The Centrality of Adversarial Thinking for Cybersecurity

2018 CAE IN CYBERSECURITY COMMUNITY Symposium

Seth Hamman, Ph.D.
Director, Center for the Advancement of Cybersecurity
Associate Professor of Computer Science
Cedarville University

CEDARVILLE UNIVERSITY

Do you see a man skilled in his work?
He will stand before kings; He will not
stand before obscure men.

CEDARVILLE
UNIVERSITY

This talk is about how to educate that level of cybersecurity professional.

(Btw, we have names for superbly skilled cyber adversaries like **Elite Hacker** and **Advanced Persistent Threat**...

but what do we call cybersecurity superstars?)

CEDARVILLE UNIVERSITY

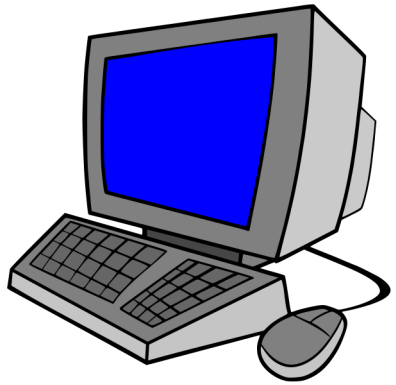
Cybersecurity is all About...

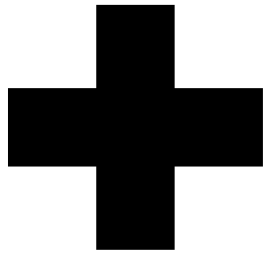
"*Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network 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.*"

— Department of Homeland Security

CEDARVILLE UNIVERSITY

Simpler Explanation





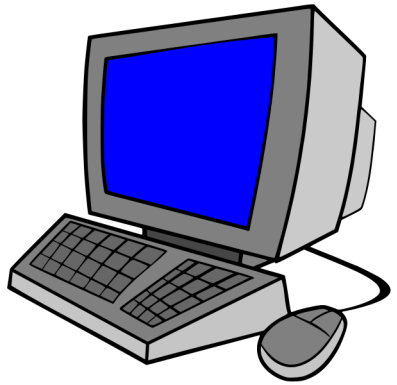
CEDARVILLE UNIVERSITY

Take Away the Computer...

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

CEDARVILLE UNIVERSITY

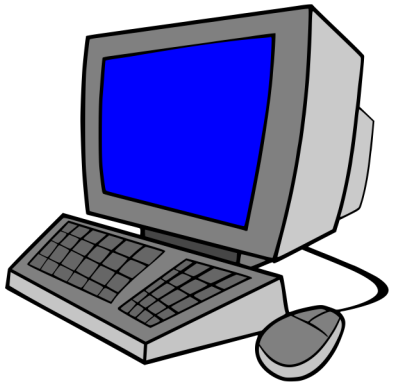
Take Away the Bad Guy...

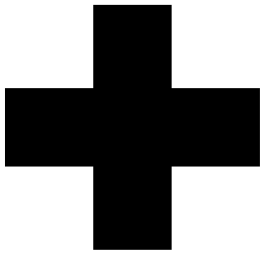


- Computer Science
- Computer Engineering
- Software Engineering
- Information Technology
- etc.

CEDARVILLE UNIVERSITY

Cybersecurity





CEDARVILLE UNIVERSITY

Bottom Line

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

We call these people **hackers**.

