Engineering Educators Bringing the World Together
2025 ASEE Annual Conference & Exposition
Palais des congrès de Montréal, Montréal, QC • June 22–25, 2025 ASEE
Paper ID #46880

International Cybersecurity Exercise: A Model for Collaborative Cyber Defense Education

Dr. Douglas W. Jacobson, Iowa State University of Science and Technology

Doug Jacobson is a University Professor in the Department of Electrical and Computer Engineering at Iowa State University. He is currently the director of the Iowa State University Center for Cybersecurity Innovation and Outreach, which has been recognized by the National Security Agency as a center of academic excellence. He has worked for years on ways to include cybersecurity in courses and the general population. Doug also created the Iowa Cyber Hub, which is dedicated to increasing the cyber workforce in Iowa. Doug has given over 300 presentations in the area of computer security. He also created the cybersecurity ambassador program targeted at the public, K-12 students, post-secondary students, and employees and is leading an effort to create a series of short videos called Cyber House Rock that help teach cybersecurity and digital safety to the public.

International Cybersecurity Exercise: A Model for Collaborative Cyber Defense Education

Abstract

This paper presents the International Cybersecurity Exercise (ICE), now named the International Cyber Defense Challenge (ICDC), a collaborative initiative started in 2022 and led by Iowa State University in partnership with the Iowa National Guard, Kosovo Security Forces, and academic institutions from the U.S., Kosovo, Northern Macedonia, and Albania. Modeled after the university's highly successful Cyber Defense Competitions (CDC), which have been held since 2005, ICE integrates U.S. high school, community college, and university teams with collegiate teams from overseas. The event engages students in a realistic, high-stakes cyber defense exercise. Teams defend networks against adversarial attacks in a virtual environment that simulates critical infrastructure scenarios, such as power grid protection.

The international exercise emphasizes active learning through a defense and survivability exercise following the CDC framework. Teams design security architectures and defend them against adversarial attacks while maintaining operational services. Leveraging a custom-built cyber range hosted by Iowa State University, the exercise enables continuous training and experiential learning outside competition periods.

This paper details the learning materials developed to support participants, how the event operates, and the outcomes from three years of competition. The exercise also strengthened international collaboration, leveraging National Guard State Partnership Programs to connect educational and military communities across borders.

Following the CDC framework, the exercise employs a design, build, and defend model in which participants construct and safeguard their networks against adversarial attacks while maintaining operational services. This paper outlines the structure of the exercise, including the scenario design process, the integration of real-world challenges, and the pedagogical goals behind fostering experiential learning and cybersecurity skills.

Plans for the exercise include expanding to additional Adriatic countries and integrating their respective National Guard units, further enhancing international collaboration through the U.S. State Partnership Program. The exercise has proven to be a scalable and effective model for cybersecurity education, bridging academic institutions and military units to develop a robust, globally aware cybersecurity workforce.

The results underscore the effectiveness of experiential learning in cybersecurity education and demonstrate the potential of the ICE to serve as a scalable model for workforce development and global collaboration in engineering education. This work contributes to the growing research on innovative curriculum design and experiential learning strategies within electrical and computer engineering (ECE) programs.

Introduction

The International Cybersecurity Exercise represents a groundbreaking approach to collaborative cybersecurity. Initiated in 2022 by Iowa State University, the exercise brings together a diverse network of participants, including the Kosovo Security Forces, the Iowa National Guard, and academic institutions from the U.S., Kosovo, Northern Macedonia, and Albania. By integrating collegiate teams from these countries with U.S. high school, community college, and university teams, ICE fosters a unique blend of international collaboration and experiential learning in cybersecurity.

After the 2024 event, the International Cybersecurity Exercise (ICE) was renamed the International Cyber Defense Challenge (ICDC). This change was made to align the name with the four other Cyber Defense Challenges (CDCs) hosted annually and to avoid confusion with the acronym ICE. For consistency in this paper, we will refer to the event as ICDC.

The International Cybersecurity Exercise builds on Iowa State University's successful Cyber Defense Competition (CDC) model, which has provided hands-on cybersecurity training since 2005. With over 90 competitions, the CDC framework emphasizes technical rigor, usability, and real-world defense strategies. Iowa State University hosts five CDCs annually, engaging students at the university, community colleges, and high schools, with ICDC serving as its international extension. The CDC model has consistently demonstrated its effectiveness in preparing participants for the evolving cybersecurity landscape [1,2]. ICDC expands the CDC's core principles of defense, survivability, and teamwork globally by bringing together students and professionals to tackle high-stakes cybersecurity challenges.

ICDC's primary objectives are fostering collaboration across borders, enhancing cybersecurity education through hands-on experiences, and equipping participants with practical defense skills. These goals align closely with the pedagogical principles of experiential learning, ensuring that participants gain technical expertise and critical soft skills like communication, teamwork, and resilience under pressure.

