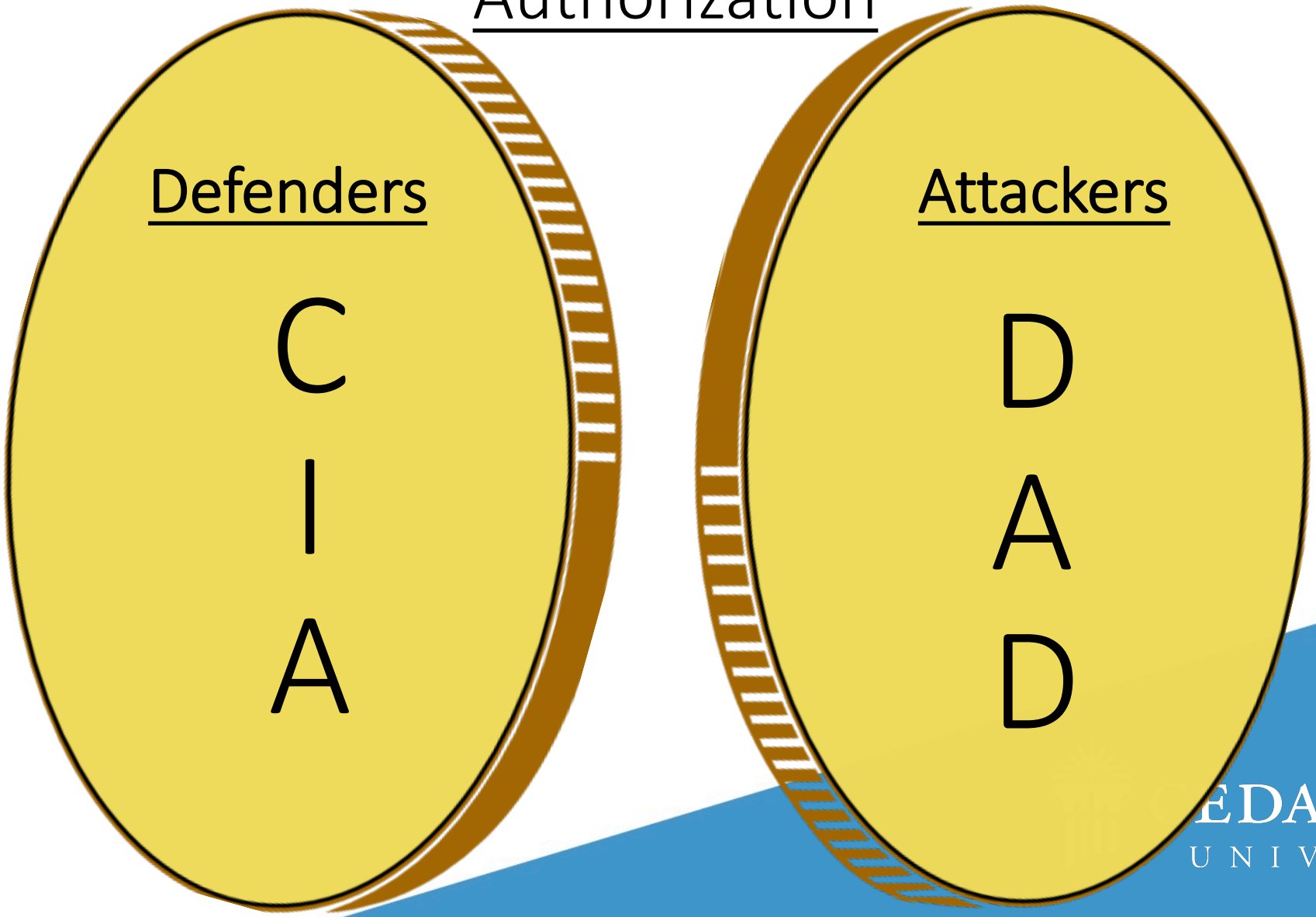
CEDARVILLE UNIVERSITY

The Essence of Cybersecurity:



CEDARVILLE UNIVERSITY

It all Boils Down to Authorization



CEDARVILLE UNIVERSITY

Bottom Line

Cybersecurity is only necessary because of the existence of people who deliberately attack computer systems and networks.

We call these people **HACKERS**.

