Journal of Cybersecurity Education, Research and Practice

Volume 2023 | Number 1 Article 6

July 2023

Compete to Learn: Toward Cybersecurity as a Sport

TJ OConnor
Florida Tech, toconnor@fit.edu

Dane Brown
US Naval Academy, dabrown@usna.edu

Jasmine Jackson
jacksonjasmine@cityu.edu

Bryson Payne
University of North Georgia, bryson.payne@ung.edu

Suzanna Schmeelk
St. John's University, schmeels@stjohns.edu

Compete to Learn: Toward Cybersecurity as a Sport

Abstract

To support the workforce gap of skilled cybersecurity professionals, gamified pedagogical approaches for teaching cybersecurity have exponentially grown over the last two decades. During this same period, e-sports developed into a multi-billion dollar industry and became a staple on college campuses. In this work, we explore the opportunity to integrate e-sports and gamified cybersecurity approaches into the inaugural US Cyber Games Team. During this tenure, we learned many lessons about recruiting, assessing, and training cybersecurity teams. We share our approach, materials, and lessons learned to serve as a model for fielding amateur cybersecurity teams for future competition.

Keywords

Cybersecurity, e-sports, competition, capture-the-flag

Compete to Learn: Toward Cybersecurity as a Sport

TJ OConnor
Florida Institute of Technology
Melbourne, FL, USA
toconnor@fit.edu
https://orcid.org/0000-0001-9707-1830

Dane Brown
US Naval Academy
Annapolis, MD, USA
dabrown@usna.edu
https://orcid.org/0000-0002-7235-548X

Jasmine Jackson
City University of Seattle
Seattle, WA, USA
jacksonjasmine@cityu.edu
https://orcid.org/0009-0009-8434-5316

Suzaana Schmeelk
St. John's University
New York, NY, USA
schmeels@stjohns.edu
https://orcid.org/0000-0003-1886-3798

Bryson Payne
University of North Georgia
Dahlonega, GA, USA
Bryson.Payne@ung.edu
https://orcid.org/0000-0003-4539-0308

I. Introduction

In the past two decades, pedagogical approaches for cybersecurity education have grown exponentially to support the demand for a skilled cybersecurity workforce. Adopting both gamification and contemporary cyber curriculum have proven successful strategies for academic engagement and recruiting [1]–[3]. During the same period, organized competitive video gaming, also known as *e-sports*, has earned recognition as a sport by the International Olympic Committee (IOC) and developed into a multi-billion dollar industry. In this work, we examine the opportunity to integrate both strategies into developing the inaugural *US Cyber Games Team.* We then share our approach, experiences, materials, and lessons learned in developing our cybersecurity team to compete in the *International Cyber Competition (ICC)* to serve as a model for fielding amateur cybersecurity teams for future competitions.

In this work, we explore the challenges of developing an amateur e-sports cybersecurity team, the US Cyber Games team. The US Cyber Games team was founded in 2021 to represent the United States at the International Cybersecurity Challenge (ICC). E-Sports has successfully transformed video gaming competition into a billion-dollar industry, complete with franchises, broadcasters, standout players, managers, and coaches. However, e-sports has seen limited adoption in the area of cybersecurity competitions. Over the previous year, we treated cybersecurity as a sport. We conducted recruiting, assessment, and development programs similar to sporting franchises. We developed and rehearsed skills in the confines of a geographically distributed team. Finally, we traveled overseas to Athens, Greece, and met for the first time before competing in the ICC competition. In the following work, we examine our recent experiences merging cyber and e-sports. Previous works suggest that organized, competitive sports, including e-sports, can help non-sports organizations achieve their goals [4]. This paper makes the following contributions by examining the following challenges we faced.

1) How did we assess, select, and develop amateur athletes to compete in international cybersecurity competitions?
2) How did we recruit and develop a diverse talent pipeline for future seasons?
3) How did we function as a cohesive team despite geographic dispersion, and not meeting face-to-face until the competition?

II. Motivation

In early January 2022, Russian hacking teams deployed a campaign of destructive malware against Ukrainian organizations. By January 15, Microsoft released indicators of compromise (IoCs) for the newly-dubbed *WhisperGate* malware that corrupted the victim's master boot record, displayed a faux ransomware note, and encrypted the victim's file system [5]. The further technical analysis identified that the malware destroyed the target data and provided no recovery mechanism. By February 23, cybersecurity researchers from SentinelLabs identified a second campaign known as *HermeticWiper*, which improved on the previous Russian attacks [6].

