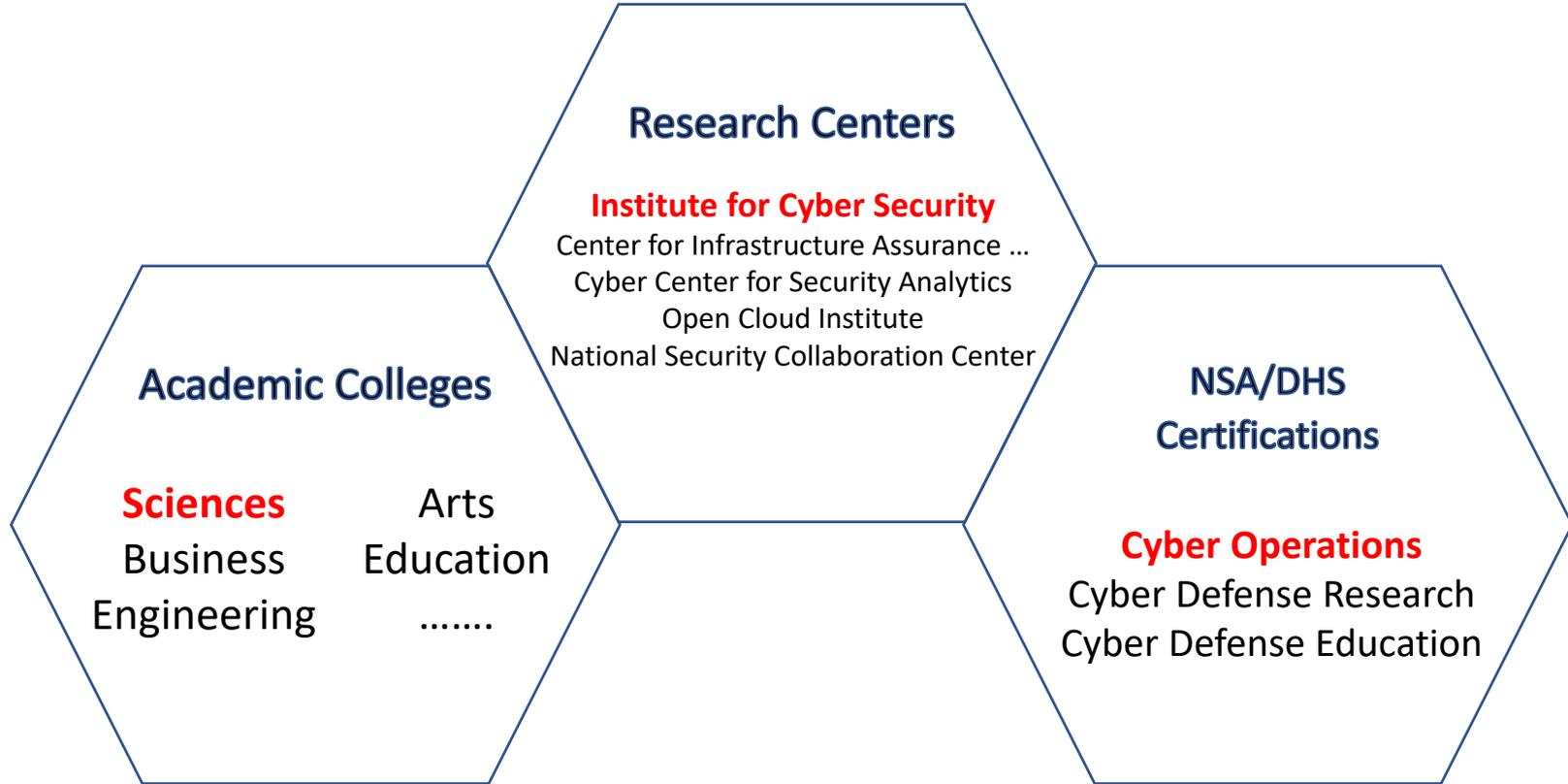# CS 6393: Cyber Security Models and Systems
CS 4593: Cyber Security Models and Systems (cross-listed)