ICDC also exemplifies the potential of collaborative frameworks such as the National Guard State Partnership Program [3], which has served as a cornerstone of this initiative. By leveraging these partnerships, the exercise strengthens ties between military and educational institutions, enabling a cross-cultural exchange of knowledge and best practices. This integration fosters a globally aware cybersecurity workforce capable of addressing emerging challenges in a rapidly evolving threat landscape.

As ICDC continues to expand its scope, it aims to involve additional Adriatic countries and their respective National Guard units, reinforcing its role as a scalable and impactful model for cybersecurity education. Through its innovative design and global reach, ICDC not only advances the state of cybersecurity training but also highlights the transformative power of international collaboration in addressing one of the most pressing challenges of our time.

This paper explores ICDC's structure, methodology, and outcomes, underscoring its effectiveness as a model for workforce development and cross-border cooperation in cybersecurity education.

Background and CDC Overview

A key factor in the ICDC's effectiveness is its reliance on the Cyber Defense Competition (CDC) model, which provides a structured, hands-on learning environment. The following section details the CDC framework, the roles of participating teams, and the cyber range technology that facilitates realistic attack-and-defense scenarios.

Central to the success of these competitions is the use of the Internet-Scale Event and Attack Generation Environment (ISEAGE), a state-of-the-art cyber range developed by Iowa State University. This testbed provides participants with an isolated, virtualized environment to experience authentic network traffic and attacks. ISEAGE supports offensive and defensive operations, allowing participants to develop skills in network configuration, system hardening, and real-time incident response [5]. Figure 1 provides a visual overview of the ISEAGE environment used during the competition.

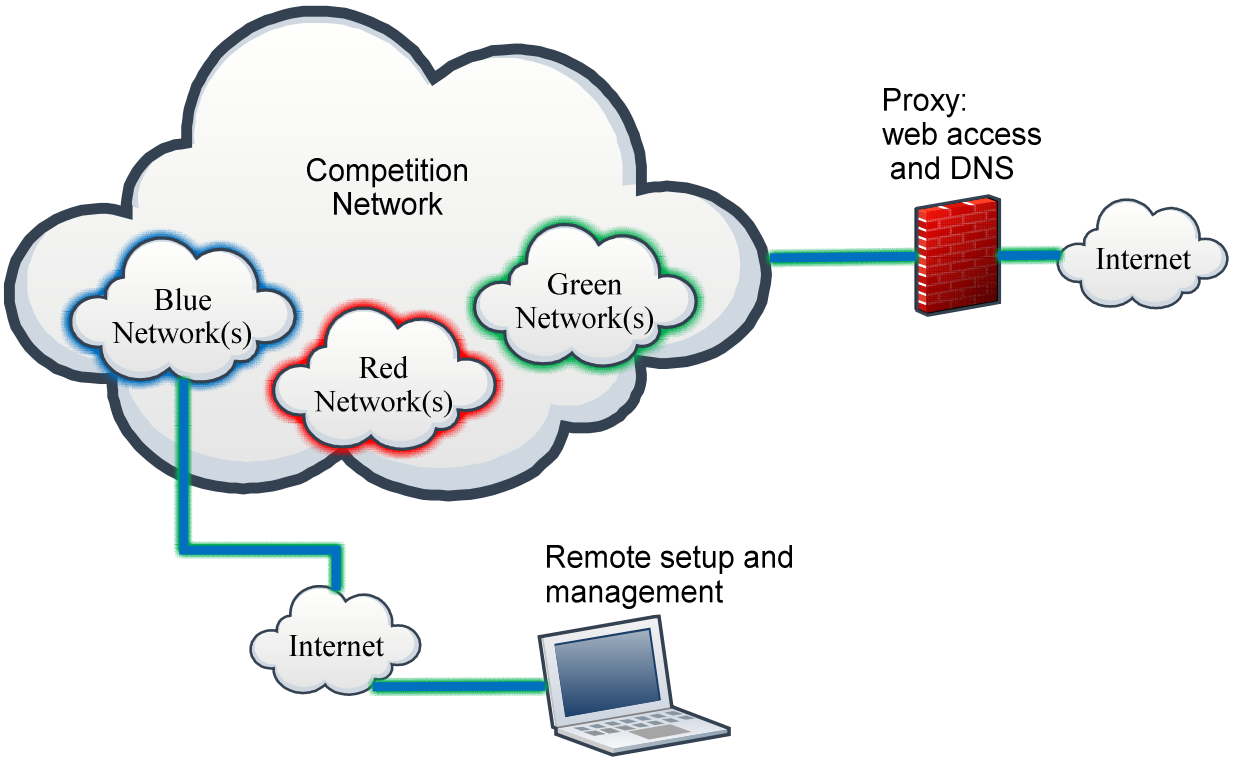

Figure 1. ISEAGE environment

ISEAGE creates a controlled virtual environment replicating the Internet, allowing participants to design, secure, and defend networks without impacting real-world systems. With its advanced capabilities, ISEAGE supports remote access, which enables participants and administrators from different locations, including international sites, to engage seamlessly in the competition.