CEDARVILLE UNIVERSITY

What a Difference Hackers Make

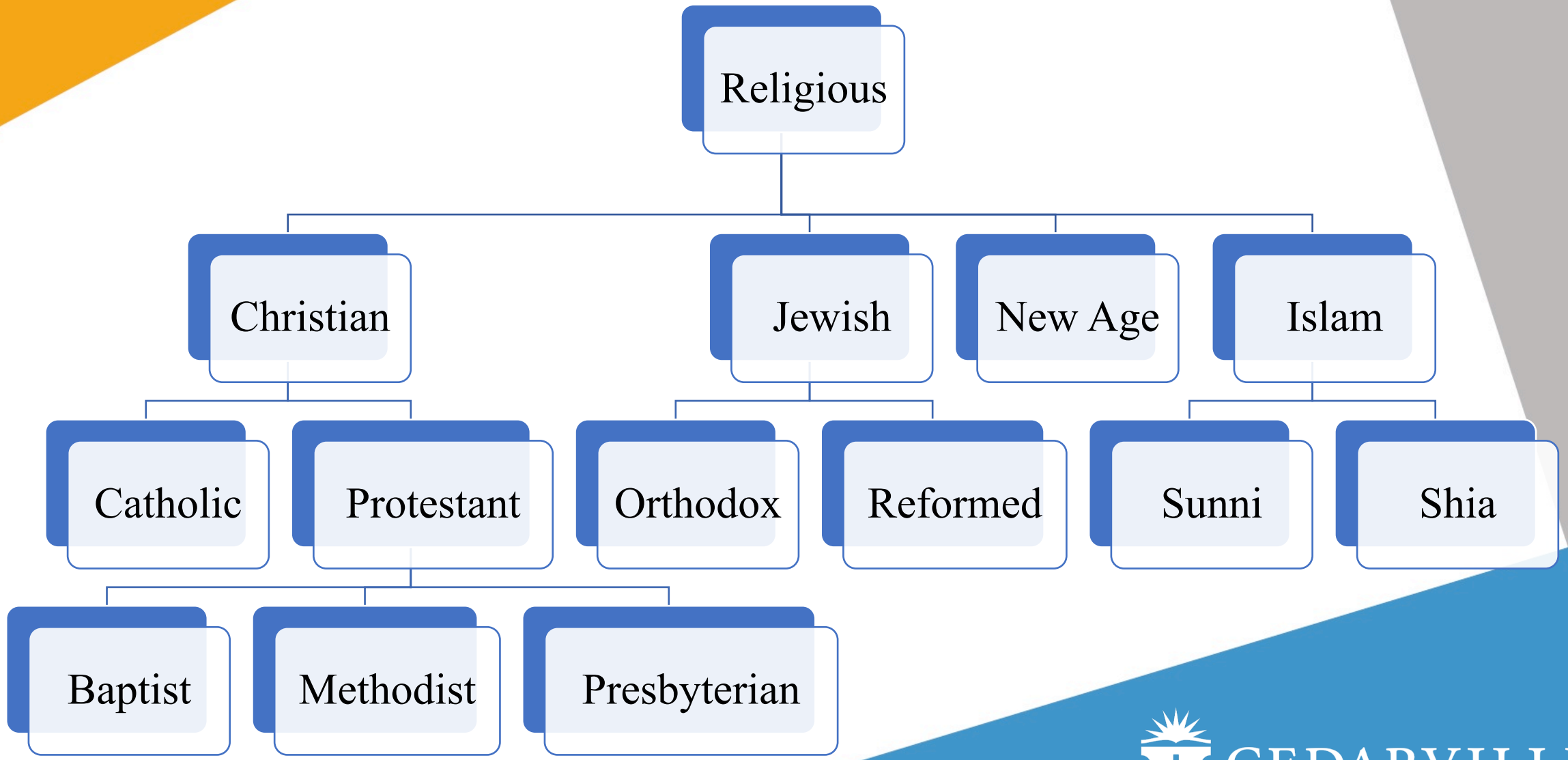
In a world without hackers...	now adding in hackers...
Random accidents cause data loss	Deliberate attacks encrypt data and backups
Software bugs frustrate users	Malicious software owns users' computers
OSs crash and work is lost	OS rootkits report everything is fine
New hires trained in phone etiquette	New hires warned about social engineering
Need an IT Help Desk to solve issues	Need a SOC to try and prevent catastrophes
Need Contingency Plans	Need Incident Response Plans
Simple log audits can recreate history	In-depth forensics needed to recreate history

