2026 ASEE ANNUAL CONFERENCE June 21–24, 2026 | Charlotte Convention Center, NC
Host Sponsor UNC Charlotte
ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION
Paper ID #51869

RedTeam at Michigan Tech: Building Cybersecurity Skills through Competitions and Collaboration

Dr. Yu Cai, Michigan Technological University

Dr. Yu Cai is a professor of cybersecurity in the College of Computing at Michigan Tech, where he also serves as the associate dean and the associate director of the Institute of Computing and Cybersystems (ICC). Additionally, Dr. Cai is the Director of the Computing Education Center, which is part of the ICC.

Dr. Cai's research interests include cybersecurity, computer networks, and computing education. He has been the lead PI on multi-million dollar external grants, with funding from sources such as the National Science Foundation (NSF), National Security Agency (NSA), and the State of Michigan. He is dedicated to applying his research to real-world challenges that positively impact society. Dr. Cai has also served as a consultant for companies like IBM and Ford, and he plays an active role as an ABET program evaluator for computing accreditation.

Wenbin Zhang, Florida International University

RedTeam at Michigan Tech: Building Cybersecurity Skills through Competitions and Collaboration

Abstract:

Student-led cybersecurity organizations play a vital role in enhancing experiential learning, teamwork, and professional development within computing education. This paper presents the structure, activities, and educational impact of Michigan Technological University's RedTeam, a student organization dedicated to advancing cybersecurity skills through hands-on engagement and peer learning. The RedTeam meets weekly throughout the academic year to conduct training sessions, technical workshops, and collaborative lab exercises covering topics such as penetration testing, network defense, digital forensics, and ethical hacking. Members also participate in regional and national cybersecurity competitions, including the National Cyber League (NCL), which provide authentic contexts for applying technical knowledge under pressure and fostering leadership and collaboration.

Beyond technical skill development, RedTeam serves as a professional community that connects students with industry experts and academic mentors through conferences, guest lectures, and outreach events. The organization collaborates closely with Michigan Tech's Cybersecurity program and the College of Computing to promote a culture of cybersecurity excellence and workforce readiness. This paper shares insights into the program's structure, success factors, and lessons learned, offering a replicable model for integrating student organizations into cybersecurity education and community engagement.

1. Introduction

Cybersecurity education faces a persistent challenge: bridging the gap between theoretical instruction and the practical, applied skills demanded by industry and government employers. While traditional coursework provides essential foundations in networking, operating systems, programming, and security principles, students often struggle to translate these concepts into real-world problem solving under time constraints and adversarial conditions. Experiential learning opportunities, particularly those that emphasize teamwork, cyber competitions, and authentic scenarios, are therefore essential to preparing students for cybersecurity careers.

Student-led organizations have emerged as an effective mechanism for delivering such experiences. Unlike formal courses, these organizations offer flexible, low-risk environments in which students can explore advanced topics, learn from peers, and develop professional identities. In cybersecurity, where hands-on skills and continuous learning are especially critical, student organizations can complement curricular offerings by providing sustained engagement beyond the classroom.

This paper presents a case study of RedTeam at Michigan Tech, a student-led cybersecurity organization designed to enhance technical competency, collaboration, and professional

development through weekly training and participation in national competitions. Over the past several years, RedTeam has been a regular and active participant in multiple regional and national cybersecurity competitions, such as the National Cyber League (NCL), eCTF, and CyberSEED. Through consistent engagement in these events, the team has achieved strong competitive results and external recognition, underscoring its effectiveness and impact as a student-led cybersecurity organization.

The goals of this paper are threefold:

1. To describe the structure and activities of RedTeam and how they align with cybersecurity learning objectives.
2. To analyze the educational and professional impact of RedTeam participation on students.
3. To identify success factors and lessons learned that can inform replication at other institutions.

