



T₃-CIDERS

Train-the-Trainer and Community Building — *Increasing CI Adoption in Cybersecurity Research*

W. Purwanto, M. Yang, P. Jiang, S. Chappell Moots, H. Wu, M. Sosonkina



NSF CyberTraining
#2320998-99



T₃-CIDERS acronym

'tē-'thrē 'sī-dər

1: A shorthand for “A Train-The-Trainer Approach to Fostering CI– and Data-Enabled Research in CyberSecurity”

A train-the-trainer program for **advanced cyberinfrastructure (CI) skills*** designed to be synergistic with research, teaching, and learning activities in cybersecurity and cyber-related disciplines.

**Focus: HPC, big data, machine learning, cryptography, parallel programming*



Cybersecurity Is a National Priority

Increasingly **cyber** and **AI** world ↔ Greater security challenges

- Complex & vulnerable cloud / cyber-physical infrastructure
- Widespread hardware and software vulnerabilities
- Bots of IoTs
- AI-generated attacks, deepfakes, ...

Cybersecurity Is a National Priority

CYBER THREATS



CYBERSECURITY

(U//FOUO) Salt Typhoon: Data Theft Likely Signals Expanded Targeting

(U//FOUO) A recent compromise of a US state's Army National Guard network by People's Republic of China (PRC)-associated cyber actors—publicly tracked as Salt Typhoon—likely provided Beijing with data that could facilitate the hacking of other states' Army National Guard units, and possibly many of their state-level cybersecurity partners. If the PRC-associated cyber actors that conducted the hack succeeded in the latter, it could hamstring state-level cybersecurity partners' ability to defend US critical infrastructure against PRC cyber campaigns in the event of a crisis or conflict. Details on the tactics used by Salt Typhoon are available in Appendix A, and guidance to help National Guard and state govern

Foreign hacker group broke into National Guard network and went undetected for > 9 months

(source: US Dept. of Homeland Security)

Major ransomware attacks now daily news
(source: Google News)

Infosecurity Magazine

Retail Ransomware Attacks Jump 58% Globally in Q2 2025

2 days ago • By James Coker



SecurityWeek

Armenian Man Extradited to US Over Ryuk Ransomware Attacks

15 hours ago • By Eduard Kovacs

BleepingComputer

M&S confirms social engineering led to massive ransomware attack

10 days ago • By Lawrence Abrams



Cybersecurity as a Research Area

- Highly active areas
- Multidisciplinary (CS, CE, EE, data science, AI/ML, information technology, information security, anthropology, law & policy, ...)
- Most likely, some at your institution are researching these topics

... except they might not be called “cybersecurity” ...

Cybersecurity as a Research Area

without “cyber” or “security”

- Trustworthy system design
- Adversarial ML
- IoT (cyber-physical systems)
- Resilience engineering
- Human-in-the-loop systems
- Data governance and compliance
- Privacy-preserving ML
- Software supply chain
- Cloud computing
- Edge computing
- Zero trust architecture
- DeepFake detection/mitigation

Cybersecurity's Demand for Advanced CI

- Rapid uptake of AI in cybersecurity research
- Simultaneous rapid development of AI and CI —
What used to be niche computing has become mainstream!
- Are we training enough people with AI/CI skills??
- Traditional academia too slow to adapt to fill the skill gap

Gap in CI Readiness in Cybersecurity

Increasing availability of CI

- Campus HPC
- ACCESS & NAIRR pilot
- Cloud resources
- AI platforms & tools

Lack of CI readiness for research

- ✗ CI not part of curricula of cyber-related majors
- ✗ Lack of intro CI for cyber fields
- ✗ Faculty not skilled in CI usage

DeapSECURE – Filling Material Gap

“Data-Enabled Advanced Computational Training Platform for Cybersecurity Research and Education” (NSF #1829771)

- Open-source, hands-on, introductory CI lesson modules for cybersecurity
- Equip students with “CI skills baseline”
 - *HPC, Big Data, Machine Learning, Crypto, Parallel Comp.*
- Prepare students to embark modern cybersecurity research



DeapSECURE Lesson Materials

- Six Carpentries-style online lessons
- Hands-on datasets, files, Jupyter notebooks
- Basic programming experience is required

Module 1: Introduction to HPC

Introduction to high-performance computing on a Linux cluster: UNIX shell interaction, SLURM job scheduler, parallel job launch. ([Lesson site](#))

Module 2: Dealing with Big Data

Introduction to Pandas, a powerful data processing framework capable of handling large amounts of data in an efficient manner. ([Lesson site](#))

