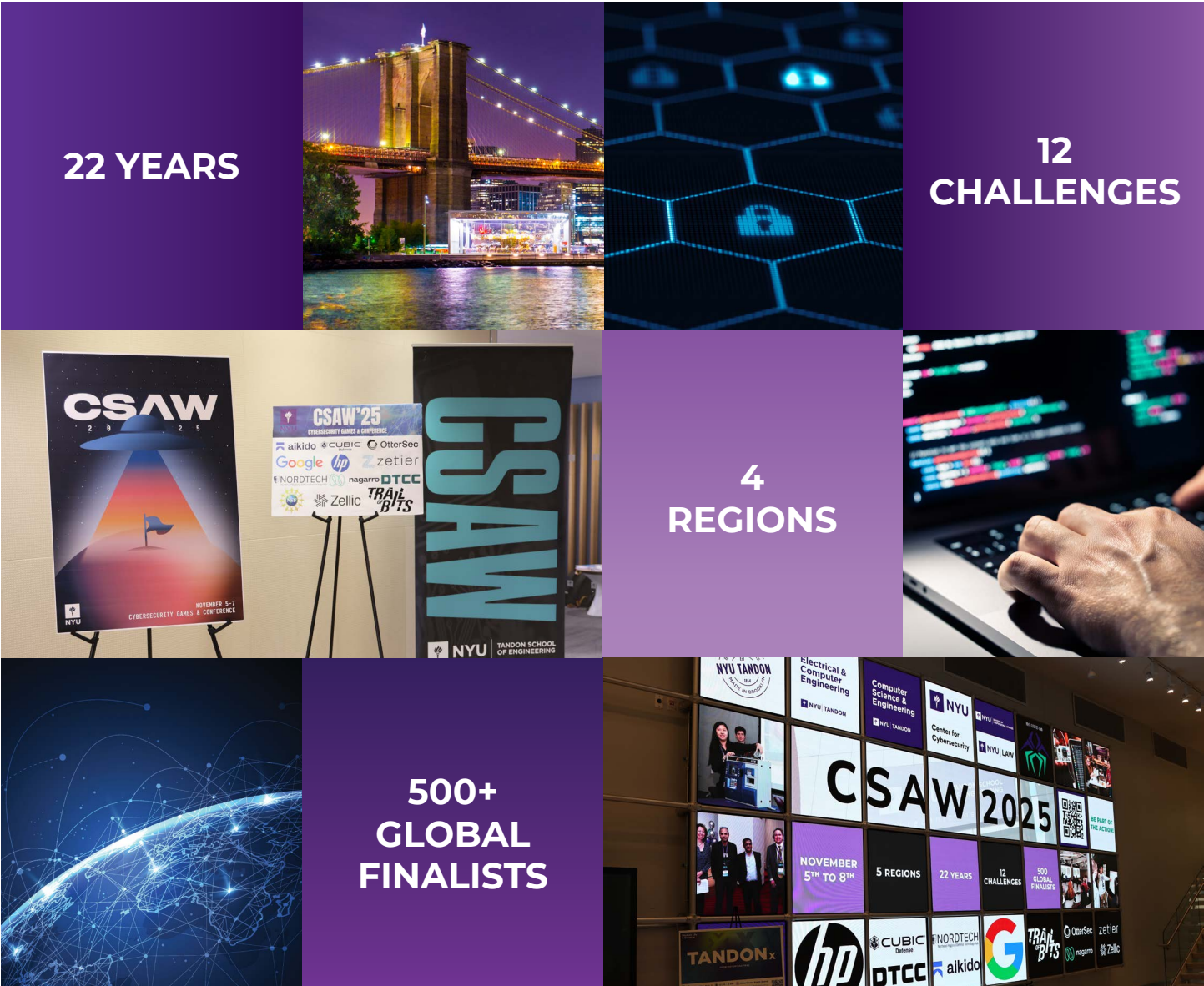


CYBERBYTE



22 YEARS

12
CHALLENGES

4
REGIONS

500+
GLOBAL
FINALISTS

CSAW '25

ADDING AI, SUBTRACTING EMERGING THREATS, MULTIPLYING CYBER PROTECTIONS

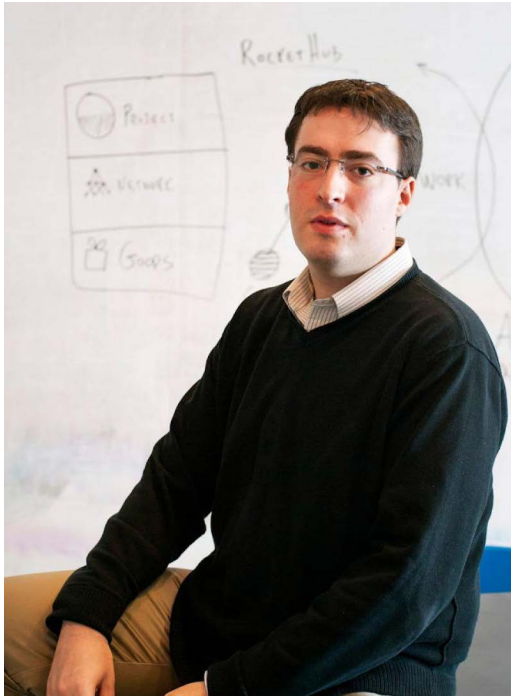
In November, 2025, CSAW, an event once known as Cybersecurity Awareness Week that has become the world's most comprehensive student-run cybersecurity event, returned to four global centers—its initial and longest running site at NYU Tandon in Brooklyn, Abu Dhabi (UAE), Kanpur (India), and Valence (France). Now in its 22nd iteration since its initial launch in 2003, the newest edition of the perennial program again served to raise global awareness of cyber issues, as it applied the combined knowledge, energy, and enthusiasm of students to the solution of real-world problems.

CENTER FOR
CYBERSECURITY

 **NYU | TANDON**

A NOTE FROM THE CSAW TEAM

From Awareness to Anticipation



Attackers are now using large language models to probe code, craft social engineering campaigns, and automate vulnerability discovery. Yet, those same models can help researchers identify weaknesses in complex systems and move toward automated repairs. The question facing educators and researchers is direct: are we preparing students to enter the shifting workforce of today and the future?

CSAW '25 put that question to the test. Across four global sites in Brooklyn, Abu Dhabi, Kanpur, and Valence, more than 3,000 participants and 500 finalists took on 12 challenges spanning AI, hardware security, manufacturing integrity, robotics, and critical infrastructure protection. Students built agentic CTF

solvers, designed AI-powered biochip authentication pipelines, and probed side-channel vulnerabilities using LLM-generated code. These were not abstract exercises. They required the same creative thinking and technical depth that cybersecurity professionals use on the job.