During both attacks, the US Cybersecurity Infrastructure Security Agency (CISA) raced to notify partners of the malware, focusing on the Industrial Control System (ICS) and Operational Technology (OT) industries to ensure Ukraine could continue industrial operations in the wake of a large-scale cyber attack [7]. Lessons from the previous 2017 *NotPetya* attack limited the damage to mostly 70 Ukranian government websites. To prevent the malware from infecting allies, The Microsoft Threat Intelligence Center (MSTIC) shared threat intelligence with NATO member states in the Baltics [8]. As the United States prepared to deliver economic sanctions against Russia, Ms. Anne Neuberger, Deputy National Security Advisor for Cyber, wargamed tabletop exercises with federal agencies to prepare for retaliation [7]. The response to *WhisperGate* highlights the need for those responsible for cyber defense to work collaboratively to achieve a shared goal, even in the presence of a skilled adversary and a stressful, high-stakes environment; we assert that this is fully analogous to a

Capture-the-Flag (CTF) Category	National Initiative for Cybersecurity Education (NICE) Knowledge, Skills, Abilities (KSAs)	NSA Center of Academic Execellence (CAE) Cyber Operations Knowledge Units (KUs)
Forensics	K0001, K0010, S0184, S0177, A0065	M4: Networking, O11: Digital Forensics
Web Vulnerabilities	K0009, K0070, S0137, A0092	O8: Software Security Analysis
Cryptography	K0403, K0018, K0487, S0138, A0099	M6: Discrete Math & Algoirthms, O13: Applied Cryptography
Reverse Engineering	K0051, K0175, K0183, S2700, S0088, A0021	M2: Software Reverse Engineering, M1: Low Level Programming
Binary Exploitation (pwn)	K0051, K0070, S0088, S0293, A0093	M9: Vulnerabilities, O8: Software Security Analysis

TABLE I
MAPPING CTF CATEGORIES TO NICE KNOWLEDGE, SKILLS, ABILITIES (KSAS), AND NSA CAE CO KNOWLEDGE UNITS (KUS)

sports team. Further, we must draw that team from a highly skilled talent pool created before the crisis.

III. PRIOR WORK

In developing a gamification approach, it proves helpful to examine the evolution of cybersecurity competitions over the past two decades. From the early days of conference CTFs to modern competitions where competitors attempt to attack satellite systems, gamification has proven an integral methodology for assessing, engaging, and recruiting cybersecurity talent.

DEF CON CTF: One of the earliest and longest-running cybersecurity competitions arose at the popular DEF CON conference in 1996 [9]. Initially a loosely defined free-for-all competition, judges decided on points based on a qualitative assessment of the competitors' offensive actions on the network. As the competition formalized, the organizers developed custom exploitable services and a series of international qualifying tournaments. To maintain innovation, competition organizers have rotated every 3-5 years. Order of the Overflow (OoO), a predominately academically aligned group, has run the competition for the previous four years. OoO's vision has seen the introduction of exciting new approaches, including *SpeedRuns* in the *DEF CON Quals*, where competitors must invent automatic exploitation techniques for rapid binary exploitation [10].

NSA Cyber Defense Exercise (CDX): The National Security Agency/Central Security Service (NSA/CSS) began hosting an annual Cyber Defense Exercise (CDX) for the five United States military service academies in 2000 [11], [12]. Students, predominately military-aligned trainees, established and defended a small business network. Volunteer attackers from the NSA's Information Assurance Directorate tried to gain a foothold into each network to exfiltrate data out of the network. CDX scoring balanced service availability with the loss of confidential information. In 2018, the competition was re-imagined as the NSA Cybersecurity Exercise (NCX), opening the competition to all NSA Center of Academic Excellence schools and adding a traditional jeopardy-style CTF, a policy competition, and a live-fire attack and defend competition [13].

Darpa Cyber Grand Challenge: In 2016, the Defense Advanced Research Projects Agency (DARPA) hosted the first automated all-machine cybersecurity tournament with a $1M prize for the winners [14]. For the first time, sophisticated programs were the contestants instead of competitors identifying, exploiting, and defending machines. This competition format led to the development of several new technologies and approaches in binary exploitation, most notably the rise of symbolic and concolic analyses. Shellphish, the third place team, released their *angr* symbolic execution framework, which has produced numerative derivative works [15]–[17].