Module 3: Machine Learning

Machine learning is an approach to program a computer to perform certain intelligent tasks without being explicitly programmed to do so. ([Lesson site](#))

Module 4: Deep Learning Using Neural Networks

Neural network is a powerful approach to machine learning that can yield extremely high accuracy on complex cognitive tasks. ([Lesson site](#))

The number of threads shows a multimodal distribution (two major peaks and two smaller peaks). It is actually interesting to plot the histogram separately for the two applications:

```
nthrds_FB = df2[df2['ApplicationName'] == 'Facebook']['num_threads']
nthrds_WA = df2[df2['ApplicationName'] == 'WhatsApp']['num_threads']
seaborn.distplot(nthrds_FB, kde=False, label='Facebook')
seaborn.distplot(nthrds_WA, kde=False, label='WhatsApp')
pyplot.legend()
```

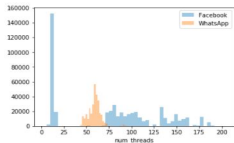


Figure: Histograms of `num_threads`, grouped by application type

Characterizing Behavior of Different Applications

The last plot shows histograms of `num_threads` drawn for individual applications. A glance of this plot visualizes about the differences between the two applications being considered. Discuss the differences you can uncover using the histogram plot.

Discussion

EXAMPLE 1: Dropping a useless feature. Create `df_mystery2` that does not have the `Unnamed: 0` field, which is not a feature at all.

```
[ ]: """Create new DataFrame which does not contain 'Unnamed: 0'.
Make sure to verify the result."""
df_mystery2 = df_mystery.drop('#T000', axis=1)
```

```
[ ]: df_mystery2 = df_mystery.drop(['Unnamed: 0'], axis=1)
df_mystery2.head()
```

EXAMPLE 2: Dropping all non-features. Apply `df_features_only` that has only features.

```
[ ]: """Create new DataFrame which does not contain 'Unnamed: 0'.
Make sure to verify the result."""
df_features_only = df_mystery.drop('#T000', axis=1)
```

EXAMPLE 3: Dropping a useless feature forever. Now remove column `Unnamed: 0` from `df_mystery` for good: we don't need to see it anymore.

Hint: This is an in-place operation which alters `df_mystery`.

```
[ ]: """Write a code to remove 'Unnamed: 0' column from the original DataFrame"""
```

<https://deapsecure.gitlab.io/lessons/>
<https://gitlab.com/deapsecure/>

T3-CIDERS – Scaling Up CI Training

Goal: Accelerate state-of-the-art research & development in cybersecurity and related fields

- **Train-the-trainer:**

Produce competent trainers to broaden utilization of CI

- **Community building:**

Foster CI-enabled cybersecurity research community of practice



T3-CIDERS – Future Trainers

Future Trainers (FTs) are drawn from

- Faculty
- Researchers
- Students
- Practitioners

Paired into **FT units**
(1 faculty + 1 student)
for collaborative
lesson development