What makes CSAW distinctive, twenty-two years into its run, is how its mission has stayed true while evolving. The "A" still stands for awareness, but the competitions now emphasize Anticipation, and Applied problem-solving. New additions this year (the Agentic Automated Capture the Flag Competition, the Operational Technology Security Competition, and Europe's TrustRobotics Challenge) reflect that shift. So does the Applied Research Competition, where winning papers ranged from satellite authentication to GPU memory attacks to AI-enabled abuse applications.

This issue captures the look and feel of CSAW '25. Competition write-ups come from the student leads and faculty who designed and ran the challenges. The Industry Speaker Series and Career Fair show how corporate and government sponsors connect the academic program to professional practice. Site reports from the European and Middle Eastern and North Africa (MENA) sites offer global perspectives, while our listing of first-place winners highlight achievements from India to France to Croatia.

None of this happens without a large collaborative network. CSAW is sustained by NYU's campuses in New York and Abu Dhabi, IIT Kanpur, the University of Delaware, Grenoble INP-Esisar at UGA, and a growing roster of partner schools, sponsors, mentors, and industry participants. That network makes a globally distributed, student-centered program possible.

At the NYU Center for Cybersecurity (CCS), we see CSAW as one expression of a broader commitment: preparing students to build solutions, publish research, and enter the profession ready for the challenges AI is creating. The students in this issue are already doing that work. We are proud of what they accomplished together, and we think you will be too.

Enjoy!