Course Introduction and Cyber Security Overview
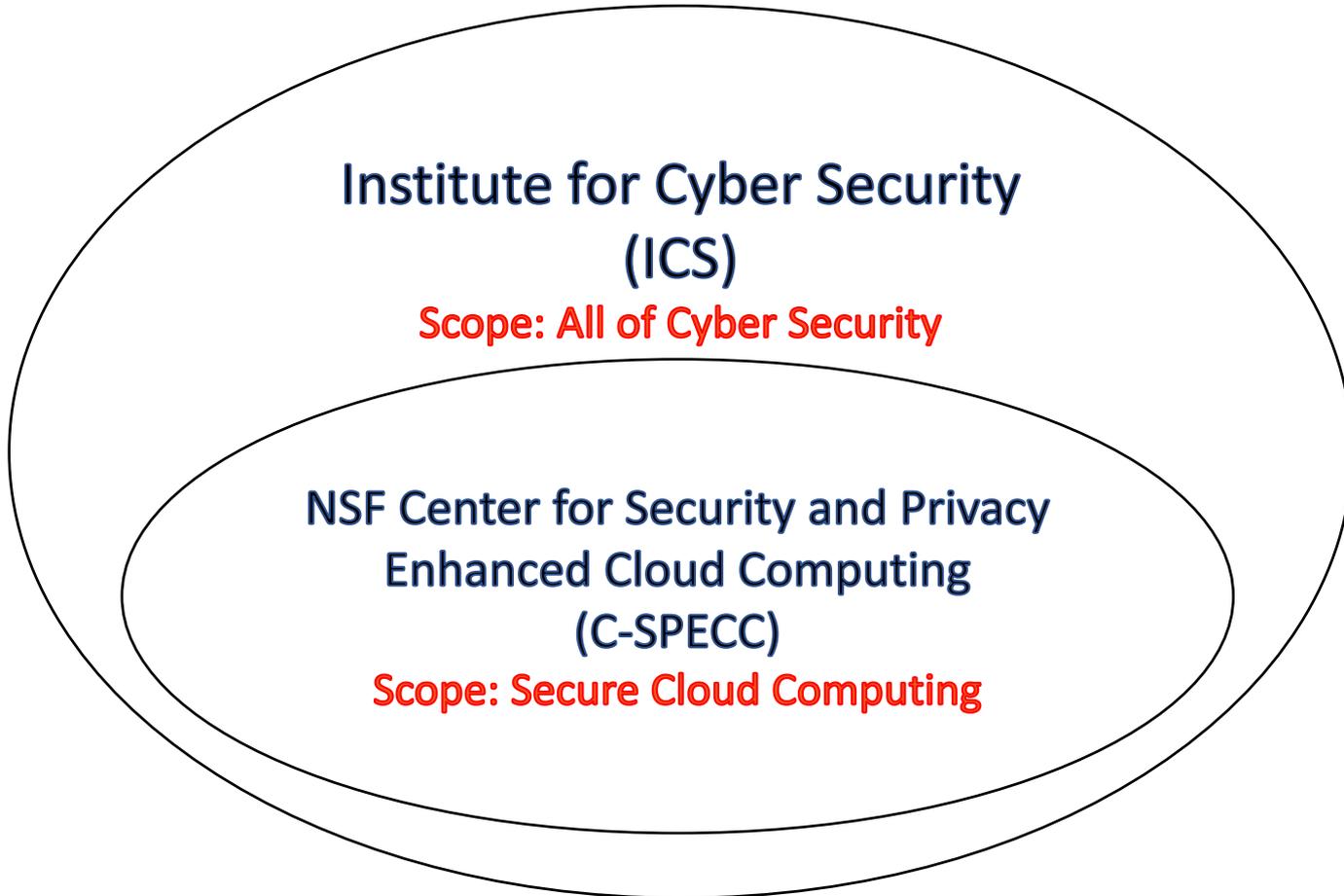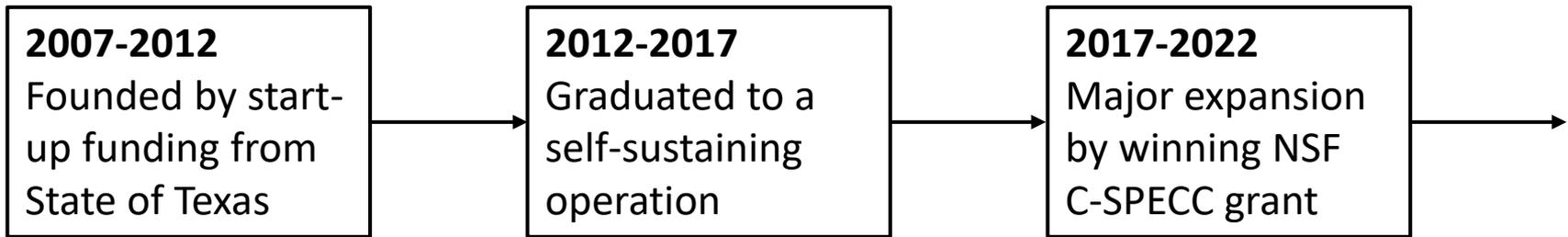
Ravi Sandhu