Setting Context

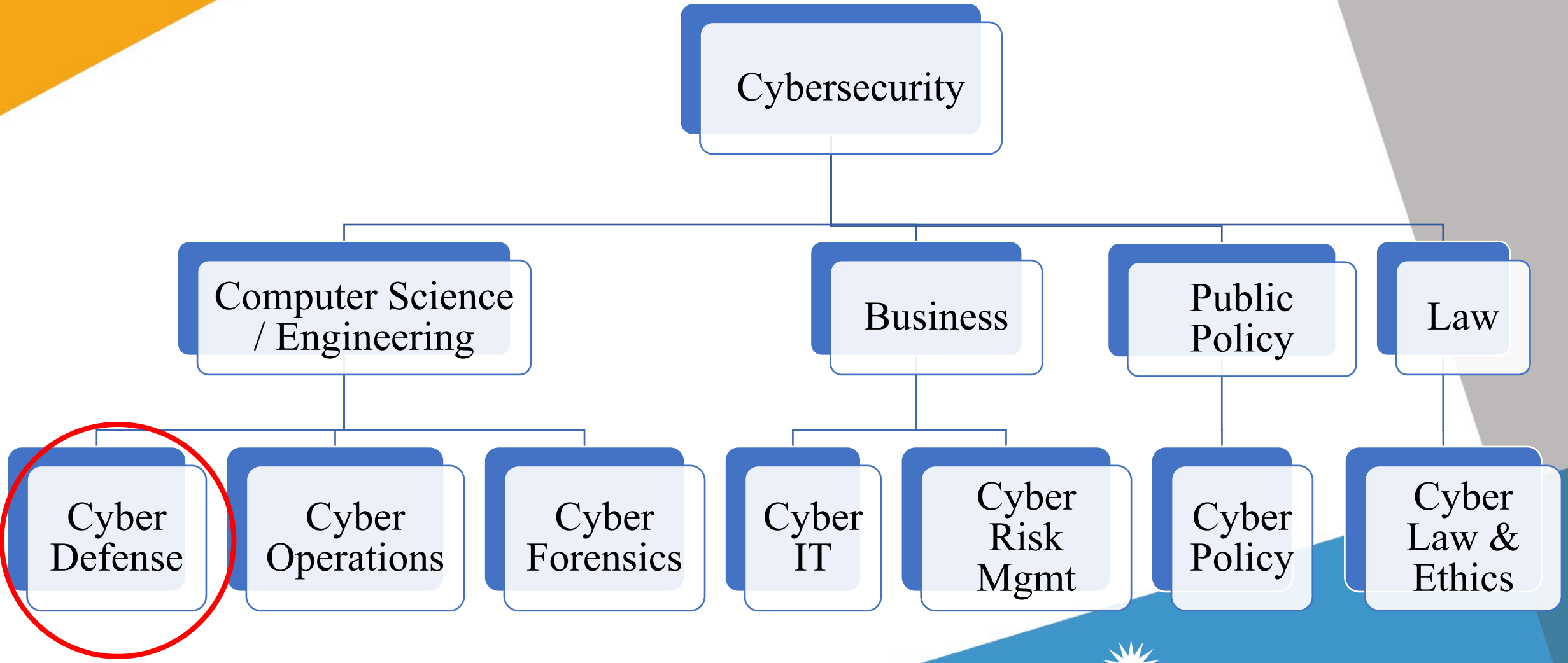
The term *cybersecurity* is very broad—it means different things to different people.

It is kind of like the term *religious*...