... with research interest in
cybersecurity and cyber-related fields

T3-CIDERS – Train-the-Trainers

Equipping **Future Trainers (FTs)** with

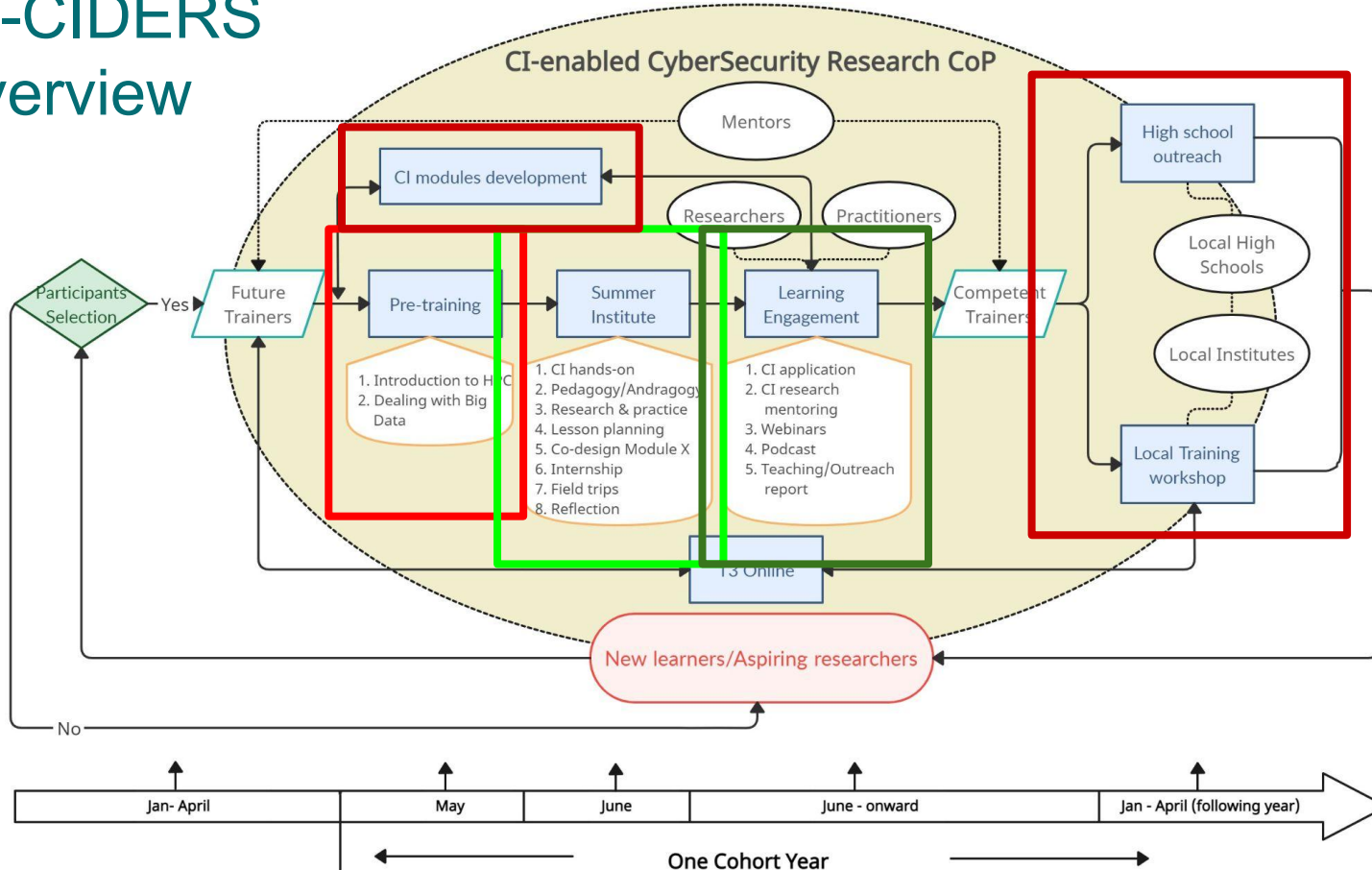
- Working knowledge of CI fundamentals
- Skill to teach CI skills to students & others
- Infusion of CI into fabric of cybersecurity research & education
- Resources for CI teaching & learning from communities at large

T3-CIDERS – Community Building

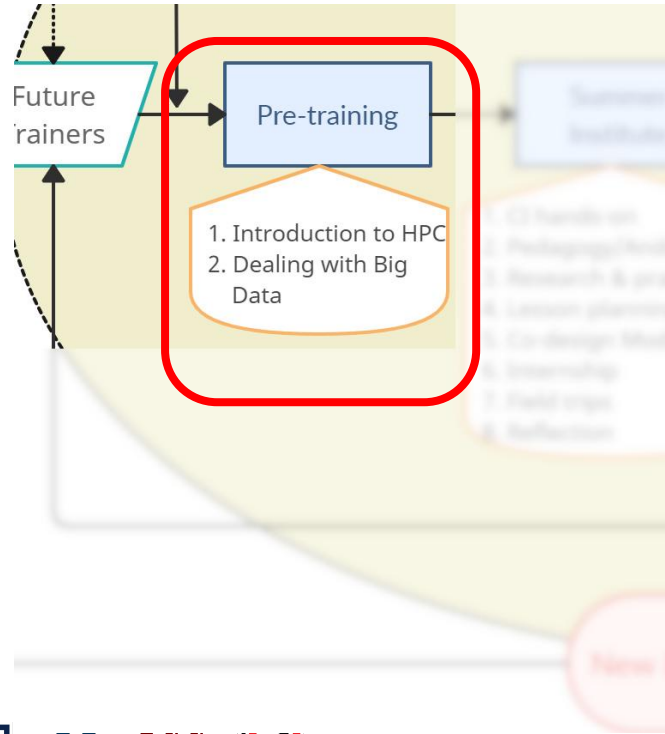
Engaging **Future Trainers (FTs)** through

- Summer Institute (bootcamp & networking)
- Regular meetups
- Community events
- Collaborative activities with cybersecurity experts, CI practitioners