Alon Hillel-Tuch

Industry Assistant Professor of Computer Science and Engineering &
Faculty Director, OSIRIS Lab
NYU Tandon School of Engineering

BY THE NUMBERS

Breaking down CSAW 2025 Global by the numbers, the event featured:

US-CANADA SITE

300+
participants

85 (approx.)
finalists

13
sponsors

7
competitions

GLOBALLY

3,000-plus
total participants in
all rounds

500-plus
finalists

12
unique global
challenges

4
global sites

**Multiple
countries**
represented



MENA

125
teams in qualifiers

120
finalists

8
countries

5
competitions

Europe

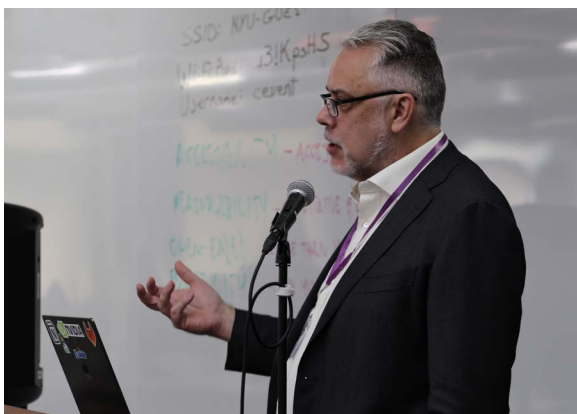
125
finalists

45
universities

14
countries

6
competitions





SPEAKER SERIES

Opening the conference at the Brooklyn site was a series of talks on topics that ranged from closing the historical separation between physical security and cybersecurity, to arguing why CTF competitions are best done in-person.

The speakers and topics were:

- Mike Wilkes, Enterprise CISO at Aikido Security in New York City, speaking on "Operational and Strategic Considerations for Using Generative AI in Security."
- Ron Eytchison, Security Officer at Trail of Bits in New York City, speaking on "Buttercup and DARPA's AI Cyber Challenge"
- Anna Staats, Cyber Engineer at Zetier, Arlington, Virginia, speaking on "From Pwn to Paycheck: Security Research as a Career." Staats focused on how to connect the skills developed in CTF and other hacking competitions to real-world applications in security research.

- Raf Portnoy, Chief Technical Officer of the Metropolitan Transit Authority and adjunct faculty at Tandon Online. Rather than a formal talk, Portnoy spoke informally on a number of security topics in a dialogue with CCS faculty member Alon Hillel-Tuch.
- Robert Chen, Founder, and Michael Debono, Security Researcher, OtterSec, speaking on "Host more (Onsite) CTFs!" The talk not only made the case for bringing more CTFs "into the physical world," but also gave tips on how to pull such events off "without melting your infrastructure or yourself in the process."
- Shawn P. Baird, Director of Offensive Security for DTCC, explored the evolving landscape of offensive cybersecurity, focusing on "the tactics of Red Team professionals and the growing impact of artificial intelligence on social engineering attacks."

After a lunch break, several of the speakers joined personnel from Snvx, Darktrace, TIAA, and Zellic, to meet with potential job seekers at the CSAW Career Fair. Attendees had the opportunity to discuss various professional options in the domain of cybersecurity, and to leave resumes for consideration for current and future openings.

LET THE GAMES BEGIN

While talks and one-on-one interactions with professionals enriched the overall experience for attendees, most of them came to their regional CSAW site to play. While two challenges—Capture the Flag and the LLM CTF Attack Challenge—launched their Brooklyn campaigns on Thursday, the remaining five—Applied Research, Hack3D, AI Hardware Attack, Embedded Security, and the OT Security Competition—kicked off on Friday, November 7. Winners were crowned in a special session the following day.

We asked a few student leads from Brooklyn and Abu Dhabi—and one faculty member—to share quick impressions of their respective competitions. Their summaries follow.



OPERATIONAL TECHNOLOGY SECURITY, BROOKLYN

Submitted by Mohamed El Atoubi, Ph.D. Student, NYU Abu Dhabi, and Student Lead, Operational Technology Security Competition

The in-person Operational Technology (OT) Security Competition debuted in Brooklyn on November 7. This pioneering event offered a unique opportunity for students to address authentic OT challenges, partner with peers, and demonstrate their proficiencies in a competitive, yet supportive, setting. Six teams participated in the final event during which they tackled three different attacks—Social Engineering, Network Intrusion, and Industrial PLC—over the course of a four hour session.