2. Background and Related Work

2.1 Experiential Learning in Cybersecurity Education

Experiential learning has long been recognized as a cornerstone of effective computing education [1, 2]. In cybersecurity, experiential approaches such as labs, simulations, capture-the-flag (CTF) exercises [9, 10], and competitions are particularly valuable because they mirror real-world adversarial environments. Prior research [4, 5, 12] has shown that hands-on security exercises improve student engagement, deepen conceptual understanding, and strengthen problem-solving skills.

Cybersecurity competitions, including CTFs and league-based challenges, have gained prominence as scalable experiential learning tools. These competitions require participants to apply knowledge across multiple domains, such as networking, operating systems, cryptography, web security, and scripting, while working collaboratively under time pressure. Studies [5, 6, 7] have reported positive impacts on student motivation, self-efficacy, and retention in cybersecurity programs.

2.2 Role of Student Organizations

Student organizations provide a unique complement to formal curricula by fostering peer learning and sustained practice [8, 11]. Unlike short-term course projects, student organizations can support longitudinal skill development over multiple years. They also create informal mentoring structures in which advanced students support newcomers, reinforcing learning for both groups.

In cybersecurity education, student organizations often serve as hubs for competition preparation, tool exploration, and professional networking. However, the effectiveness of such organizations depends on clear structure, faculty support, and alignment with

academic programs. This paper contributes to the literature by offering a detailed account of how one such organization operates and sustains impact over time.

3. Organization Structure and Governance

3.1 Institutional Context

Michigan Technological University is a public research university with a strong emphasis on engineering, computing, and applied sciences. The Cybersecurity program within the College of Computing offers undergraduate and graduate degrees that emphasize both theoretical foundations and applied skills. RedTeam operates within this ecosystem as a co-curricular organization that complements formal instruction.

RedTeam is open to students from multiple majors, including Cybersecurity, Computer Science, Information Technology, Software Engineering, Electrical Engineering, and related disciplines. This interdisciplinary composition reflects the reality of modern cybersecurity teams, which often draw expertise from diverse technical backgrounds.

Faculty advisors from the Cybersecurity program provide mentorship, curricular alignment, and logistical support, while preserving the student-led nature of the organization. This balance allows RedTeam to remain agile and responsive to student interests while maintaining academic rigor.

Michigan Tech is designated by the National Security Agency (NSA) as a National Center of Academic Excellence in Cyber Defense (CAE-CD) and a National Center of Academic Excellence in Cyber Research (CAE-R). Michigan Tech is the only institution in Michigan to hold both CAE-CD and CAE-R designations, reflecting its leadership in cybersecurity education, research, and outreach.

3.2 Leadership Model

RedTeam is governed by a student executive board consisting of a president, vice president, training coordinator, competition coordinator, and outreach lead. Leadership positions are filled annually through elections, ensuring continuity while providing leadership opportunities to a broad range of students.

Each role has clearly defined responsibilities. For example, the training coordinator designs weekly technical sessions, while the competition coordinator organizes team participation in external events such as NCL. This division of labor distributes workload and mirrors professional team structures in cybersecurity organizations.

3.3 Faculty and Institutional Support

Faculty advisors meet with RedTeam leaders periodically, provide guidance on technical topics, and help connect students with external opportunities. Institutional support from the College of Computing includes access to lab space, computing resources, and modest

funding for competition fees and travel. This support is critical to sustaining participation and lowering barriers to entry for students.

RedTeam benefits from modest but sustained financial support secured by its faculty advisors to enable key extra-curricular activities. This funding is used to support student participation in cybersecurity competitions, conferences, and related professional development events. Funding sources include faculty-led research grants, research center incentive grants, and internal College of Computing awards. Although limited in scale, this financial support plays an important role in reducing participation barriers, expanding experiential learning opportunities, and ensuring the long-term sustainability of RedTeam activities.

4. RedTeam Activities

4.1 Weekly Meetings and Training Sessions

RedTeam meets weekly throughout the academic year. Meetings typically follow a structured format that includes:

- A short briefing on upcoming competitions or events.
- A technical training session led by student officers or advanced members.
- Hands-on lab exercises conducted in small groups.

