T3-CIDERS: Train-the-Trainer and Community Building to Increase Cyberinfrastructure Adoption in Cybersecurity Research and Education

Wirawan Purwanto
DTT Research & Cloud Computing Services
Old Dominion University
Norfolk, VA, USA
wpurwant@odu.edu

Mohan Yang
Educational Administration and Human Resource Development
Texas A&M University
College Station, TX, USA
mohanyang@tamu.edu

Peng Jiang
School of Interdisciplinary Informatics
University of Nebraska Omaha
Omaha, NE, USA
pjiang@unomaha.edu

Shanan Chappell Moots
The Center for Educational Partnerships
Old Dominion University
Norfolk, VA, USA
schappel@odu.edu

Masha Sosonkina
Electrical & Computer Engineering
Old Dominion University
Norfolk, VA, USA
msosonki@odu.edu

Hongyi Wu
Electrical & Computer Engineering
The University of Arizona
Tucson, AZ, USA
mhwu@arizona.edu

Abstract

T^3-CIDERS is a train-the-trainer program to increase the adoption of advanced cyberinfrastructure (CI) and data skills into the fabric of research and education in cybersecurity and cyber-related disciplines. T^3-CIDERS trains faculty, researchers, and students as "future trainers" (FTs) with hands-on technical and instructional skills to enable more people to effectively leverage CI in cybersecurity. The program includes a series of technical pre-training modules, a weeklong summer institute, ongoing learning engagements conducted over an academic year; it culminates with the FTs conducting locally tailored CI-infused training events at their respective home institutions. Ultimately, T^3-CIDERS aims to build a "CI+cybersecurity" community of practice as the cohort continues to practice and teach CI skills in their teaching and research activities. This paper describes the vision and implementation of T^3-CIDERS with the first cohort starting in year 2024. Based on the lessons learned through the in-person cohorts, a fully online program will be developed to expand the reach of T^3-CIDERS to a broader audience. T^3-CIDERS responds to the need to close the CI and data skill gap to meet the increasing challenges in securing the digital world.

CCS Concepts

• **Security and privacy** → *Cryptography*; • **Computing methodologies** → *Machine learning*; *Parallel computing methodologies*; • **Computer systems organization** → **Parallel architectures**; • **Social and professional topics** → **Computing education**;

Keywords

Cyberinfrastructure, cybersecurity, research, train-the-trainer, pedagogy, HPC, parallel computing, big data, machine learning, non-degree training, hands-on

ACM Reference Format:
Wirawan Purwanto, Mohan Yang, Peng Jiang, Shanan Chappell Moots, Masha Sosonkina, and Hongyi Wu. 2025. T3-CIDERS: Train-the-Trainer and Community Building to Increase Cyberinfrastructure Adoption in Cybersecurity Research and Education. In *Practice and Experience in Advanced Research Computing (PEARC '25), July 20–24, 2025, Columbus, OH, USA.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3708035.3736021

PEARC '25, Columbus, OH, USA

ACM ISBN 979-8-4007-1398-9/25/07
https://doi.org/10.1145/3708035.3736021

1 Introduction

Research in cybersecurity addresses an urgent need to protect our increasingly digital world. As cyber threats continue to evolve in scale, sophistication, and damages, ongoing research helps us stay ahead of emerging threats and develop more effective defenses. Training for current and future cybersecurity workforce must also keep pace with new challenges as well as progress in tools and techniques required to secure rapidly evolving cyber systems. In this constant race between cyber defense and attacks, *cyberinfrastructure* (CI) has played an increasingly important role to provide the capabilities to assess cyber risks, identify and mitigate threats, and achieve defense in depth [9]. CI refers to "computational systems, data and information management, advanced instruments, visualization environments, and people, all linked together by software and advanced networks to improve scholarly productivity and enable knowledge breakthroughs and discoveries not otherwise possible" [27].

One important component of CI is the high-performance computing (HPC) systems, which have recently become more available to academic cybersecurity researchers in the U.S. through the NSF-funded ACCESS program [1, 4], and even to wider audience through the recently established pilot National AI Research Resources (NAIRR Pilot) program [16]. Both programs also offer cloud resources, including Jetstream 2, Amazon Web Services, Google, and

Azure. The emergence of powerful artificial intelligence (AI) tools such as generative AI and large language models (LLMs), fueled by advances in HPC technology and availability, has brought CI hardware and software technologies into the forefront of cyberspace. For example, federal agencies, including the Cybersecurity and Infrastructure Security Agency (CISA) now employ AI in many of their cybersecurity operations for improvement [5]: AI tools are utilized to detect anomalous behavior in network data, bolstering their ability to defend against cyber threats [13, 26]. AI-based natural language processing (NLP) is also adopted for the computerized detection of personally identifiable information (PII) in information security [14]. It involves NLP for identifying potential PII in the Automated Indicator Sharing service submissions, with consideration for privacy protection and compliance with laws and regulations. A classification-based AI model is also employed for assigning confidence values to cybersecurity danger indications in supporting prioritization of potential danger in its response. Hence, the use of AI, coupled with the availability of HPC systems to train and fine-tune AI models, especially the large-scale ones, has become increasingly instrumental in research, development, and implementation of cybersecurity everywhere.

1.1 Challenges in CI Readiness in Cybersecurity Research and Education

Despite the availability of CI and its importance in strengthening the security of cyber-systems, there is still a significant gap in the preparedness of the cybersecurity workforce and researchers to leverage CI. Indeed the challenge is systemic with many factors: (1) CI topics are not yet integral in standard cybersecurity curricula in many universities [18, 29]; (2) Many faculty members are not informed or skilled in the use of CI [6, 17]; (3) Considering that cybersecurity is a multidisciplinary field at the intersection of computer science, software engineering, mathematics, anthropology, sociology, law and policy, students often come with different levels of preparedness toward learning CI skills [15, 25]; (4) Finally, introductory-level CI lessons with direct relevance to cybersecurity are scarcely available for community adoption. These factors must be overcome in order to achieve widespread adoption of CI in cybersecurity research and education. The remedy to the challenge at this scale must involve the community of researchers and educators [2].