One challenge we faced in designing the competition was how to tailor the technically-heavy content for a broad audience, as we wanted the event to be open to anyone interested in learning about operational security and cybersecurity in general. We succeeded in doing this by mixing the format and styling of traditional cybersecurity CTF challenges with the more complex operational technology concepts.

First and second place awards in the inaugural competition went to two different teams of NYU Tandon graduate students. Amber Mohsin and Yilin Yang captured first place, while Yash Nagare and Gitikaa Babbar took second place. The organizers gave a special award to Honore Mandiamy of CUNY's New York City College of Technology for Best Social Engineering Attack.



BIOHACK 3D, ABU DHABI

*Submitted by Navajit Singh Baban,
Postdoctoral Associate, NYU Abu Dhabi*

Biochips, those tiny lab-on-a-chip marvels revolutionizing diagnostics, drug discovery, and point-of-care testing, are game-changers in healthcare, and the global biochip market is now on track to hit \$26B by 2030. However, this potential profitability makes it susceptible to a number of very real risks—including counterfeiting (which the World Health Organization estimates affects 2-3% of global trade), IP theft, tampering, and supply chain vulnerabilities. Such risks can also compromise patient safety and biomedical research.

In the wake of these concerns, the fourth edition of the Biochip Security Hackathon, better known as BioHACK3D, returned to NYU Abu Dhabi on November 7. This year's edition challenged

participants to design AI-powered authentication schemes using melt-electrowritten (MEW) QR Codes. MEWs are unique stochastic identifiers that resist cloning, and enable tamper-proof authentication-based security. The hackathon was jointly organized with IIT Kanpur, IIT Kharagpur, IIT Guwahati, and IIT Roorkee, with judges and mentors drawn from both NYU/NYU Abu Dhabi and these IITs.

Twelve teams from across the UAE participated in the preliminary virtual round, with 5 teams making the finals. The victorious first place team from NYU Abu Dhabi—Maulen Mukhatbek, Airin H. and Youssef Ben Arab—proposed a sophisticated, reproducible authentication pipeline that excelled in all three tasks by using biometric-style metrics to demonstrate reliability. Reflecting on the win, Mukhatbek wrote: “We worked on an AI based approach for authenticating physical biochips, combining ideas from cybersecurity, machine learning and bioengineering. It was a challenging but very rewarding experience.”

See you at BioHACK3D 2026 – stronger, smarter, and more secure!!!



EMBEDDED SECURITY

*Submitted by Lars Folkerts, Ph.D. Student, University of Delaware,
and ESC Global Student Co-Lead*

How well can Large Language Models (LLMs) identify side-channel vulnerable code? This was the central theme of the 2025 Embedded Security Challenge, which invited competitors to deploy leading LLMs, such as ChatGPT and Gemini, against classic embedded security vulnerabilities on the Chipwhisperer Nano board.

Embedded Security Winners: The First Place SigPwny Team from the University of Illinois, Urbana-Champaign (USA) at the CSAW US/Canada Awards Presentation

The competition—one of several CSAW challenges that accepted entries from multiple geographic regions—focused on two critical types of hardware attacks: power side-channels, which can be exploited to reveal sensitive information; and fault injection attacks (FIAs) that can force the chip into an insecure state at a critical moment. Success hinged on the teams' ability to craft highly specific prompts that would guide the LLMs towards these insecurities, and generate the necessary code to collect power traces, perform complex analysis, and ultimately execute the exploit. The results of the competition strongly emphasize that AI models, when properly directed by human expertise, can become formidable tools for both offense and defense in embedded systems.

HACK 3D, BROOKLYN

Submitted by Dr. Nikhil Gupta, Professor of Mechanical and Aerospace Engineering, NYU Tandon

(Photo Caption): Hack 3D Winners: Jason Blocklove from NYU Tandon (r), representing the 1st place team, and Caleb Norton from Texas A&M University, representing the 3rd place team.

Over the past decade, the National Science Foundation-supported Hack3D competition has established itself as a leading platform for driving awareness and innovation at the intersection of cybersecurity and manufacturing. The 10th edition of Hack3d, which focused on digital manufacturing and additive systems, was held November 7 as part of the annual CSAW '25 event at NYU Tandon in Brooklyn.