Training topics are selected to align with both curricular content and competition requirements. Common topics include penetration testing methodologies, Linux system administration, network traffic analysis, digital forensics, scripting for automation, and secure configuration of systems.

4.2 Peer Learning and Mentorship

A defining feature of RedTeam is its emphasis on peer-led instruction. Advanced students often design and deliver training sessions, reinforcing their own knowledge while supporting newer members. This model fosters a collaborative culture and reduces intimidation for students who may be new to cybersecurity.

Peer mentorship also occurs informally during lab exercises and competition preparation. New members are encouraged to ask questions and experiment without fear of failure, creating a psychologically safe learning environment.

4.3 Cybersecurity Competitions as Authentic Learning

RedTeam regularly participates in the National Cyber League (NCL), a nationwide competition that includes individual and team-based challenges across multiple cybersecurity domains. NCL provides a structured, progressive set of challenges that align well with educational objectives.

Participation in NCL requires sustained preparation, including tool familiarity, time management, and teamwork. RedTeam uses NCL as a focal point for training during the fall and spring semesters, integrating competition challenges into weekly sessions.

Competitions provide authentic contexts that are difficult to replicate in traditional coursework. Students must make decisions under time pressure, prioritize tasks, and collaborate effectively. These experiences help students develop not only technical skills but also soft skills such as communication, leadership, and resilience.

Competition results also serve as external validation of student learning and program effectiveness. Strong performance reinforces student confidence and enhances resumes, while weaker results prompt reflection and continuous improvement.

4.4 Professional Development and Community Engagement

RedTeam regularly hosts guest speakers from industry, government, and academia. These sessions expose students to real-world career paths, emerging threats, and professional expectations. Speakers often include alumni, which further strengthens the sense of community and continuity.

Members are encouraged to attend cybersecurity conferences and regional events when possible. RedTeam also participates in outreach activities, including demonstrations for K–12 students and community cybersecurity awareness events. These activities reinforce students' professional identities and communication skills.

5. Assessment and Impact

5.1 Survey Design and Participants

To evaluate the educational and professional impact of RedTeam participation, an assessment survey was administered during the 2025–2026 academic year. A total of 15 valid responses were collected from active RedTeam participants. The instrument included Likert-scale items (1 = strongly disagree to 5 = strongly agree) and retrospective pre–post self-assessments designed to measure perceived changes in technical skills, experiential learning outcomes, career motivation, and sense of community. Descriptive statistics and paired-sample analyses were used to summarize responses across four domains: (1) technical skill development, (2) experiential and competition-based learning, (3) career motivation and professional development, and (4) community, belonging, and retention.

5.2 Technical Skill Development

Retrospective pre–post measures indicate consistent and substantial perceived improvement across core cybersecurity competencies. Mean ratings increased in Linux system administration (2.07 to 3.20), network scanning and reconnaissance (1.73 to 2.73), and vulnerability analysis fundamentals (1.67 to 3.30). Gains were also observed in defensive monitoring and incident response (1.47 to 2.53), digital forensics fundamentals

(1.80 to 3.00), scripting and automation (1.67 to 2.80), secure configuration and system hardening (1.67 to 2.87), and technical documentation (1.80 to 2.87). Team-based technical problem solving showed the largest increase, from 1.93 to 3.53.

Paired t-tests indicate that all observed gains are statistically significant ($p < .001$ across all skill areas), with very large effect sizes (Cohen's d ranging from 0.97 to 1.93). The strongest effects were observed in team-based technical problem solving ($t = 7.48$, $d = 1.93$) and vulnerability analysis ($t = 12.00$, $d = 2.09$), while even the smallest effects, such as technical documentation ($t = 3.76$, $d = 0.97$), remain well above conventional thresholds for large effects. These results suggest that sustained participation in weekly hands-on training sessions and competition preparation activities provides meaningful opportunities for applied learning that complement formal coursework. The magnitude and consistency of gains across domains underscore the value of peer-led practice environments in reinforcing and extending curricular content.

