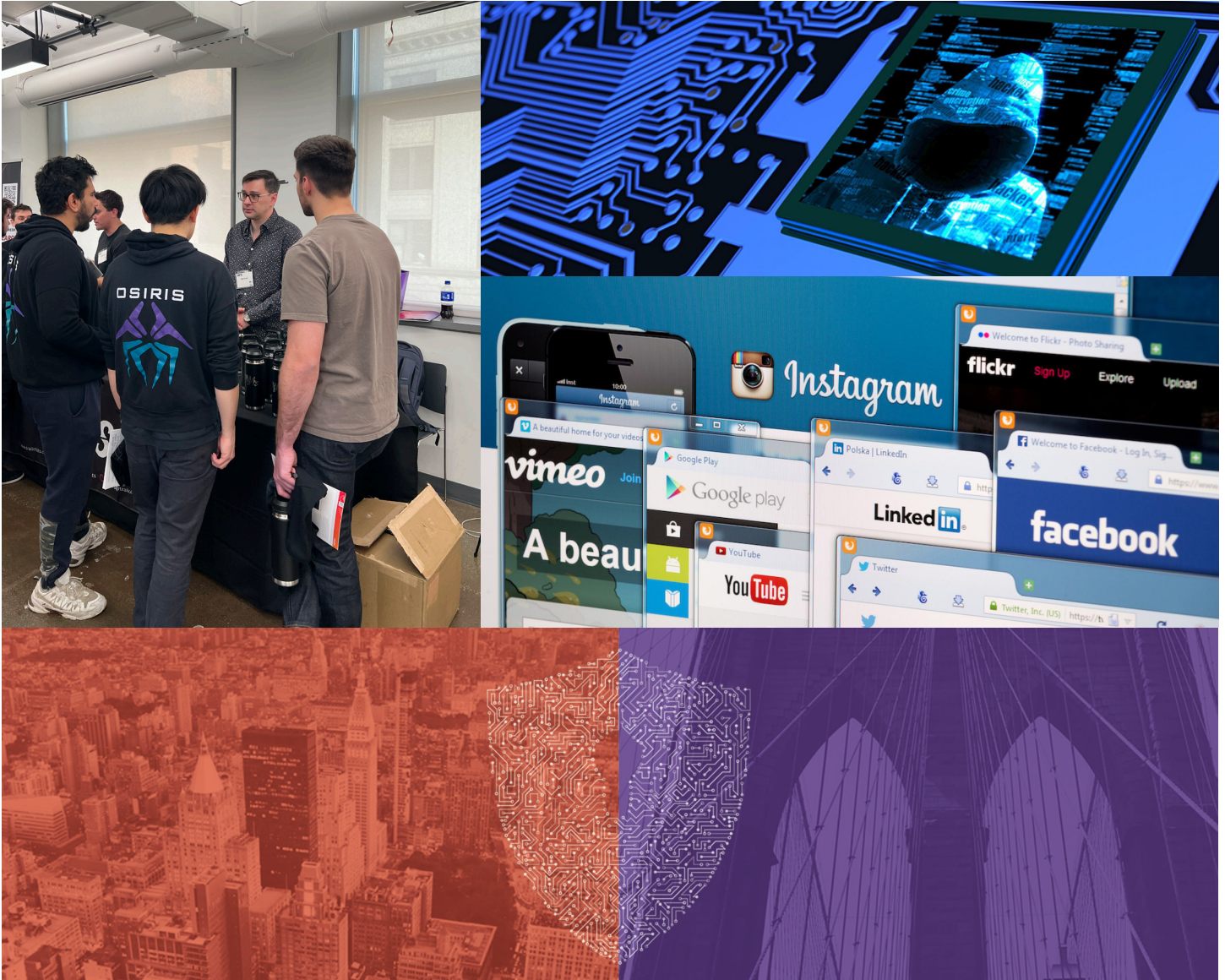


# CYBERBYTE

CELEBRATING THE BLENDED ENGINEERING HERITAGE OF NYU TANDON SCHOOL OF ENGINEERING



## A Quarter-Century at the Forefront of Cybersecurity

In 2024, we're celebrating some major milestones at NYU Tandon, including 170 years since we were founded and 10 years since the merger with Polytechnic University. In addition, it's been 25 years since one of the very first cybersecurity courses in the nation was taught at our school; 20 years since the launch of CSAW, which has grown into the most comprehensive student-run cyber event in the world; and 15 years since the Center for Cybersecurity was founded and our first cybersecurity master's degree was offered.

Here's to many more years of innovation and accomplishment.

CENTER FOR  
CYBERSECURITY





---

## A NOTE FROM THE EDITOR- IN-CHIEF

Perhaps one of the most insidious cybercrime trends of the last decade has been the increased deployment of technologies that can distort the truth. From deepfake techniques that can transform digital images or maliciously edit verbal messages, to disinformation campaigns designed to undermine facts or shift opinions, it often feels like reality itself is under attack.

As we enter a presidential election year, a heightened ability to sort truth from lies becomes particularly crucial. Thus, it seems like an appropriate time to spotlight the faculty and students of the Center for Cybersecurity who are at the leading edge of detecting, preventing, and/or mitigating deepfakes and misinformation. This time around, we're excited to let some of our talented Ph.D. students—Brian Timmerman (who graduates in May), Bruno Coelho, and Aditya Sirish A Yelgundhalli—shine some light on their current work in this arena. Timmerman, along with CCS faculty members Dr. Brendan Dolan-Gavitt, Dr. Siddharth Garg, and Dr. Rachel Greenstadt, and Tandon Ph.D. alum Kevin Gallagher, recently explored the development of two key deepfake discussion platforms to learn more about how these spaces are utilized by their members.

Meanwhile, Coelho, along with his colleagues in the CCS-affiliated Cybersecurity for Democracy project, has published a study on the important differences in the content of political advertising campaigns between English-language and Spanish-language political ads, and what this difference could mean as Latin voters play an increasingly more important role in US politics. Lastly, Yelgundhalli summarizes a new security project called gittuf that adds granular write permissions to a Git repository, permitting any user to verify that agreed upon policies were followed. This protects against unauthorized modifications of software at any stage in its development.

We round out our look at the topic by checking in on current developments in deepfakes research conducted by CCS cofounder Dr. Nasir Memon. Lastly, we get a different perspective on the topic by profiling CCS cochair Randal Milch from the NYU Law School. Milch provides insights on the important role of law and policy in counteracting deceptive cyber strategies.

This Spring 2024 issue also features a conversation with graduate student Sofija Jancheska and a chat with recent M.S. graduate Abhinav Kore, who is now a senior cybersecurity engineer at Workday, as well as a look at a few of the Ph.D. candidates who led new challenges at CSAW '23.

And while we're noting some important anniversaries in cybersecurity education at Tandon (see cover), we're also marking the kick-off of NYU's "170 Years of Engineering" celebration, which honors the founding of engineering programs at NYU and Polytechnic University—two strong traditions that merged to forge an even stronger future. Our students, faculty, and alumni have had a hand in some of the most transformative technologies of the last 170 years, and there's more on the horizon as we fight deepfakes, prevent identity thefts, develop more secure systems, and all the other work you'll read about in this issue.

Enjoy!

**Dr. Quanyan Zhu,**  
Editor in Chief

---



## IN THIS ISSUE

|                                      |    |
|--------------------------------------|----|
| A NOTE FROM THE EDITOR-IN-CHIEF      | 2  |
| RESEARCH FOCUS: DEFLECTING DECEPTION | 4  |
| FACULTY PROFILE: RANDAL MILCH        | 9  |
| PH.D. PROFILE: SOFIJA JANCHESKA      | 12 |
| ALUMNI PROFILE: ABHINAV KORE         | 14 |
| WRAPPING UP CSAW '23                 | 16 |
| CCS NEWS                             | 27 |
| EVENTS                               | 28 |
| AWARDS AND HONORS                    | 29 |

## STAFF



Editor in Chief  
**Quanyan Zhu**



Editorial Copy Writer  
**Lois Anne DeLong**





## A PEEK INSIDE A DEEPAKE COMMUNITY

Can a platform devoted to executing deepfakes be considered a community? And, if so, what needs does it fulfill for its members? In a recent research project Brian Timmerman, a Ph.D. candidate in Computer Science and Engineering who works with Dr. Rachel Greenstadt on privacy issues, took a closer look at a particular platform called MrDeepFakes (NSFW content warning). The goal was to determine whether people were accessing the platform to initiate or purchase a deepfake, or to just learn more about the technology. As it turns out, the answer was a little bit of both. Here's how Brian explains his work.

"Deepfakes have become a dual-use technology with applications in the domains of art, science, and industry. However, the technology can also be leveraged maliciously in areas such as disinformation, identity fraud, and harassment. In response to the technology's dangerous potential, many deepfake creation communities have been deplatformed. Included in this purge was the technology's originating community, r/deepfakes. When MrDeepFakes (NSFW) opened in February 2018, just eight days after the removal of r/deepfakes, it did so as a privately owned platform. It also claimed for itself the title of the largest deepfake creation and discussion platform currently online. Positioning itself as a community hub stands in contrast to the site's main purpose, which is hosting nonconsensual deepfake pornography, or manipulated pornographic images of public figures produced without consent.

## RESEARCH FOCUS:

# DEFLECTING DECEPTION, DAUNTING DECEIVERS, DEFENDING DATA

In many ways, disinformation attacks or deepfake recordings may be the most insidious of all cyber threats because they seek to destroy the very tentpoles on which our society depends. Disinformation, particularly in times of crisis, such as the recent Covid pandemic, undermines trust in the media, government, science, and the notion of a concrete reality. And, deepfakes can damage reputations and unduly influence crucial decision-making, such as choosing political candidates.

In this article we offer a small sampling of how NYU researchers are combating these threats. We start by getting some first-hand insights into three recent research initiatives headed by current CCS-affiliated Ph.D. students. Our research summaries conclude with new projects from the CCS-affiliated Secure Systems Laboratory, and two recent research contributions from CCS co-founder Professor Nasir Memon.



Utilizing both qualitative and quantitative analysis methods, we studied both MrDeepFakes and r/deepfakes to learn how these platforms were and are used by their members, as well as to identify how deepfakes-as-disinformation is viewed by the community. On both platforms, our team found the most common content type is purely technical in nature. Looking at the thoughts and opinions voiced by those who post on MrDeepFakes, we found a culture of

distrust toward alternative spaces regarding deepfake discussion, as well as a defensive posture regarding how deepfakes are seen by society as a whole. The researchers identified that this has contributed to an environment where the most resource-rich place to learn a deepfake skill set is also the primary market hub for nonconsensual deepfake pornography.”

Timmerman’s research is documented in a paper entitled “Studying the Online

Deepfake Community,” which was published in the proceedings of the 2023 Trust and Safety Research Conference. The paper was coauthored by Pulak Mehta, Progga Deb, Dr. Brendan Dolan-Gavitt, Dr. Siddharth Garg, and Dr. Greenstadt, all of NYU Tandon, and Tandon Ph.D. alumnus Dr. Kevin Gallagher, now an assistant professor at Universidade Nova de Lisboa in Portugal. You can read the paper at <https://doi.org/10.54501/jots.v2i1.126>.



## INFORMATION EQUITY

Bruno Coelho is a Computer Science Ph.D. Candidate at NYU’s Tandon School of Engineering who work with Dr. Damon McCoy to pursue projects that, in his words “utilize artificial intelligence (AI) for social good.” This interest has led to such diverse projects as creating a smart insect trap to detect dengue-carrying Aedes mosquitos, and analyzing illegal timber transport in the Amazon rainforest. Currently, he is focused on multilingual Natural Language Processing (NLP) techniques as applied to Spanish-language political ads. This work, done in association with Cybersecurity for Democracy (CfD), a CCS-affiliated research center, led to an analysis of differences between English and Spanish-language political ads during the 2020

U.S. presidential election. A paper based on this study was published in *In Proceedings of the ACM Web Conference 2023 (WWW’23)* in May 2023, and is available at <https://dl.acm.org/doi/10.1145/3543507.3583425>.

