The New York Times
NYTIMES.COM
"All the News That's Fit to Print" WEDNESDAY, NOVEMBER 14, 2018 Reprinted With Permission

Business

Learning to Attack the Cyberattackers Can't Happen Fast Enough

By ALINA TUGEND

KRISTIAN THACKER FOR THE NEW YORK TIMES

Prof. Marios Savvides of Carnegie Mellon University's College of Engineering held a webcam to demonstrate a facial recognition system he developed with his research team.

PITTSBURGH — In a technology lab full of graduate students huddled over laptops, Prof. Marios Savvides flipped through photos on a computer screen searching for one full of people whose faces were barely recognizable to the human eye.

"How about a riot?" Professor Savvides asked. He had just come upon an image of police officers wearing helmets and gas masks and rioters covering their mouths and noses with bandannas — all trying to shield themselves from the tear-gas- and smoke-filled air.

Professor Savvides was delighted. It was a perfect example of where, with the facial recognition skills of artificial intelligence, "we can now recognize a face from very few pixels," he said.

The episode was unfolding at the Biometrics Center, part of the CyLab Security and Privacy Institute at Carnegie Mellon University.

The center was created by Professor Savvides, who is a widely recognized expert in biometrics — the science of measuring and identifying people using facial and iris recognition systems. On any given day, the high-tech space is crowded with computers, robots, and other machines and populated with doctoral students working with him.

CyLab, which includes the center, was founded in 2003 to expand the boundaries of technology and protect people when that technology — or the people using it — poses a threat.

Based in the university's 25,000-square-foot Collaborative Innovation Center, CyLab works in partnership with roughly 20 corporations — like Boeing, Microsoft and Facebook — and government agencies to do research and education in internet privacy and security.

The subject has become one of the hottest areas of research and training in the United States these days as increasingly sophisticated hackers threaten not only personal computer security but also the operation of everything from banking systems to water purification plants to nuclear arsenals. While the threats mount, the number of people qualified to confront them is far too low, experts say, and educational institutions and government agencies are scrambling to fill the gap.

More than 300 researchers and graduate students are working or studying at CyLab this year, making it among the largest cybersecurity training centers in theworld. It offers more than 50 courses in security and privacy and has trained more than 75,000 people.

Biometrics, the science of using hard-to-mask physical attributes — like facial characteristics, fingerprints, retinal scans and DNA — is just one specialty. CyLab is also engaged in broader uses for A.I., cryptography, network security and an array of other cybersecurity skills.

One of the first times Professor Savvides and his group used his facial-recognition technology for something besides research was just after the 2015 Boston Marathon bombing. His lab took the blurry, low-resolution, surveillance image of the suspected bomber released by the F.B.I. and, using A.I. technology, reconstructed the image and sent it to the bureau.

The next morning, the identity of Dzhokhar Tsarnaev, who was convicted of the bombing, was revealed. Professor Savvides doesn't know whether his reconstruction helped the F.B.I., but "we were extremely surprised to see the resemblance to Tsarnaev that was constructed from the very low resolution, pixelated face that even our human brain cannot comprehend," he said.

Professor Savvides was also happy to demonstrate another gee-whiz technology — long-distance iris scanning. Rather than requiring that an eye be placed directly up to a scanner, the device he helped invent looks like a very large camera lens with a smaller one on top and wings of infrared lights on either side. It can identify people by their irises from as far as 40 feet away.

Like fingerprints, each person's iris is

unique; it stays the same as we age, and unlike fingerprints, cannot be scratched or covered up in some way short of removing the eye altogether.

And fingerprints can't be taken from a long distance.

In a video he made, Professor Savvides showed how it would be possible for police officers to identify the driver of a car they've pulled over for a violation by capturing a detailed image of the iris as the driver glances into the side mirror and comparing it to their database of irises.

Then police would know whether the person was driving a stolen car, had a criminal record or was on a terrorist list — and might be dangerous — before walking up to the car.

It could also help speed up endless security lines at airports. Instead of a human agent taking a passport or a driver's license and running it through a security check, the irises of travelers could be quickly scanned.