CEDARVILLE UNIVERSITY

What a Difference Hackers Make!

A world WITHOUT hackers...	A world WITH hackers...
Accidents and hardware failures cause you to lose your data	Ransomware attacks take your data captive!
Your computer is slow and buggy	Attackers use trojan horse malware to hide in your computer

CEDARVILLE UNIVERSITY

The Hallmark of the Discipline of Cybersecurity

Discipline	Approach	Fundament Mindset
Mathematics	Constructing Proofs	Logical Thinking
Computer Science	Writing Programs	Algorithmic Thinking
Cybersecurity	Security Practices	Adversarial Thinking

ILLE
UNIVERSITY

Adversarial Thinking

Do you see a person skilled in his work? He will stand in the presence of kings.

(Ancient Jewish Proverb)

But what exactly does **adversarial thinking** mean?

In order to be sure we are imparting it to our students, we have to be able to define it.

It comes down to the **definition of thinking**...

CEDARVILLE UNIVERSITY

Sternberg's Triarchic Theory

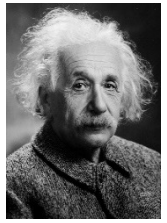
Area	Description	Popular Conception
Analytical	Mathematical ability and logical reasoning	Book smarts
Creative	The ability to make unique connections and original insights	Creative ability
Practical	The ability to plan, strategize, and accomplish goals	Street smarts

CEDARVILLE UNIVERSITY

Thinking Like a Hacker

Q2: What enables him to identify innovative ways to break software and subvert security measures?

Creative



Analytical

Practical

Q1: How do his book smarts contribute to his hacking prowess?

Q3: How does he plan attacks and overcome obstacles so he can succeed without getting caught?

CEDARVILLE UNIVERSITY

Adversarial Thinking Defined

Definition:

Adversarial thinking is the ability to embody the ***technological capabilities****, the* ***unconventional perspectives****, and the* ***strategic reasoning*** *of hackers.*

To the extent a person can do this, that person will be able to:

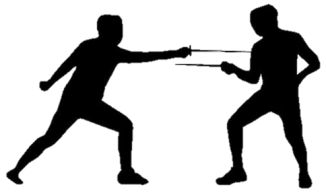
- Compete with hackers on a level playing field (**analytical**)
- Find and fix vulnerabilities before hackers have an opportunity to exploit them (**creative**)
- Anticipate future attacks, thwart attacks in progress (**practical**)

CEDARVILLE UNIVERSITY

A solid cybersecurity education must equip you for...

The Technological Battle of

Might



The Creative Battle of

Skill

The Strategic Battle of

Wits

CENTER FOR THE ADVANCEMENT OF CYBERSECURITY
PR 22:29
CEDARVILLE UNIVERSITY

CEDARVILLE UNIVERSITY

Adversarial Thinking Learning Outcomes

Dimension	Learning Outcome	Example	All About
Technological Capabilities	Understand computer technology at a deep level (e.g., networking protocols, programming languages, and operating systems)	Command-line Kung Fu	Leveling the playing field
Unconventional Perspectives	Identify unconventional uses of software and protocols that could be exploited as attack vectors by hackers	XSS Attacks	Employing the “hacker mindset”
Strategic Reasoning	Anticipate the strategic actions of hackers, including where, when, and how they might attack, and their tactics for evading detection	Trojan Horse Malware	Anticipating and thwarting attacks

Strategic Reasoning

Of the three dimensions of adversarial thinking, the one most likely to be overlooked is the strategic dimension