Collegiate Competitions: Over the two previous decades, several cybersecurity competitions have arisen in academia [18]–[21]. The Collegiate Cyber Defense Competition (CCDC) emerged in 2004 at Texas A&M University, resulting from the work of academia, government, and students [19]. With significant corporate sponsorship, CCDC has become a popular attack-defense defense-focused competition with a series of qualifying regional tournaments. Conversely, the Collegiate Penetration Test Competition (CPTC) also recently emerged in 2015 as a regional-based tournament but focused on scoring academic teams on their ability to compromise networks and services [20]. The National Cyber League (NCL) debuted in 2011 as a Jeopardy-style competition focused on individual competitors and skills. In recent years, over 13,000 competitors have participated in the NCL [21]. The NCL first debuted the idea of treating competition as an e-sport by providing scouting reports that depict a competitor's strengths and weaknesses.

US Space/Air Force Hack-A-SAT: In 2020, the United States Space Force and Air Force jointly created the *Hack-A-Sat* competition [22]. The competition predominately focuses on analysis and binary exploitation alongside a space-based theme. Competitors compete in an initial Jeopardy-style CTF qualifying round. The final event is an attack-defense round, where they must defend and compromise the digital twin of a satellite. Arguably one of the more exciting competitions due to the space-based theme, Hack-A-SAT has pitted top international CTF teams (Solar Wine, PPP, Dice Gang) against each other in the finals [22].

IV. DESIGN

The following section examines our recruitment, assessment, and development approach for the initial season of the US Cyber Games.

A. Qualifying Open CTF

The US Open CTF competition identified talented cybersecurity competitors with the skills necessary to compete

```
// Modified Canary Insertion
0000345c  55              push    rbp
0000345d  4889e5          mov     rbp, rsp
00003460  4881ecf0000000  sub     rsp, 0xf0
00003467  4889bd18ffffff  mov     qword [rbp-0xe8], rdi
0000346e  90              nop     // Patching by-product
0000346f  6847435355      push    0x55534347

// Modified Canary Check
0000352e  4881e947435355  sub     rcx, 0x55534347
00003535  90              nop     // Patching by-product
00003536  90              nop     // Patching by-product
00003537  7405            je      0x353e
00003539  e8b2ebffff      call    __stack_chk_fail
```

Listing 1. Solutions for challenges like this custom stack canary required collaborative analysis and communication among teammates

Fig. 1. During the draft, we presented *baseball cards*, depicting the athlete's specialization and strengths.

for a slot on the US Cyber Games team. In 2021, the Virginia Cyber Range hosted and designed the US Open. The 2021 Open focused broadly on cybersecurity topics, including forensics, reconnaissance, networking, cryptography, web vulnerabilities, and reversing engineering. The 2021 Open identified 70 players with the skills necessary to move to the Combine event. In 2022, coaches and athletes developed the event based on our collective experience in the inaugural International Cyber Competition (ICC). The 2022 Open CTF focused on binary exploitation, reverse engineering, cryptography, web vulnerabilities, and forensics. The introduction and prevalence of the more challenging binary exploitation category mirrored the ICC experience. Further, we mapped the challenge categories to NIST workforce competencies and the Academic Objectives for the NSA Center of Excellence Cyber Operations academic criteria [23]–[25] as depicted in Table I. The 2022 open identified 83 players with the skills necessary to move to the Combine event. For others to build on our initial work, we published the 2022 Open CTF challenges at https://github.com/tj-oconnor/cyber-open-2022.

B. Combine Invitational

Similar to the National Football League Combine, the US Cyber Games Combine served as an invitational event to showcase and test athletes' knowledge, skills, and abilities. The 2021 Combine event lasted six weeks, with athletes participating in weekly competitions, training, and group work. In assessing the athletes' interpersonal and team skills, we purposely selected athletes with disparate skill levels to work collectively on challenging problems. Each week, athletes worked together via Discord chat and voice to solve complex problems in constrained time. In addition to recording quantitative results in the form of solutions, we observed and recorded qualitative actions where athletes demonstrated strong communication and leadership. For each team, we identified one athlete that made the team stronger through their interpersonal skills. At the end of each week, we scrambled the athletes into new teams. We designed this unique approach to identify skilled contestants who can work collaboratively on a team.