1.2 Bridging the Skill Gap Through CI Training

As the first step toward bridging the gap in CI skills in cybersecurity, a non-credit, non-degree CI training program named "DeapSECURE" [22] was developed at Old Dominion University (ODU). DeapSECURE offers six open-source CI lesson modules [20] that are designed to provide gentle, novice-friendly, hands-on introduction to HPC, big data, machine learning/AI, cryptography, and parallel programming. As detailed in our earlier work [19], the hands-on activities are built on top of Python, Jupyter, Unix shell, and are designed to train learners to make an effective use of an HPC platform. The purpose of the DeapSECURE project is to equip students with foundational CI knowledge and skills and prepares them to use CI resources, tools, and services to succeed in cutting-edge cybersecurity research and industrial cybersecurity projects [22]. The topics and skills taught in these lessons form a "CI skills baseline" to empower the learners to begin using CI and provide a pathway for further learning. DeapSECURE adopts the principle of authentic learning [8] by designing the hands-on activities based on real cybersecurity research use cases and datasets. We continuously taught and improved this lesson series six times as workshops and summer institutes at ODU from 2018–2023; the experiences and lessons learned from these efforts have been published [7, 19, 21, 22]. These workshops and institutes positively impacted as many as 200 students and researchers through these years. In the latter years (2021–2023), DeapSECURE summer workshops were instrumental in "booting up" CI skills for undergraduate students who joined the Cybersecurity Research Experience for Undergraduates summer research program held at ODU. From this, it became evident that the benefits of this type of CI training need to be replicated at many other institutions, which calls for the producing of more trainers to meet this need at scale. A community survey distributed in 2021 to faculty and researchers across the Commonwealth of Virginia identified a strong interest to adopt DeapSECURE training, with half of the respondents nodding to the research needs as well as a "train-the-trainer" approach to promulgate CI training.

2 Overview of the T^3-CIDERS Program

2.1 Vision and Goal

T^3-CIDERS (short for "Train-The-Trainer Approach to Fostering Cyberinfrastructure- and Data-Enabled Research in CyberSecurity") is a new train-the-trainer program [23, 24] which aims to promulgate CI readiness into cybersecurity and cyber-related disciplines on a broad scale. This paper describes the vision, goal, blueprint of T^3-CIDERS with its major phases and contents, and reports a brief experience of the first cohort. Funded by the U.S. National Science Foundation (NSF), T^3-CIDERS is collaboratively developed at ODU, the University of Arizona, University of Omaha at Nebraska, and Texas A&M University.

The goal of T^3-CIDERS is to accelerate state-of-the-art research and development in cybersecurity and cyber-related fields by (1) preparing competent trainers to broaden the utilization of advanced CI in these disciplines, and (2) fostering a CI-enabled cybersecurity research community of practice [23]. T^3-CIDERS addresses the aforementioned skill gap in the near term by producing *future trainers* (FTs) who are equipped with working knowledge of CI fundamentals and ability to teach these skills to students and colleagues in their own communities. In a longer term, the development and infusion of these skillsets along with awareness of research in cybersecurity across many educational institutions in the nation would result in future cybersecurity workforce and researchers that are competent in the utilization of CI to support their mission and accelerate research in securing and defending cyber systems. This effort would ultimately foster a diverse community-of-practice consisting of FTs as well as cybersecurity experts, CI practitioners and CI professionals. T^3-CIDERS, therefore, is both a *train-the-trainer* and a *community building* program.