T3-CIDERS Overview

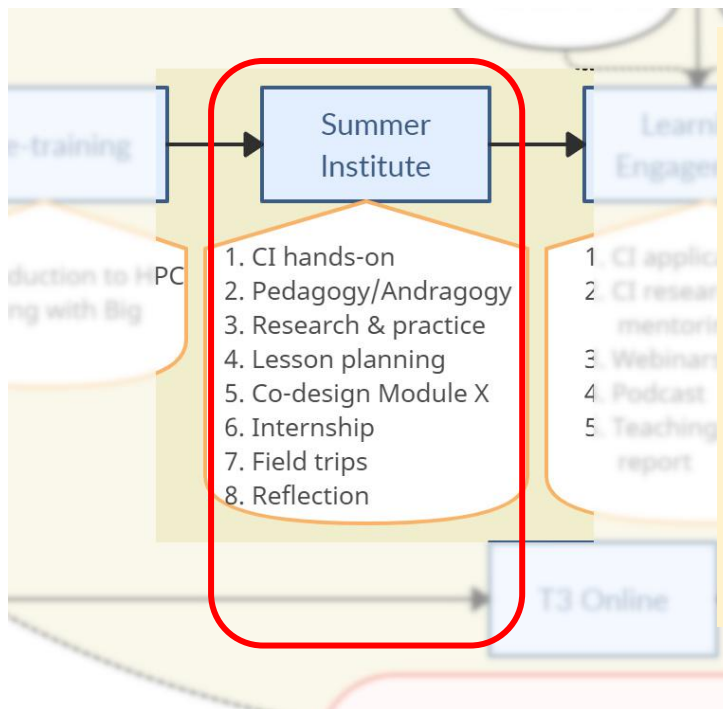


Phase 1: Pre-training



- Virtual, self-paced course, group discussions
- ~ 4-week long
- Focuses on CI skill baseline
- Based on DeapSECURE HPC & Big Data modules

Phase 2: Summer Institute

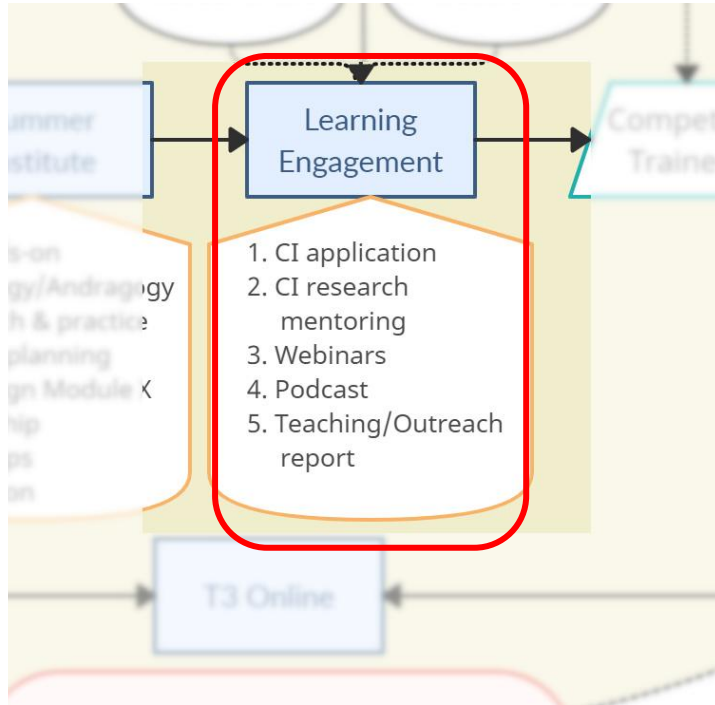


- In-person train-the-trainer
- One week
- Immersive CI & pedagogy lessons
- FT outcomes: initial lesson plan, teaching demo