Listing 1 depicts a partial challenge from the Combine Invitational. In this activity, we challenged the athletes to develop a binary exploitation technique for a web server. However, we compiled the binary with several protection mechanisms that complicated the difficulty of writing the exploit. As one of these protection mechanisms, we patched the binary with a custom stack canary. Typical AMD64 Linux Canaries for ELF executables end in two null bytes, making these easily identifiable with a memory leak. However, we patched in a custom value ("USCG") for the canary. We then observed how the athletes handled this increased difficulty. We observed an interesting dynamic on the first team that solved this challenge. The teams' most talented binary-exploiter routinely communicated with their teammates, despite having a higher skill level—this communication and listening to their teammates aided in rapidly developing a solution. One teammate noticed the NOP instructions left by patching the binary. While they incorrectly labeled these instructions as a *nop-sled*, they identified an anomaly. As the team further analyzed this area, they collaboratively quickly discovered the custom canary. This event depicted the importance of balancing soft and technical skills of the athletes.

C. Team Draft & Selection

Next, we selected athletes in a live-stream Draft Event. At the draft, we identified 20 primary athletes and five alternates to serve on our national team based on the assessment data from the US Open and Combine events. Rather than establishing our selection based on the aggregate skill of all

domains, we choose each athlete to serve a specific purpose on the team (e.g., binary reverse engineer, web application exploiter, network forensic analyst.) Like baseball scouts trying to find the best left-handed pitcher, we endeavoured to identify a vulnerability researcher with experience in the ARM and MIPS architectures. To aid in our understanding of the candidates, we created *player profile cards* for each athlete that highlighted their strengths. Figure 1 depicts the baseball card for our CTF team captain, who showed strong communication and managerial skills alongside a breadth of technical depth across all domains. While streaming the event live, we praised and highlighted the technical abilities of each athlete and discussed the reason for their selection. Similar to the National Basketball Association (NBA) draft, a commentator analyzed each prediction and debated the merits of our choices.

D. Team Infrastructure

We tried several communication and training platforms during the team's inaugural season to coordinate over the geographic dispersion of our team. Eventually, we settled on Discord as a collaborative communications platform. Discord is a VoIP and instant messaging social platform that has gained popularity in *e-sports.* This platform establishes role-based access control, which allowed us to partition our team into sub-groups and committees (e.g., captains, coaches, ctf-team, reverse-engineers, forensic-analysts.) Discord also supports various integrations with other platforms via webhooks. We leveraged this for real-time notifications when athletes solved problems in the US Open. Additionally, we leveraged the managed CTF service, CTFD.io, to host the US Open, Combine Event, and internal team events [26]. CTFD.io provides an accessible framework to host competitions by hosting services, a themeable challenge scoreboard, and external integration to platforms like Discord. CTFD.io proved ideal for hosting micro-services, such as an exploitable binary or vulnerable web application. In contrast, we leveraged Google Cloud Compute to establish more extensive networks and systems to train for the attack-defense competition. The cloud-based platform allowed us to construct more sophisticated connections between interdependent systems and limit the network ingress and egress.

E. Development Program

In the 2021 Draft, our team faced several difficult decisions. Unfortunately, we selected a group that collectively lacked diversity. Three out of five of our coaches identified as an underrepresented gender or race in computer science. However, we chose predominately white male athletes, with only two athletes identifying their gender as other than male and two identifying their race as other than Caucasian. In response, we established the *Development Program* to coach, mentor, and teach URM athletes using best practices for approaching digital divide [27]–[31]. Thirteen athletes participated in the Development Program, with five identifying their gender as other than male and eight identified as an underrepresented race. Five athletes received scholarship packages with three-month subscriptions to *TryHackMe* (THM), *HackTheBox* (HTB), and *Offensive Security's* PEN-200 course. We conducted a 12-week cohort-style training program, where athletes rotated bi-weekly through different technical specialties (reverse engineering, binary exploitation, web vulnerabilities, network forensics, and cryptography). Athletes who completed the Development Program received an invitation to the following season's Combine. During the development program, athletes participated in capture the flags (CTFs) to strengthen and retain skills learned in the Development Program. Following completion of the development program, three (out of 13) athletes participated in the optional Season II Open CTF despite an automatic bid to the Combine event. The development program athletes individually placed in the top 10%, 30%, and 40% brackets. The athletes showed the most growth in the topic of reverse engineering, which an underrepresented minority coach taught during the program. Despite the increased difficulty in the Season II Open, the three participating athletes significantly improved their overall reverse engineering scores. Following completion of the development program, we conducted a voluntary and anonymous Institutional Review Board (IRB) approved rotation survey, which we discuss in our Lessons Learned Section V.