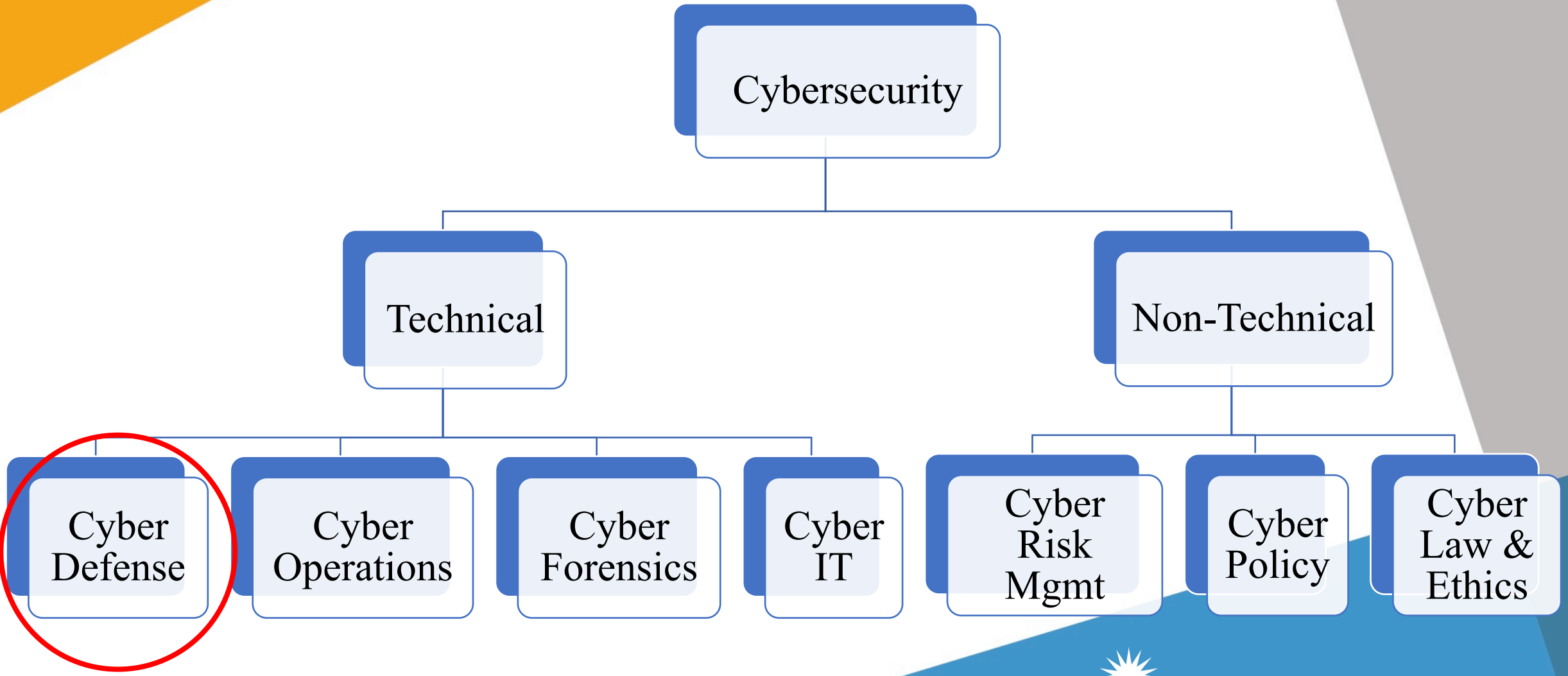
CEDARVILLE UNIVERSITY



CEDARVILLE UNIVERSITY



CEDARVILLE UNIVERSITY



CEDARVILLE UNIVERSITY

The title of this talk...

The Centrality of Adversarial Thinking for Cybersecurity

CEDARVILLE UNIVERSITY

The title of this talk...

The Centrality of Adversarial Thinking for ~~Cybersecurity~~ Cyber Defense

CEDARVILLE UNIVERSITY

Cyber Defense

Protecting computer systems and networks from hackers (i.e., ensuring CIA) in the cyber trenches.

CEDARVILLE UNIVERSITY

NIST Cyber Framework

The **Protect** Function supports the ability to limit or contain the impact of potential cybersecurity events and outlines safeguards for delivery of critical services

The **Detect** Function defines the appropriate activities to identify the occurrence of a cybersecurity event in a timely manner

CEDARVILLE UNIVERSITY

NICE Cyber Framework

Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks

CEDARVILLE UNIVERSITY

So how do we best educate superstar cyber defenders?