Game theory is the study of strategic reasoning

CEDARVILLE UNIVERSITY

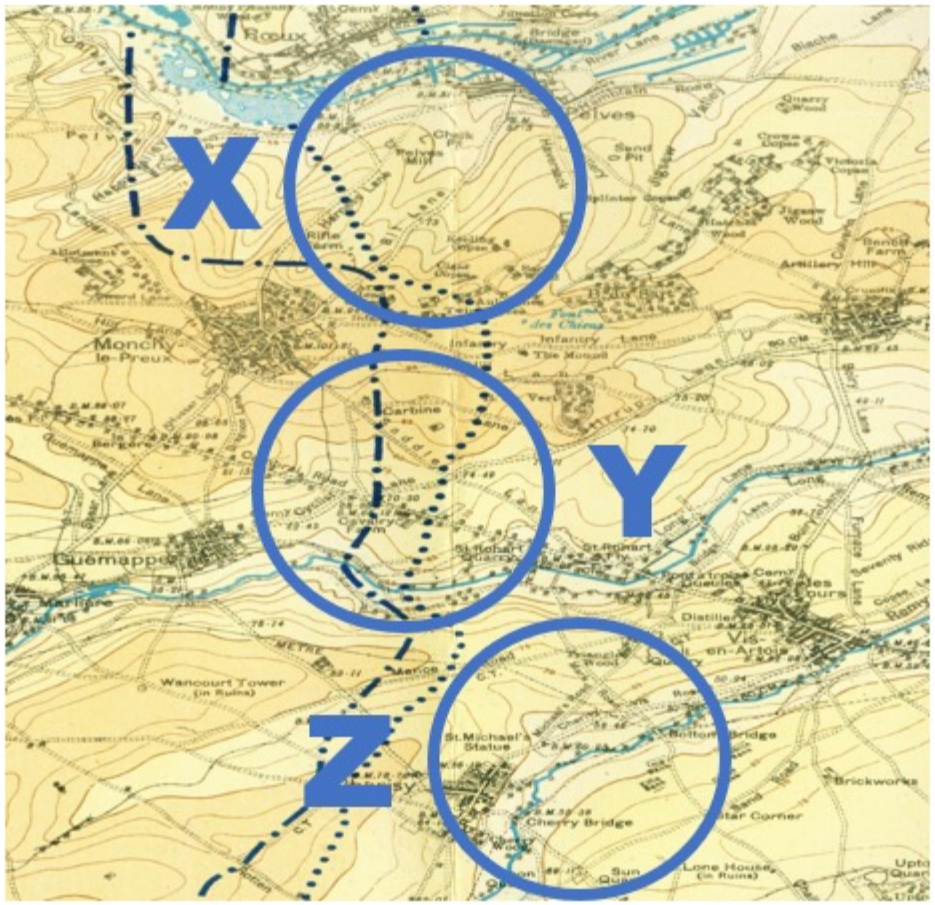
Thinking About What Your Adversary is Thinking About