Phase 2: Summer Institute Contents

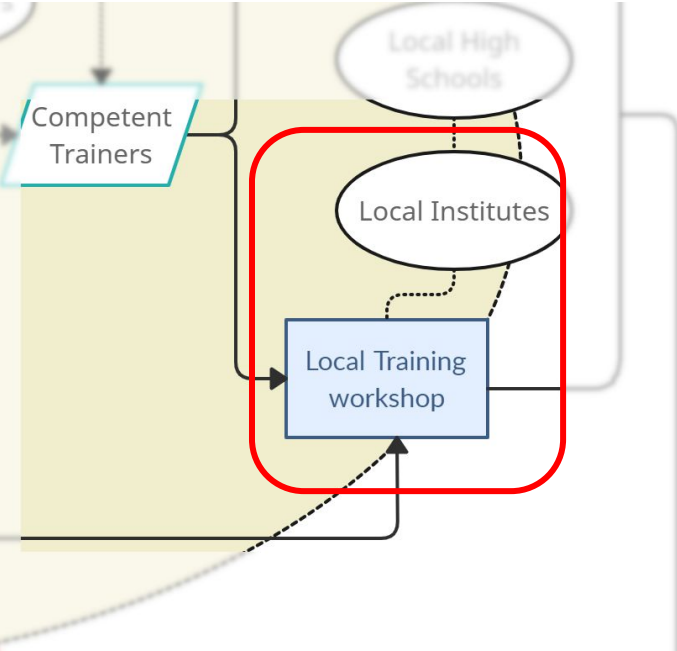
- Overview of CI topics (ML, NN, CRYPT, PAR) with hands-on
- Basics of education with demo of lesson planning/teaching
- Studio: FTs creating their CI training lesson plan
- Cybersecurity expert & K-12 educator panels
- “Module-X” brainstorming
- Demo of teaching CI topics by FTs

Phase 3: Learning Engagement



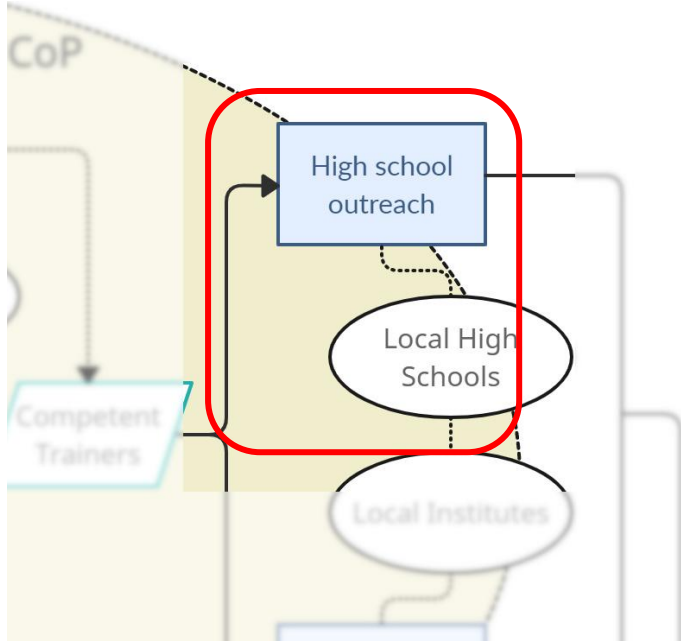
- FTs completing their lesson plan & preparing for teaching
- Regular virtual check-ups
- Webinars, discussions, sharing of teaching experiences

Phase 4: Local CI Training



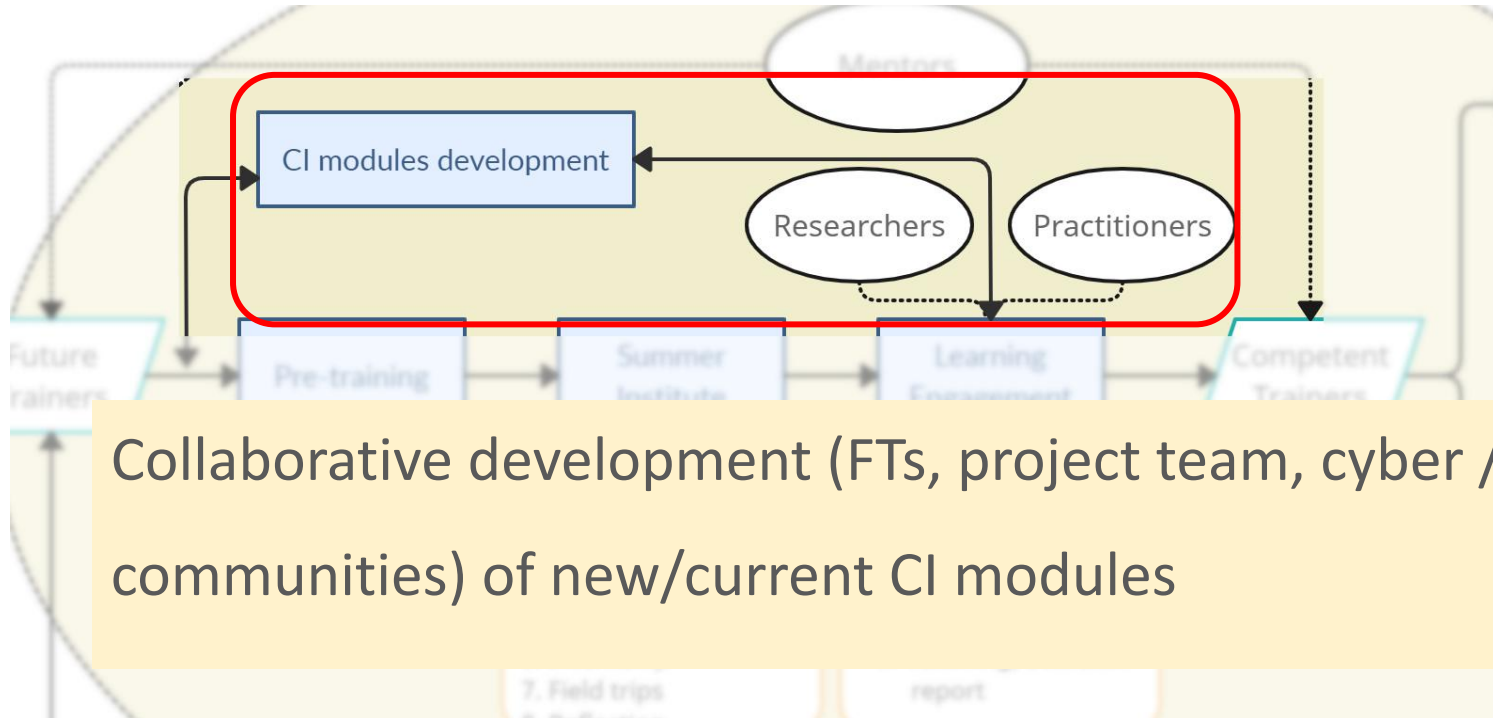
- FTs delivering their lesson at their home institutions, tailored to meet local needs
- **Mandatory** outcome of train-the-trainer