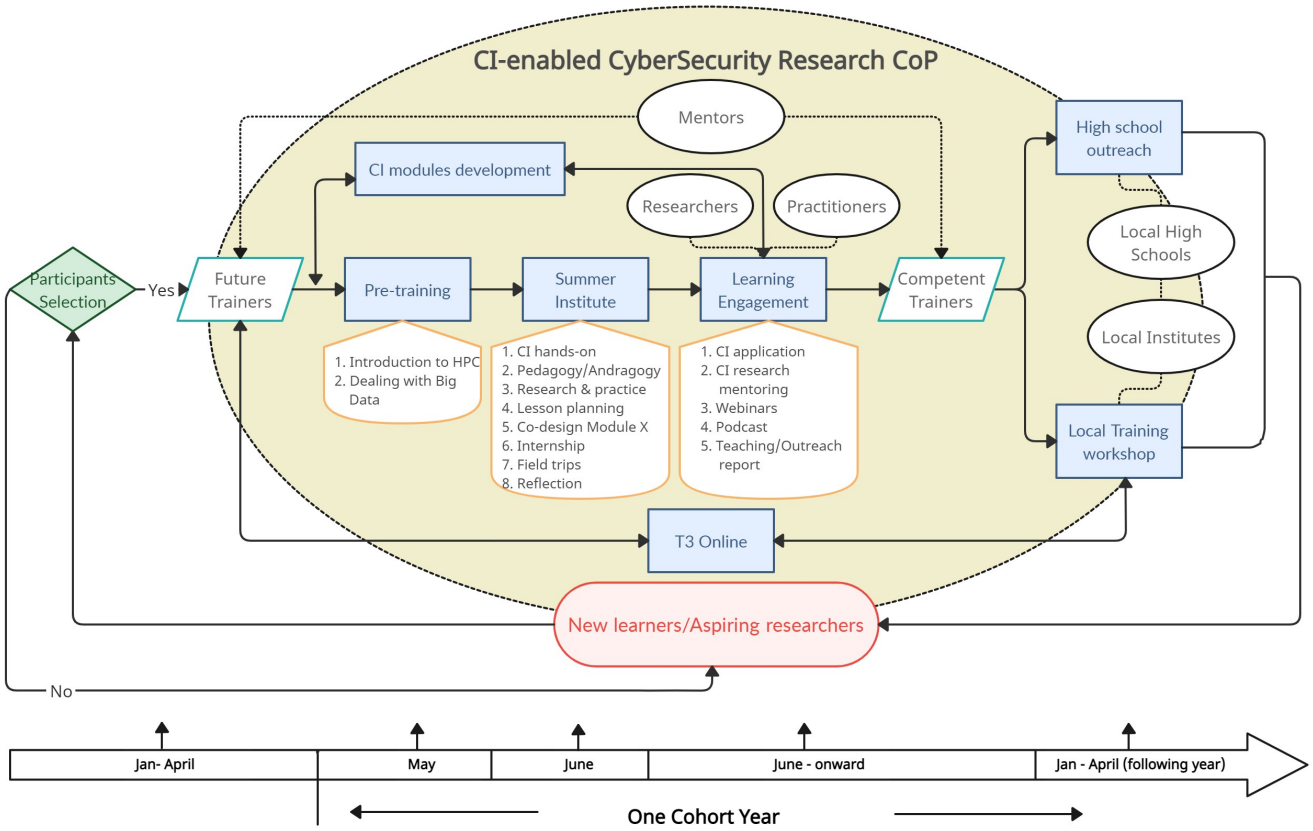

Figure 1: A schematic overview of T^3-CIDERS activities in the context of the community-building effort (signified by the large yellow oval). Rectangular blocks represent the major activities ("phases") of T^3-CIDERS described in the text. Small, white oval blocks represent parties and communities that are involved in, or impacted by, the activities. Through the series of activities, the *future trainers* would be trained to become *competent trainers* and part of the community of practice. (The timing of the activities was estimated at the inception of the project; the actual event timings are described in the text.)

2.2 Target Audience: The Future Trainers

As the target audience of the T^3-CIDERS program, the FTs are recruited from university faculty, researchers, students, and practitioners with interests in cybersecurity and cyber-related fields. As detailed later in this paper, the program engages these FTs as a cohort through a year-long engagement that is intended to be synergistic with research, teaching, and learning activities carried out by the FTs. As a prerequisite to participate in T^3-CIDERS, FTs need to possess basic problem-solving and computer programming skills, as well as an aptitude to learn to teach. Prior or current research and/or teaching experience in cybersecurity-related fields will be beneficial, as well as experience in using CI in these contexts. We do not assume, however, that FTs are experienced or skilled in CI methods, such as big data or machine learning, or have used HPC, as T^3-CIDERS curriculum provides matriculation in this area. As an integral required part of the program activities, the FTs must commit to conduct training activities transmitting these CI skills to others in their respective academic communities. To encourage collaboration, the FTs are clustered into "FT units" by pairing one faculty (or researcher) and one or two students. Finally, activities are planned within the program to encourage collaborations and community building among FTs as a CI- and cybersecurity-focused community of practice.

2.3 Program Structure

T^3-CIDERS is designed to train and engage the FTs through a year-long comprehensive program. The diagram in Fig. 1 shows the timeline of the program with all the interconnected parts. Altogether, these parts support the overarching endeavor to build up CI competencies and a community-of-practice of CI- and data-powered cybersecurity research. Besides the FTs and project team, T^3-CIDERS activities would also include and embrace existing cybersecurity researchers and practitioners to become part of the community. This comprehensive approach consists of six major activities, or *phases*: (1) Pre-training; (2) Summer Institute; (3) Learning Engagement; (4) Local Training; (5) K-12 Outreach; (6) Development of additional CI modules (also called "Module-X" to indicate the topics yet to be determined). Except for pre-training and summer institute, the rest of the phases do not take place in a strictly successive manner. T^3-CIDERS eventually aims to impact local institutions

and communities where the FTs reside through local training and K-12 outreach activities. The T^3-CIDERS training curriculum includes (1) foundational hands-on competencies in CI methods; (2) effective pedagogical and instructional design skills; (3) exposure to state-of-the-art cybersecurity research; and (4) collaborations and community building.

2.4 Major Phases and Contents

Phase 1: Pre-training. The pre-training focuses on CI skills baseline, covering HPC, Unix shell, Python/Jupyter, and Pandas. Two lesson modules from DeapSECURE (HPC and Big Data) were adapted and presented to FTs as a four-weeks long, self-paced, virtual training prior to the Summer Institute. The materials include text- and video-based lessons, journal and news articles, case studies, and hands-on Jupyter notebooks. Activities include group discussions on relevant cybersecurity issues and how HPC and big data can help address them. The intent of pre-training is to ensure that all the FTs gain the necessary hands-on skills and literacy for CI foundations in preparation for their time at the Summer Institute. Additionally, the pre-training lessons serve as (1) an exemplar of introducing CI platform or method to novice learners; and (2) resources for FTs to reuse or adapt for their own teaching activities.

Phase 2: Summer Institute. This phase serves as the cornerstone of the core "train-the-trainer" for the FTs. For the 2024 and 2025 cohorts, the Summer Institute takes place as an in-person, week-long event—July/August 2024 at ODU for the 2024 cohort, and planned to be at the University of Arizona in January 2026 for the 2025 cohort.[1] During this week, participants immerse themselves in both the technical (the "CI" contents) and pedagogical (the "T^3") components, facilitated by experts and peers alike. The in-person Summer Institute provides many opportunities for team building and social interactions which help FTs to network and lay the foundation for the subsequent engagements and collaborations. The contents of the institute for the 2024 cohort are as follows:

- **Brief overview of CI topics** drawn from DeapSECURE lessons: Machine Learning (traditional), Deep Learning, Cryptography (including homomorphic encryption), and Parallel Programming (total time: 8 hours). Each topic includes a lecture-style overview (about one hour long) and lab time using hands-on materials (Jupyter notebooks and activities on the HPC terminal; also about one hour long). Presently, some faculty members and students are familiar with machine learning and deep learning. Other contents, such as homomorphic encryption and parallel programming, may be unfamiliar to most FTs. The purpose of this overview is therefore for the FTs to acquire a broad perspective and basic understanding of the CI techniques, as well as initial hands-on experiences in these. Additionally, some strategies for teaching their learners, including the use of competitions and challenges, are presented to provide ideas for effective teaching.
- **Basics of education** (total time: 3 hours). This is a broad overview of education to teach the FTs the elements of effective teaching and education. The materials include common learning theories, instructional design, learning need analysis, defining learning objectives, assessment methods, instructional (teaching) methods, as well as technology tools that can be leveraged for teaching.
- **Demonstration of lesson planning, teaching, and assessment** (total time: 30 minutes). Our team member showcased an interactive demo of planning, delivery, and assessment of a hands-on lesson on a cybersecurity topic.
- **Studio sessions** (total time: 3 hours). During the studio sessions, FTs are guided to create a lesson plan for their own CI training, including defining the topic, target learners, learning objectives, and building the outline of the lesson. They are encouraged, but not required, to draw from resources provided by the DeapSECURE lessons.
- **Cybersecurity expert panel** (total time: 30 minutes), where we invite cybersecurity practitioners to have a panel discussion on current real-world cybersecurity challenges and pressing issues, as well as their solution strategies. This session is expected to offer valuable perspectives on how CI plays a role in the practical implementation of cybersecurity.
- **K-12 educator panel** (total time: 30 minutes). We invite a number of K-12 educators to discuss their experiences of teaching cybersecurity and technology-related contents to K-12 students. This activity provides an insight into the level of literacy and interest of cyber technology among today's youths, as well as effective ways to reach out to them.
- **Brainstorming on "Module-X"** (total time: 1 hour). This collaborative discussion between the FTs and the T^3-CIDERS team aims to identify additional training topics needed by the community to better address common gaps in preparing students for current research activities. Because cyber-technology and its security issues are rapidly evolving, research in cybersecurity and its skill requirements continue to change. While the core CI modules used in T^3-CIDERS facilitates competencies in basic CI skills (many of which are actually common to many disciplines), the community may need additional training modules that are geared toward specific cybersecurity research areas. This "Module-X" brainstorming is intended to uncover the needs, which will be followed up in further engagements to mobilize the FTs and the cybersecurity research community to build these additional training materials.
- **Demonstration of CI teaching by FTs** (total time: about 3 hours). This is the capstone activity at the end of the Summer Institute, where each FT unit presents a short demonstration of teaching based on the CI lesson plan built through the week. The demonstration is given in front of the entire cohort, which serves as the audience to the teaching, as well as provides feedback on the teaching session.

All these sessions (lectures, discussions, teaching demonstrations) were recorded and made available to the FT cohort for review at a later time.

[1] The institute may be offered in the winter or another time of the year due to practical reasons; but for convenience, we will colloquially refer to it as the *Summer Institute* in this paper.

Phase 3: Learning Engagement. By the end of the Summer Institute, the FTs would have completed an initial brainstorming of their own CI lesson plans and outlines. The FTs will continue completing the lesson plan and build out the lesson materials, drawing from the guidance and resources provided at the Institute. The T^3-CIDERS team will continue to engage them through virtual meetings to provide the necessary support for each FT team to complete and deliver their own local trainings. Furthermore, the project team plans to engage the FTs through a series of virtual meetings (about once a month) to further their CI journey together, through webinars, discussion panels, sharing of local training experiences. This ongoing engagement fosters an inclusive and supportive community of practice and encourages continuous professional development.

Phase 4: Local Training. As part of their enrollment with T^3-CIDERS, FT units are obligated to conduct local CI training activities at their own academic communities. This will be the delivery of the lessons planned by them during the Summer Institute. Since FTs come from different backgrounds and academic settings, these local training activities should be tailored to the needs observed at their own institutions. This training may take various formats, such as a hands-on CI+cybersecurity workshop similar to DeapSECURE workshop; a CI-focused webinar; one-on-one or small group CI mentoring in a research group; inclusion of CI method into a coursework and/or lab session; creation of a new coursework to teach a CI subject; competitions and hackathons. The specific kind of training to be conducted by a FT unit depends on the specific needs at their institution, the background of the students or mentees, as well as the desired outcomes of the training. Throughout continual engagement, the T^3-CIDERS team provides the necessary support to the FTs in preparation, logistics, assessments for the best learning experience. The FTs are encouraged to consider the long-term planning for CI-related knowledge infusion, so that these local training activities will be sustained beyond their cohort year.

Phase 5: K-12 Outreach. The formation of new workforce begins well before the students enter into their college education. As part of an optional activities of T^3-CIDERS, the FTs are strongly encouraged to promote awareness of cybersecurity, research in cybersecurity, and the role of CI to students at their local K-12 schools. Such outreach activities will open up the students' perspective and aspiration to pursue a potential career in the field of cybersecurity.

Phase 6: "Module X". The "Module-X" phase refers to the community-driven development of current and additional CI training modules that will collectively enrich the availability of CI training materials for the entire cybersecurity research and education community. This will entail long-term engagements of the T^3-CIDERS project, cohort members, and experts and practitioners to identify the gaps and build the training contents. During this phase, we will utilize the same design approach (described in the next section) by which T^3-CIDERS is built. Over time, this activity will grow the portfolio of cybersecurity-relevant CI training materials that the community can utilize to effectively onboard new members to participate in cutting-edge cybersecurity research and projects.

A Holistic Approach to Broaden CI Adoption in Cybersecurity. The six phases of T^3-CIDERS constitute a holistic approach toward broadening the adoption of CI in cybersecurity research and education. The first two phases (Pre-training and Summer Institute) provides the initial "boot camp" to raise up competent trainers. The Learning Engagement is an ongoing effort to foster the community connections among FTs and other researchers and practitioners. The Local Training, K-12 Outreach, and "Module X" activities are the expected outcomes and sustained activities facilitated by the T^3-CIDERS program. These phases engage the diverse constituents of cybersecurity community—researchers, educators, practitioners, experts, and students—and are expected to contribute toward the common goal of building a more secure digital society.