This feature is especially critical for events like the International Cyber Defense Challenge, where teams from multiple countries participate simultaneously.

ISEAGE facilitates secure and limited Internet access through its air-gap gateway and proxy servers, ensuring participants can interact with necessary external resources without compromising the integrity of the competition network. For example, teams can perform DNS lookups or access websites through a controlled proxy. This functionality allows students to integrate Internet-dependent services into their networks while maintaining a safe and isolated environment. The testbed also incorporates robust monitoring systems, including the IScorE platform, which tracks the availability and functionality of Blue Team services during the competition. These tools ensure fair scoring and provide real-time feedback on team performance.

ISEAGE's architecture supports the four-team structure central to the Cyber Defense Competition (CDC) model, with dedicated virtual networks for the Blue (defense), Red (attack), Green (user), and White (judge) teams. Each team operates within its isolated subnet, interconnected through the competition network, ensuring realistic interaction while maintaining role-specific focus. ISEAGE also provides debugging and management tools for the White Team, allowing for seamless oversight and troubleshooting throughout the event. These advanced features create an immersive, high-fidelity training environment that mirrors real-world cybersecurity operations.

The CDC model is designed to replicate real-world cybersecurity dynamics, with each team playing a critical role in the exercise. Their specific responsibilities are outlined below:

1. **Blue Team (Defenders):** Comprising student participants, the Blue Team is tasked with designing, implementing, and maintaining a secure network based on the competition's scenario. They act as the organization's IT and security professionals, defending their systems from attacks while ensuring operational continuity for essential services. Their role requires technical skills, strategic planning, and adaptability to respond to emerging threats. We also allow a guest division, which, for the ICDC, comprises teams from the Kosovo security forces and the Iowa National Guard. The only difference for a guest team is that they are not competing for trophies.
2. **Red Team (Attackers):** The Red Team comprises cybersecurity professionals and experienced hackers who simulate real-world adversaries. Their mission is to exploit vulnerabilities in the Blue Team's systems, testing the robustness of the defensive measures. The Red Team employs various attack techniques, from penetration testing to social engineering, providing an authentic and high-pressure environment for the defenders. The National Guard also provides red team members for the International Cybersecurity Exercise.
3. **Green Team (Users):** Representing the everyday users of an organization's IT systems, they interact with the network and services the Blue Team provides. They perform routine activities such as sending emails, accessing websites, and using file-sharing services. Their feedback on usability and availability contributes to the scoring, emphasizing the importance of maintaining functional and user-friendly systems under attack.

4. **White Team (Judges and Overseers):** Acting as the referees and administrators, the White Team oversees the competition, ensuring adherence to the rules and objectives. They monitor team performance, resolve disputes, inject anomalies, and score the Blue Team based on their ability to secure systems, provide services, and recover from attacks. The White Team plays a crucial role in maintaining the fairness and integrity of the competition. The white team comprises around seven undergraduates who are paid to develop and run the 5 CDCs we host yearly. In addition, members of the Iowa National Guard are on site in Kosovo to help run the event and deal with any issues.

The ICDC timeline

Pre-event: The International Cyber Defense Challenge begins weeks before the competition with the release of a detailed scenario outlining the organization's infrastructure, objectives, and security challenges. Teams use this time to design and implement their defensive strategies, including configuring prebuilt systems, setting up new servers, and documenting their network architectures within the ISEAGE environment. This preparatory phase allows participants to familiarize themselves with the tools and requirements of the competition.

Scenarios are crafted to simulate real-world organizational challenges, such as defending a financial system, securing critical infrastructure, or protecting sensitive data during a cyber crisis. The scenario includes a detailed description of the organization, its IT assets, and the services it must provide. These elements guide the Blue Team in designing their defense strategies and network architecture. In 2024, we also produced a short video to introduce the scenario to the blue teams and to explain the scenario in simple terms.

In the three weeks leading up to the competition, the Blue Team is provided with a mix of prebuilt systems and the opportunity to build additional systems to meet the scenario's requirements within the ISEAGE environment. The prebuilt systems often include legacy servers, outdated software, or misconfigured devices that mimic real-world constraints, such as budget limitations or inherited vulnerabilities. Teams must evaluate these systems, apply patches, and reconfigure them for security and efficiency.

Simultaneously, the Blue Team creates new systems to deliver the required services, such as web servers, email platforms, or file-sharing networks. This phase allows participants to experiment with various tools and technologies, implement firewalls and intrusion detection systems, and establish access controls. Teams also document their configurations and decisions, preparing reports that the White Team reviews before the competition begins.