The preliminary rounds, held October 6 and 7, saw an incredible turnout, with teams showcasing impressive creativity and technical depth. In the finals a team from NYU Tandon School of Engineering—Jason Blocklove, Md Raz, and Khaled Al Mutawa—captured the top award, with teams from Ohio State University and Texas A&M University placing second and third placing second and third, respectively.

A huge thank you to our judges — Dr. Vikas Varshney of the Air Force Research Laboratory, Chris Adkins of Materialise, and Dr. Yash Parikh of EOS — for their time, expertise, and thoughtful evaluations. In addition, we thank Dr. Mark Yampolskiy of Auburn University for generously providing the dataset used to develop the problem for the final round.



Hack 3D Winners:

Jason Blocklove from NYU Tandon (r), representing the 1st place team, and Caleb Norton from Texas A&M University, representing the 3rd place team.



HACK MY ROBOT, ABU DHABI

In November 2025, the Hack My Robot (HMR) competition returned to CSAW MENA for its fourth consecutive edition. This year marked the highest number of qualification round participants to date, as 79 students on 23 teams from 4 countries competed for an invitation to the finals at New York University Abu Dhabi.

Co-organized by the S.M.A.R.T. Construction Research Group, the competition brings real-world use cases and construction-site context to the challenge. A common emphasis among all finalist teams was the real-world risks of Robot Operating System (ROS) 1, especially its limited built-in authentication and authorization. These limitations can enable attacks like man-in-the-middle and data injection. The teams emphasized that these vulnerabilities are also safety critical in connected construction environments, where robots operate in proximity to people and other equipment.

The winning team from Jordan University of Science and Technology stood out by developing an automated hacking tool that specifically targeted vulnerabilities in ROS 1. The team demonstrated how vulnerabilities can be operationalized quickly into repeatable attack workflows.

Evaluating these outcomes was a highly competent panel of judges: Christoforos Vasilatos (cybersecurity researcher), Abdulla Abdullayev (cybersecurity manager in a construction company), Erika Pärn (research scientist working on construction technologies and cybersecurity), and Nader Kayali (cyber forensics consultant).

The workshop concluded with a commitment to continued collaboration between NYU Abu Dhabi and the Dubai Police. In summarizing the workshop on the official conference Instagram page, organizers complemented the “insightful discussions, academic rigor, and forward-thinking ideas” of the session and marked it as a standout moment on this year’s agenda.

GLOBAL PERSPECTIVES:

HIGHLIGHTS FROM OTHER CSAW SITES

CSAW is truly a global affair and our report on the events of 2025 would not be complete without checking in with our global sites. Below are reports from CSAW Europe, and CSAW MENA. Thanks to Léane Lattard, Assistant CSAW Europe coordinator at Grenoble INP-Esisar, UGA, and Hari Ramasubbu, Senior Center Coordinator at the Center for Cyber Security at NYU Abu Dhabi, for providing details and descriptions of their respective events.