Bruno provided the following summary of this work, as well as some insights on other studies he has conducted in this arena for CfD.

“‘Propaganda Política Pagada: Exploring U.S. Political Facebook Ads en Español’ analyzes how equitable access to political communication was in the United States during the 2020 elections.

Using data collected from the Facebook Ad Library, we observe that Spanish speakers were served different types of ads from different types of advertisers than English speakers, and in lower amounts.

To put the numbers into perspective, we find only 1.17% of the ads were in Spanish, even though approximately one-eighth of the adult US population speaks Spanish, indicating a sizable under-represented demographic that is not prioritized on political advertisement.

Besides the amount of content, important aspects of representative information include who is producing it and how they choose to communicate it. We believe government communications ought not to discriminate and we found that both the U.S. federal government and local state agencies seem to do an adequate job of providing announcements on Facebook in minority languages. However, political parties and candidates have more leeway in how they solicit votes and, in general, do not target Spanish speakers in their native language. Furthermore, even when they do, we find less diversity in the amount of topics the content addresses, showing a difference in how these populations are targeted. Lastly, the overall lower proportion of ‘core’ political ads leaves the field open to other types of advertisers. For-profit companies especially (e.g. subdivisions of Meta) are relatively big spenders in Spanish content, mostly through neutral get-out-the-vote information.

We believe further fine-grained ad targeting transparency data from these private companies would allow for a more thorough analysis of these ads, something particularly important considering that even a skewed distribution of neutral ads has the potential to sway election results.”

Coelho adds, “This work helped to inform changes to Cybersecurity for Democracy’s Ad Observatory topic modeling system, an easily searchable database of information contained in political advertising on Facebook and other social media.”

## GLOBAL FACT-CHECKING



Another recent project “in the vein of determining the accurate representation of information,” Coelho continues, “looked at the effectiveness of LLMs (Large Language Models) in fact-checking across a diverse set of regions. Results show that models consistently underperformed in determining the factuality of statements stemming from the Global South (Latin America, Middle East, Africa) when compared to the Global North (Europe, North America, Asia-Pacific).

Overall, our results indicate the need for culturally aware and geographically diverse model training and evaluation. Such changes are vital for achieving equitable computational systems worldwide, and advancing equitable technological benefits across diverse international contexts. The full paper can be read at <https://arxiv.org/abs/2401.17839>.”

Looking at what may be ahead for political advertising on social media, Coelho points to legislation passed in Europe that, in his words, “puts further pressure on how social media platforms target users with political advertisements, and the transparency reports they must provide.” The General Data Protection Regulation (GDPR) gives individuals more control over their personal data and mandates that “clear consent” must be given before an individual’s personal data can be processed (see <https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/>). The GDPR has already cost Meta (formerly Facebook) 1.2 billion euros (\$1.3 billion) for transferring data collected from Facebook users in Europe to the United States without consent (see the NY Times article at <https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html>.) Coelho concludes, “It’ll be interesting to see how these changes might affect U.S. legislation and how advertisers change their strategies given the growing trend of political advertisement shifting to online platforms and the growing significance of Latino voters.”

According to its website, Cybersecurity for Democracy is a “multi-university center for problem-driven research and research-driven policy,” Co-led by Dr. McCoy and Tandon Ph.D. alumnae Dr. Laura Edelson, who is also an Assistant Professor of Computer Science at Northeastern University Khoury College of Computer Sciences, the C4D conducts “cutting-edge cybersecurity research to better understand the distorting effects of algorithms and AI tools on large online networks and work with platforms and regulators to help all parties understand the implications of our findings and develop solutions.”

## STRENGTHENING METHODS OF ATTESTATION

Another important defense strategy against misinformation is proof of authenticity. Several projects from the Secure Software Laboratory at NYU Tandon fall under this wider perspective of discouraging or preventing misrepresentation. Recently the lab, which is directed by Associate Professor Dr. Justin Cappos, formally introduced two new projects, gittuf and SBoMit. The former protects against unauthorized edits and changes in versioned software, while the latter provides an improved SBOM format-independent method for enhancing attestations. Late last year, both projects were adopted by the Open Source Security Foundation, a cross-industry forum of the Linux Foundation that works for the collaborative improvement of open source software security.

Aditya Sirish A Yelgundhalli, a Ph.D. candidate who has been the main driving force behind the gittuf project since its inception, summarizes that work as follows: “To deliver trustworthy software, it is imperative we secure the entire software supply chain, from the writing of source code, through the build processes, to distribution. Today, most software is written and updated using source code management tools, of which Git is the most popular. While Git has a number of security-related features, it lacks support for granular policies, such as which developers are trusted to make changes to a project, which part of a project a developer can make changes to, and so on. The new framework, known as gittuf—the “tuf” part of the name acknowledges







the SSL secure software strategy on which it is based—addresses these shortcomings without having to rely on centralized, unauditable systems that today are the only way to enforce such rules. By adding granular write permissions to a Git repository, gittuf allows any user to verify that agreed upon policies were followed. These policies can ensure changes were approved by at least two developers, and enables policy verification for historic repository changes using contemporaneous policies.”

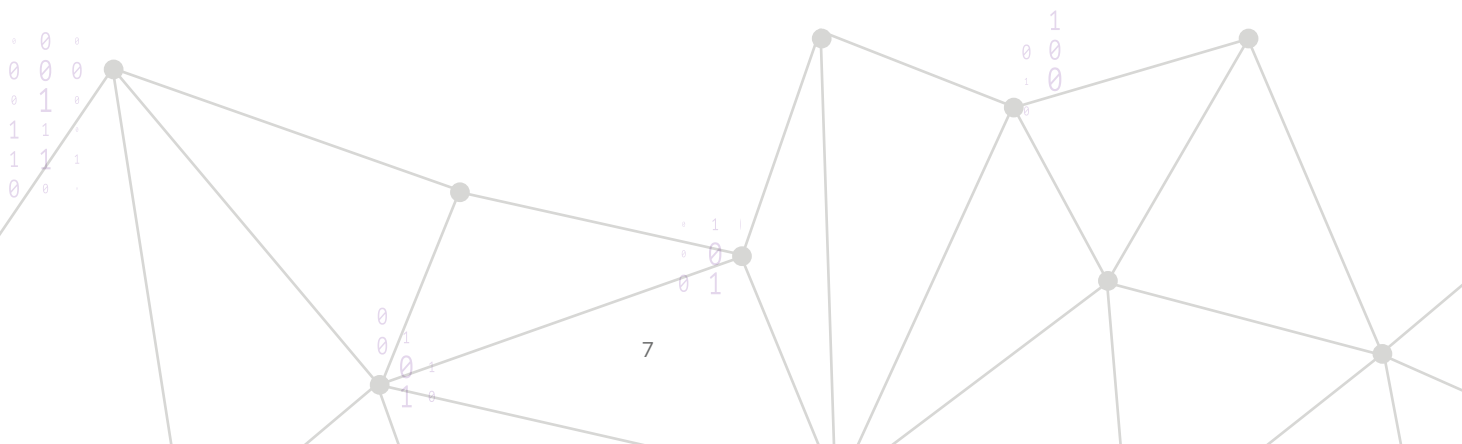
The other project, SBoMit, also borrows from an existing technology developed at the Secure Systems Laboratory, in this case a supply chain security strategy called in-toto. Developed along with partners across industry, including TestifySec and the Lockheed Martin Corporation, SBOMit closes an existing gap in current SBOM technology by providing confirmation that all the processes involved in creating the software were properly executed to generate the final SBOM.

The introduction of SBoMit comes at a time when SBOMs have emerged as a mandated security strategy in many of the U.S. government responses. The website for the Cybersecurity and Infrastructure Security Agency labels SBOMs as “a key building block in software security and software supply chain risk management.” As explained in a blog co-written by Cappos, an SBoMit “can be formatted in any preferred SBOM style,” and “references the original SBoMit document from which it was created. The document uses in-toto attestations, which are generated during the software build steps,” and “includes cryptographically signed metadata about every step involved in the software’s development, along with a

policy outlining the required procedures.” The blog emphasizes that adding signed metadata and a policy “significantly reduces the risk of accidental errors, such as skipping steps,” and by using in-toto attestations, “SBOMit enhances the ability to securely recover from compromises and to detect and thwart malicious activities within an organization.”

You can read more about SBoMit at <https://openssf.org/blog/2023/12/13/introducing-sbomit-adding-verification-to-sboms/>, and gittuf at <https://openssf.org/blog/2024/01/18/introducing-gittuf-a-security-layer-for-git-repositories/>.

In addition to the new projects mentioned above, The Archive Framework or TAF is an existing SSL project that clearly falls into the category of “defending the truth.” Developed in collaboration with the Open Law Library (<https://openlawlib.org/>), TAF “leverages TUF’s security capabilities to protect Git repositories and provide archival authentication.” The goal is to “ensure that “documents stored in Git repositories remain accessible and verifiable, not just in the immediate future, but for decades and even centuries to come.” TAF is already being used by several governments, including the District of Columbia, to secure their laws, and by two libraries, including the University of Wisconsin Law Library. The D.C. law library, secured with TAF, is publicly accessible on GitHub at <https://github.com/DCCouncil>. (Note: TAF was profiled in the Spring 2023 issue of CyberByte, which can be found at [https://drive.google.com/file/d/1nT8oqTK4NMhY6s9AEIMYRNV5V\\_GU-Lye/view](https://drive.google.com/file/d/1nT8oqTK4NMhY6s9AEIMYRNV5V_GU-Lye/view).





## PREVENTING IDENTITY FRAUD WITH AN ASSIST FROM BIOLOGY

CyberByte gives the last word on this topic to Center for Cybersecurity co-founder Dr. Nasir Memon. In the fight against deepfakes, few have been on the frontlines longer than the now Interim Dean of Computer Science, Data Science, and Engineering at NYU Shanghai. Three years ago, working with Dr. Pawel Korus, a research assistant professor at Tandon, Memon explored end-to-end optimization of photo acquisition and distribution (See <https://arxiv.org/pdf/1902.10707.pdf>). More recently, he collaborated with NYU colleagues Govind Mittal and Chinmay Hegde on a new technique for detecting real-time deepfakes on live video. Named “GOTCHA,” the technique employs a series of challenges, including facial expression, view angle, and ambiance, or digital manipulation of webcam feeds to “target vulnerabilities in the structure of modern deepfake generators and create perceptible artifacts for the human eye while inducing robust signals for machine learning-based automatic deepfake detectors.” As noted in a report entitled “GOTCHA: Real-Time Video Deepfake Detection via Challenge-Response” (see <https://arxiv.org/pdf/2210.06186.pdf>), when the research team evaluated the system “on a novel dataset of live users emulating deepfakes,” it revealed that the system “provides consistent, measurable degradation of deepfake quality, showcasing its promise for robust real-time deepfake detection when deployed in the wild.”

Memon has also advanced research in biometrics, an increasingly important defensive strategy against deepfakes and identity theft. Defined by the U.S. Department of Homeland Security as “measurable biological (anatomical and physiological) and behavioral characteristics that can be used for automated recognition (see <https://www.dhs.gov/biometrics>),” biometric techniques make it much harder for individuals to forge credentials that could grant them access to secure facilities and operations. Face recognition systems in particular have been employed at border crossings and in other applications where accurate identification is crucial. Yet, the models used to train these systems may not be sufficiently representative in terms of demographics. As a result, biases may be introduced that can have serious societal and security implications. Memon’s team addressed this issue by proposing a methodology that “generates unbiased data from a biased generative model using an evolutionary algorithm.” As described in the abstract to his paper, “Zero-shot Demographically Unbiased Image Generation from an Existing Biased StyleGAN,” Memon and his team were able to “generate a large racially balanced dataset of 13.5 million images, and show that it boosts the performance of facial recognition and analysis systems whilst reducing their biases.” The paper, which was co-authored by Tandon Associate Professor of Computer Science and Engineering Julian Togelius, and students Anubhav Jain and Rishit Dholakia, is available at <https://www.techrxiv.org/doi/full/10.36227/techrxiv.24634239.v1>.