We provide learning materials through our Innovate-IT website [6], which schools that are new to the CDC-style exercises use. We also have a support website [7], which provides access to the rules and additional setup information. The white team also maintains a Discord server to answer questions and provide additional support.

This preparatory period is crucial for fostering collaboration, honing technical skills, and instilling a sense of ownership among participants. It ensures that the competition is a test of

defensive capabilities and a comprehensive learning experience reflecting real-world cybersecurity challenges' complexities.

Exercise: On the event day, the competition phase starts, an intense eight-hour attack session, during which the Blue Teams (defenders) must maintain service availability while fending off sophisticated attacks from the Red Team (attackers). Simultaneously, the Green Team (users) interacts with the systems to ensure usability, and the White Team (judges) monitors compliance with competition rules and records scoring data.

During the competition, the white team will introduce anomalies that are intentional, real-world-inspired disruptions introduced during the International Cybersecurity Exercise to test participants' adaptability and problem-solving skills. These events simulate unexpected challenges that cybersecurity professionals might face, such as system failures, insider threats, or sudden requests for configuration changes. Examples of anomalies include fire drills requiring teams to leave their workstations, mandated installation of insecure software, or simulated physical tampering with network hardware. Anomalies introduce complexity and encourage teams to balance their defensive strategies with maintaining service availability and responding to dynamic organizational needs. Their inclusion ensures the competition reflects the unpredictable nature of real-world cybersecurity environments.

We also use Twitch to provide a way for the two sets of blue teams to see what is happening. We project the feed from Kosovo into the blue team room. The Twitch feed and the public-facing scoring system also allow spectators to view the competition.

The scoring system (IScorE) is a way to show real-time scoring and indication of the participating teams' technical, strategic, and operational capabilities. Points are distributed across multiple categories, including service uptime, documentation, anomaly responses, usability, and Red Team interactions. IScorE also serves as a way for spectators and teams to keep track of the system's current status and point totals. The scoring system is outlined below.

- **Service uptime**, which accounts for 20% of the overall score, is monitored by an automated system, IScorE, that checks the availability of required services every five minutes. Teams earn points for consistently operational services, emphasizing maintaining functionality under attack.
- **Flags**, representing critical data or system elements, are another significant component of scoring, contributing 20% to the overall score. Blue Teams start with full credit for their flags, but each flag captured or planted by the Red Team deducts 100 points. To mitigate this loss, Blue Teams can submit detailed reports explaining how the compromise occurred, the actions taken to resolve the issue, and measures to prevent future breaches. Based on the quality of these reports, teams can recover up to 50 points per flag.
- **Documentation** also plays a crucial role, accounting for 10% of the score. Teams must submit White Team documentation, which details their network design and security measures, and Green Team documentation, which provides user-friendly instructions for accessing and using network services. These documents' thoroughness, clarity, and professionalism significantly influence the scoring.

- Additionally, **intrusion reports** submitted during the competition allow Blue Teams to analyze and document detected attacks. These reports, worth 5% of the total score, are evaluated based on their detail, evidence, and proposed mitigation strategies.
- The **Green Team**, representing users, contributes 20% of the score through usability evaluations. They assess the accessibility and functionality of the Blue Team's services, highlighting the balance between security and usability.
- Finally, **anomalies** simulate real-world IT challenges, accounting for 15% of the score. Successfully addressing anomalies requires teams to demonstrate adaptability and problem-solving skills under pressure. The Red Team also provides an evaluation score (10%) based on the Blue Team's security measures, responses, and overall conduct during the competition.

This multi-faceted scoring system ensures that teams are evaluated on their technical acumen and ability to communicate effectively, adapt to challenges, and maintain operations based on the scenario.

Debrief and awards: The event concludes with a debrief and award ceremony following the attack phase. The debrief is a critical component of the exercise, serving as a reflective and educational conclusion to the competition. During this session, members of the Red Team (attackers) share insights into their strategies to exploit vulnerabilities, providing the Blue Teams (defenders) with valuable feedback on their defensive measures. Participants discuss what worked well, areas for improvement, and lessons learned from both sides. The debrief also allows judges (White Team) to provide an overview of the competition, highlight exceptional performances, and clarify scoring decisions. This collaborative dialogue fosters a deeper understanding of cybersecurity principles, equipping participants with practical knowledge to apply in future scenarios. We use a Zoom link to allow a joint debriefing.

Analysis of the First Four Years of ICDC

Over four years, ICDC has engaged diverse teams of students, faculty, and professionals from multiple countries, including the United States, Kosovo, Northern Macedonia, and Albania. With each iteration, the exercise has expanded its scope, refined its methodologies, and enhanced its impact. The table below shows the growth of the exercise.