Team	CTF Rank	Attack-Defend Rank	Overall Score
Europe	1	2	12961
Asia	2	1	10724
United States	3	4	7765
Oceania	4	3	7447
Canada	5	5	3643
Latin America	6	6	1722
Africa	7	7	981

TABLE II
OUR TEAM EARNED THE BRONZE MEDAL AT THE INTERNATIONAL CYBER COMPETITION, LEARNING VALUABLE LESSONS ABOUT DRAFTING SPECIALTIES, COLLABORATION IN A DISTRIBUTED ENVIRONMENT, AND IDENTIFYING RULE BORDER CASES.

F. International Cyber Competition (ICC)

In July 2022, the European Union Agency for Cybersecurity (ENISA) hosted the International Cyber Challenge (ICC) Competition [32]. The two-day event pitted seven regionally aligned teams against each other in a Jeopardy Style and Attack-Defend competition. ENISA coordinated for separate vendors to develop creative challenges for each day. The CTF event focused on the traditional binary exploitation (pwn), reverse engineering, cryptography, web vulnerabilities, and forensic categories. Overall, cryptography proved the most challenging topic for our team as we placed less emphasis during preparation. *CryptoHack*, a well-known vendor, created some tough challenges that required discrete mathematics algorithmic attacks to compromise cryptographic algorithms. The vendor for the Attack-Defend competition developed six custom services that each team internally secured and

externally exploited. Each team hosted the services in a Docker Container. The Attack-Defend vendor created a custom scoreboard that displayed the results of each round of attacks, measuring the service uptime and services compromised by each team. Table II depicts the final scores from the two days of competition, with our team earning the Bronze medal place.

V. Lessons Learned

In the following section, we explore our lessons learned from the initial season of the US Cyber Games. We discuss the challenges of drafting the right specializations for the team, functioning across four time zones, and examine boundary rules for competition. Next, we recognize the success of our development program and the building of international partners in the cyber domain.

A. Challenges

Drafting Specialties Before Problems: The inaugural nature of the competition introduced challenges across all teams. One of these challenges was understanding and predicting the required specialties. Initial competition correspondence emphasized on *internet-of-things* devices, *escape rooms*, *hardware hacking*, and *Windows domain* security. This led our team to overly specialize during the draft. For example, we selected binary exploiters with strength in embedded architectures such as MIPS and ARM. Further, we hand-picked teammates with specialties in security and exploiting Windows domains. However, as the competition materialized, the organizers established the categories as binary exploitation (25%), reverse engineering (20%), cryptography (20%), web exploitation (20%), and forensics (15%.) Further, the organizers increased the complexity of the cryptographic challenges by hiring a well-known vendor who could write tough challenges. In addition, the organizers eliminated Windows domain exploitation from the competition and conducted the attack-defense competition in an entire Linux environment. As the competition categories and environments were only finalized weeks before the event, we could not internally reorganize and redraft teammates to handle the unique challenges. In contrast, the first-place European team patiently waited to draft their team until the environment became clearer. This problem reiterates a well-known problem in cybersecurity; you can only draft cyber specialists after knowing the challenge you may face.

Functioning in Geographically Distributed Team: Having a team spread across over a dozen states and four time zones created numerous challenges, beginning with finding synchronous training and competition times that worked for both east-coast and west-coast players and coaches. In addition, the cyber athletes ranged in age from 18 to 26. Hence, the training schedule not only had to work around college class schedules, midterm, and final exams but around work schedules, including evening and night shift work for some participants at various stages. The team infrastructure and technology platforms that we discussed in Section IV helped address some of these challenges. We intend to divide the team into east-coast and west-coast coaching staffs to address this challenge in future seasons. We hypothesize that this will allow for broader participation among team members in each time zone and around their work and school schedules and enable the addition of scrimmage events between the *east* and *west conferences*. The team showed considerably strong collaboration, conflict-resolution, communication, and leadership/followership skills during the International Cyber Competition, considering it was their first face-to-face experience. In contrast, the first-place European team competed in regional face-to-face events and European Cybersecurity Challenge (ECSC). Further, the European team coordinated several face-to-face coordination meetings before the competition. We hypothesize that these face-to-face meetings helped strengthen the European team by accelerating group development phases [33]. In future seasons, we intend to replicate the European model of face-face coordination meetings before the competition.