True colors: Illustration from “Zero-Shot” paper showing intra-class variations in expression (first row), poses (second row), and illumination (third row) using latent directions in the StyleGAN latent space. The study proved these variations work well across demographics while preserving the identity.





## FACULTY PROFILE:

RANDAL  
MILCHSHAPING CYBER  
PROTECTION THROUGH  
LAW AND POLICY

The Co-Chair of the NYU Center for Cybersecurity and Faculty Co-Director of the M.S. in Cybersecurity Risk and Strategy Program, Randal Milch came to NYU after serving as the General Counsel and head of public policy at Verizon Communications. At Verizon, he chaired the company's Executive Security Council charged with overseeing information security across all Verizon entities. Previously, Milch was responsible for national security matters at Verizon, and served as the senior cleared executive. Earlier in his career, Milch was a partner in the Washington, DC office of Donovan Leisure Newton & Irvine. Milch holds a JD from New York University School of Law and a BA from Yale University. He now serves as a Distinguished Fellow at the NYU Reiss Center on Law and Security, and as a Professor of Practice at the NYU School of Law.

**CyberByte:** What was your entry point into cybersecurity? And, what training or background prepared you for these responsibilities?

**Milch:** As the General Counsel of Verizon, I was guided and supported by many talented lawyers in the legal department. One great lawyer, Jack, supported the contracting efforts of the IT department and had a Masters in Computer Science. Not long after I became General Counsel, we discussed the security of Verizon's vast digital infrastructure and the information that traveled on it. Each of our units had its own Chief Information Officer (CIO), and Jack told me that each CIO boasted that his unit "had the best security in the world." Jack knew that the anecdote would unsettle me: the boasting CIO's obviously couldn't all be right, and it was probably the case that they were all, in fact, wrong.

After some investigation I went to the CEO and suggested that—at the time—our cyber security posture was best described as lucky rather than good, and that we needed to have a coordinated effort to get better across all of our networks. He thought this was a good idea and, since I raised the issue, put me in charge. This plunged me into cybersecurity: creating a senior executive level steering committee (the business unit heads, and their CIOs), deciding on programs to better our security posture; setting and enforcing goals; creating meaningful and regular board-level briefings; and creating employee education (luckily, all with Jack's invaluable support).

I had no specialized training, but the task I faced was not a technical one. The job was about understanding our overall security posture; getting executives and technologists to agree on programs to make it better; and keeping their feet to the fire to ensure that the various programs were funded and completed. Verizon remained lucky, but became much closer to "good."

**CyberByte:** What changes have you seen in the cyber landscape over the past decade or so? Obviously the threats have gotten more sophisticated as the technology has matured, but do you see differences in approaches, policies, attackers, etc.?

**Milch:** From the attack side, I think the rise of ransomware has had a far-reaching

effect. Victim companies now have to decide whether to cooperate with their attacker—and if so, how—in the hopes of regaining access to their information or systems or in return for a hacker's promise to delete stolen information. This can be a complicated decision.

From the defense side, the desire and ability to hold corporate victims of cyber attacks "accountable" has increased dramatically over the past decade. Ten years ago, class actions on behalf of individuals whose information had been stolen had a tough go of it in court, and the various levels of government were relatively uninvolved. The situation is entirely different today, yet it's hard to find positive effects from a security standpoint.

**CyberByte:** What brought you to academia after so many years in the corporate world? And what was that transition like?

**Milch:** Even as a practicing lawyer I always had a strong affiliation with the NYU Law School, serving as a Trustee and participating on various panels and as a guest in some classes. After I left practice the then Center on Law and Security was a logical place to explore my interests in national security and cyber security. Participating more fully at the Law School certainly brought with it a change of pace—by its nature, academia entertains more discussion and less directed action. But getting to interact with brilliant faculty and students made the transition much easier.

**CyberByte:** What specific programs—courses, workshops/speaker programs, publications—has the Law School initiated to address issues like disinformation, deepfakes or other cyber crimes?

**Milch:** One of my first efforts at the Center for Law and Security was to see if the Law School and the Tandon School could join forces in addressing the mixed technical/legal/policy issues around cybersecurity. Luckily, Professor (and now Dean) Memon was an eager and gifted co-conspirator in these efforts, and the Computer Science department supported our efforts. Our "Cybersecurity: Law and Technology" seminar attracted both Tandon graduate students and law students, and was the

progenitor of the current Master of Science Cybersecurity Risk & Strategy program, which is jointly provided by the Law School and Tandon. The current NYU Center for Cybersecurity -- another Tandon/Law School joint venture -- has regular programming on current cybersecurity issues.

**CyberByte:** In terms of policy, what actions do you think would have the most significant impact in defending individuals and institutions from cyber crimes? In particular, what can be done from a policy or legal perspective to prevent the dissemination of disinformation?

**Milch:** First it is important to note that the “dissemination of disinformation” and “cyber crimes” are two very different things; only in rare instances would disseminating a lie be a crime. Having the government directly intervene to prevent disinformation (or misinformation or malinformation) from being peddled instead raises very serious First Amendment issues. The First Amendment severely limits the government’s role in policing truth and falsehoods. Generally, those harmed by disinformation must fend for themselves by suing for libel, intellectual property infringement, or misappropriation of name or likeness. That is admittedly a long and tough road because the law provides internet platforms with strong protection from lawsuits by those who may be harmed by third party speech on those platforms. This is in addition to the protections provided against government actions by the First Amendment.

Efforts to protect individuals and institutions from cyber crime should start with the individuals and institutions themselves. I think the role of government here should be one of providing incentives to pay attention to cybersecurity, to increase cyber hygiene at the personal and institutional level, and to encourage a safety and security culture. Unfortunately, the current direction of government is to pile on regulatory burdens at the institutional level in an effort to increase security through punishment. At the same time, our current direction is to hold individuals absolutely harmless even if they take few or no security measures and promiscuously spread their private information across the internet. Granted, it is hard for individuals to make themselves completely secure, but I think that people can and should take some steps to be safer online. Nevertheless, I think that we are trending toward the wrong incentives in both situations.

**CyberByte:** Do you foresee more regulations emerging that would specifically attempt to address these threats?

**Milch:** I don’t foresee any widespread, successful regulations addressing disinformation. Some states are experimenting with disinformation regulations in the context of elections, but these regulations -- assuming they pass constitutional muster -- will only be respected by legitimate candidates and their campaigns; anonymous bad actors on the internet won’t really care. The wide availability of generative AI platforms that can create convincing audio and visual fakes will put pressure on governments to take action, but I think that most criminal efforts with these convincing fakes are covered by existing criminal sanctions against fraud.

**CyberByte:** Tell me a bit about your work with the Reiss Center on Law and Security. What specific issues does the Center address and how does its work dovetail with the concerns of the Center for Cybersecurity?

**Milch:** The Reiss Center and the Center for Cybersecurity (CCS) are close siblings. CCS hived off of the Center on Law and Security in 2016, which in turn became the Reiss Center in 2018.



**Reiss Center on  
Law and Security**  
NYU School of Law

The Reiss Center does exceptional work on national security issues, and CCS is lucky to be able to coordinate with the Reiss Center on the cybersecurity aspects of national security.

In addition to jointly working on public-facing content, I’ve been lucky enough to write occasionally for the Reiss Center’s blog, *Just Security* (<https://www.justsecurity.org/>). Most recently, Dr. Edward Amoroso, Distinguished Research Professor of Computer Science and Engineering at Tandon, and I jointly authored a piece on the FBI acting as the IT department



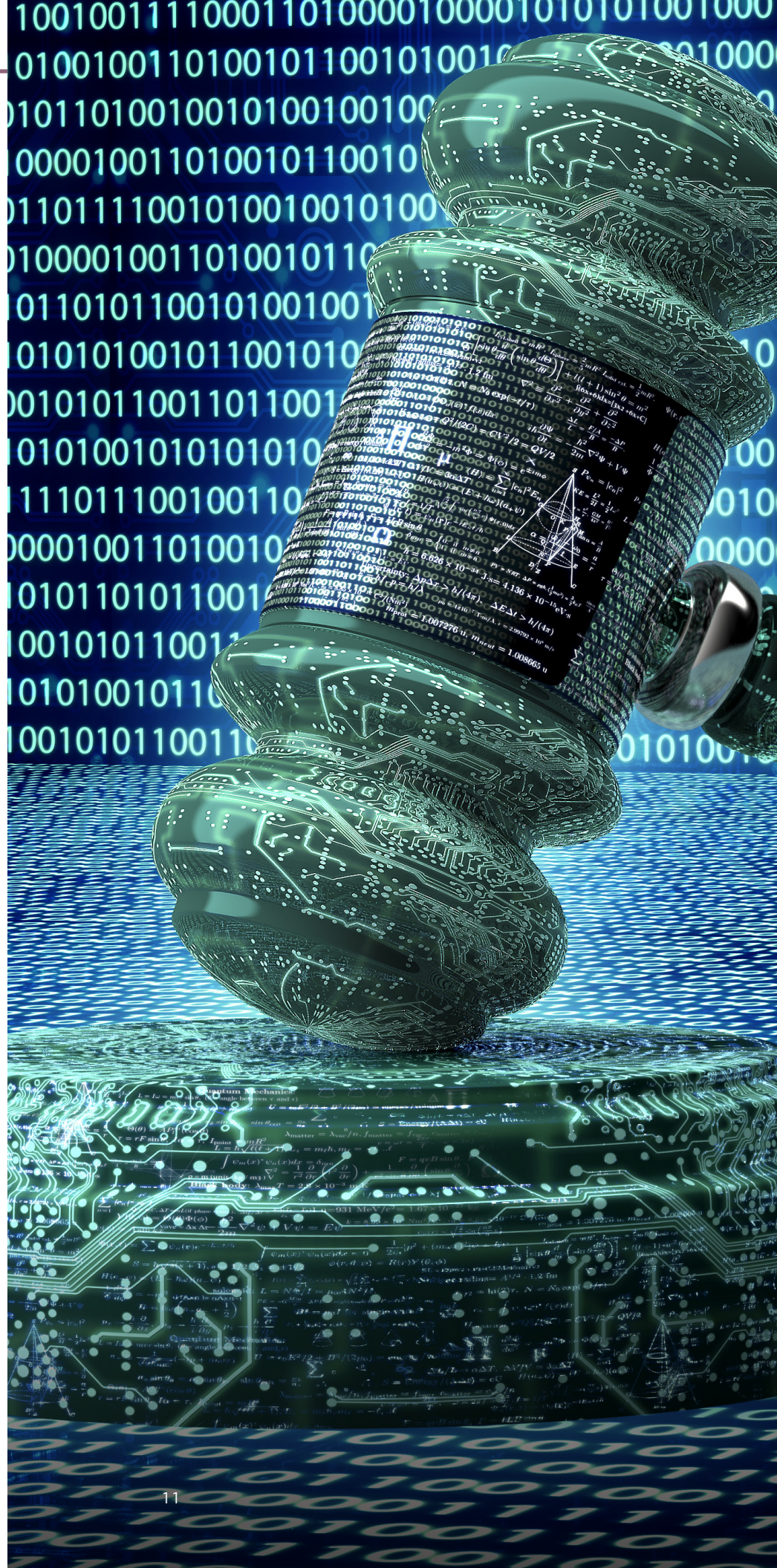
of last resort in certain situations (See <https://www.justsecurity.org/75955/hack-to-patch-by-law-enforcement-is-a-dangerous-practice/>).

**CyberByte:** You also serve as the Faculty Co-Director of the M.S. in Cybersecurity Risk and Strategy (MSCRS) Program. What do you think is the most important takeaway from this program? And, how are the program's graduates making an impact in the real world?

**Milch:** The MSCRS program is a great demonstration that cybersecurity education can and should include both technical and legal training in order to be effective. We are completing our fifth year and there are now more than 150 graduates of the program in place across the private sector and the government. These graduates are bringing their training to bear on critical cyber issues. You can meet a sample of our students and read their stories at <https://cybersecurity-strategy-masters.nyu.edu/admissions/student-spotlight/>. The success of the program is incredibly gratifying. *(Editor's note: See a short article about the most recent cohort in the Events section of this newsletter.)*

**CyberByte:** What one thing from a legal or policy perspective do you think all cybersecurity professionals should be aware of?