Teams	2022	2023	2024	2025
Kosovo	10	8	16	14
Northern Macedonia			1	1
Albania			1	2
Iowa State University	3	2	2	3
U.S. High schools	2	3	3	4
U.S. Community Colleges	1	1	3	3
Other U.S. universities			4	4
Total	16	14	30	31

Below, we examine the successes, challenges, and lessons learned from the first four years of ICDC. By analyzing participant feedback, technical outcomes, and organizational improvements,

we explore how the program has matured into a model for experiential learning and international collaboration. From its initial focus on network defense in 2022 to the integration of critical infrastructure scenarios in 2024, ICDC has consistently pushed the boundaries of cybersecurity education, offering participants a realistic, high-pressure environment to hone their skills. The following analysis highlights key milestones and insights from each year, setting the stage for continued growth and innovation in 2026 and beyond.

2022 ICDC Highlights:

The inaugural International Cybersecurity Exercise in May of 2022 focused on providing participants with a robust introduction to network design and defense of network systems. The exercise featured a scenario that tasked teams with securing the systems of a fictional financial trading platform, requiring a comprehensive approach to cybersecurity. Participants engaged in tasks such as hardening legacy systems, configuring secure services, and mitigating vulnerabilities in an environment designed to simulate real-world challenges. The event emphasized the importance of technical expertise and strategic decision-making, creating a well-rounded educational experience.

Despite being the first iteration, the 2022 exercise was successful, marked by minimal connectivity issues and strong participant engagement. Feedback highlighted the value of the hands-on learning experience, with students and faculty praising the realism and complexity of the exercise. However, the event also revealed areas for improvement, particularly in communication and scheduling. These insights provided a foundation for refining future exercises, ensuring smoother operations and enhanced participant experiences in subsequent years.

2022 Scenario: Securing a Financial Trading Platform

The 2022 International Cybersecurity Exercise centered on a fictional company, Creating Diverse Currencies Inc., specializing in retail trading and stock management. Participants were tasked with performing a comprehensive security audit and hardening the company's IT infrastructure. The scenario involved securing several critical systems, including:

- **Active Directory (AD):** Centralized authentication for the organization's users, ensuring secure user management and LDAP queries.
- **Database Server:** A PostgreSQL database running on an outdated Ubuntu system that stored sensitive financial data and user accounts.
- **Website:** The main interface for users to conduct stock trading and manage investments consists of a React-based and Node.js backend.
- **GitLab Server:** A repository hosting the company's custom trading code, requiring rigorous access control for developers and administrators.
- **IoT Smart Plug:** A simulated IoT device controlling essential services, highlighting the vulnerabilities of connected devices.

Participants defended these systems from adversarial attacks while ensuring system availability for legitimate users, emphasizing the criticality of secure coding practices and infrastructure resilience.

2023 ICDC Highlights:

The second year of the ICDC, held in May of 2023, built on the successes of its predecessor while introducing new elements to enhance the experience. Participation expanded to include additional Iowa State University and Kosovo teams, reflecting a growing interest in the exercise. The scenario for 2023 focused on protecting the network infrastructure of a fictional corporate distribution company, presenting participants with challenges such as mitigating insider threats, securing outdated systems, and improving fault tolerance. Teams were required to balance defense with usability, ensuring their systems met the needs of both end-users and organizational objectives.

One notable enhancement in 2023 was the introduction of a six-hour defense phase, providing teams with a concentrated period to test their strategies against adversarial attacks. This iteration also saw an increased role for local mentors and faculty, fostering stronger collaboration and participant support. Feedback from this year emphasized the importance of timely communication and better utilization of tools like Discord and Twitch. These lessons informed planning for future exercises, underscoring the need for clear expectations and robust technical infrastructure to support the event.

2023 Scenario: Securing a Corporate Distribution Network

The 2023 scenario concerned protecting the fictional Corporate Distribution Company (CDC) network infrastructure. Participants addressed challenges posed by insider threats, outdated systems, and poorly secured configurations. The company's systems included:

- **Active Directory Services:** Deploying a secondary domain controller provides centralized domain management and redundancy.
- **Certificate Authority:** Ensuring secure communication by issuing certificates for internal services.
- **File Sharing (SMB):** Managing and securing shared resources within the organization.
- **E-Commerce and Inventory Management Website:** A web application requiring secure integration with an SQL database and Active Directory.
- **Communication Services:** Including an Exchange server for internal email communication.

Participants were required to mitigate potential insider sabotage, improve fault tolerance, and address vulnerabilities left by former contractors. The scenario emphasized secure configuration management, active defense, and documentation of network changes.

2024 ICDC Highlights:

The 2024 exercise marked a significant milestone in the program's evolution, expanding its scope to include teams from Albania and Northern Macedonia. The exercise scenario centered on defending critical infrastructure, specifically the power grid of the fictional city of Ivory City. This complex challenge required participants to secure interconnected systems, including generator controls, MQTT brokers, and monitoring applications, against simulated sabotage. The scenario highlighted the interplay between cyber and physical security, pushing teams to develop innovative solutions to protect essential services.