Defining Rule Boundaries: We encountered challenges with nebulous rules during the initial competition. The Docker deployment in the ICC Attack-Defend competition introduced some of this difficulty, as teams attacked the resources of each container. The European and US teams were both attacked with SYN and TCP-Full Connect Scans that attempted to exhaust the resource constraints of the CPU processing power and network resources, respectively. Arguably the TCP-connect scans could have been mitigated by modifying the Docker configuration. However, these configuration changes could not have prevented the CPU exhaustion. While the agreed-upon ruleset prevented resource-exhaustion attacks, coaches and judges had difficulty agreeing if these attacks were outside the scope of available attacks. This led to a six-hour debate. While the US team filed a protest, the European team moved their services off-site to Amazon AWS to avoid resource exhaustion and starvation. This critical and well-thought-out decision allowed the European team to overcome the problem regardless of the internal judging debate. Ultimately, the judges decided the attacks were out of scope, returning all the service-level-agreement points to every team for the first four hours of the competition. Moving forward, it proves helpful to identify the border cases for exploiting the rules and having clearly defined and agreed upon rule conditions. As we discovered, it proved untenable to debate a border case during the excitement of competition.

B. Successes

Cyber as a Team Sport: Although team-based cybersecurity competitions have been previously implemented, we believe that our approach is the first to be predominately designed as a competitive sport. This sport-oriented implementation included the management, the team selection process, uniforms and equipment, and content production. We designed an organizational structure and season to mirror professional sports teams. This structure consisted of a coaching staff and technical expert mentors that refined athletes' skills before the competition. We implemented a management organization, similar to a front

office led by a commissioner and management team. This team coordinated the competition, agreed on a ruleset, and oversaw finance and travel arrangements. Another aspect that draws a parallel to sports is team selection. In contrast to most CTF teams that rely on self-organization and selection, our team held tryouts and evaluated technical and soft skills. We drafted athletes and announced leadership on a live-streamed event. Our management organization oversaw the branding responsibility to ensure the athletes represented themselves and the country. They designed and issued team uniforms to athletes and coaches, with custom jerseys and matching track pants. Players also received t-shirts, stickers, and custom gear from sponsors for their participation. Management provided players with the highest-end gaming devices, including custom keyboards, mice, headsets, and a loaner laptop. Although nuanced, we believe these small details add value to making a sport instead of a competition. Sports differ from athletic competitions due to the production value. ENISA held the ICC at a large open-aired venue in Greece, overlooking the Parthenon. This venue accommodated eight teams, the ICC staff, and a moderate number of spectators, including several European and US government officials. Like an arena, athletes had a designated area to self-organize for the competition. An interactive scoreboard live-streamed the competition for fans following worldwide. We believe this inaugural approach demonstrated many of the first steps to transforming cyber into a sport.

Developmental Program: A critical success was the development of a talent pipeline for underrepresented minorities on our team. We conducted a voluntary and anonymous survey to understand and continue to grow our developmental program. Nine (out of 13 athletes in the program) responded. As an aggregate, athletes reported learning new tools, methodologies, and cybersecurity disciplines. They enjoyed the mentorship and the ability to ask questions from mentors. Further, athletes commented positively about interaction with mentors. They identified that they enjoyed the live sessions and the ability to engage in asynchronous dialogue via Discord between sessions. However, athletes expressed challenges with time conflicts, schoolwork, work, and personal activities. Afterward, we identified that the coaches were in a single time zone, separate from half of the development program. Athletes also reported that we could improve the program by including more formal coursework and materials. Despite these obstacles, athletes reported they learned more in a few weeks of hands-on, specialized instruction in cybersecurity domains than they might otherwise learn in a full-semester course.