5.3 Experiential Learning and Competition Impact

Survey responses indicate that competitions and practice exercises serve as central mechanisms for learning. Students reported strong agreement that participation enabled them to develop skills not deeply covered in coursework ($M = 4.47$), learn new tools more quickly ($M = 4.67$), and approach unfamiliar technical problems more effectively ($M = 4.53$). Respondents also reported improvements in teamwork and collaboration ($M = 4.40$), technical communication ($M = 4.27$), and time-management skills during competitions ($M = 4.00$). Increased awareness of ethical cybersecurity practice was also reported ($M = 4.60$).

These findings align with prior research emphasizing the importance of competition-based learning as an authentic context for skill development. Regular engagement with timed, adversarial challenges appears to promote adaptability, tool proficiency, and collaborative problem solving. These skills that are essential for professional cybersecurity practice but difficult to replicate in traditional classroom environments.

5.4 Career Motivation and Professional Development

Participation in RedTeam was associated with strong indicators of career motivation and professional growth. Students reported increased interest in cybersecurity careers ($M = 4.73$), greater motivation to pursue internships or co-op opportunities ($M = 4.33$), and increased interest in professional certifications ($M = 4.07$). Many respondents indicated that RedTeam helped them identify specific areas of cybersecurity interest ($M = 4.80$), strengthen their resumes or professional portfolios ($M = 4.27$), and build confidence in technical interviews ($M = 4.27$).

These outcomes suggest that co-curricular engagement through RedTeam contributes not only to technical competence but also to professional identity formation and workforce

readiness. Exposure to competitions, peer mentorship, and industry engagement appears to reinforce students' commitment to cybersecurity career pathways.

5.5 Community, Belonging, and Retention

Survey results further indicate that RedTeam provides a supportive and inclusive learning environment. Respondents reported feeling welcomed when joining the organization (M = 4.60) and described RedTeam as a supportive learning community (M = 4.60). Students indicated that they could rely on peers for assistance when encountering technical challenges (M = 4.47) and experienced an increased sense of belonging within the cybersecurity community (M = 4.53). Most respondents reported that participation made them more likely to remain in their major or program (M = 4.60).

These findings highlight the importance of peer mentorship and community-building in sustaining student engagement. The student-led structure of RedTeam appears to foster a psychologically safe environment in which members can experiment, ask questions, and build confidence, thereby supporting persistence in cybersecurity programs.

5.6 Summary of Impact

Overall, the assessment results demonstrate that participation in RedTeam is associated with meaningful perceived gains in technical competence, experiential learning, professional development, and sense of community. Statistically significant improvements were observed across all measured technical skill domains, with large effect sizes indicating substantial perceived growth. Students also reported strong impacts on career motivation, professional confidence, and belonging.

Although findings are based on self-reported data from a single institution and a modest sample size, the results provide evidence that structured, student-led cybersecurity organizations can play a significant role in enhancing experiential learning, workforce readiness, and student engagement within computing programs.

5.7 Achievements and Recognition

Over the past several academic years, RedTeam has demonstrated sustained competitive excellence and received external recognition that underscores its impact as a student-led cybersecurity organization. In national competitions such as the National Cyber League (NCL), RedTeam has consistently achieved top-tier results, including national rankings within the top 25 teams, multiple top-100 individual placements, and a best-ever individual finish of 5th nationally among thousands of competitors. The team has also performed strongly in capture-the-flag events, earning podium finishes and prizes in large-scale competitions such as CyberSEED, as well as wins and advanced distinctions at conference-based challenges including CypherCon and AI Village.

Beyond competitive performance, RedTeam's achievements have received formal recognition from state and federal leaders, including commendations from the Governor of

Michigan and a U.S. Senator, highlighting the team's representation of Michigan Technological University on a national stage. Collectively, these outcomes have contributed to broader institutional recognition of the College of Computing's cybersecurity programs and position RedTeam among the leading collegiate cybersecurity teams in the United States.