This iteration featured an eight-hour defense phase, allowing for deeper engagement and more extensive testing of strategies under high-pressure conditions. Enhanced collaboration between international teams further enriched the experience, fostering cross-cultural exchange and teamwork. In addition, we moved the event date from May to February, allowing more U.S. teams to participate since the students were still in school. While the event was widely praised for its realism and educational value, challenges such as communication gaps and managing anomalies were identified. These lessons underscored the importance of continuous improvement, setting the stage for even greater success in 2025 as the exercise aims to refine its operations and broaden its impact.

2024 Scenario: Defending Critical Infrastructure – The Power Grid

The 2024 exercise escalated in complexity, focusing on critical infrastructure defense. Teams were tasked with securing the fictional city of Ivory City's power grid against malicious actors. Key systems included:

- **Generator Control Systems:** Managing power output based on commands from the backend server.
- **MQTT Broker:** Facilitating communication between the generator and other grid components.
- **Frontend Web Application:** Providing operators with control over grid operations and monitoring capabilities.
- **Backend Server:** Centralized logging and communication hub for the grid.
- **Camera System:** Providing security footage for situational awareness.

The scenario simulated real-world stakes, with teams needing to ensure uninterrupted energy supply while identifying and neutralizing sabotage attempts. This exercise highlighted the interplay between physical and cyber elements, requiring expertise in critical infrastructure cybersecurity. As mentioned above, in 2024, we created a video to help explain the scenario in a context targeted at getting students excited [8].

2025 ICDC Scenario

The 2025 International Cyber Defense Challenge (ICDC), which will take place after the submission of this paper, features a cutting-edge scenario centered on securing the internal network of a 3D printing company, Cyber Print. This fictional organization, which serves personal and manufacturing clients, faces critical cybersecurity challenges as it prepares to launch a new internet-facing website for uploading 3D models. Participants will tackle

vulnerabilities such as SQL injection, privilege escalation, and improperly sanitized user inputs, reflecting real-world issues in database management and service configurations.

The exercise highlights the complexities of highly interconnected networks, including Remote Desktop Protocol (RDP) to access multiple systems, from employee workstations to servers managing files for 3D printing. Teams will address challenges such as securing firewalls, mitigating information leakage, and protecting the web management interface of the company's virtual 3D printers. The scenario also incorporates anomalies to simulate dynamic challenges, such as hidden messages in 3D printing files, encryption-related tasks, and simulated fire drills, to test participants' adaptability under pressure.

With Cyber Print's new website launch imminent, participants must conduct an extensive security audit and create employee training materials. This year's ICE emphasizes the importance of proactive threat identification, effective firewall and privilege management, and fostering secure development practices. The 2025 event was designed to enhance further the educational value and international collaboration that have become hallmarks of ICDC. We had roughly the same number of teams participating in the 2025 ICDC as in 2024. The 2025 ICDC was the first year the Iowa National was not embedded in Kosovo during the event. They worked with the Kosovo security forces, who helped coordinate the event in Kosovo.

Funding Model

At present, ICDC operates on a combination of funding sources. The event itself is primarily supported by company donations, which finance the production of event materials such as T-shirts, trophies, and meals for participants. These contributions also enable the maintenance of the ISEAGE cyber range, ensuring a robust technical infrastructure for the exercise. The Electrical and Computer Engineering Department at Iowa State University provides funding for the salaries of the students who design and run the CDCs and ICDC. Additionally, the Iowa National Guard plays a crucial role by funding travel and operational costs for deploying personnel to Kosovo. This collaboration ensures the smooth execution of the event and highlights the importance of military-academic partnerships in sustaining ICDC's impact. Maintaining and diversifying these funding streams will be essential for ICDC's continued growth and long-term success.

In recent years, universities in Kosovo, Northern Macedonia, and Albania have stepped up to support the competition by raising funds for event essentials, including T-shirts, food, and other supplies. Their contributions have enhanced the participant experience and reinforced regional investment in cybersecurity education. This growing local support demonstrates the value that ICDC holds for participating institutions and their commitment to its future success.

To further expand ICDC into additional Adriatic countries, we are actively working to identify new funding sources, including government grants, international cybersecurity initiatives, and private-sector partnerships. Securing additional resources will enable greater regional participation, improve logistical support, and ensure the long-term sustainability of the competition. These efforts will strengthen ICDC's role as a premier international cyber defense challenge, fostering collaboration and skill development across borders.