Building International Partners: Developing international partners proves critical to the success of national interests in cybersecurity. We observed that amateur competition proves a viable means to develop early partnerships and allies. We share one experience that highlights this experience. During the ICC, one binary exploitation challenge proved extremely successful in frustrating competitors. The *Twist* challenge consisted of an ARM binary that contained a relatively simple buffer overflow to exploit with *return-oriented-programming*. We observed the US team athletes develop a proof of concept exploit that worked on their local machine within an hour of the start of the competition. However, the athletes struggled to exploit the remote binary hosted by the competition organizers. Since the competition organizers provided the binary and working environment, the US athletes filed a protest that the remote service was not correctly functioning. The organizers rejected the protest after identifying that the European and, ultimately, Asian teams had correctly solved the challenge. Following the competition, we examined the binary and concluded the US athletes' solution should have correctly worked. After the tournament ended, the European team hosted all teams at a beach barbecue. Over the course of the dinner, one European athlete presented their solution to the *Twist* problem to our team and other competitors. They recognized early that the conference organizers had hosted a different binary remotely than locally. So they used *blind-hacking* techniques to recover components for the attack [34]. Impressed with this approach and freely sharing of information, we included a similar challenge in our 2022 Cyber Open tournament as depicted in Listing 2.

```
Welcome to Twist v2.0.
Some file contents may have shifted on upload.
Debug Mode Enabled; calling 0x401385
nil |0x401490 |nil |nil |0x7f22103e6670 |0x7ffd8a23ecf0
You can dance in a hurricane
but only if you are standing in the eye >>>
```

Listing 2. In homage to a creative solution shared by the European and Asian teams for a problem during the ICC, we created a replica problem for our 2022 Cyber Open that introduced a similar challenge and solution to US competitors.

VI. Conclusion

In this paper, we explored the inaugural season of the *US Cyber Games team*. We share our approach, competition challenges, experiences, and lessons from this experience for others to build on our initial success. We explored our strategies for recruiting, assessing, and selecting an amateur team to compete in an international competition. Further, our lessons highlighted the need to develop and own responsibility for a development pipeline to grow underrepresented groups on our team. We believe this work presents the first steps toward treating cybersecurity as a sport, which offers a valuable opportunity for developing the next generation of cybersecurity professionals.

References

[1] J. Bernd, D. Garcia, B. Holley, and M. Johnson, "Teaching cybersecurity: Introducing the security mindset," in *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 2*. Providence, RI: ACM, 2022, pp. 1195–1195.

[2] J. G. Hall, A. Mohanty, P. Murarisetty, N. D. Nguyen, J. C. Bahamón, H. Ramaprasad, and M. Sridhar, "Criminal investigations: An interactive experience to improve student engagement and achievement in cybersecurity courses," in *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 1*. Providence, RI: ACM, 2022, pp. 696–702.

[3] T. OConnor, "Helo darkside: Breaking free from katas and embracing the adversarial mindset in cybersecurity education," in *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 1*. Providence, RI: ACM, 2022, pp. 710–716.

[4] B. Heere, "Embracing the sportification of society: Defining e-sports through a polymorphic view on sport," *Sport management review*, vol. 21, no. 1, pp. 21–24, 2018.

[5] Cybersecurity & Infrastructure Security Agency, "Alert (aa22-057a): Destructive malware targeting organizations in ukraine," February 2022. [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

[6] C. . I. S. Agency, "Malware analysis report (ar22-115a): Hermeticwiper," April 2022. [Online]. Available: https://www.cisa.gov/uscert/ncas/analysis-reports/ar22-115

[7] J. E. B. David E. Sanger and K. Conger, "As tanks rolled into ukraine, so did malware. then microsoft entered the war," February 2022. [Online]. Available: https://nyti.ms/3XktWb0

[8] T. Burt, "The hybrid war in ukraine," 2022. [Online]. Available: bit.ly/3W5UI6k

[9] DEF CON, "Def con ctf archive," 2022. [Online]. Available: https://bit.ly/3Z8nHcg

[10] A. D. Yan Shoshitaishvili, Jeff Crowell, "The order of the overflow," 2016. [Online]. Available: https://oooverflow.io/ooo-dc-cfo-proposal.pdf

[11] R. Fanelli and T. OConnor, "Experiences with practice-focused undergraduate security education," in *Cyber Security Experimentation and Test (CSET)*. Washington, DC: USENIX, August 2010, pp. 1–8.

[12] W. M. Petullo, K. Moses, B. Klimkowski, R. Hand, and K. Olson, "The use of {Cyber-Defense} exercises in undergraduate computing education," in *2016 USENIX Workshop on Advances in Security Education (ASE 16)*. Austin,TX: USENIX, 2016, pp. 1–8.

[13] National Security Agency, "Nsa cyber exercise (ncx)," 2022. [Online]. Available: https://www.nsa.gov/Cybersecurity/NSA-Cyber-Exercise/

[14] J. Song and J. Alves-Foss, "The darpa cyber grand challenge: A competitor's perspective," *IEEE Security & Privacy*, vol. 13, no. 6, pp. 72–76, 2015.