CEDARVILLE UNIVERSITY

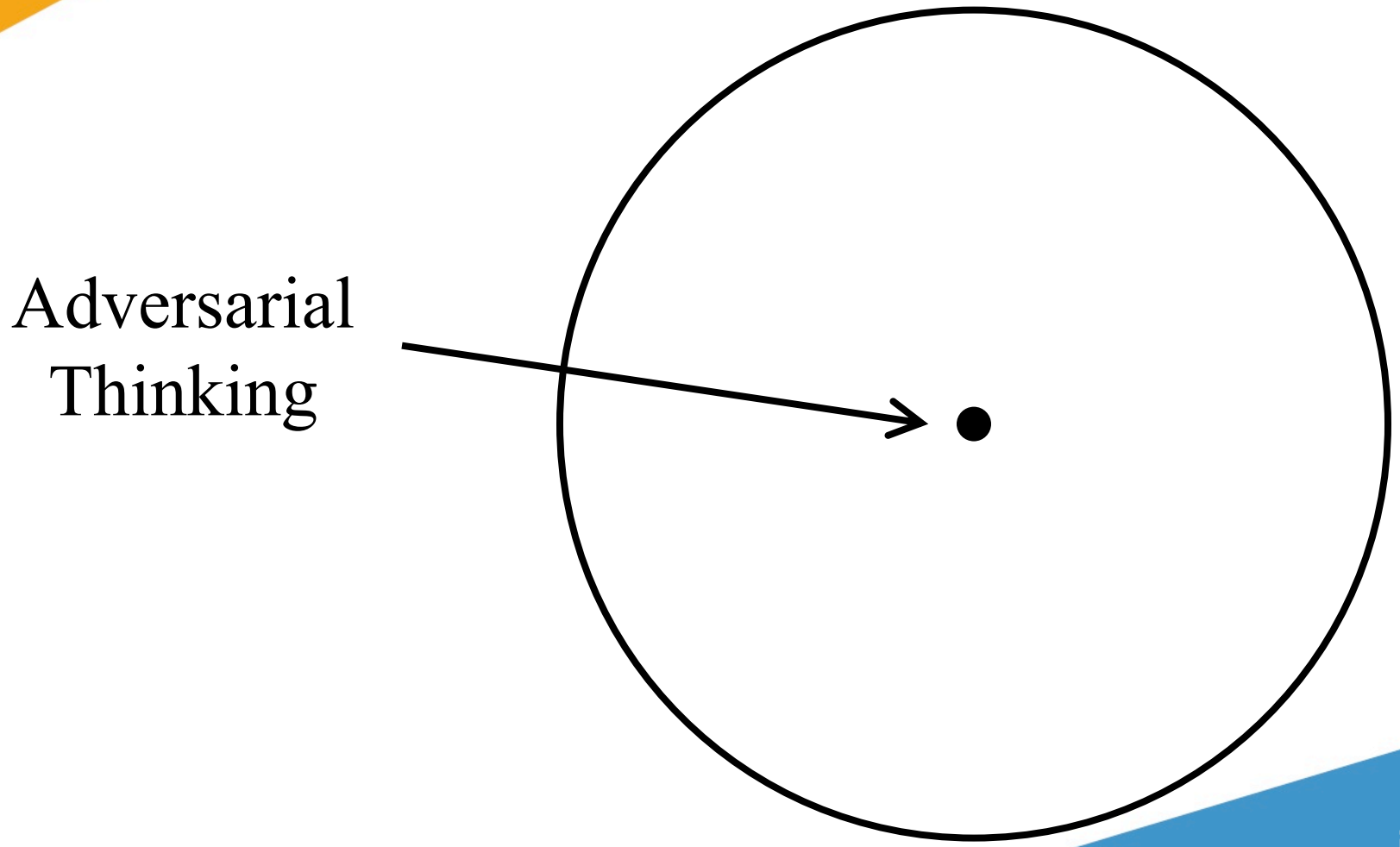
We teach adversarial thinking and keep it at the center of the educational experience.

CEDARVILLE UNIVERSITY

Because cybersecurity is all about stopping the bad guys.

CEDARVILLE UNIVERSITY

Cyber Defense Education



CEDARVILLE UNIVERSITY

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 boils down to the **definition of thinking**...

CEDARVILLE UNIVERSITY

3 Primary Ways of Thinking

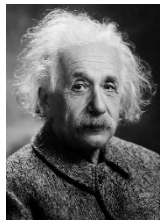
1. Solving a math problem — What is 18 × 20?
2. Making novel connections and generating creative insights — What does game theory have to do with cybersecurity?
3. Setting goals and making plans to accomplish goals — How do I go about earning my next promotion?

CEDARVILLE UNIVERSITY

Sternberg's Triarchic Theory

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

Thinking Like a Hacker



Analytical

How do his book smarts contribute to his hacking prowess?

Creative

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

Practical

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

CEDARVILLE UNIVERSITY

Application to Hackers

Area	Hacker Application	Example	Summary
Analytical	Understanding technology at a deep level, including computer networking protocols, programming languages, and operating systems	Command Line Ninja	Technological Capabilities
Creative	Identifying unsafe security assumptions through manipulating and stretching technology in unexpected ways	XSS Attack	Unconventional Perspectives
Practical	Reasoning strategically to plan and execute attacks, evade detection, and overcome obstacles	Social Engineering	Strategic Reasoning

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

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

CEDARVILLE UNIVERSITY

Learning Outcomes

Dimension	Learning Outcome	All About
Technological Capabilities	Understand computer technology at a deep level (e.g., networking protocols, programming languages, and operating systems)	Leveling the playing field
Unconventional Perspectives	Identify unconventional uses of software and protocols that could be exploited as attack vectors by hackers	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	Anticipating and thwarting attacks

The Point

Cybersecurity education is more than just adversarial thinking...

but adversarial thinking must never be too far removed from whatever specific topic we are teaching.