Outcomes and Impact

Over four years, the International Cyber Defense Challenge has proven to be a transformative cybersecurity education and collaboration initiative. With participation growing from 16 teams in 2022 to 31 in 2025, the exercise has created a platform for students to engage in experiential learning while fostering cross-cultural collaboration. The diverse mix of high school, community college, and university teams from Kosovo, the United States, and, more recently, Albania and Northern Macedonia has enhanced the program's global reach, reinforcing its role as a model for international education.

ICDC has had a profound educational impact, equipping participants with practical cybersecurity skills through hands-on experiences. Students gained technical proficiency in securing networks, mitigating vulnerabilities, and responding to adversarial attacks. Beyond technical skills, ICE fostered critical soft skills such as teamwork, communication, and problem-solving under pressure. Feedback from participants and faculty consistently highlighted the value of this real-world simulation in preparing students for careers in cybersecurity.

The exercise also strengthened international collaboration, leveraging the U.S. National Guard's State Partnership Program to build connections between academic and military institutions across borders. Teams from Kosovo, supported by their local faculty and the Iowa National Guard, showcased remarkable growth in their capabilities, reflecting the benefits of sustained mentorship and training. For U.S. participants, ICDC provided a unique opportunity to work alongside international peers, broadening their perspectives and understanding of global cybersecurity challenges.

One notable outcome has been the institutional partnerships formed through ICDC. Faculty from Kosovo institutions have developed a tradition of collaboration, sharing best practices and co-hosting events with their U.S. counterparts. This growing network can potentially drive long-term cybersecurity education and workforce development improvements in all participating regions.

The Cyber Defense Competitions offered at Iowa University support several cybersecurity degrees within the Electrical and Computer Engineering Department. These degrees include the ABET-accredited B.S. in Cyber Security Engineering degree. Iowa State University is also a charter National Center of Academic Excellence in Cyber Defense Education (NCAE-CDE), which requires that students participate in cybersecurity competitions as part of its designation. These competitions are critical to the co-curricular activities offered to the students, ensuring students gain practical, hands-on experience defending networks and responding to cyber threats. This aligns with the university's mission to produce highly skilled cybersecurity professionals.

Although we have not formally measured the impact of ICDC, evidence from similar competitions strongly supports its benefits in enhancing technical proficiency and career preparedness. Unlike gamified cybersecurity challenges focusing on abstract scenarios, ICDC is a real-world, defense-based exercise where students use industry-standard tools, build and secure actual systems, and defend themselves against live attacks. This approach ensures they develop skills directly applicable to cybersecurity roles in government, industry, and academia.

Cybersecurity competitions have proven to be a valuable educational tool, offering students hands-on experience defending networks, problem-solving under pressure, and applying theoretical knowledge in practical scenarios. Studies on competitions like the National Cyber League (NCL) [9] and the DOE CyberForce Competition® [10] highlight their effectiveness in increasing student engagement, motivation, and skill development [11,12]. Research suggests that students participating in these events gain critical thinking skills, teamwork experience, and real-world cybersecurity expertise that directly translate to professional readiness [13].

These competitions serve as active, challenge-based learning environments that provide students with real-world experience in network defense, adversarial thinking, and incident response. Research shows that hands-on cyber defense exercises increase engagement, skill retention, and career readiness [11]. They integrate technical and non-technical skills, including team coordination, leadership, communication, and decision-making under pressure, which is critical for cybersecurity professionals [13]. Furthermore, cybersecurity competitions align with national educational standards, as student participation is required for the National Centers of Academic Excellence in Cyber Defense Education (NCAE-CDE) designation [11]. This recognition highlights the academic value and workforce impact of competitions like ICDC.

The growing cybersecurity workforce gap, estimated to exceed 500,000 positions in North America alone, underscores the importance of hands-on training programs [14]. Cyber competitions like ICDC provide an authentic environment where students apply cybersecurity knowledge in scenarios that closely mirror real-world job functions. Unlike traditional coursework or gamified exercises, ICDC emphasizes defending live systems using industry-standard tools rather than abstract challenges or simulations [15]. Studies on cyber defense exercises indicate that students who participate in these competitions gain a competitive advantage in the job market, as employers increasingly view competition experience as an indicator of problem-solving ability and technical competency [12].

Diversity remains a significant challenge in cybersecurity education and workforce development. Research suggests that cyber competitions can serve as a pathway to increase participation among underrepresented groups, mainly when structured to be inclusive and accessible [16]. Studies have shown that introducing cybersecurity competitions at high school and community college levels improves engagement among women and minority students, fostering long-term interest in cybersecurity careers [17]. ICDC's international collaboration with Kosovo, Northern Macedonia, and Albania further expands access to hands-on cyber education, helping bridge the global cybersecurity skills gap while fostering cross-cultural exchange and cooperation.