3 Program Design, Development, Evaluation

3.1 Design Process

In designing our program, we adapted the Successive Approximation Model (SAM) as shown in Figure 2, which consists of three phases: preparation, iterative design, and iterative development. During the preparation phase, we gathered as much background information as possible based on previous experiences, such as the prior DeapSECURE program, and conducted multiple rounds of content and context analyses. Due to the lack of access to our first cohort when we started the design process, we deployed a nine-stage iterative process to create ten learner personas with the facilitation of generative AI tools, including ChatGPT and Claude [12]. The learner personas provided invaluable insight and design empathy as we proceeded with the design content without actual learner data. Below we highlighted a couple of analysis phases:

- Harness AI-generated personas for inclusive design. Facing a critical challenge of designing an effective train-the-trainer program without direct access to initial learner data, we developed a nine-stage iterative process for creating and refining AI-generated personas following Kouprie and Visser's (2009) *Discover–Immerse–Connect–Detach* framework [11]. *Discover*: (1) Data collection; *Immerse*: (2) Initial LLM persona generation, (3) Ethical review, (4) Stakeholder feedback; *Connect*: (5) LLM persona refinement I, (6) LLM persona refinement II and new persona generation, (7) Persona evaluation and refinement III; *Detach*: (8) Training design; *Discover*: (9) Learner feedback and pilot testing.
- Conduct content and context analysis. The design team conducted multiple rounds of content and context analyses to finalize the scope and specific content with the insight of the training and performance contexts. For example, we conducted tasks analyses with guiding questions (such as, write the learning goals delineated in your training requirement analysis).

3.2 Content Development Process

Development of T^3-CIDERS training contents. The content development of the technical and pedagogical for T^3-CIDERS follows the abovementioned design process. This process took place in the Spring of 2024 for delivery at the 2024 Summer Institute. The Pre-Training and Summer Institute contents were organized and presented as a course on a Canvas platform and made accessible to the FTs before, during, and after the Summer Institute.

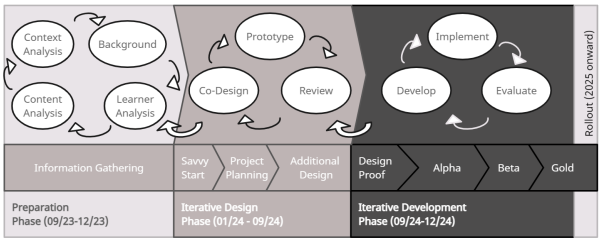

Figure 2: The iterative design and development process of T^3-CIDERS, which is roughly subdivided into three major phases: Preparation, iterative design, and iterative development. Refer to Sec. 3.1 for complete explanation.

Continuous improvement of technical modules (DeapSECURE). The "DeapSECURE" lesson modules receive continuous improvement during this project to mature them as ready-to-use lessons for wide deployment. The project PIs meet regularly on a weekly basis with several teaching assistants to polish the lessons and add new components that are deemed essential for new learners to acquire. Feedback received during the Summer Institute also propel the improvement of the lessons' usability. We expect that this process will be sustained through the adoption of these lessons by the FTs for their local teaching activities.

3.3 Plan of Assessment

Evaluation Formats. We use a multi-level and multi-phased evaluation approach before, during, and after the program. The evaluation includes both formative and summative plans with a mixed-method design for data triangulation. Formative evaluation focuses on the effectiveness; it will be conducted at different points of the program for continuous improvement. Summative evaluation focuses on the results and impacts of the entire project. Kirkpatrick's *Four-Level Evaluation* approach [10] will guide the design and implementation of the evaluation: (1) *Reaction*: Future trainers' engagement, perceived relevance of the program, and satisfaction; (2) *Learning*: The intended knowledge, skills, and attitude (KSA), confidence, and commitment acquired; (3) *Behavior*: FTs' application of what they learned during the training to their home institutions, also referred to as *transfer of training*; (4) *Results*: Desired outcomes achieved after the program. During the course of the project, T^3-CIDERS conducts multiple surveys and interviews to assess the program's contents and effectiveness, FTs' attitude, learning, and teaching plan. The detailed evaluation is described below:

Before the Program. A pre-survey was sent out to the FTs who were enrolled in the program before the training activities of their cohort commence. It includes questions to identify FTs' demographic characteristics, reactions toward the program, motivation, needs, and attitudes that need to be considered in designing and redesigning the program. It also provides insights into FT's target learners and helps us further tailor the content and instruction. Interviews were conducted with several FTs to understand their prior experiences, expectations, and attitudes toward the program. This qualitative data provided further insights into participants' needs.

During the Summer Institute. During the Summer Institute, observational notes were taken to track the FTs' behavior, interactions with peers, and engagements. This helped in assessing their involvement and learning application. FTs were requested to submit daily reflections, documenting their experiences and thoughts during the program. These help ensure that learning is an iterative process, with participants and our project team, continually improving their understanding and teaching methods. For example, during the 2024 Institute, some participants experienced challenges in absorbing the technical contents during the first day of the institute; however, they were able to review the complete T^3-CIDERS course materials hosted on Canvas. Therefore, we adjusted the schedule on the second day to make sure participants had enough time to review the course materials before introducing any technical content. Such timely feedback provides an effective channel for us to understand the states of each participant and steer the program on a daily basis.

After the Summer Institute. Following the Summer Institute, a post-institute survey was sent out to gauge FTs' satisfaction with the program, their views on the relevance of the content, and their confidence in applying the skills they acquired. These results were compared with the pre-survey to identify any shifts in attitudes and technical abilities that occurred throughout the program. After each FT unit conducts their local training or outreach activity, a survey will be distributed to their attendees to gather feedback and assess the effectiveness of their training efforts. Additionally, surveys and interviews will be conducted with the students taught by the FTs through their respective local training to evaluate how well the training has been transferred to their environments. As each cohort year comes to a close, we will begin examining the Return on Expectations (ROE). This will involve conducting semi-structured interviews with participants, the program coordinator, and training mentors to gather insights into their experiences, the program's structure, activities, content, and instructors.

4 The First Cohort Experience: Year 2024–2025

The call for the first cohort of T^3-CIDERS was issued in Spring 2024. We disseminated this announcement through various community channels: through Virginia's research computing professional network (MARIA), Commonwealth Cyber Initiative member network, and various cybersecurity researcher connections. In total, 8 faculty and researchers as well as 12 graduate and undergraduate students with varied backgrounds joined the first cohort and attended the 2024 Summer Institute. These FTs came from multiple states (Washington, Texas, Virginia, North Carolina, and New York) and types of institution (in regards to whether they are R1 research universities), reflecting the program's broad geographic reach from the first year.