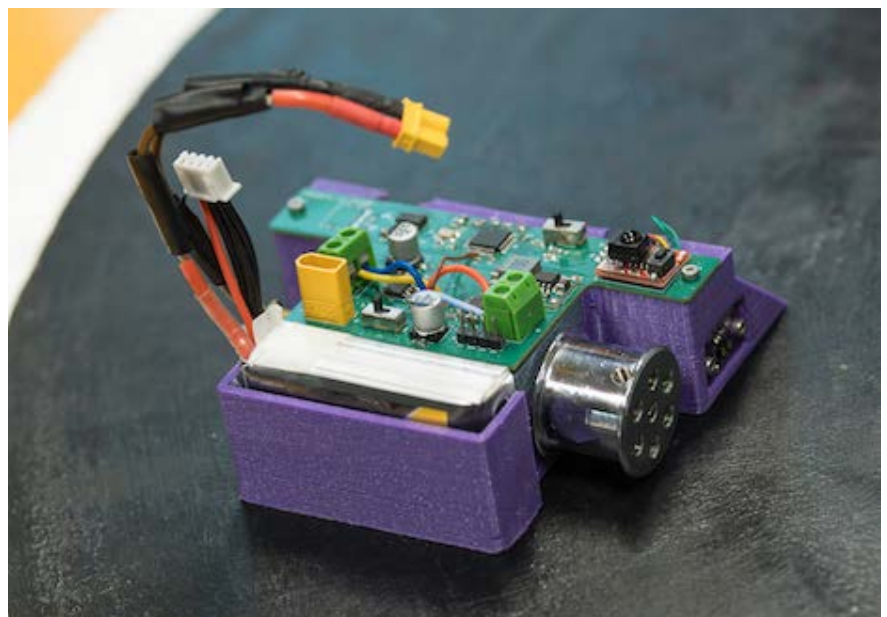
EUROPE

The CSAW Europe event packed a lot of activities, camaraderie, and information into a two day program at Grenoble INP-Esisar, UGA in Valence, France. The event was held November 13 and 14, 2025, and drew a record-breaking 83 on-site attendees to a program marked by diversity, expertise, and incredible community energy. All totaled the event, including qualifying rounds, engaged nearly 900 participants, including staff, competitors and speakers.

Following up on the success of the Cybersecurity Awareness Communication Challenge (CAC²), launched last year to engage students from all disciplines in raising awareness of cybersecurity threats and best practices, organizers introduced an exciting new competition for 2025. The TrustRobotics Challenge was designed to “bridge the gap between theoretical research and practical validation.” Unlike traditional paper-centric events, the TrustRobotics Challenge required participants to demonstrate their solutions in a realistic simulation or an experimental setting, and to demonstrate safety, resilience and trust in robotic systems. A dedicated session was also organized to allow in-depth technical discussions and networking with leading experts. The new competition was well-received, drawing finalists from Belgium, Bulgaria, Croatia, France, Germany, Italy and Romania.

CAC² also returned for 2025, challenging participants to teach the general public about phishing and spoofing attacks. Other competitions run on November 14 included Applied Research, Embedded Security, Capture the Flag, and the Red Team Competition for high school students, which aims to point young people towards future cybersecurity careers. The latter event is open to all high school students in metropolitan France, and was co-created by Grenoble INP-Esisar, UGA in partnership with Root-Me, a platform for learning computer security and hacking.

Rounding out the program was a welcoming social event on 11/13, networking opportunities, and campus visits from K-12 schools.





MENA

CSAW'25 at NYU Abu Dhabi brought together brilliant student competitors, industry leaders, and innovators from across the region for a dynamic celebration of cybersecurity talent and learning. As part of the world's largest student-run cybersecurity event, CSAW continues to serve as a launchpad for emerging cyber professionals, combining competitions, real-world problem-solving, and powerful networking opportunities.

The program began with an inspiring keynote by H.E. Doctor Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government. The talk set the tone for an engaging and insightful day that included a panel discussion on the “Cybersecurity Landscape and Careers in the UAE.” Moderated by Dr. Lilas Alrahis of Khalifa University in Abu Dhabi, the panelists—Sukiraman Manivannan (CPX), Simon Reiniche (Innixus / CyberE71), and Sarfaraz Kazi (HivePro)—explored how AI, local innovation, and national strategies are shaping the region's cybersecurity future. From bridging the talent gap to fostering public-private collaboration and startup growth, the session offered valuable perspectives for students and professionals eager to build impactful careers in cybersecurity. Complementing the discussions, the CSAW Career Fair provided students with direct access to leading employers, including CyberE71, Lockheed Martin, and CENSUS.

The heart of CSAW MENA is its world-class competitions. Winners in each category demonstrated exceptional problem-solving abilities. Below is a quick summary of the various challenges hosted at the site.

Capture The Flag: Thirty-seven participants from four different countries competed in the final round, with 10 teams emerging as finalists out of a total of 90 teams in qualifying rounds.

Hack My Robot: See the full write-up on this competition in the “Let the Games Begin” section above.

Applied Research Competition: From cutting-edge technologies to novel approaches in threat detection and mitigation, the research presentations showcased the forefront of cybersecurity research.

BioHack 3D: See the full write-up on this competition in the “Let the Games Begin” section above.

LLM CTF Attack Competition: Collectively, 14 teams and 41 participants accepted the challenge to design prompts or automated frameworks that can leverage Human-in-the-loop LLMs to identify vulnerabilities and capture flags across a number of threat categories, including web exploitation, reverse engineering, and forensics.