CENTER FOR THE ADVANCEMENT OF CYBERSECURITY
PR 22:29
CEDARVILLE UNIVERSITY

CEDARVILLE UNIVERSITY

The Colonel Blotto Game

Colonel Alto

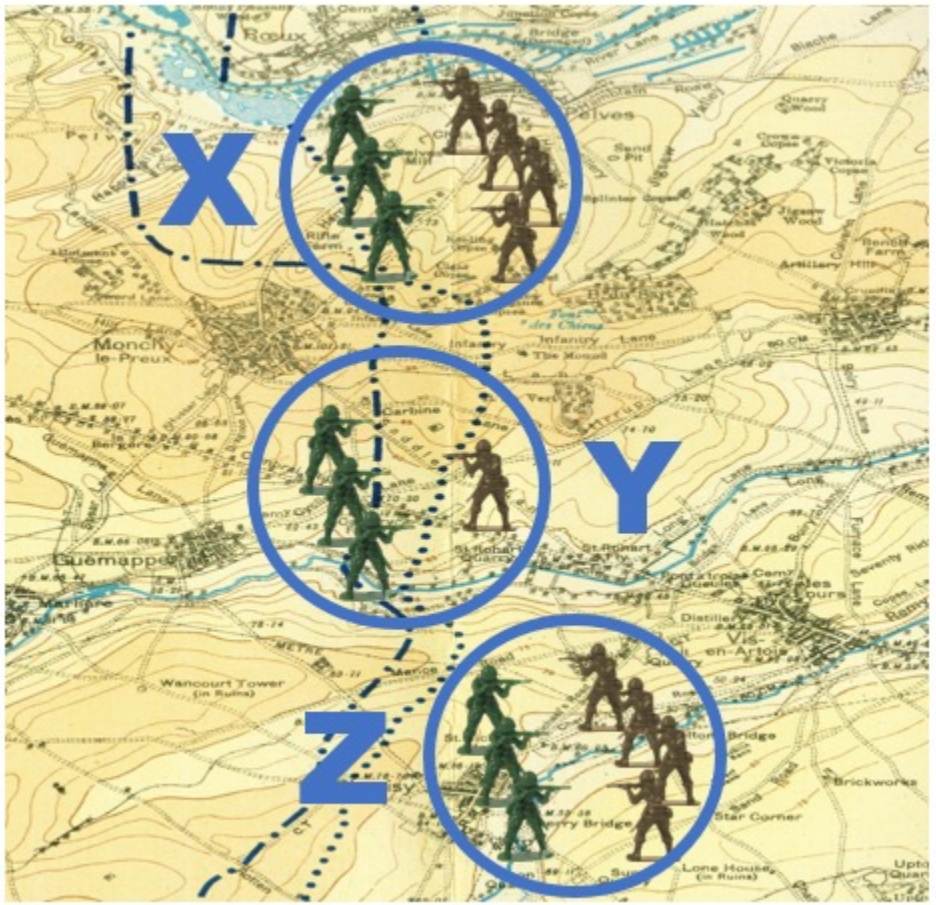


Colonel Blotto

CEDARVILLE UNIVERSITY

The Colonel Blotto Game

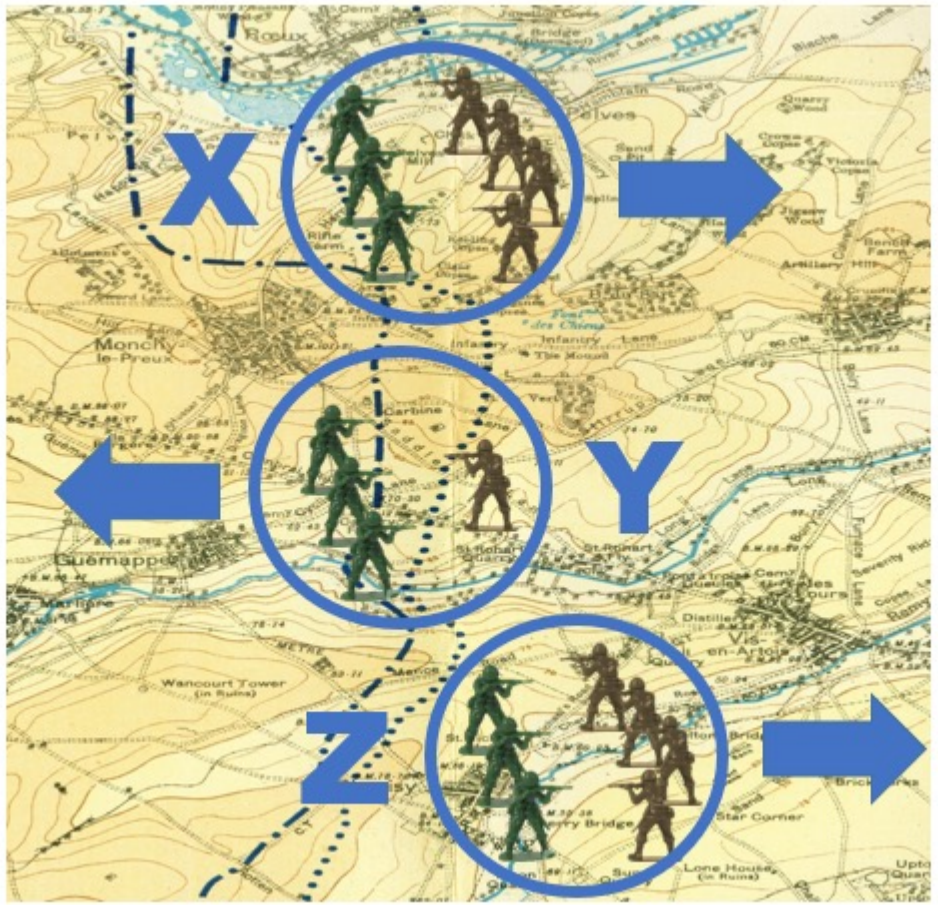
Colonel Alto



Colonel Blotto

The Colonel Blotto Game

Colonel Alto



Colonel Blotto

CEDARVILLE UNIVERSITY

Exercise: DDoS Attack

To play, visit https://cyberops.cedarville.edu/cb

Website	A	B	C	D	E	F
Value	**1**	**1**	**1**	**1**	**1**	**1**
Protection (must sum to 120)	?	?	?	?	?	?