4.1 Participant Background

Figure 3 shows the distribution of the FTs by their academic status: Six FTs were tenured or assistant professors, three held research positions, and the remaining are students—split almost evenly between graduate and undergraduate students. In terms of gender representation, 17 male and 3 female FTs were registered. Figure 4 shows the spread of study majors and/or research areas indicated by the FTs. Each FT may choose more than one area, therefore the sum of the frequencies is greater than the number of the FTs. The

choices of the subject areas and their frequencies illustrate a strong alignment of our proposed program to the research interests of the participants: with majority studying and/or researching cybersecurity topics, followed by AI, computer science, data science, and other computer-related fields. A handful came from business-oriented background. One FT self-identifies as an HPC system engineer, which was a unique addition to this cohort. The mutual focus in CI- and Cybersecurity-related topics serves as the cornerstone in building a community of practice of CI-competent cybersecurity researchers and scholars.

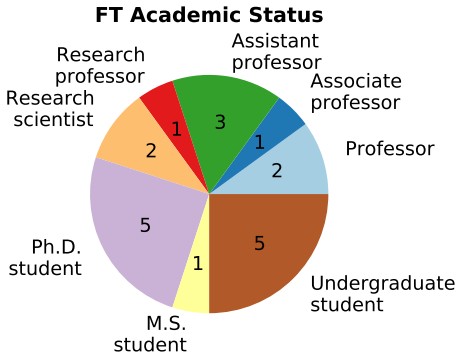

Figure 3: Academic status distribution of the 2024 cohort.

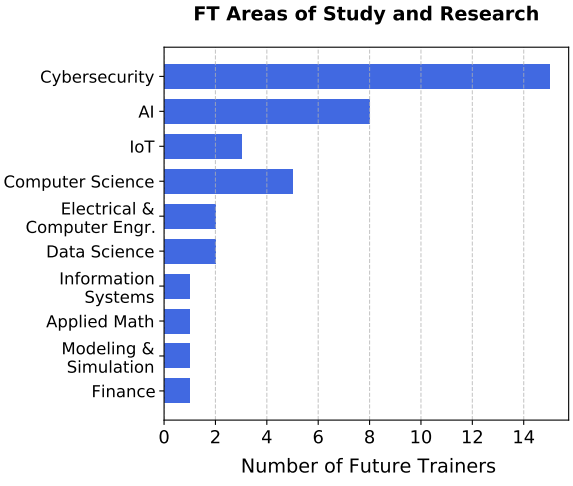

Figure 4: Areas of study or research indicated by the FTs (2024 cohort). Note that each participant may indicate multiple study and/or research areas.

4.2 Pre-Training and 2024 Summer Institute

The 2024 Summer Institute was conducted in July 29–August 2 at ODU campus ground in Norfolk, Virginia. Prior to attending the Summer Institute, The FTs were onboarded to a Discord group messaging platform used to facilitate discussions, ongoing collaborations, and community building. They also took the two pre-training modules (HPC and Big Data) hosted as a Canvas course. This same course was expanded throughout the Summer Institute to contain the rest of the T^3-CIDERS technical and pedagogical lesson materials. More details on the Summer Institute can be found in Refs. [23, 28].

4.3 Learning Engagement

After the Summer Institute and continuing through the end of each cohort year, the project team has been maintaining regular engagements with the FTs through virtual meetups. The initial engagements primarily focuses on following up the FTs' lesson plan development to monitor their progress on the lesson development and local training planning, providing feedback and support to help them refine their plans until the local training is implemented. From January 2025 onward, monthly research webinars and meetups are planned to engage both FT units and the broader community, allowing participants to present their research, share teaching experiences, and learn from each other. Additionally, we plan to invite external speakers to discuss recent advancements in HPC, education, cybersecurity research, etc., extending the reach of T^3-CIDERS to a wider community. The team also explored and discussed collaboration opportunities with and among the FTs, which would be continued beyond the cohort year.

4.4 "Module-X"

Beginning in Spring 2025, an ongoing engagement between the project team and the FTs has led to the identification of a potential topic at the intersection of AI and cybersecurity to be developed as the first "Module-X" lesson. This is a work in progress; we will report its outcome in a future publication.

4.5 Outcomes and Reflections

The evaluation process is ongoing as the cohort is completing their local training activities. However, we have been able to gather valuable feedback through daily reflections and pre-/post-Summer Institute surveys. During recruitment, we were surprised to find a significant interest from undergraduate students, indicating the program's appeal beyond the initially expected audience of graduate students and faculty. Their participation shows that the program can benefit students from a broader range of educational backgrounds with advanced CI training. The daily reflections offered immediate feedback, helping us refine and improve the program in real-time. These reflections also highlighted participants' enthusiasm and the diverse teaching activities they plan to implement after the training. Although it is challenging to predict the exact types of teaching and training that will result from the cohort's local efforts, the creative and varied plans shared by participants, as well as the lessons they demonstrated at the end of the Summer Institute, are promising.

An initial evaluation of the pre- and post-Institute surveys indicated encouraging results. For example, despite the small number of responses (16–20), we noted positive scores with little deviation in the FT's motivation and perception of teaching abilities for CI topics. The self-assessed knowledge of CI topics also was strongly

increased, as well as their confidence to apply and teach these. There are other areas which indicate the need for improvement, such as the expectation of the training as well as the relevance and value of the training.

Overall, the first Summer Institute was met with a very positive response. As the evaluation continues, the project team will use the feedback, along with their reflections, to enhance the content of future T^3-CIDERS offerings. We look forward to gaining more in-depth feedback through upcoming interviews and focus groups, which will help us better understand the program's long-term impact on participants' professional growth and how well they can apply what they have learned.

4.6 Future Cohorts

During the NSF project funding period, we plan to open at least two more cohorts. The next recruitment of 2025 cohort started in May 2025, and the next project institute will be held at the University of Arizona, Tucson, in January 2026. Additionally, the fully online adaptation of T^3-CIDERS is being designed and prepared, which will greatly increase the availability of this train-the-trainer program to a broader audience, irrespective of their geographical locations. The participants in the online adaptation will constitute another planned cohort.