L190118
Spring 2019

Cyber Security at UTSA

I·C·S
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy
Enhanced Cloud Computing

Research Centers

Institute for Cyber Security
Center for Infrastructure Assurance …
Cyber Center for Security Analytics
Open Cloud Institute
National Security Collaboration Center

Academic Colleges

Sciences   Arts
Business   Education
Engineering   …….

NSA/DHS Certifications

Cyber Operations
Cyber Defense Research
Cyber Defense Education

A strategic priority since 2000

World-Leading Research with Real-World Impact!

UTSA
Computer Science

ICS & C-SPECC

Institute for Cyber Security
(ICS)
Scope: All of Cyber Security

NSF Center for Security and Privacy
Enhanced Cloud Computing
(C-SPECC)
Scope: Secure Cloud Computing

World-Leading Research with Real-World Impact!

UTSA
Computer Science

The Institute for Cyber Security

C·SPECC
Center for Security and Privacy
Enhanced Cloud Computing

MISSION
Sustained excellence in graduate-level sponsored research

| **2007-2012** Founded by start-up funding from State of Texas | → | **2012-2017** Graduated to a self-sustaining operation | → | **2017-2022** Major expansion by winning NSF C-SPECC grant | → |

➢ Established world class laboratories for: Secure cloud computing & Malware research

In collaboration with:
College of Engineering
College of Business
College of Education
Open Cloud Institute
Cyber Center for Security & Analytics
Partnership with 4 NISD High Schools:
Harlan, Woodson, Taft, Business Careers

World-Leading Research with Real-World Impact!

UTSA Computer Science

ICS
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy
Enhanced Cloud Computing
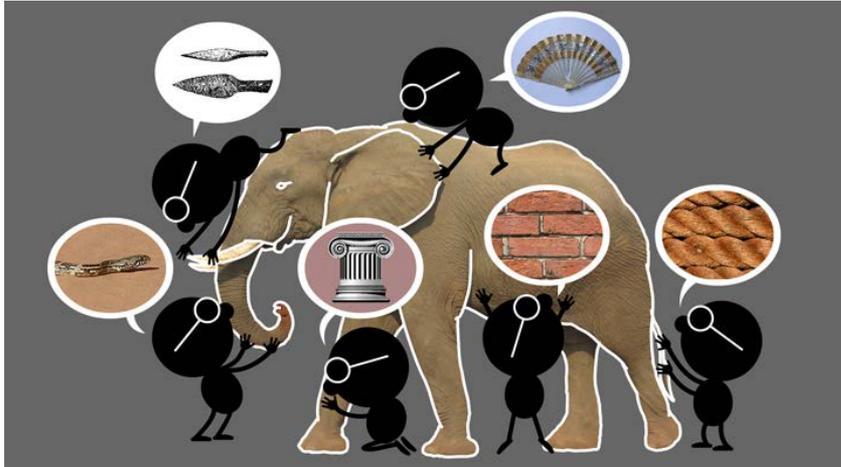
Elephant Problem

Applied vs Foundational Science: Cyber-elephants require applied and foundational combined

Present vs Future Focus: Rapidly evolving cyber-elephants require future focus

Cyber-Elephant Problem

World-Leading Research with Real-World Impact!