6. Lessons Learned and Conclusion

Several factors have contributed to RedTeam's success:

1. Student ownership: A student-led model fosters engagement and sustainability.
2. Faculty mentorship: Light-touch faculty involvement ensures alignment without stifling initiative.
3. Competition integration: Regular participation in competitions provides clear goals and motivation.
4. Inclusive culture: An emphasis on peer support lowers barriers for newcomers.

Institutions seeking to replicate this model should prioritize institutional support, clear leadership structures, and alignment with academic programs.

In conclusion, RedTeam at Michigan Tech demonstrates the powerful role that student-led organizations can play in cybersecurity education. By combining weekly hands-on training, competition-based learning, and professional development, RedTeam provides a scalable, sustainable model for enhancing experiential learning and workforce readiness. The lessons learned from this case study may inform the design of similar organizations at other institutions seeking to strengthen cybersecurity education through co-curricular engagement.

Acknowledgment

This project is supported by the National Science Foundation under Awards No. 2043022 and No. 2247492.

References

1. Schafeitel-Tähtinen, T., & Lazarov, W. (2025). Teaching and learning cybersecurity using Capture the Flag: effectiveness comparison between university students in Finland and Czechia. Computer Applications in Engineering Education, 33(5), e70082. doi:10.1002/cae.70082

2. Christian Servin and Kristine Christensen. (2025). Professional Dispositions++: Elevating Collaborative and Experiential Learning in Two-Year Programs. In Proceedings of the 26th ACM Annual Conference on Cybersecurity & Information Technology Education (SIGCITE '25).

3. Sashank Narain, Pranathi Rayavaram, Christopher Morales-Gonzalez, Matthew Harper, Maryam Abbasalizadeh, Krishnaa Vellamchety, and Xinwen Fu. (2025). Practical Cybersecurity Education: A Course Model Using Experiential Learning Theory. In Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1 (SIGCSETS 2025).

4. Wolfgang Vigl and Svetlana Abramova. 2024. Design and Use of Privacy Capture-the-Flag Challenges in an Introductory Class on Information Privacy and Security. In Proceedings of the 2024 on Innovation and Technology in Computer Science Education V. 1 (ITiCSE 2024).

5. Mouhssine, Y., Boutrachech, H., moumen, A. (2025). Bridging Theory and Practice: The Educational Impact of Cybersecurity Competitions. In: Boudriki Semlali, BE., Ben Abdel Ouahab, I., Angeletti, F. (eds) Technological Innovations for Sustainable Development. DATA 2025. Lecture Notes in Information Systems and Organisation, vol 81. Springer.

6. Beauchamp, C., Matusovich, H. (2024). A Mixed-Method Study Exploring Student Motivation for Participating in Cybersecurity CTF Competitions. Cybersecurity Pedagogy and Practice Journal, 3(1), pp.4-26.

7. Yu Cai and Todd Arney. Cybersecurity Should be Taught Top-Down and Case-Driven. In Proceedings of the 18th Annual Conference on Information Technology Education, 2017.

8. Curtice Gough, Carl Mann, Cherrise Ficke, Maureen Namukasa, Meredith Carroll, and TJ OConnor. 2024. Remote Controlled Cyber: Toward Engaging and Educating a Diverse Cybersecurity Workforce. In Proceedings of the 55th ACM Technical Symposium on Computer Science Education (SIGCSE 2024).

9. Zack Kaplan, Ning Zhang, and Stephen V. Cole. A Capture The Flag (CTF) Platform and Exercises for an Intro to Computer Security Class. In Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 2 (ITiCSE '22).

10. Connor Nelson and Yan Shoshitaishvili. 2024. PWN The Learning Curve: Education-First CTF Challenges. In Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE 2024).

11. Klinger, M. B. 2024. Improving Belonging and Connectedness in the Cybersecurity Workforce: From College to the Profession. Journal of Cybersecurity Education, Research and Practice, 2024(1), Article 17.

12. Chola Chhetri. 2023. "It was a one of a kind experience:" Student Experiences and Pedagogical Design of a Project-based Hands-on Cybersecurity Pen-testing Course. In Proceedings of the 24th Annual Conference on Information Technology Education (SIGITE '23).