5 Development of T^3-Online Program

T^3-CIDERS Online (or also known as "T^3-Online") is a self-paced asynchronous course specifically designed for online FTs who seek to sharpen their CI technical and pedagogical competencies. T^3-Online is currently under design and preparation based on the lessons learned in the first cohort. T^3-Online will become an OER (Open educational resources) available publicly, targeting cybersecurity research and education communities nationwide and internationally. The development of T^3-Online will be an ongoing task for continuous improvement. We plan to adapt SAM [3] with three major phases, as shown earlier in Fig. 2, to leverage the feedback from our participants and experts in iterative design and development of the T^3-Online program.

T^3-Online will be offered to those who are interested in this program but are not able to travel to attend it in person in 2025 and 2026 cohorts. At the end of the Summer Institute in 2024, there are already two teams signed up for the T^3-Online waiting list due to the time conflict to travel to ODU in summer 2024. Those participating in T^3-Online will attend our post-Summer Institute events such as virtual learning engagements. We plan to begin testing the T^3-Online by the end of 2025 and roll out the course starting in 2026. Upon project completion, T^3-Online will be available to the public beyond 2026.

6 Conclusion

T^3-CIDERS [24] is a holistic, community-focused initiative that has already made a significant impact on the growing and systemic need for advanced CI expertise in cybersecurity research and education. T^3-CIDERS is a train-the-trainer that aims to build community around the practice of CI and cybersecurity research. Its holistic approach consists of six major phases: (1) Pre-training; (2) Summer Institute; (3) Learning Engagement; (4) Local CI Training; (5) K-12 Outreach; (6) "Module-X" (community-driven development of additional CI training modules). In the first cohort (2024), eight faculty and professionals have participated in its first Summer Institute as *future trainers* (FTs) along with twelve students. Several local trainings have been successfully completed by the FTs in their own institutions. Building on our earlier cybertraining program "DeapSECURE" [20], T^3-CIDERS provides comprehensive training to prepare the current and future generation of cybersecurity professionals to tackle emerging challenges through the skillful use of advanced CI. Through the "Module-X" activity facilitated by T^3-CIDERS, new technical CI contents are being developed with the input from FT units and fostering a supportive community of practice as evidenced through the ongoing engagement activities between the project and FT units. The positive feedback from the Summer Institute participants and their local training activities speak further that T^3-CIDERS program is on the right track to reach its objectives in promulgating CI skills in the fabric of cybersecurity education and workforce development.

Acknowledgments

Funding for this program comes from the U.S. National Science Foundation CyberTraining grants #2320998 and 2320999. The authors graciously acknowledge the support from ODU School of Cybersecurity for hosting the 2024 Summer Institute, and ODU Research and Cloud Computing group for the use of their Wahab HPC cluster for conducting the CI training activities. The Wahab cluster is supported in part by National Science Foundation's grant CNS-1828593, "MRI Acquisition: A Reconfigurable Computing Infrastructure Enabling Interdisciplinary and Collaborative Research in Hampton Roads". We also gratefully acknowledge the contributions of our teaching assistants and project coordinators to the success of this program: Jiawei Chen, Sylvia Cooper, Kayla Curtis, Kristin Herman, Chunyu Hu, Nolan Lovett, Dorothy Parry, Jael Perales, Elexiah Smart. The authors thank Dr. Nitin Sukhija from Slippery Rock University of Pennsylvania for his review of the pre-training materials.

References

[1] ACCESS 2022. *Advanced Cyberinfrastructure Coordination Ecosystem: Services & Support (ACCESS).* https://access-ci.org/

[2] Shaaron Ainsworth, Margaret Honey, W. Lewis Johnson, Kenneth R. Koedinger, Brandon Muramatsu, Roy D. Pea, Mimi Recker, and Stephen Weimar. 2005. Cyberinfrastructure for Education and Learning for the Future: a vision and research agenda. https://telearn.hal.science/hal-00190625 Computing Research Association report.

[3] Michael Allen and Richard Sites. 2012. *Leaving ADDIE for SAM: An agile model for developing the best learning experiences.* Association for Talent Development.

[4] Timothy J. Boerner, Stephen Deems, Thomas R. Furlani, Shelley L. Knuth, and John Towns. 2023. ACCESS: Advancing Innovation: NSF's Advanced Cyberinfrastructure Coordination Ecosystem: Services & Support. In *Practice and Experience in Advanced Research Computing 2023: Computing for the Common Good* (Portland, OR, USA) *(PEARC '23).* Association for Computing Machinery, New York, NY, USA, 173–176. doi:10.1145/3569951.3597559

[5] Cybersecurity and Infrastructure Security Agency. 2025. *CISA Artificial Intelligence Use Cases.* Retrieved 2025-06-14 from https://www.cisa.gov/ai/cisa-use-cases

[6] Cybersecurity and Infrastructure Security Agency. 2025. *CISA Cybersecurity Education and Career Development.* Retrieved 2025-06-14 from https://www.cisa.gov/resources-tools/programs/cybersecurity-education-career-development

[7] Bahador Dodge, Jacob Strother, Rosby Asiamah, Karina Arcaute, Dr. Wirawan Purwanto, Dr. Masha Sosonkina, and Dr. Hongyi Wu. 2022. DeapSECURE Computational Training for Cybersecurity: Third Year Improvements

and Impacts. http://www.modsimworld.org/papers/2022/MSVSCC_2022_InfrastructureSecurityMilitary.pdf

[8] Jan Herrington and Ron Oliver. 2000. An Instructional Design Framework for Authentic Learning Environments. *Educational Technology Research and Development* 48, 3 (2000), 23–48. doi:10.1007/BF02319856

[9] Curtis M. Keliiaa and Jason R. Hamlet. 2010. *Assessment of Current Cybersecurity Practices in the Public Domain: Cyber Indications and Warnings Domain.* Technical Report SAND2010-4765. Sandia National Laboratories, Albuquerque, NM. doi:10.2172/992337

[10] James D Kirkpatrick and Wendy Kayser Kirkpatrick. 2016. *Kirkpatrick's Four Levels of Training Evaluation.* Association for Talent Development.