**Milch:** I think that all cyber professionals need to be aware of the increasing regulation around cybersecurity. Cyber regulation occurs in a piecemeal fashion. It might be that a company has a federal regulatory agency which sets cyber policy. If the professional works for a public company, then attention has to be paid to the Securities and Exchange Commission's disclosure requirements around cyber "incidents." But even if a company has no federal regulator, and is private, a state might enact its own set of rules for all companies of a certain size or character operating in that state. Any hack is a bad day for some cyber professionals; it only gets worse when the regulators come in after the fact to shoot the wounded.







## PH.D. PROFILE:

# SOFIJA JANCHESKA

## FINDING COMMON GROUND BETWEEN LANGUAGES, CULTURES, AND TECHNICAL CHALLENGES

**CyberByte:** I understand you did your undergraduate work at NYU Abu Dhabi. What made you choose that school to start your academic journey?

**Jancheska:** During my senior year of high school, I heard about NYU Abu Dhabi, and later discovered two acquaintances of mine were studying there. I reached out to them, and hearing about their experiences further sparked my curiosity about the school.

Upon applying to NYU Abu Dhabi, I attended a Candidate Weekend, where I participated in a trial undergraduate class, explored the campus on Saadiyat Island, and met students from 40+ countries. It was during this weekend that I truly felt the essence of what NYU Abu Dhabi and the United Arab Emirates had to offer—an inclusive, dynamic environment that inspired intellectual curiosity and cross-cultural understanding. It became clear to me that NYU Abu Dhabi would be the perfect place to pursue my academic journey while simultaneously fulfilling my passion for exploring different cultures and perspectives.

Three years later, as an NYU Abu Dhabi student, I got the opportunity to spend a semester at NYU's campus in New York City. During this time, I learned about Tandon's Center for Cybersecurity, and made connections with many PhD students, including a few advised by Professor Ramesh Karri. I was fascinated by the biochip security and LLM-related work that Professor Karri has been leading, so I began my research in the field with his support and guidance.

**CyberByte:** During your time at NYU, you have engaged in a diverse number of studies. What skills do you think you developed from these projects and how do these skills fit with your current work?

**Jancheska:** I have intentionally immersed myself in such different projects for two main reasons: 1) to find a topic that I feel passionate to explore further and 2) to push myself to learn something new, as all these research projects allowed me to develop both technical and interpersonal skills. From a technical aspect, each project required getting familiar with a different set of tools and background knowledge. For instance, I learned about deep learning models through my work in biochip security, and I refined my data manipulation and interpretation skills by looking for patterns in YouTube statistics during the pandemic. And, from an interpersonal skills perspective, many of my projects have been collaborative, which taught me the importance of teamwork, good communication and listening. I feel like these skills will be transferable to any new project in the future.

**CyberByte:** I was quite impressed when your vitae mentioned your ability to speak six different languages. First, I'm curious to know how you mastered so many. And, second, do you think this fluidity in natural languages has helped you grasp and master computer languages?

**Jancheska:** As mentioned earlier, I was born and raised in Macedonia, so my native language is Macedonian. I also grew up speaking Serbian because of my grandparents, who were born in Yugoslavia where Serbo-Croatian was an official language. I began learning French

in elementary school, and have continued consuming Francophone media and music throughout the years. During a study away semester in Paris, I had a chance to polish my French skills even further and I ended up graduating with a minor in French. Additionally, I had a few courses in Turkish in high school and I was surrounded by Turkish-speaking friends there, so I also became fluent in Turkish. Finally, the majority of my high school courses were taught in English, so I also mastered English.

To answer the second part of your question, I believe that this fluidity in several human languages has helped me immensely in grasping new programming languages and tools. The intimidation of not knowing how to express myself and the process of learning rules from scratch is very similar to what I feel when learning a new programming language or tool. And, once I get the logic, it is not very hard to master the syntax. But, practice is what really makes all these languages stay in my mind!

**CyberByte:** What other advantages do you think your multilingual ability might lend to your educational journey?

**Jancheska:** Being multilingual opens the doors to a wider range of people and the ability to form better relationships with them. I feel like I can connect to people on a deeper level if I speak their language and am familiar with their culture. Another important advantage is the ability to access a wider range of resources. Sometimes just reading a book in an author's native language is more authentic than reading a translation. Last but not least, being multilingual inevitably brings me closer to learning about people's cultures, which also makes it easier for me to understand their mindset, opinions, and philosophy of life. This is particularly useful when working on real-life projects as this diversity is the key to success!

**CyberByte:** Another area you have addressed in your research is secure biochips (See Bio-FP: Biochip Fingerprints for Authentication at [https://www.researchgate.net/publication/377507144\\_Bio-FP\\_Biochip\\_Fingerprints\\_for\\_Authentication](https://www.researchgate.net/publication/377507144_Bio-FP_Biochip_Fingerprints_for_Authentication)).

Can you touch on your contribution to this investigation and how it may apply to your other research work?

**Jancheska:** Biochips are used in many areas, including point-of-care testing, clinical diagnostics, and biological computing. Because of this, they are vulnerable to intellectual property attacks. With Professor Karri's biochip research group, we developed a novel authentication method called biochip-level fingerprinting (Bio-FP) to handle these threats. The method directly prints unique patterns onto biochips through the use of a melt-electrospinning printing technology. Next, a layer of polydimethylsiloxane (PDMS) is applied to mask these identifiers. Crucially, we included a fluorescent dye within the Bio-FPs so that they could be identified when exposed to UV light. These dyed Bio-FPs are verified by spectral analysis, which maps the intensity-wavelength response to verify their authenticity.

We extended our scheme for differentiating between counterfeit and authentic biochips by using several image pre-processing techniques, and multiple deep learning models for fine-tuning and transfer learning. As a result, we achieved a 95.8% classification accuracy!

This approach may be of use beyond biochips in a variety of contexts where authentication and anti-counterfeiting methods are essential. Our method also contributes to the integrity and progress of biotechnology and related industries by combining methods from material science, optics, and deep learning to provide a reliable approach to protecting biochips.

**CyberByte:** Your most recent research looks at how effective large language models can be at solving Capture the Flag challenges. What is the real-world potential significance of this research? And, what applications might its results have beyond just success in CTF competitions?

**Jancheska:** This research is designed to inspire critical reflection on technological advancements like artificial intelligence. I believe such critical thinking is not only essential for leveraging technological innovations effectively, but also for

motivating thought about the ethical and legal implications of emerging technologies. By engaging in such reflections, we can work towards establishing ethical frameworks and regulatory measures that balance innovation with societal values and concerns.

**CyberByte:** Despite your study's results pointing to GPT having a higher success rate in solving Capture the Flag challenges than humans, the paper written about this work (see <https://arxiv.org/abs/2402.11814>) also notes that adding human feedback to LLMs can decrease failure and improve performance. What does this suggest in terms of future collaboration between LLMs and human developers?

**Jancheska:** Our experiments showed that having a human in the loop is essential for guiding the LLM conversations in the right direction, and for yielding correct and more effective results. We further noticed that when individuals with a cybersecurity background, like CSAW competitors, interact with LLMs they can successfully navigate challenges like CTFs. Professor Karri even had the unique idea to add a new competition category to the 2023 CSAW event called LLM Attack Challenge. In this contest participants are required to use LLMs to solve CTF challenges (See our CSAW coverage on [page 21](#)).

LLMs excel in fast data manipulation and task execution, while humans have unique cognitive abilities to think and rationalize. By uniting these strengths, I believe we can not only boost performance, but also ensure a more holistic understanding of complex challenges, which will lead to more impactful solutions. I am very eager to see where this work takes us because this research is led by an amazing team. I am grateful for being advised by Professor Karri, Professor Brandon Dolan-Gavitt and Professor Siddharth Garg, and for working together with my colleague Minghao Shao.

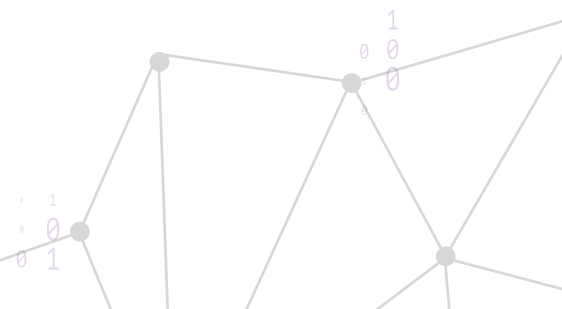
**CyberByte:** You mention that an aspect of your future investigations will revolve around "the legal and ethical guardrails" on ChatGPT over time. What type of criteria do you think may be needed in applying LLMs to this work to make sure these guardrails are introduced and enforced?

Jancheska: From a research standpoint, I think we should communicate with the LLMs in two different ways. By acting appropriately, we set an example for other users to follow. But, to verify whether guardrails are properly introduced and enforced we must also behave like attackers. We can test these technologies by making unethical requests that would bypass the existing legal restrictions. This behavior should be research-oriented only and aim to improve existing ethical measures.

**CyberByte:** Your vitae indicates that you have been very active with CSAW over the years. What particular benefit do you think this involvement has brought to your life and/or work?

**Jancheska:** I love CSAW because it is a student-run event that has allowed me to spend time with the brightest people in the cyber community, attend engaging competitions, and interact with representatives from our sponsoring companies. Over the years, I have had many roles with CSAW, both in Abu Dhabi and in New York. At first, I was a participant in both the Capture The Flag and Applied Research competitions. Later, with the support of Professor Karri who is the global director of CSAW, I was a sponsor host and a participant host. He even placed such trust in me that I designed CSAW's t-shirts for two years in a row! All these roles taught me how to handle pressure more effectively, and made me realize the importance of raising awareness in our community about cyber threats, especially with today's speed of technological advancements.

Another thing I love about CSAW is that the event is never the same. As mentioned earlier, Professor Karri initiated a new competition category called LLM Attack Challenge during CSAW 2023. This is a great example of how CSAW evolves with all the new technology as well. And, I am excited to see what next year's CSAW events bring us!





## ALUMNI PROFILE:

ABHINAV  
KORERECOUNTING CYBER  
REALITIES LEARNED ON  
THE JOURNEY FROM  
TANDON TO WORKDAY

**by Chinmay Tompe, NYU Tandon M.S. Alumnus and Senior Research Fellow with Veermata Jijabai Technological Institute (VJTI), Mumbai, India**

Abhinav Kore is a Senior Cybersecurity Engineer at Workday in McLean, Virginia. He received his Master of Science (M.Sc.) degree in Computer Engineering from New York University and his Bachelor's of Technology (B.Tech.) degree in Electrical, Electronics, and Communications Engineering from GITAM Deemed University in Hyderabad, India. He made significant contributions at IronNet Cybersecurity, and at Qualtrics before assuming his current post.

**CyberByte:** Can you provide a brief overview of your journey from your undergrad education to your first full time position at IronNet?

**Kore:** Of course. I pursued my undergraduate degree in Electronics and Communications engineering at GITAM University. Although the coursework was initially focused on electronics, an elective in network fundamentals ignited my interest in cybersecurity. It gave me a holistic perspective on how the internet works and about the systems that are built upon it. Transitioning to NYU in 2014 for my Master's in Electrical Engineering, I delved deeper into network engineering courses like Network Security. That's how my journey began.

While I was a student, I actively engaged in labs, worked on configuring routers from scratch, and collaborated with research students who guided me about certifications and navigating the industry.

This hands-on experience, coupled with certifications like CCNA, CCNP, and Security+, opened doors to interviews. Ultimately, I secured a position as a Network Security Engineer with IronNet, a Virginia-based cybersecurity startup, where I contributed to building a behavioral analytics product for network traffic anomaly detection. This product can be described as a combination of anomaly detection and behavioral analytics, and holds a unique position among existing market products.