CEDARVILLE UNIVERSITY

The Reason

Adversarial thinking is **indispensable** to our discipline

&

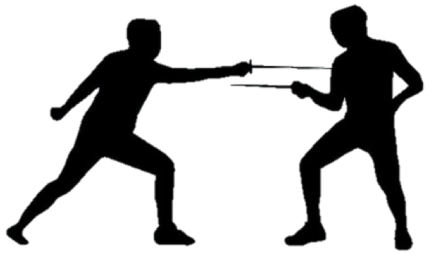
Adversarial thinking is the **main distinctive** of our discipline

CEDARVILLE UNIVERSITY

So how do we best educate cybersecurity superstars?

CEDARVILLE UNIVERSITY

We properly equip them for...



The technological
Battle of Skill

The hacker mindset
Battle of Insight

The strategic
Battle of Wits

CEDARVILLE UNIVERSITY

National Cybersecurity Curriculum Project

CLARK includes an Adversarial Thinking Module that uses **game theory** to teach **strategic reasoning** to **cybersecurity** students.

CEDARVILLE UNIVERSITY

3 B’s of Security video link:
https://youtu.be/2s8KrLN7GRE

CEDARVILLE UNIVERSITY

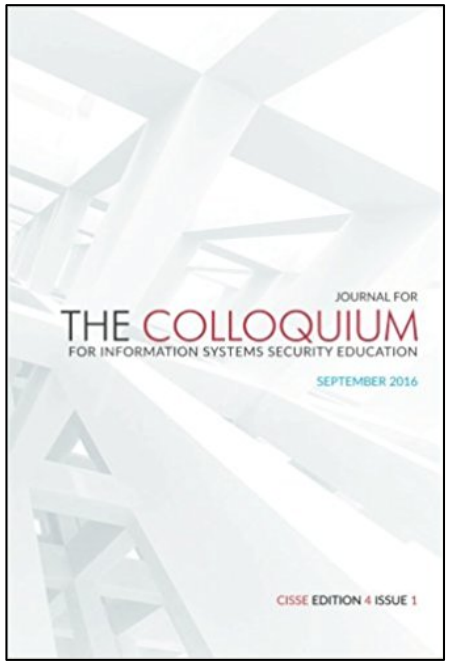
Parting Thought

If we get so focused on any one best practice, technology, tool, etc., that we forget about the bad guys, we do so at our own peril.

We must remember The Reason it All Exists!

CEDARVILLE UNIVERSITY

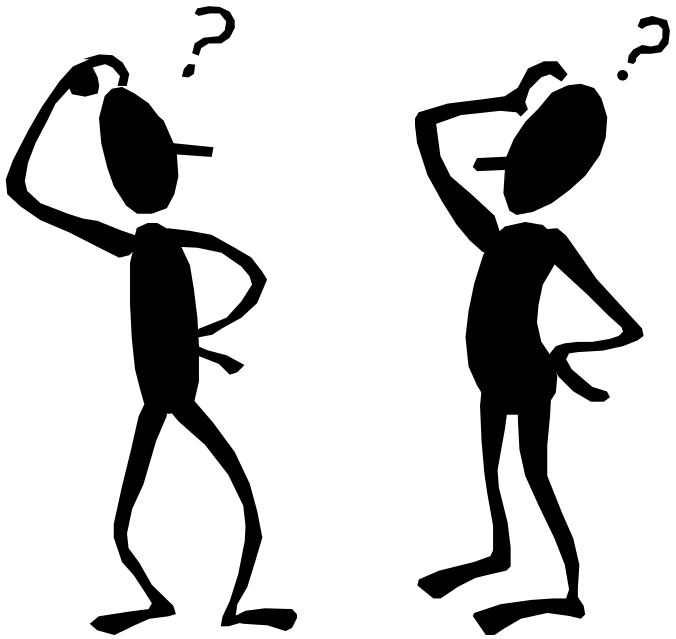
Further Reading



Teaching Adversarial Thinking for Cybersecurity

Teaching Game Theory to Improve Adversarial Thinking in Cybersecurity Students

CEDARVILLE UNIVERSITY



CEDARVILLE UNIVERSITY