UTSA
Computer Science

Holistic Cyber Security

Objectives

POLICY   ATTACKS

Enable   What?   Why?   Respond

↕

Enforce   Defend

P
R
O
T   How?   D
E   E
C   T
T   ⟷   E
                                              C
           Complement   T

Mechanisms

World-Leading Research with Real-World Impact!

Control of read and write is fundamental to all three

**INTEGRITY
modification**

**AVAILABILITY
access**

**CONFIDENTIALITY
disclosure**

World-Leading Research with Real-World Impact!
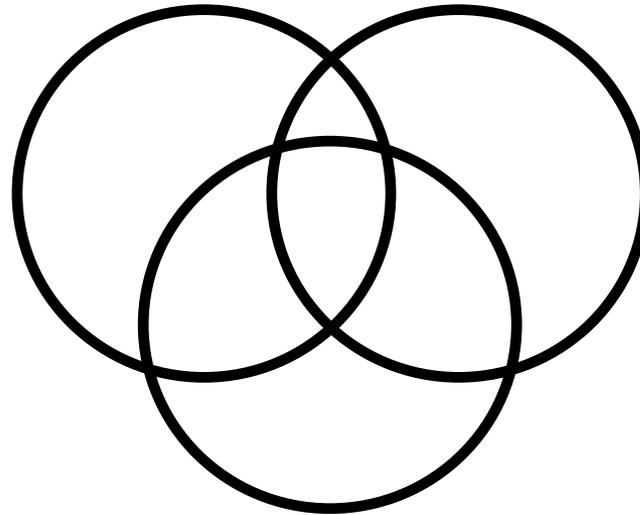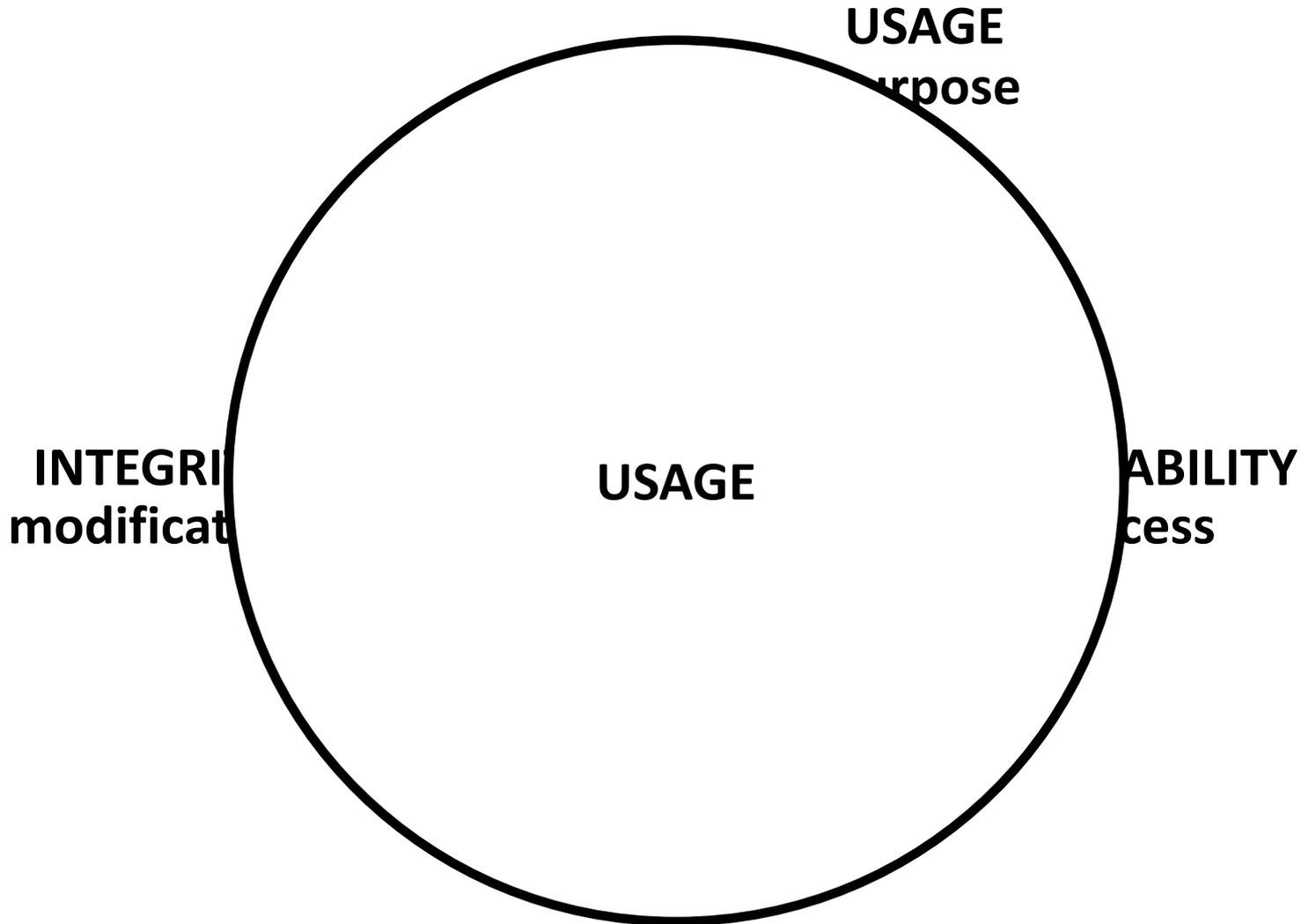
USAGE
purpose