[15] T. Shellphish, Phrack: Cyber Grand Shellphish, 2017. [Online]. Available: http://www.phrack.org/issues/70/4.html

[16] F. Wang and Y. Shoshitaishvili, "Angr-the next generation of binary analysis," in *2017 IEEE Cybersecurity Development*. Cambridge, MA: IEEE, 2017, pp. 8–9.

[17] T. OConnor, C. Mann, T. Petersen, I. Thomas, and C. Stricklan, "Toward an automatic exploit generation competition for an undergraduate binary reverse engineering course," in *Innovation and Technology in Computer Science Education (ITiCSE)*. Dublin, Ireland: ACM, July 2022.

[18] S. Bratus, "What hackers learn that the rest of us don't: notes on hacker curriculum," *IEEE Security & Privacy*, vol. 5, no. 4, pp. 72–75, 2007.

[19] A. Carlin, D. P. Manson, and J. Zhu, "Developing the cyber defenders of tomorrow with regional collegiate cyber defense competitions (ccdc)." *Information Systems Education Journal*, vol. 8, no. 14, p. n14, 2010.

[20] B. S. Meyers, S. F. Almassari, B. N. Keller, and A. Meneely, "Examining penetration tester behavior in the collegiate penetration testing competition," *ACM Transactions on Software Engineering and Methodology (TOSEM)*, vol. 31, no. 3, pp. 1–25, 2022.

[21] D. Manson and A. Carlin, "A league of our own: the future of cyber defense competitions," in *Communications of the IIMA*, vol. 11. New Orleans, LA: IIMA, 2011, p. 1.

[22] US Air Force, "Hack-a-sat," 2022. [Online]. Available: https://hackasat.com

[23] R. Petersen, D. Santos, M. Smith, and G. Witte, "Workforce framework for cybersecurity (nice framework)," 2020.

[24] NSA, "Academic requirements for designation as a cae in cyber operations fundamental," 2022. [Online]. Available: https://bit.ly/3i9MNH9

[25] T. J. Burns, S. C. Rios, T. K. Jordan, Q. Gu, and T. Underwood, "Analysis and exercises for engaging beginners in online CTF competitions for security education," in *2017 USENIX Workshop on Advances in Security Education (ASE 17)*. Vancouver, BC, Canada: USENIX, 2017.

[26] K. Chung, "Live lesson: Lowering the barriers to capture the flag administration and participation," in *2017 USENIX Workshop on Advances in Security Education (ASE 17)*. Vancouver, BC, Canada: USENIX, 2017.

[27] S. R. Fisk, T. Wingate, L. Battestilli, and K. T. Stolee, "Increasing women's persistence in computer science by decreasing gendered self-assessments of computing ability," in *Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education V. 1*. Providence, RI: ACM, 2021, pp. 464–470.

[28] M. S. Peteranetz, A. E. Flanigan, D. F. Shell, and L.-K. Soh, "Future-oriented motivation and retention in computer science," in *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*. Baltimore, MD: ACM, 2018, pp. 350–355.

[29] C. Swain and T. Pearson, "Bridging the digital divide: A building block for teachers," *Learning and Leading with Technology*, vol. 28, no. 8, pp. 10–13, 2001.

[30] S. Krause-Levy, M. Minnes, C. Alvarado, and L. Porter, "Experience report: Designing massive open online computer science courses for inclusion," in *Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education V. 1*. Virtual Event: ACM, 2021, pp. 95–101.

[31] A. Ibrahim, C. Gunn, L. Mitchell, and S. Khattab, "Rethinking the bottleneck in diversifying the cybersecurity talent pool: What actions can we take and how can we measure success?" in *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 2*. Providence, RI: ACM, 2022, pp. 1194–1194.

[32] European Union Agency for Cybersecurity, "International cybersecurity challenge (icc)," 2022. [Online]. Available: https://bit.ly/3GERr9B

[33] B. W. Tuckman and M. A. C. Jensen, "Stages of small-group development revisited," *Group & organization studies*, vol. 2, no. 4, pp. 419–427, 1977.

[34] A. Bittau, A. Belay, A. Mashtizadeh, D. Mazières, and D. Boneh, "Hacking blind," in *2014 IEEE Symposium on Security and Privacy*. San Jose, CA: IEEE, 2014, pp. 227–242.