Phase 5: K-12 Outreach



- FTs interacting with K-12 students regarding cyber / CI awareness
- Optional

Phase 6: “Module-X”



Collaborative development (FTs, project team, cyber / CI communities) of new/current CI modules

Assessment Plan

What being measured:

- *Reactions*: engagement, perceived relevance, satisfaction
- *Learning*: knowledge, skills, attitude
- *Behavior*: application of learning, transfer of training
- *Results*: outcomes

Assessment Plan

When:

- *Pre-survey*: demographics, motivation, needs, expectations, prior preparation
- *Reflections* (during Summer Institute)
- *Post-surveys*: post-SI, post-local-teaching experiences, satisfaction, attitude

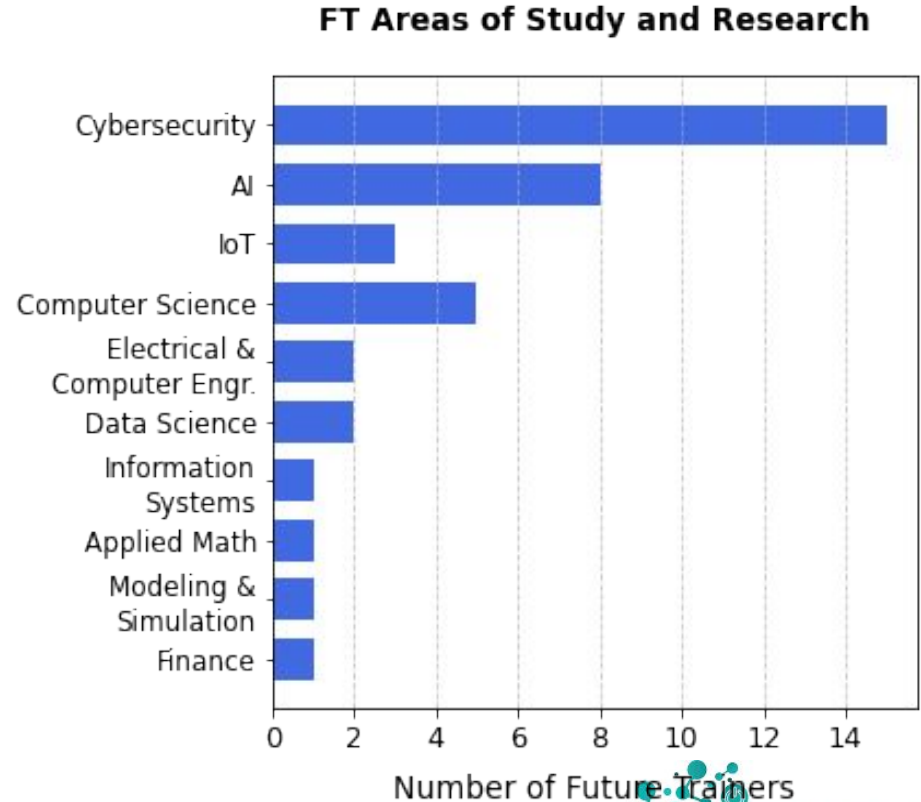
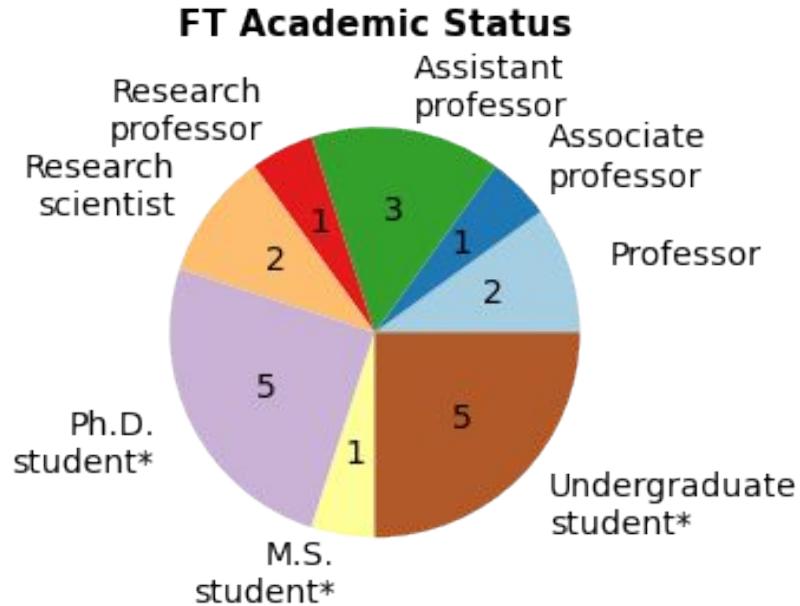
2024 Cohort