While gamification is often used in cybersecurity education to enhance engagement, research highlights the superior value of hands-on cyber defense exercises over traditional gamified learning methods [16]. Unlike Capture-the-Flag (CTF) challenges, which often emphasize isolated problem-solving, ICDC requires students to design, secure, and defend complex networks against live attacks, mirroring the operational roles in government and industry settings. Cyberdefense exercises better prepare students for real-world adversarial environments, developing the skills necessary for incident response, network security, and critical infrastructure protection [15].

As ICDC expands, its workforce development role will only grow. Engaging participants from multiple countries, ICDC fosters international collaboration, enhances cross-border cybersecurity preparedness, and helps cultivate a new generation of cyber defenders. As more universities and National Guard units join, the competition will continue to strengthen the cybersecurity workforce by providing participants with practical, high-stakes experience that prepares them for the evolving threat landscape.

Challenges and Lessons Learned

While ICDC has achieved significant success, its growth has also presented challenges. One recurring issue has been communication, particularly across time zones and between teams located in different countries, and early years highlighted the need for more explicit roles and responsibilities, more timely dissemination of information, and streamlined coordination among participants. Improvements such as using tools like Discord and Twitch for real-time updates and streaming have mitigated some issues but require further refinement.

Technological and logistical challenges were also evident, particularly in the early years. In 2023, bandwidth limitations in Kosovo impacted connectivity, underscoring the importance of robust infrastructure. The need for a dedicated cyber range in Kosovo emerged as a critical requirement to support year-round training and reduce reliance on external systems. Such an investment would enhance local capabilities and expand the exercise's scalability to include more countries.

Another lesson learned was the importance of tailoring scenarios and timelines to the needs of participants. For instance, extending the defense phase from six hours in 2023 to eight hours in 2024 allowed teams more time to fully engage with the challenges, resulting in a richer learning experience. Similarly, releasing scenarios earlier in preparation enabled teams to better plan their strategies and refine their setups. In 2025, we released the scenario 4 weeks before the exercise to give the teams additional time.

Conclusion and Future Directions

The International Cyber Defense Challenge (ICDC) has rapidly evolved into a premier platform for cybersecurity education, fostering experiential learning, international collaboration, and workforce development. Built on the foundation of Iowa State University's Cyber Defense Competition (CDC) model, ICDC has expanded its reach beyond the U.S., engaging students and professionals from Kosovo, Northern Macedonia, and Albania. Integrating high school, community college, and university participants with military and academic partners has provided a real-world, high-pressure environment that strengthens technical and soft skills, such as teamwork, communication, and resilience.

Looking ahead, ICDC is on a path toward continued growth and impact. Plans to incorporate additional Adriatic countries will introduce diverse perspectives, further enriching the learning experience and expanding the network of cybersecurity professionals across the region. Greater collaboration with U.S. National Guard units through the State Partnership Program will

strengthen mentorship opportunities and facilitate the exchange of best practices between academic institutions and military organizations.

ICDC will integrate cyber-physical elements into future scenarios to enhance realism and relevance, reflecting the increasing complexity of cybersecurity threats in areas such as power grids, water systems, and transportation infrastructure. These additions deepen participants' understanding of critical infrastructure defense, ensuring they are better prepared for emerging challenges.

However, achieving these ambitious goals will require sustainable funding and infrastructure investments. While corporate donations have supported ICDC's early success, securing additional resources through grants, government partnerships, and sponsorships from global cybersecurity firms will be essential for scaling the program. Establishing a dedicated cyber range in Kosovo and potentially other partner countries would provide year-round training opportunities and reduce reliance on external infrastructure, ensuring a more resilient and scalable model for international engagement.

Ultimately, ICDC's success highlights the power of hands-on learning, cross-border collaboration, and innovative training models in cybersecurity education. By expanding its global reach, refining its technical infrastructure, and strengthening institutional partnerships, ICDC will continue to serve as a leading model for cyber defense education. Its ongoing evolution will help prepare the next generation of cybersecurity professionals, fostering a globally aware, technically proficient, and adaptive workforce ready to tackle future cybersecurity challenges.

Acknowledgments

The success of the International Cybersecurity Exercise (ICE) would not have been possible without the support and collaboration of numerous individuals and organizations. We extend our deepest gratitude to Iowa State University's Center for Cybersecurity Innovation and Outreach for their vision and leadership in creating this transformative initiative. I want to extend a special thanks to the Kosovo Security Forces and the Iowa National Guard, whose participation and logistical support were instrumental in executing the exercise and fostering international collaboration.

We also acknowledge the contributions of academic institutions from Kosovo, Northern Macedonia, Albania, and the United States, whose students and faculty brought their dedication, expertise, and enthusiasm to each iteration of the ICDC. The generous support from sponsoring companies provided the resources needed to run the event and maintain the ISEAGE cyber range. Finally, we recognize the commitment of the White Team, National Guard members, and all mentors who guided participants and ensured the exercise's success. Their efforts have created a legacy of collaboration, learning, and innovation in cybersecurity education.