GLOBAL FIRST-PLACE ROUND-UP



AGENTIC AUTOMATED CTF (GLOBAL)

Kamdin Bemby, Rochester Institute of Technology (USA); Daniel Mayer, Christopher Newport University (USA); George Filippov, University of Central Florida (USA); Zander Chen and Wentao He, New York University (USA)

AI HARDWARE ATTACK (GLOBAL)

Indian Institute of Technology, Kanpur (India)
Soham Panchal, Ananthan R, Jugal Pahuja, and Ramya Rasika S R

APPLIED RESEARCH COMPETITION

Europe | Joshua Smailes, University of Oxford (England), presenting *SatIQ: Extensible and Stable Satellite Authentication using Hardware Fingerprinting*

MENA | Hamza Mouhcine, Qatar Computing Research Institute (Qatar), presenting *LLMxCPG: Context-Aware Vulnerability Detection Through Code Property Graph-Guided Large Language Models*

US-Canada Social Impact | Daniel Olszewski, University of Florida, Gainesville (USA) presenting *Analyzing the AI Nudification Application Ecosystem*

US-Canada Technical Impact |

Shaopeng Lin, University of Toronto (Canada) presenting *GPUHammer: Rowhammer Attacks on GPU Memories are Practical*

BioHack 3D (Global)

NYU Abu Dhabi (UAE) Maulen Mukhatbek, Airin Haque, Youssef Ben Arab

CAPTURE THE FLAG

Europe | Great Britain, Alexander Shaw and Rob Derry, Warwick University, Coventry; Andrej Ljubic, University of Oxford; Harry Chen, University of Cambridge

MENA | Ecole Polytechnique Sousse (Tunisia)

Dahmani Toumi, Chebbi Jasser, Badreddine Chamkhi, Mehdi Bel Haj Amor

US-Canada | Andrew Effenhauser and Allen Chang, Georgia Tech, Atlanta (USA); Nathan Wong, University of Hawaii, Mānoa (USA); Tanush Madanbhavi, Rochester Institute of Technology (USA)

CYBERSECURITY AWARENESS COMMUNICATION CHALLENGE (EUROPE ONLY)

Grenoble INP-Esisar, UGA (France)
Valentine Un and Baptiste Bonnet

EMBEDDED SECURITY CHALLENGE

Europe | Sapienza University of Rome (Italy)
Kristjan Tarantelli, Francesco Bianchi, Simone Di Maria and Federico Angelilli

India | Manipal Institute of Technology (India)
Krish Pandey, Anshuman Shukla, Aryan Saraf, Venkataraman Seshadri

US-Canada | University of Illinois, Urbana-Champaign (USA)
Minh Duong, Cygnus Qiu, Krishnan Shankar, and Shovan Jagadev

HACK3D (GLOBAL)

NYU Tandon School of Engineering, Brooklyn (USA)
Jason Blocklove, MD Raz, and Khaled Al Mutawa

HACK MY ROBOT

MENA | Jordan University of Science & Technology Ar Ramtha (Jordan)
Hashem Alsalthi, Yazan Alrousan, Khalid Amoura, Qutibah Ananzeh

LLM CTF Attack Competition

India | IIT (Indian School of Mines) Dhanbad (India)
Rachit Kumar Pandey and Sanjib Behera

MENA | New York University Abu Dhabi, UAE
Pearl Rwauya, Simon Grange, and Safa Al Almeri

US-Canada | NYU Tandon, New York (USA)
Shiv Thaker, Samkit Shah

Red Team Competition (Europe only)

Lycée Pierre Termier, Grenoble (France)
Nmapéro

TrustRobotics (Europe Only)

University of Zagreb (Croatia)
Luka Sikdar and Branimir Caran

Craig Newmark Philanthropies Funds New Cybersecurity Clinic at NYU to Defend Under-Resourced Nonprofits, Schools, and Community Organizations from Cybercrime



Craig Newmark. Photo by Ian Gittler



Under-resourced organizations carry an outsized share of cyber risk in this country, and they shoulder it largely alone. NYU brings together the law, engineering, and policy chops to actually do something about it, and to train the cyber civil defenders we'll need for decades to come.

- Craig Newmark

Founder, craigslist and Craig Newmark Philanthropies



NYU | TANDON

CENTER FOR CYBERSECURITY

cyber.nyu.edu