At IronNet, I implemented innovative solutions, decrypting TLS traffic and configuring firewalls on cloud technologies. Working in a startup environment provided me with ample opportunities for learning and innovation, and fostered my growth in the field. The behavioral analytics product I mentioned above is challenging to categorize precisely, but it aligns with products like Wildfire of Palo Alto or Guard Duty from AWS. It operates within the data center, monitoring the internet traffic across the entire organization with say around 50 sensors that are connected to the backend for computation. These sensors analyze traffic and can be centralized in a data center or hosted on the cloud.

**CyberByte:** Before joining IronNet, you interned at Technical Consulting & Research, Inc., serving as a cybersecurity analyst. Could you elaborate more on what this position entailed?

**Kore:** Initially, that stint began as a one-month summer internship. During this time, I had limited hands-on tasks, and the focus was on mentors providing architectures and datasets for threat modeling on client websites or locations. Interns like myself engaged in weekly mentor sessions to discuss threat models, fostering a relationship resembling the dynamics of a security champion and security partner. I received positive feedback on the quality of threat models and documentation, which motivated me to continue volunteering. This extended engagement allowed me to conduct independent research and self-directed learning, which became a significant takeaway from the experience. I got to work on architectures and data that was going to be implemented on some of their client's websites or locations. It was an experience that laid the foundations for my career.

**CyberByte:** What were some significant moments of learning and instances where you were able to shine as an engineer during this internship?

**Kore:** One such instance was a project that involved assisting a client in migrating data centers to the cloud and optimizing services. The challenge was evaluating a new tool to scan the network and identify traffic patterns and critical applications. Beyond standard threat modeling, I ventured into uncharted territory by performing a third-party vendor risk assessment, a relatively new concept at the time. This involved utilizing emerging tools like OneTrust, a platform to assess the trustworthiness of vendors based on certifications and industry acceptance. This unique approach gained attention, highlighting the breadth of cybersecurity beyond traditional red and blue teaming. It also exposed me to diverse concepts like third-party risk management and Governance, Risk, and Compliance (GRC) that often go unnoticed in standard cybersecurity coursework.

Lastly, the internship allowed me to explore many other dimensions of cyber security. One such technical sector is data governance, a critical area in today's cybersecurity landscape and one that requires more attention. Cybersecurity decisions hinge on data classification and the required security controls for each dataset. Another dimension is Zero Trust, a continuous process with the motto of "trust, but verify." This acknowledges that the process will persist and evolve as more products address individual pillars of zero trust over time.

**CyberByte:** Along with this internship, what played a major role in securing your first full time position in the industry?

**Kore:** As a non-U.S. citizen in the cybersecurity field, getting into the industry was challenging, especially during graduate school. The key to success was constant networking, reaching out to mentors, and keeping options open. Despite lacking credentials and certifications, I took a proactive approach that included self-directed learning through

platforms like the Linux Academy to address gaps identified during interviews. The journey included acquiring skills in Cisco and cloud environments, AWS certifications, Python scripting, and HackerRank problem-solving. It took me around six months post-graduation to secure a job, with internships and volunteer work playing a crucial role in maintaining my status during this period. The diverse experiences helped build resilience and taught me valuable lessons in navigating the cybersecurity job market.

**Cyberbyte:** How crucial were certifications and HackerRank/LeetCode in securing your initial job, and to what extent did they play a role in maintaining and performing well in your role?

**Kore:** Certifications might not always be necessary to land a job, but they can serve as substitutes for any gaps in experience, thus boosting your résumé and helping to showcase skills to potential employers. While certifications like CCNA were beneficial in getting interview calls, they were not the sole factor in securing jobs. Understanding the technology, gaining hands-on experience, and showcasing skills during interviews mattered more.

As for LeetCode, many questions in MAANG (Meta, Amazon, Apple, Netflix, and Google) interviews are sourced from platforms like LeetCode, making it a valuable resource for newcomers entering software development. However, security roles often involve understanding code for different purposes, such as application security (AppSec) and DevSecOps. Security engineers need to grasp the overall design, identify potential vulnerabilities, and secure systems proactively. The distinction lies in the proactive nature of security engineers compared to the more development-centric approach of software developers.

**Cyberbyte:** Reflecting on your 4-plus years at IronNet, can you please elaborate on specific projects/ areas you worked on and your satisfaction with the outcomes?

**Kore:** At IronNet, the startup environment allowed for substantial impact, innovation, and freedom to experiment with new

technologies. I often found myself addressing challenges at customer locations and was given the opportunity to create more efficient solutions. This experience prompted a transition from a networking engineer to a network security role, involving responsibilities like building and automating designs on AWS using tools like Terraform and CloudFormation. The skills acquired during this period, coupled with certifications, facilitated an easy transition to my next role at Workday.

**Cyberbyte:** What are your thoughts on the digital privacy of internet users, and how does your experience shape these views?

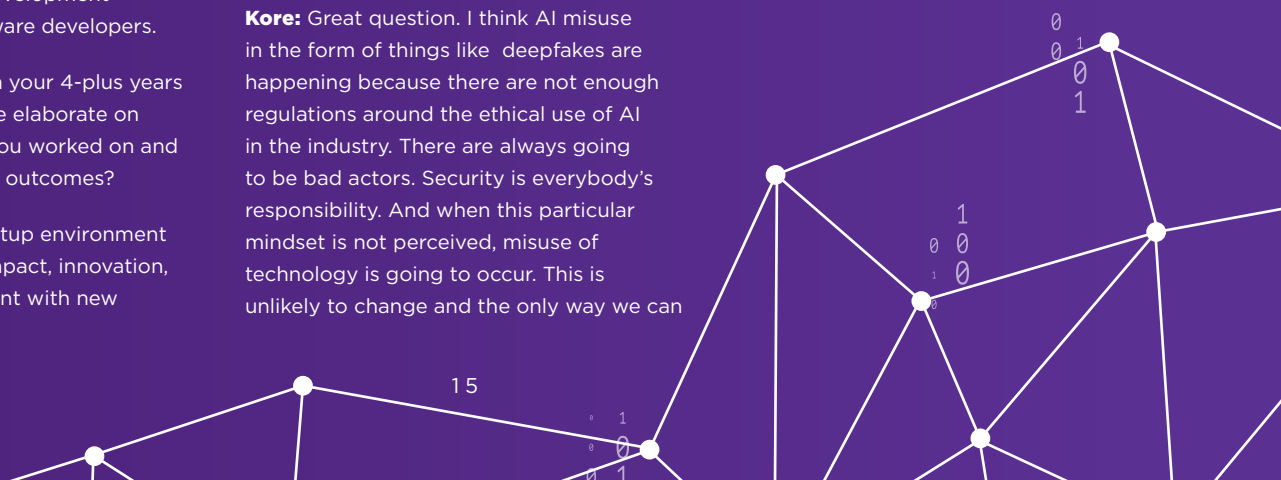
**Kore:** I collaborate closely with our internal privacy teams and, as part of a global organization, I've gained a comprehensive perspective on privacy matters. When considering consumers, it's crucial to be mindful of online activities, comprehend terms and conditions, and safeguard Personally Identifiable Information (PII). I advocate for utilizing Two-Factor Authentication (2FA) and adopting secure technologies, such as password managers. Additionally, we should exercise caution regarding our online postings and agreements to terms and conditions. From a regulatory standpoint, Europe has stricter data privacy regulations, notably the General Data Protection Regulation implemented in 2018, which enforces significant penalties for data breaches. Furthermore, it's imperative to grasp the significance of the "right to forget" principle, allowing users to request the deletion of their data from platforms.

**Cyberbyte:** With the rise of deepfakes, misinformation and fake news that aim to distort the facts, how do you, in a personal and professional capacity, "defend the truth" ?

**Kore:** Great question. I think AI misuse in the form of things like deepfakes are happening because there are not enough regulations around the ethical use of AI in the industry. There are always going to be bad actors. Security is everybody's responsibility. And when this particular mindset is not perceived, misuse of technology is going to occur. This is unlikely to change and the only way we can

fight this is by promoting more education and awareness on how to be secure in the digital world. The usual targets are going to be people and communities who are using technology but are not tech savvy, and do not have the ability to protect themselves. For instance, our parents know how to use a smartphone but might not know how to handle transactions, and might be vulnerable to security issues. By spreading awareness, we can help people identify correct information from misinformation, and tell trustworthy information from untrustworthy lies. It is a long journey, and these issues might not be solved anytime soon but, as with any technology, governments will need to change the policies and laws around it, and eventually the regulations.

As we saw with the case of ride sharing, when Uber entered the tech industry, there weren't many laws applicable to ride sharing apps because it was a new thing. But now, the laws have changed and the regulations and policies around it have changed too.







## CSAW '23 CELEBRATES TWO DECADES OF CHAMPIONING CYBERSECURITY AWARENESS

Though it marked the 20th edition of the program, CSAW '23 spent much more time looking forward than looking back. The four day event, held in Brooklyn and at four other global sites, continued to frame new areas of cyber concern through its competitions, lectures, and activities.

Several new competitions made their debut this year, all of them highlighting the increased significance of artificial intelligence in both the creation and prevention of new cyber threats. One of the three challenges, BioHack3d, also represents a new field of application for the CSAW competition, marking the first challenge to engage in life science issues.

### On a global level, CSAW can be summarized as follows:

- 3,000-plus total participants in all rounds
- 500-plus finalists
- 16 partner organizations
- 12 unique global challenges
- 5 global sites

### As announced in a news story released by NYU in late November, "by-the-numbers" at the Brooklyn site were as follows:

- 931 registrants
- 51 teams in the Capture the Flag finals
- 40 research posters displayed
- 14 sponsors
- 7 competitions

In this article, we fill in the stories behind these numbers by presenting an overview, in both text and photos. We also share some "backstage insights" from the new competitions—BioHack 3D, which was held at the CSAW MENA site; LLM Attack Challenge, held at both the Abu Dhabi and Brooklyn sites; and AI Hardware Attack Challenge, held only in Brooklyn. Lastly, we close with a comprehensive list of all of this year's first place winners.

The NYU Center for Cybersecurity thanks its 2023 partners: NYU OSIRIS Lab, the NYU Center for Global Affairs, NYU Cyber Fellows, NYU Wasserman Center for Career Development, NYU Tandon Career Hub, the Interdisciplinary Centre for Cyber Security and Cyber Defense of Critical Infrastructures at IIT Kanpur, the NYU Abu Dhabi Center for Cyber Security, the University of Delaware College of Engineering, Grenoble Alpes Cybersecurity Institute, Valencia Research Laboratory, Grenoble INP Institut d'ingénierie et de management, the Modern Microprocessors Architecture Lab at NYU Abu Dhabi, Global CyberPeace Challenge, and CTFd.

Corporate and government sponsors for CSAW'23 US-Canada were Con Edison, Synopsys, T.Rowe Price, Snyk, Darktrace, Intel, TIAA, HP, Google, DTTC, Zelic.io, Trail of Bits, the NYSTAR/NYU Center for Advanced Technology in Telecommunications, and the National Science Foundation.









Featured CSAW speakers from left to right: Patrick Schläpfer, Brendan Dolan-Gavitt, student coordinator Sofija Jancheska, Mariana Raykova, Dan Guido

## CYBER SPECIALISTS SET THE STAGE

At the Brooklyn site, CSAW '23 began on November 7 with a series of talks by cyber professionals from academia and industry. Leading off was Dr. Mariana Raykova, a research scientist from Google's Private Computing Group who works in the areas of cryptography and security, and served on the Privacy Preserving Techniques Task Team that advised the U.N. Global Working Group on Big Data. In what could be considered the keynote address for the program, Raykova described Google's commitment to anonymizing personal data in its datasets despite the ever-increasing size of those datasets. She also described her contributions to ongoing research in private information retrieval, and zero knowledge proofs.