8 faculty/researchers
+ 12 students

⇒ **8 FT units**

State	Num of People
Virginia	12
Texas	4
Washington	2
North Carolina	1
New York	1

2024 Cohort



2024 Cohort – Onboarding & Keeping Touch

- Messaging platform: Discord
- Shared Google drive for collaborative workspace
- Pre-training: HPC, Unix shell, Big Data (Pandas), Cybersecurity research & application discussions
- Office hours during pre-training

2024 Cohort – Learning Engagement


- Meeting with FT units to follow-up their teaching plans & debrief after teaching
- Newsletter email updates
- (Planned) Webinar and/or community discussions
- Mentoring of one undergraduate and three graduate students on lesson & workshop development

2024 Cohort – CI Teaching Activities

- Lab session on federated learning (upgrade existing course)
- Hands-on workshops on machine learning and/or HPC intro
- Seminar presentation on transformer architecture
- Video tutorial on Unix shell CLI

2024 Cohort – High School Outreach

[Ctrl+Alt+Elite](#) [About Us](#) [Getting Started](#) [Practice Resources](#) [Higher Education](#) [Workshops](#)



Elexiah Smart
Student at Old Dominion University
studying Electrical Engineering and
Modeling & Simulation Engineering

📍 Old Dominion University
🏠 T3-CIDERS Logistics Coordinator
✉ Email

Ctrl + Alt + Elite: Level Up Your Skills With the Command Line

This website was developed to house all necessary materials and resources needed for students to participate in the T3-CIDERS Introductory Workshop on Computer Command-Line Interface, created by Elexiah Smart under the guidance of Dr. Wirawan Purwanto, Dr. Peng Jiang, Dr. Mohan Yang. In this workshop, high school students learn about the command-line interface (CLI), a fundamental yet powerful way to interact with computers.

What is the Command Line Interface?

The Command Line Interface (CLI) is a text-based interface used to interact with software and operating systems. It requires users to type commands into a terminal to perform simple and/or complex tasks, such as

- File manipulation
- Program execution
- System administration

Uses of the CLI

CTRL + ALT + ELITE

LEVEL UP YOUR COMPUTING SKILLS WITH THE COMMAND LINE

Ever wondered how tech pros navigate computers like wizards—without a mouse? Join us for a hands-on UNIX Command Line Interface (CLI) workshop where you'll learn to:

- 1 MASTER ESSENTIAL COMMANDS
- 2 NAVIGATE FILES LIKE A PRO
- 3 BOOST YOUR EFFICIENCY



ON DEMO
Gain experience with Linux and macOS, to see what's next! There's a prize involved...

HIGHER EDUCATION
Join us to explore career paths where these computational skills are in demand and how to pursue them.