CEDARVILLE UNIVERSITY

Wait, what does game theory have to do with cybersecurity again?

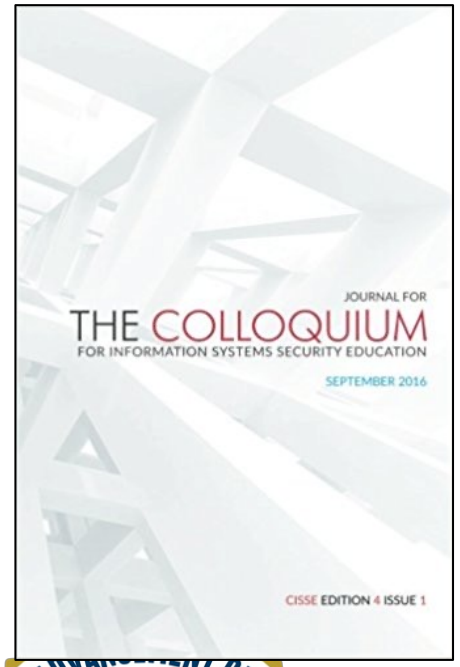
CEDARVILLE UNIVERSITY

Conclusion

- Cybersecurity, at its essence, is an adversarial conflict – without adversaries, there is no such thing as cybersecurity
- Therefore, **adversarial thinking is central to cybersecurity**
- Learning about game theory for cybersecurity makes sense because **adversarial thinking requires strategic reasoning**, and game theory is the study of strategic reasoning
- The major takeaway from game theory is that **one must consider strategic situations primarily from the perspective of the adversary**, not primarily from one's own perspective
- The overarching goal of this lesson is two-fold:
  - To make indelible the association between **strategic reasoning and cybersecurity**
  - To **produce enduing strategic-mindedness** in cybersecurity students