[11] Merlijn Kouprie and Froukje Sleeswijk Visser. 2009. A Framework for Empathy in Design: Stepping into and out of the User's Life. *Journal of Engineering Design* 20, 5 (2009), 437–448. doi:10.1080/09544820902875033

[12] Nolan Lovett, Mohan Yang, Kristin Herman, Belle Li, Masha Sosonkina, Wirawan Purwanto, Peng Jiang, and Hongyi Wu. 2025. Harnessing AI-Generated Personas for Inclusive and Engaging Training Design. *Journal of Applied Instructional Design* (2025). Manuscript under review.

[13] Willian Tessaro Lunardi, Martin Andreoni Lopez, and Jean-Pierre Giacalone. 2022. Arcade: Adversarially regularized convolutional autoencoder for network anomaly detection. *IEEE Transactions on Network and Service Management* 20, 2 (2022), 1305–1318.

[14] Luca Mainetti and Andrea Elia. 2025. Detecting Personally Identifiable Information Through Natural Language Processing: A Step Forward. *Applied System Innovation* 8, 2 (2025), 55.

[15] Madhav Mukherjee, Ngoc Thuy Le, Yang-Wai Chow, and Willy Susilo. 2024. Strategic approaches to cybersecurity learning: A study of educational models and outcomes. *Information* 15, 2 (2024), 117.

[16] NAIRR 2023. *The National Artificial Intelligence Research Resource (NAIRR) Pilot.* https://nairrpilot.org/

[17] National Science Foundation. 2025. *NSF Cybersecurity Focus Area.* Retrieved 2025-06-14 from https://www.nsf.gov/focus-areas/cybersecurity

[18] National Security Agency. 2025. *NSA Centers of Academic Excellence.* Retrieved 2025-06-14 from https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

[19] Wirawan Purwanto, Bahador Dodge, Karina Arcaute, Masha Sosonkina, and Hongyi Wu. 2024. DeapSECURE Computational Training for Cybersecurity Students: Progress Toward Widespread Community Adoption. *The Journal of Computational Science Education* 15 (2024), 2–9. Issue 1. https://doi.org/10.22369/issn.2153-4136/15/1/1

[20] Wirawan Purwanto, Issakar Doude, Yuming He, Jewel Ossom, Qiao Zhang, Liwuan Zhu, Jacob Strother, Rosby Asiamah, Bahador Dodge, Orion Cohen, Jiawei Chen, Chunyu Hu, Dorothy Parry, Peng Jiang, Masha Sosonkina, and Hongyi Wu. 2024. DeapSECURE Lesson Modules. https://deapsecure.gitlab.io/lessons/

[21] Wirawan Purwanto, Yuming He, Jewel Ossom, Qiao Zhang, Liuwan Zhu, Karina Arcaute, Masha Sosonkina, and Hongyi Wu. 2021. DeapSECURE Computational Training for Cybersecurity Students: Improvements, Mid-Stage Evaluation, and Lessons Learned. *The Journal of Computational Science Education* 12 (2021). Issue 2. https://doi.org/10.22369/issn.2153-4136/12/2/1

[22] Wirawan Purwanto, Hongyi Wu, Masha Sosonkina, and Karina Arcaute. 2019. DeapSECURE: Empowering Students for Data- and Compute-Intensive Research in Cybersecurity through Training. In *Proceedings of the Practice and Experience in Advanced Research Computing on Rise of the Machines (learning)* (Chicago, IL, USA) *(PEARC '19)*. ACM, New York, NY, USA, Article 81, 8 pages. doi:10.1145/3332186.3332247

[23] Wirawan Purwanto, Mohan Yang, Peng Jiang, Masha Sosonkina, and Hongyi Wu. 2024. T3-CIDERS: Fostering a Community of Practice in CI- and Data-Enabled Cybersecurity Research through a Train-the-Trainer Program. In *Eleventh SC Workshop on Best Practices for HPC Training and Education (BPHTE'24).* https://sc24.conference-program.com/presentation/?id=ws_bphpcte103&sess=sess752 Article accepted for publication on The Journal of Computational Science Education.

[24] Wirawan Purwanto, Mohan Yang, Peng Jiang, Masha Sosonkina, Hongyi Wu, Jael Perales, and Kayla Curtis. 2024. T3-CIDERS Project Website. https://sites.wp.odu.edu/t3-ciders/

[25] Mubashrah Saddiqa, Kristian Helmer Kjær Larsen, Robert Nedergaard Nielsen, and Jens Myrup Pedersen. 2023. Building a diverse cybersecurity workforce: A study on attracting learners with varied educational backgrounds. *Journal of Cybersecurity Education, Research & Practice* 2024, 1 (2023).

[26] Jay Sinha and M Manollas. 2020. Efficient deep CNN-BiLSTM model for network intrusion detection. In *Proceedings of the 2020 3rd International Conference on Artificial Intelligence and Pattern Recognition.* 223–231.

[27] Craig A. Stewart, Stephen Simms, Beth Plale, Matthew Link, David Y. Hancock, and Geoffrey C. Fox. 2010. What is cyberinfrastructure. In *Proceedings of the 38th Annual ACM SIGUCCS Fall Conference: Navigation and Discovery* (Norfolk, Virginia, USA) *(SIGUCCS '10).* Association for Computing Machinery, New York, NY, USA, 37–44. doi:10.1145/1878335.1878347

[28] T3-CIDERS Team. 2024. *2024 Summer Institute Report.* Retrieved 2025-06-26 from https://sites.wp.odu.edu/t3-ciders/summer-institute-2024/

[29] Binh Tran, Karen C Benson, and Lorraine Jonassen. 2023. Integrating Certifications into the Cybersecurity College Curriculum: The Efficacy of Education with Certifications to Increase the Cybersecurity Workforce. *Journal of Cybersecurity Education, Research and Practice* 2023, 2 (2023).