The second speaker, Dan Guido, addressed the question of whether LLMs will enhance or threaten security, and provided insights on how the availability of capable AI models presents new offensive opportunities that defenders must be able to counter. Guido, CEO and founder of the software security company Trail of Bits, opened





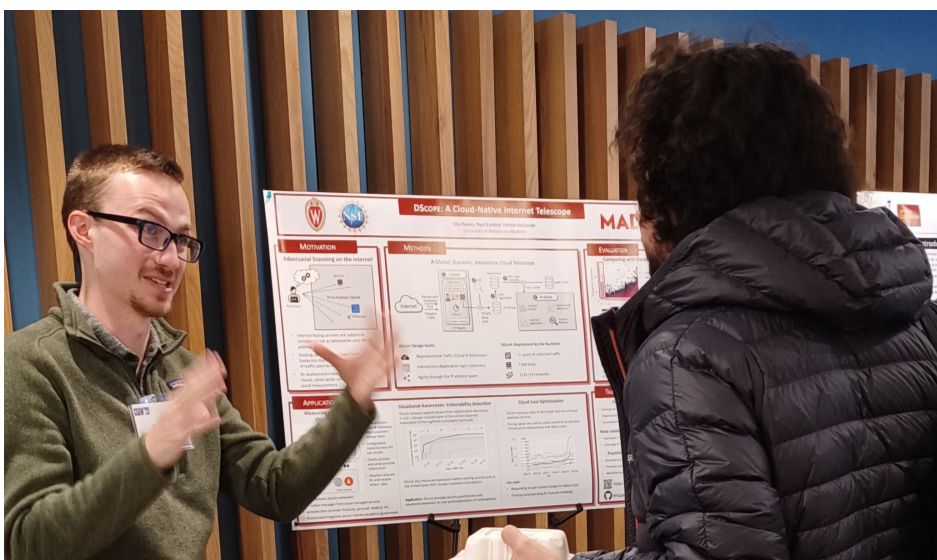
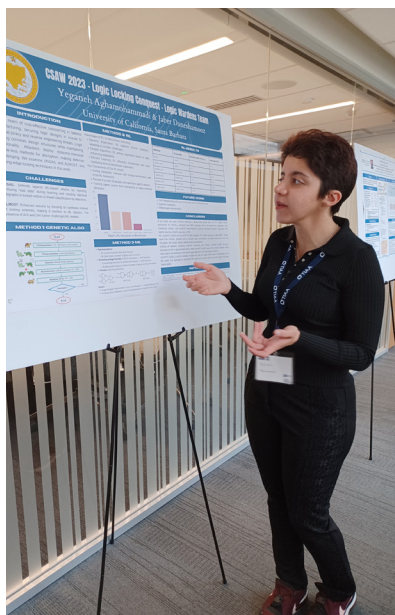


his talk by recounting his long association with CSAW, which began as a participant in the initial 2003 program. His return this year as a CSAW speaker and sponsor representative was a full circle moment, and he affirmed the role the program played in guiding him towards a career in cybersecurity.

Patrick Schlöpfer, Senior Malware Analyst at HP, Inc., followed Guido's comments with advice on "staying ahead in the Wild West of cybercrime." His talk offered a look at the current threat landscape and discussed some of the projects being addressed by HP's threat research team. Lastly, Brendan Dolan-Gavitt, an Associate Professor in the Computer Science and Engineering Department at NYU Tandon offered an overview of "The Present and Future Use of LLMs in Software Security." Dolan-Gavitt, focused his presentation on the answers to three questions: What does the use of these models mean for software security? What can they do today? And, what might they do soon?"

After a lunch break, several of the meeting speakers joined representatives from snyk, the Metropolitan Transit Authority, Darktrace, TIAA, efabless, Consolidated Edison, NYSTAR, the National Science Foundation, Synopsys, T. Rowe Price, Zellic, and The Depository Trust & Clearing Corporation (DTCC) at the CSAW Career Fair. For several hours, participants got to discuss career options in the domain of cybersecurity with working professionals drawn from a variety of technical contexts.

CSAW was originally conceived as a competition and 20 years later, wrestling with practical problems in cybersecurity remains the heart and soul of the event. So, on Friday, November 8, Brooklyn site attendees got to compete in or observe the finals of seven such events. In addition to perennial contests, such as Capture the Flag (the only competition held at all five sites), the US-Canada site also hosted the Applied Research Competition, Embedded Security, Hack3D, and Logic Locking competitions, along with the debut of the AI Hardware Competition and the Large Language Model Attack challenge.





## NEW COMPETITIONS ON THE BLOCK

Over the past few years, CSAW has served as a successful barometer of emerging cyber threats through the contests it has chosen to develop. CSAW '23 continued this trend.

### **AI Hardware Competition**

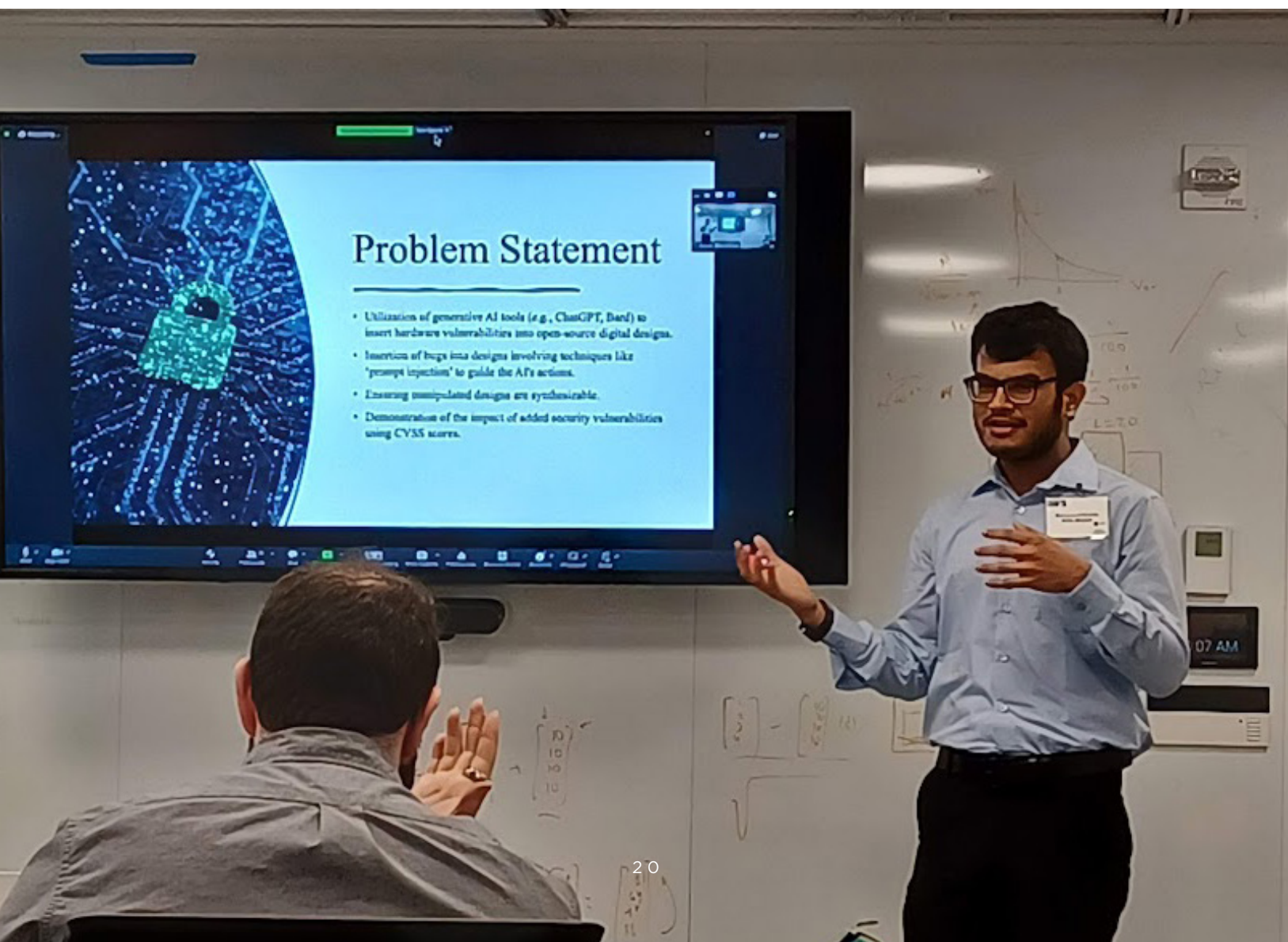
**by Jason Blocklove, Ph.D. Candidate in Electrical and Computer Engineering, NYU Tandon**

With the rapidly increasing industry interest in generative AI for hardware design and development, concerns about the ability to maliciously leverage this new kind of tool are also growing. The aim of this competition was to have students use generative AI to insert and exploit security vulnerabilities in open-source hardware projects. In doing so, participants would demonstrate how generative AI, specifically large language models, can be used to add malicious defects to a design with much less effort than needed for a manual attack. Participating teams were tasked with finding an open-source digital hardware project, adding security bugs using LLMs, demonstrating the effects of those bugs, and finally determining the severity of the resulting vulnerabilities.

We were somewhat surprised by just how easy it was for students—even those with minimal hardware design experience—to insert some potentially devastating security bugs. Those with more hardware experience were able to leverage the tools to insert bugs that would not only be extremely difficult for most hardware verification processes to find, but could also completely invalidate the security functions already in place. We had anticipated some strong contenders, but were thoroughly shocked by the severity of the bugs introduced using just natural language.

For its first year, both myself and the other organizers feel the event went very well. We had 8 finalist teams from 4 different countries, all of whom did very well. Picking the winners was surprisingly difficult and we're looking forward to improving the competition for next year.

Looking toward the future, we may seek to add some additional structure to the competition and change up the specific goals to keep it fresh from year to year. The competition was kept extremely open-ended by design --- we wanted to see what students would come up with --- but that made judging their efforts rather difficult. We ended up with a wide range of different types of projects and vulnerabilities that were not necessarily simple to compare.





### ***Large Language Model Attack Challenge*** **By Minghao Shao, Ph.D. Student, NYU Tandon**

This competition offers a novel take on the CTF format. In contrast to traditional competitions where participants complete challenges using their cybersecurity knowledge, this contest focuses on the design of engineering prompt techniques. Contestants in groups of one to three were asked to solve challenges using their knowledge to guide the Large Language Models (LLMs) to generate the solution. This competition aimed to explore the potential of LLMs for offensive security related challenges. Incredibly, six teams competed in the competition's inaugural year in New York, and two teams faced off in the competition held in Abu Dhabi.

During the final round of CSAW 23, we held in-person demonstrations at both sites that included brief student presentations about their findings. What surprised me was that, despite using the same challenge database, the teams still came up with different solutions to the puzzles. For example, one team repeated the experiment to avoid the interference of the randomness of LLMs, while another team tried to solve the challenges using different models.

Thanks go to Boyuan Chen, my student lead counterpart at NYU Abu Dhabi, and faculty members Drs. Ramesh Karri, Siddharth Garg, and Brendan Dolan-Gavitt at NYU Tandon, and Muhammed Shafique at NYU Abu Dhabi.





### ***BioHack3d***

**By Navajit Singh Baban,  
Postdoctoral Associate at  
NYUAD/NYU**

It was an absolute pleasure to organize BioHack3D, the groundbreaking workshop and hackathon focused on biochips (Labs-on-a-Chip) and associated 3D printing cyber-physical security and systems. This event was organized in close collaboration with New York University Abu Dhabi's Bioengineering Program, Advanced Manufacturing Workshop (AMW), led by Jorge Montalvo, and the International Genetically Engineered Machine (iGEM) team, led by Rashik Chand.





Biochips are devices used for biological computing. Think of them as analogous to computer chips, but instead of using current, they employ fluid flow, voltage, pneumatic pressure differences, and soft elastomeric valves as transistors. They play a significant role in diagnostics and biomedical research. Due to COVID-19, the demand for these biochips has grown significantly, while extensive use of 3D printing and other related state-of-the-art technologies for manufacturing has expanded supply. However, due to a horizontal supply chain and outsourcing, malicious cyber-physical attacks and intellectual property theft continue to pose threats to these security-critical devices. Thus, to raise awareness about the cyber-physical security of biochips

and associated 3D printing products in an era of global pandemics and point-of-care technologies, a new CSAW event named BioHack3D, was introduced.