VISIT OUR WORKSHOP'S WEBSITE FOR MORE PRACTICE AND INFO!



OLD DOMINION UNIVERSITY | T3-CIDERS

Wed, April 9, 2025 | After School

<https://lexiluthor05.github.io/Ctrl-Alt-Elite/>

2024 Cohort – “Module-X”

- Collaboration between T3-CIDERS team and one FT group
- Content: Short hands-on module at the intersection of AI & cybersecurity
- Target completion: end of summer 2025

2024 Cohort: SI Evaluation (Preliminary)

Comparing pre-survey ($n=20$) and post-survey ($n=16$) mean scores:



Mean scores increase in:

- Factors that motivated participant to join project
- Perceptions of Teaching and Assessment methods for CI instruction
- Perceptions of participants' own Teaching Competencies for CI topics



Statistically significant increases in:

- Knowledge of CI topics ($p < .01$)
- Application of CI techniques in participants' own research or work ($p < .05$)
- Confidence in ability to teach CI topics to others ($p < .01$)



Improvements needed in attitudes: eagerness to participate, expectations of training, relevance & value of the program, ...

2025 Cohort – *Opening Soon!*

Enrollment open: August 2025

Pre-training: Fall 2025

Winter Institute:

The University of Arizona

January 5–9, 2026



**Sign up for our
Interest List!**

T3-CIDERS

**A Train-the-Trainer Approach to
Fostering CI- and Data-Enabled Research in Cybersecurity**
Cyberinfrastructure (CI) refers to advanced computers and methods (big data, artificial intelligence, etc.) which enable cutting-edge research. The T3-CIDERS Train-the-Trainer program will empower you to teach CI competencies to enhance research and teaching in cybersecurity.

Project Overview
Accelerate state-of-the-art research in cybersecurity and related fields by:

- Preparing competent trainers to broaden utilization of CI in research
- Fostering a CI-enabled cybersecurity research community of practice

What Will You Learn?
T3-CIDERS will introduce effective training and instructional design methods, to prepare you to teach advanced CI domains such as:

- high-performance computing
- big data
- machine learning
- cryptography
- parallel programming

Who Can Join?

- Faculty
- Researchers
- Practitioners in cybersecurity related fields
- Students (paired with a faculty member)

Winter Institute Dates:
January 5-9, 2026
University of Arizona
Tucson, AZ

Benefits:

- Hands-on CI training modules relevant to cybersecurity and cyber-related research
- Evidence-based training and design methodology
- Support for developing local CI training activities and cybertraining proposal writing
- Community of practice in CI
- Monetary assistance for attending the Winter Institute and conducting local CI training

Train-the-Trainer Outcomes:

- Apply CI techniques in cybersecurity research
- Develop & conduct CI training in local academic communities

Join our Interest List:
tinyurl.com/T3ciders-signup

Visit our website:
sites.wp.azd.edu/t3-cidrs/

The T3-CIDERS training program is a collaborative project of Old Dominion University, the University of Arizona, Texas A&M University, and the University of Nebraska Omaha, funded by the U.S. National Science Foundation CyberTraining grants #2520998 and #2320999.

OLD DOMINION
UNIVERSITY

THE UNIVERSITY
OF ARIZONA

TEXAS A&M
UNIVERSITY

UNIVERSITY OF
NEBRASKA
OMAHA

Contact Us:
t3ciders@gmail.com



Summary

T3-CIDERS: train-the-trainer & community building to broaden adoption of CI in cybersecurity research

- Cohort-based “future trainers” (FTs), year-long program
- FTs trained in CI fundamentals & pedagogy skills
- FTs diffuse CI knowledge & skills to their local communities
- 2024 cohort impacts & teaching outcomes are encouraging

Acknowledgments

PIs: Masha Sosonkina (ODU), Hongyi “Michael” Wu (U. Arizona), Wirawan Purwanto (ODU), Mohan Yang (Texas A&M), Peng Jiang (U. Nebraska Omaha)

Evaluator: Shanan Chappell Moots (ODU)

TAs & coordinators: Ted Birkland, Jiawei Chen, Sylvia Cooper, Kayla Curtis, Kristin Herman, Chunyu Hu, Chunlin Huang, Nolan Lovett, Dorothy Parry, Jael Perales, Elexiah Smart



Funding: NSF CyberTraining grants #2320998, 2320999



Engage with Us — *We Need You!*

T3-CIDERS: Building a community of FTs, cybersecurity & CI experts centered around CI-enabled cybersecurity research/practice

Connect with us:



t3ciders@gmail.com

sites.wp.odu.edu/t3-ciders

[Join our Interest List!](#)