Covers privacy and intellectual property protection
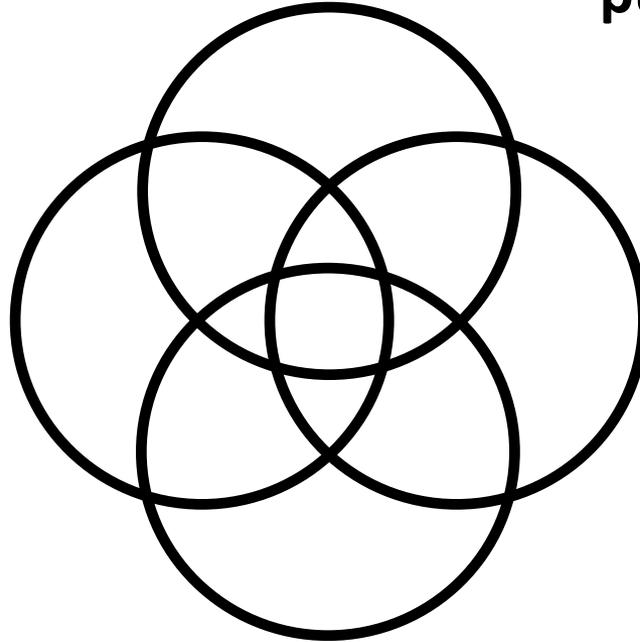
INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

World-Leading Research with Real-World Impact!

USAGE
rpose

INTEGRI
modificat

USAGE

ABILITY
cess

World-Leading Research with Real-World Impact!

"My dear, here we must run as fast as we can, just to stay in place. And if you wish to go anywhere you must run twice as fast as that."

— Lewis Carroll, Alice in Wonderland

> The ATM (Automatic Teller Machine) system is
>> ❖ secure enough
>> ❖ global in scope
> Similarly
>> ❖ on-line banking
>> ❖ e-commerce payments

World-Leading Research with Real-World Impact!

> ➤ US President's nuclear football
> ➤ Secret formula for Coca-Cola

World-Leading Research with Real-World Impact!

- ➤ Analog hole
- ➤ Inference
- ➤ Side channels
- ➤ Insider threat
- ➤ Detection is impossible
- ➤ Protection is impossible
- ➤ …..

ICS Major Research Thrusts

TECHNOLOGIES

➢ Access Control

➢ Policy

➢ Malware

➢ Detection and Forensics

➢ Blockchain

➢ Artificial Intelligence

➢ Machine Learning

➢ Data Provenance

➢ ….

APPLICATION DOMAINS

➢ Cloud Computing

➢ Internet of Things (IoT)

➢ Social Networks

➢ Big Data

➢ Mobile Platforms

➢ Enterprise

➢ Insider Threat

➢ Scientific Infrastructure

➢ ….

Goal: Broaden and Deepen

World-Leading Research with Real-World Impact!