CEDARVILLE UNIVERSITY

Further Reading



Teaching Adversarial Thinking for Cybersecurity

Teaching Game Theory to Improve Adversarial Thinking in Cybersecurity Students

CENTER FOR THE ADVANCEMENT OF CYBERSECURITY
PR 22:29
CEDARVILLE UNIVERSITY

CEDARVILLE UNIVERSITY

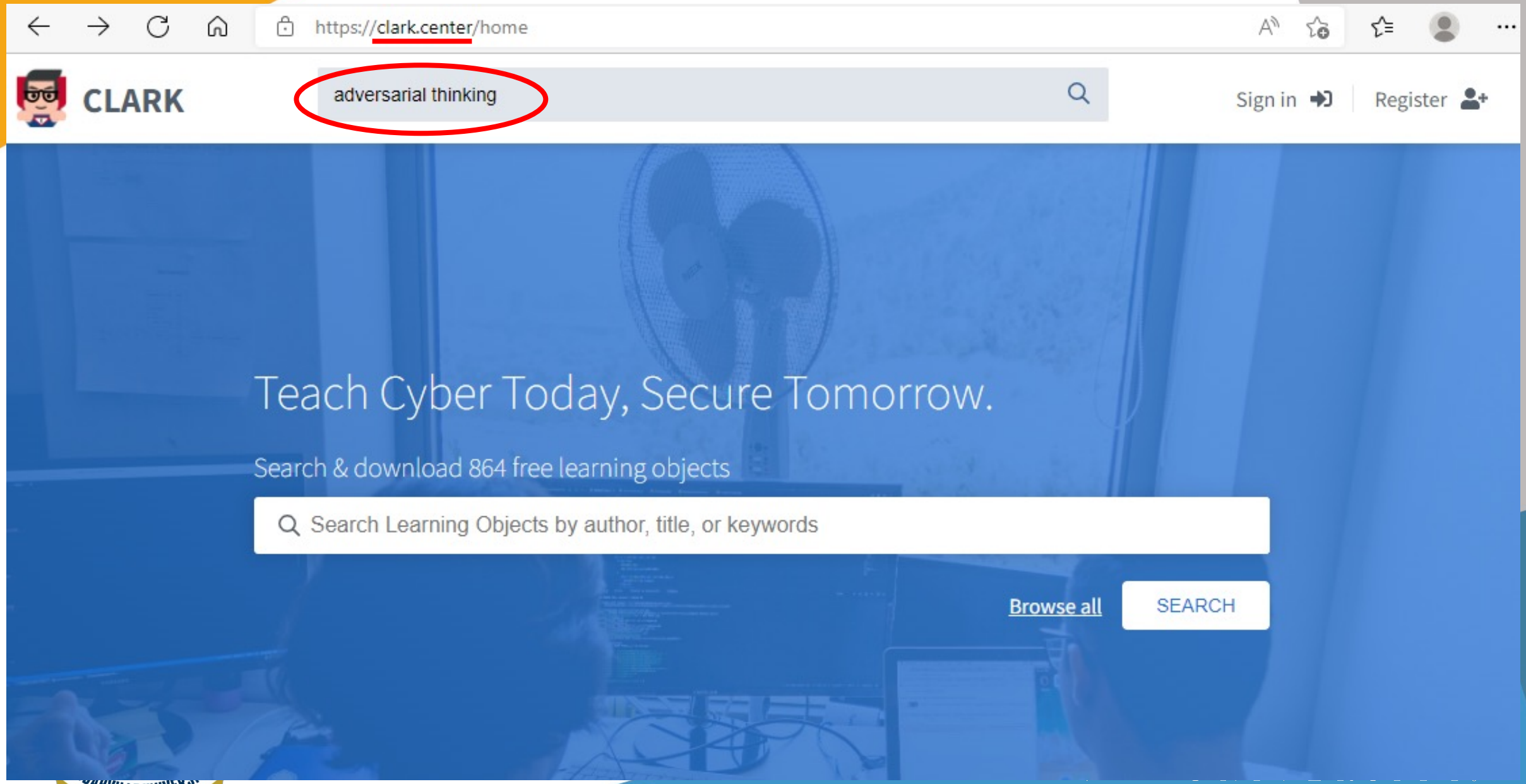
CHAPTER

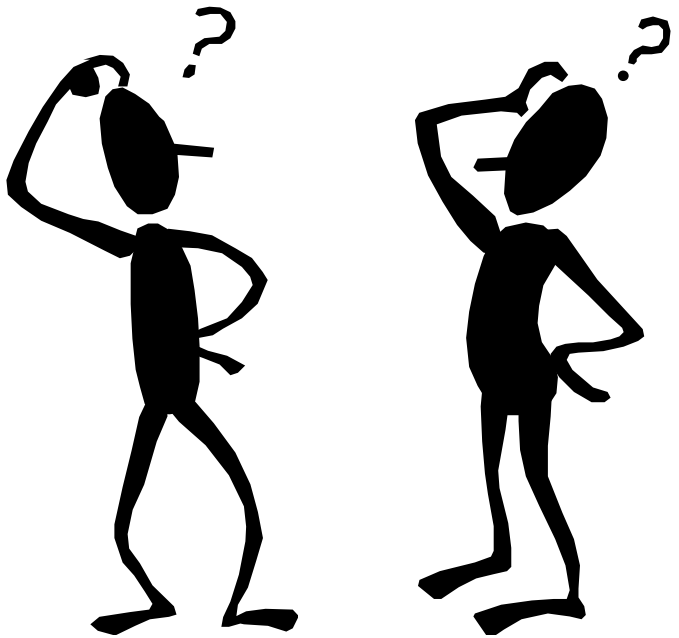
17 APPLYING BEHAVIORAL GAME THEORY TO CYBER-PHYSICAL SYSTEMS PROTECTION PLANNING

S.T. Hamman*,†, K.M. Hopkinson*, L.A. McCarty†

The Air Force Institute of Technology, WPAFB, OH, United States Cedarville University, Cedarville, OH, United States†*

RVILLE
ERSITY.


https://clark.center/home
CLARK
adversarial thinking
Sign in
Register
Teach Cyber Today, Secure Tomorrow.
Search & download 864 free learning objects
Search Learning Objects by author, title, or keywords
Browse all
SEARCH



CEDARVILLE
UNIVERSITY

Dr. Seth Hamman
Director, Cybersecurity
Cedarville University
Cedarville, OH
shamman@cedarville.edu
https://www.linkedin.com/in/sethhamman-cedarville/