Twenty teams from all over the United Arab Emirates participated in the virtual qualifying round, with five of the teams making it to the final round: Team Korea (NYUAD), Team Wollongong (University of Wollongong, Dubai), Team Baku Baku (NYUAD), Team UAE (Khalifa University, United Arab Emirates), and Team Behrooz (NYUAD). The grand prize of a \$500 Amazon gift card was won by Team Korea, made up of Sunghyeon Kim, Seung-Jean Kang, and Haram Jeong. Congratulations to them!!!

I would like to extend my sincere appreciation to all the organizers, participants and judges: Professors Ramesh Karri, Michail Maniatakos, Rafael (Yong-Ak) Song, Ozgur Sinanoglu, and Vijayavenkataraman Sanjairaj; and staff and students Jorge Montalvo, and Gopinathan Janarthanan, Rashik Chand, Julio Z., Prithwish Basu Roy, Jenna Khanfar, and other members of NYUAD iGEM. In addition, I'd like to thank Hari Ramasubbu, the CCSAD Center for Cyber Security Abu Dhabi, and New York University Abu Dhabi Engineering, for their invaluable assistance and support. Thank you all so very much for making BioHack3D a grand success!!!







## GLOBAL PERSPECTIVES: HIGHLIGHTS FROM CSAW MENA AND CSAW EUROPE

Rounding out our coverage of CSAW '23, we were able to gather some information on two of the other CSAW global sites—CSAW MENA, held at NYU Abu Dhabi in United Arab Emirates from November 9-11, and CSAW Europe, held at Grenoble INP-Esisar in Valence, France, from November 9-10. Thanks to Hari Ramasubbu, Senior Center Coordinator at the Center for Cyber Security at NYU Abu Dhabi, and Anne-Laure Duee, CSAW Europe coordinator at Grenoble INP-Esisar, for providing details and descriptions of their respective events.

### MENA

CSAW serves as a platform for experiential learning and aims to inspire students to pursue education and careers in the field of cybersecurity. It brings together cybersecurity researchers, students and professionals from across the region to share knowledge, engage in friendly competition, and contribute to the advancement of cybersecurity. This year's edition, which marked the 10th anniversary of programming at the MENA global site, was a resounding success. With the addition of two new competitions, bringing the total to five, the number of students and researchers participating in the final rounds increased to 88. This reflects a 90% surge in participant numbers compared to previous years.

The site hosted the following competitions:

**Capture the Flag:** 37 participants in 10 teams competed in the final round, out of a total of 90 participating teams

**Applied Research Competition:** 5 participants in the final round

**Hack My Robot:** In its second year as a CSAW MENA exclusive competition, this year's challenge saw 23 teams compete, of which 5 advanced to the finals. The initial round focused on autonomous excavators, highlighting the critical safety risks of potential compromises, while the final round challenge asked students to hack a construction environment robot and disrupt its functionalities.

**BioHack 3D:** Making its debut this year, and making history as the first workshop and hackathon solely dedicated to biochip security and its intersection with 3D printing technology, the competition drew 20 teams to its virtual qualifying round. Five elite teams advanced to the final round.

**LLM Attack Challenge:** Debuting at both the Brooklyn and Abu Dhabi sites this year, the MENA finals included 4 participants and recognized first and second place winners.

In addition to the competitions, CSAW MENA also included a Cyber Security Open House on November 10, where attendees could network with industry professionals and ask questions of cyber experts.



## EUROPE

The CSAW Europe event packed a lot of activities, camaraderie, and information into a two-way program at Grenoble INP-Esisar in Valence, France. By the numbers, the program encompassed:

130 Finalists

14 Countries

35 Universities

6 Competitions

200 School Children

As the numbers suggest, the latest edition of CSAW Europe was designed to serve a broad spectrum of individuals. By cooperating with other institutions and running parallel programs, the 2023 event was able to engage local primary, middle, and high school students in hands-on challenges and demonstrations, and to spread cyber awareness in industry through a series of lectures and workshops. These included the CSAW Europe Conference that examined current cybersecurity skills challenges on the continent, and Cyberday workshops to encourage best practices when it comes to managing passwords, and resisting social engineering or IoT-related attacks.

The event also included a research-oriented program on the theme of system security using Physical Unclonable Function (PUF) technology, and a Red Competition in which 10 high school teams implemented such cybersecurity methods as digital investigation, vulnerability recognition, and penetration testing to determine how a hacker managed to penetrate a system.

## GLOBAL WINNERS ROUND-UP

Below are the names of all the first place winners across the CSAW global landscape that we could gather. Our congratulations to all the global winners in this year's competitions.

### AI Hardware Attack (US-Canada only)

- HeHee 2023, Guonhua Yin, Xinze Wang, Xi Wang, Tsinghua University (China)

### Applied Research Competition

- **Europe** | Piergiorgio Ladisa, SAP Security Research & Université de Rennes (France), presenting *SoK: Taxonomy of Attacks on Open-Source Software Supply Chains*
- **MENA** | Priyanka Dodia, Qatar Computing Research Institute (Qatar), presenting *Exposing the Rat in the Tunnel: Using Traffic Analysis for Tor-based Malware Detection*
- **US-Canada** | Jackson Sippe, University of Colorado-Boulder (USA), *How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic*

### BioHack 3D (Abu Dhabi only)

- Team Korea, NYU Abu Dhabi (UAE)  
Sunghyeon Kim, Seung-Jean Kang, and Haram Jeong

### Capture the Flag

- **Europe** | nt/ain - ETH Zurich, Switzerland  
Philippe Dourassov, Aaron Hodel, Yorik Zoger, Luc Fisch
- **MENA** | Team\_7even, École Supérieure en Sciences et Technologies de l'Informatique et du Numérique (ESTIN) (Algeria)  
Mohammed Reda Sbahi, Chiheb Chahine Yaici, Yahia Hachemi, Mohamed El Amine Boukerfa

### US-Canada | Stackphish

Audrey Dutcher and Michael Tompkins-Arizona State University (USA); Xenia Dragon-Northeastern University (USA); Lukas Dresel - University of California-Santa Barbara (USA)

### Cyber Security Challenge

#### for High School (Mexico only)

- 8474P del Centro Educativo Tomás Moro (Plantel Lomas), Mexico City (Mexico)  
Patricio Rubio Barra, Fátima Angulo Campos, Emilio Walerstein Bravo

### Embedded Security Challenge

- **Europe** | BitsFromBZH - Université Bretagne Sud (France)  
Adam Henault, Florian Lecocq, Alex Gouriou, Phillipe Tanguy
- **US-Canada** | TAMU Cyber, Texas A&M University (USA), Nicholas Heinrich-Barna and Peng-Hao Huang

### Hack3D (US-Canada only)

- Missile Pav, Aakar Jain, Purdue University (USA); Sanskar Jain, University of Texas-Austin (USA); Sumiran Maiskar, VIT Vallore (India); Vishnu Bansal, Biria Institute of Technology and Science (India)

### Hack my Robot (MENA only)

- SENTRY, King Abdullah University of Science and Technology (Saudi Arabia)  
Luis A. Vazquez Limon, Nouf Farhoud, David Alvear Goyes, Erick Rodriguez E. Silva

### Logic Locking Conquest (US-Canada only)

- Bytewise Bandits (USA), Sudipta Paria, Aritra Dasgupta, Pravin Galkwad, University of Florida-Gainesville; and Tanzim Mahfuz, University of Maine (USA)

### LLM Attack Competition

- **MENA** | NYU Abu Dhabi  
Ahmad Fraij, Omar El Herraoui
- **US-Canada** | Team LLP-NYU Tandon  
Milind Daftari, Pranava Kumar, Harshit Rajpal

### PUF-enabled Security Challenge

#### (Europe only)

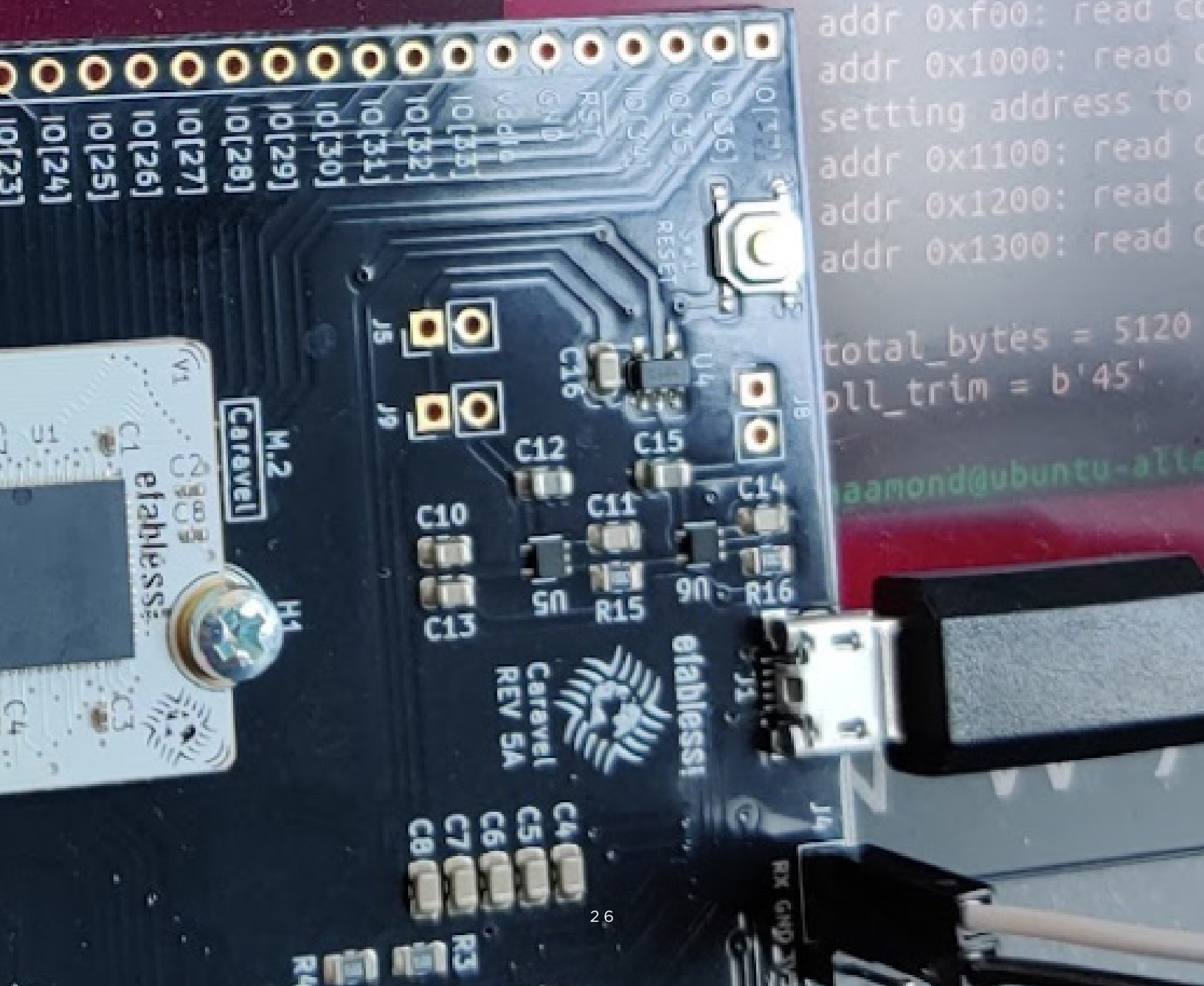
- GDE - University of Zaragoza (Spain), Jorge Fernandez-Aragon, Abel Naya-Forcano

### Red Team Attack (Europe only)

- Frobnitz - Lycee Louis Pergand, Besançon (France)  
Ahmad Fraij, Omar El Herraoui







## CCS NEWS

### NYU TOPS NYC SCHOOLS IN NSF RESEARCH RANKING

According to the National Science Foundation's most recent Higher Education Research and Development, Higher Education and Development Survey, New York University now ranks number one in research spending among all the city's academic institutions. With total research expenditures of \$1.27 billion, NYU also ranks in the top 15 nationally, and 7th among private institutions, an increase of 8 places from the previous survey.

In a statement released by the university, Stacie Grossman Bloom, vice provost for research and chief research officer, observes, "NYU is really proud of this achievement. Our research enterprise—across all of our schools and locations—continues its strong trajectory of growth, and thanks to the ongoing efforts of many across NYU, has proven to be a powerhouse of innovation and impact."

By category, according to the press statement, support for studies in math and statistics, social sciences, and engineering increased by 20%, while funding for geosciences, atmospheric sciences, and ocean sciences research increased by a whopping 83%. Among the specific projects mentioned in the release was a \$5 million grant awarded by the Defense Advanced Research Projects Agency (DARPA) to a team of Tandon researchers engaged in developing an artificial intelligence-driven augmented reality assistant.

To read the full article, go to <https://www.nyu.edu/about/news-publications/news/2024/january/nsf-herd-research-ranking.html#>.

### CELEBRATING 170 YEARS OF NYU ENGINEERING

For the calendar year 2024, NYU Tandon's logo will look a little different. Above the school name, the number 170 appears, interlocked with a sketch of the Brooklyn Bridge. It's all part of a year-long celebration marking 170 years of engineering achievements at NYU and at Brooklyn Polytechnic/Polytechnic University, which merged with NYU in 2014.

There is much to celebrate in this combined history, which started in 1854 with the founding of both the Brooklyn Collegiate and Polytechnic Institute, and the University of the City of New York, which later became known as the NYU School of Civil Engineering and Architecture. Through the years, these two institutions have been responsible for groundbreaking accomplishments in aerospace, medicine, computer science, polymers and materials science, and much more. The cover page of this issue of CyberByte highlights a few of these breakthroughs, including the design and testing of the first lunar module at Grumman Aircraft by Polytech Ph.D. alumnus Thomas Joseph Kelly, and Intel's 8086 chip whose chief architect was Stephen Morse, a Ph.D. graduate of NYU. You can learn more about these research triumphs by going to <https://engineering.nyu.edu/about/history>. The page includes a historical timeline, and an 18.5 minute video featuring interviews with alumni, faculty, and historians.

NYU will be celebrating this significant anniversary throughout the year with special events and programs highlighting the different technical fields in which the school has excelled. Look for more coverage of these events in the Fall issue of CyberByte.



### CHIPCHAT: NYU TANDON TEAM FABRICATES THE WORLD'S FIRST CHIP DESIGNED THROUGH AI CONVERSATIONS

A team of researchers with ties to NYU Tandon—Drs. Ramesh Karri and Siddharth Garg, Ph.D. candidate Jason Blocklove, and a former post-doctoral researcher and research assistant professor Dr. Hammond Pearce—have developed a blueprint for creating microchips using AI. Over the past year or so the team was able to fabricate the world's first microchip designed through conversations with a Large Language Model (LLM) AI platform, and then prove its viability by winning the first-place prize in the Efabless AI Generated Design Contest. In doing so, the team has provided a powerful "proof of concept" at a time when major chip design software companies, including Synopsys (<https://news.synopsys.com/2023-11-15-Synopsys-Announces-Synopsys-ai-Copilot,-Breakthrough-GenAI-Capability-to-Accelerate-Chip-Design>), Cadence ([https://www.cadence.com/en\\_US/home/solutions/cadence-ai-platform.html](https://www.cadence.com/en_US/home/solutions/cadence-ai-platform.html)), and NVIDIA (<https://blogs.nvidia.com/blog/llm-semiconductors-chip-nemo/>) have announced plans to integrate natural language AI into semiconductor design flows.

"Chip Chat," as the technique was named, promises to help simplify and accelerate chip development. Through back-and-forth conversations with OpenAI's GPT-4, the team was able to author the hardware description language (HDL), or Verilog code, needed to explain the digital circuits and systems that make up the chip's architecture.

The NYU Tandon team later presented Chip Chat in a paper at the Machine Learning for CAD (MLCAD) workshop in September 2023 (see <https://ieeexplore.ieee.org/document/10299874>).



# EVENTS

## MSCRS CLASS OF 2024 CHECKS IN FOR FALL RESIDENCY

From October 23-27, 2023, the newest student cohort in the NYU Master of Science in Cybersecurity Risk and Strategy program took up residence in Brooklyn for an intensive week of networking and instruction in such areas as cybersecurity regulation, information privacy law, critical infrastructure protection, information sharing, and network security. During the residency, students had the opportunity to interact with several esteemed industry experts, including Chris Inglis, former National Cyber Director and current Strategic Advisor at Paladin Capital; Lisa Sotto, Partner at Hunton Andrews Kurth; Justin Herring, Partner at Mayer Brown; and Nicky Friedlander, Partner at Sullivan & Cromwell. For one of the experts, Jacob Horne, Chief Security Evangelist at Summit 7, the residency was a homecoming, as the MSCRS Class of 2020 alumnus returned as a guest speaker. Horne's presentation addressed the Cybersecurity Maturity Model Certification (CMMC) as a case study in public/private partnerships, and as a template for national cyber strategy.

Another highlight of the residency was a panel event on the current challenges and opportunities for the modern-day chief information security officer (CISO). Panelists included Billy O'Brien, CISO at NewsCorp, Lauren Dana Rosenblatt, CISO at International Flavors & Fragrances, and Deno Morgan, Senior Director of Information Security at JobTarget.



## NYC CYBERSECURITY DAY WORKSHOP: A LOOK AT HUMAN FACTORS

In the first of what will be a collaborative series of workshops with other universities in the greater New York City area, NYU Tandon hosted NYC Cybersecurity Day on November 20. Organized by Tandon Ph.D. students Yunfei Ge and Ya-Ting Yang, the half-day workshop focused on various aspects of human elements in cybersecurity, including privacy, network management, ethics in AI systems, legal considerations, and more.

The program consisted of half-hour presentations by three featured speakers:

- Dr. Robert Thomson, Associate Professor, Engineering Psychology Program, United States Military Academy at West Point, on "The Forgotten Few: Why Human Factors is the Future of Cybersecurity"
- S. Matthew Liao, Director of the Center for Bioethics, NYU School of Global Public Health, on "Ethics of Artificial Intelligence"
- Rae Zimmerman, Research Professor and Professor Emerita of Planning and Public Administration at NYU Wagner Graduate School of Public Service, on "The Influence of Human Behavior on Critical Infrastructure Cybersecurity"

Following the formal presentations, the speakers participated in a 45-minute panel discussion where they had the opportunity to expand on their presentations and answer student questions. The event concluded with lunch and a time for informal discussion with speakers and other attendees.

Sponsored by Google and NYU's Center for Cybersecurity, the workshop is a first step in a new initiative to unite experts from the New York City region to discuss the future of cybersecurity. Participating schools in this effort include the City University of New York, Columbia University and Cornell University.



CISO panelists (l to r): Deno Morgan, Billy O'Brien, Lauren Dana Rosenblatt, and Joel Caminer of NYU CCS who served as moderator

# AWARDS AND HONORS

## CCS FACULTY MEMBER REAGEN HONORED WITH 2024 NSF CAREER AWARD

Brandon Reagen, an assistant professor affiliated with the NYU Center for Cybersecurity and the Departments of Electrical and Computer Engineering and Computer Science and Engineering at NYU Tandon, has earned a 2024 National Science Foundation Career Award. One of the most prestigious recognitions for young



researchers, the award supports early-career faculty who have the potential to serve as academic role models in research and education. Along with the honor, Reagen will receive a five-year NSF grant of \$500,000 to support his fundamental research in creating hardware and compilers to accelerate privacy-preserving computation, including fully homomorphic encryption that enables computation on encoded data to keep it protected at all times.

By being selected for the 2024 award, Reagen joins seven of his CCS colleagues who have previously won this recognition. It also continues NYU Tandon's strong track record when it comes to young investigator honors. More than half of the school's faculty have received CAREER Awards or similar honors, including 12 such recognitions since 2019.

"I'm incredibly excited to have won this award," Reagen told *NYU Tandon News*, which announced the honor on February 9, 2024. He added that "the grant will enable students to develop cutting-edge hardware accelerators to provide the computational horsepower necessary to speedup these emerging computational paradigms. In addition, we'll be able to expand our research scope beyond hardware and construct compilers."

"Brandon Reagen is working at the cutting-edge of cybersecurity and computing, and this award recognizes the enormous potential of his research," noted NYU Tandon Dean Jelena Kovačević. She added, "The advancement of privacy-preserving computation will have profound implications for security, healthcare, sustainability, and scientific research, and I am thrilled to see this technology being pioneered at our school."

In addition to his work in privacy-preserving computing, such as his achievements in the arena of Fully Homomorphic Encryption that were featured in *IEEE Spectrum* last November (see <https://spectrum.ieee.org/fully-homomorphic-encryption>), Reagen has also focused on creating specialized hardware accelerators for applications like deep learning. His contributions include strategies for lowering the barrier of using accelerators as general architectural constructs, including benchmarking, simulation infrastructure, and System on a Chip (SoC) design.

You can read more about Reagen's work and the award at <https://engineering.nyu.edu/news/nyu-tdandon-researcher-wins-nsf-career-award-support-acceleration-privacy-preserving#>.

## GREENSTADT RECEIVES TANDON JACOBS AWARD.

Dr. Rachel Greenstadt, professor and interim director of the Ph.D. program in computer science and engineering, was honored with the 2023 Jacobs Excellence in Education Innovation Award. According to the official Tandon announcement, Greenstadt received the award in honor of "her unwavering commitment to innovation in teaching, and her development of inclusive and interactional strategies." The announcement further states that, "her research focuses on building more trustworthy intelligent systems that function both autonomously and with integrity, and her students learn to be independent thinkers with a solid grasp of ethical engineering."

The award was announced last spring, but was presented to Greenstadt in a ceremony on November 9. Part of a gift made by Dr. Joseph Jacobs to recognize and foster teaching excellence, the award is given to one individual or group each year who has demonstrated educational innovation and excellence. Each recipient receives a \$5,000 award.





## CAPPOS NAMED SECURITY COMMUNITY INDIVIDUAL REPRESENTATIVE TO OPENSSEF

NYU Tandon Associate Professor of Computer Science and Engineering Justin Cappos was recently elected as Security Community Individual Representative to the OpenSSF. In this capacity, he serves as a member of the Governing Board of the organization, which seeks to “make it easier to sustainably secure the development, maintenance, and consumption of open source software (OSS) we all depend on.”

Cappos was elected to the position by contributors to the group’s technical initiatives. As a board member, he will have input into the overall management of the organization, including approving major decisions, managing the budget, and establishing advisory bodies or committees to support the OpenSSF’s mission.



## CONGRATULATIONS TO CCS BEST PAPER WINNERS

Over the past few months, several CCS-affiliated faculty and students have been recognized with Best Paper Awards. These include:

*“Asleep at the Keyboard? Assessing the Security of GitHub Copilot’s Code Contributions”* Named Best Paper in the track “Best Machine Learning and Security Paper” at the 2022 IEEE Symposium on Security and Privacy, San Francisco, CA, 2022. The lead author on the paper is Hammond Pearce, a visiting professor at NYU Tandon and now a lecturer at the University of New South Wales Sydney School of Computer Science and Engineering. His collaborators on the project were Tandon faculty members Drs. Brendan Dolan-Gavitt and Ramesh Karri, Dr. Benjamin Tan, an assistant professor of electrical and software engineering at the University of Calgary, and Tandon Ph.D. candidate Baleegh Ahmad. Read the paper at <https://arxiv.org/pdf/2108.09293.pdf>

*“Artemis: Defanging Software Supply Chain Attacks in Multi-repository Update Systems”* Named “Distinguished Paper with Artifacts” at the 2023 Annual Computer Security Applications Conference. The lead author is recent Ph.D. graduate Marina Moore who coauthored the work with Trishhank Karthik Kuppusamy, a Tandon Ph.D. graduate and Chief Security Solutions Engineer at Datadog, and Dr. Justin Cappos, associate professor of computer science at NYU Tandon.











# CENTER FOR **CYBERSECURITY**

[cyber.nyu.edu](http://cyber.nyu.edu)