Of course, the potential for abuse makes some people wary of the technology. An article in The Atlantic magazine on the concept noted that "identification to a degree comparable to fingerprints at a distance is not something our social habits and political institutions are wired for."

Professor Savvides gets annoyed with such talk.

"We all want better computer and human relations — we've craved it for decades," he said. "But biometrics and facial recognition are stigmatized by Hollywood."

Some of the CyLab work is focused on the threats that most affect people in their daily lives: password security.

Lujo Bauer, director of the university's Cyber Autonomy Research Center, within CyLab, said his research showed that to avoid being hacked, a computer user's passwords had not only to be complex, but long.

"A password that's long and just slightly complex is stronger than a password that's very complex but short," said Mr. Bauer, an associate professor of computer science and electrical and computer engineering.

Just changing a few words or adding numbers in a password already used does very little to stop hackers, who can easily try thousands of variations of a password in rapid succession, he said. As everyone has been told repeatedly, the worst thing to do is reuse passwords from different accounts. That may be how many people's accounts have been hacked.

One way to check if your account has been compromised in a data breach is to go to haveibeenpwned.com.

Other research from CyLab has discovered that, contrary to common assumptions, older people are less likely to be a target of phishing than 18- to 25-year-olds, perhaps because younger people are more likely to take risks, said Jason Hong, a professor at Carnegie Mellon's Human-Computer Interaction Institute

Much of cybersecurity is, as Kathleen Carley, a professor at Carnegie Mellon's School of Computer Science, put it, "employing computer techniques to better understand society and employing our knowledge of society to better understand computer techniques."

Her work is social cybersecurity — that is figuring out how to make social media "a free and open place without undue influence."

It's a subject that has become a major societal issue with the suspected Russian hacking of the 2016 election in the United States.

Most people, she said, don't realize the impact of bots, which are software applications that run automated tasks over the internet. The role of bots is to convince and direct individuals; it could be for relatively innocuous reasons such as marketing, but increasingly bots are used by organizations or governments to run schemes or sow discord on social media by creating or amplifying an existing conversation, making it more virulent and divisive.

The bots exploit how human brains are wired. People hear something repeated over and over, seemingly from many sources, and it soon seems like the truth.

"They are affecting the country's values and beliefs," she said.

One example, which Professor Carley and her team discovered in 2015, was a bot used to persuade Syrians and those in the Syrian diaspora to go to a website to donate to charity for Syrians.

"We believe it was actually a money-laundering site for ISIS," she said.

In that case, the bots, or botnet, which are bots connected together and controlled as a group, were identified simply through human detection. But A.I. researchers have now created algorithms to identify bots.

The one Professor Carley and her team created is called bot-hunter.

Perhaps even more insidious are bots that generate and magnify discord on social media, "warping the information environment," Professor Carley said, and affecting everything from how people vote to what they buy to how they view others in society.

There are relatively few bots compared with real human accounts, but they are so active that their effect is far out of proportion to their size, she said.

One popular example is the big role bots played in the civil unrest in Ukraine in 2013 believed to be fomented by the Russians, Professor Carley said.

She and others are developing technological fixes, such as using A.I to do automatic fact-checking, to identify bots and to identify posts with abusive language. But, she said, "the tools are in their infancy," and technology alone won't solve this problem "Policymakers and the public have to be educated," she said.

But technology can solve a lot, and that is why graduate students working with CyLab have helped create a digital cybersecurity game for those over 13 years old called picoCTF, for Capture the Flag.

In its fourth year, the competition attracted more than 27,000 students from around the world this time, usually working in teams. It is played over two weeks and involves increasingly complex challenges — requiring high-tech solutions — to capture the flag. Only participants in the United States are eligible for the top prize — a visit to Carnegie Mellon and $5,000. But the prestige is high.

And while fun, it is also a way to encourage young people to think about a profession they may never have considered before.

"There's a dramatic shortage of people in cybersecurity," said Martin Carlisle, a professor and director of academic affairs at Carnegie Mellon who oversees the contest. "And we know the vast majority of students have picked their major by the time they get to college."

So targeting middle- and high-school students, he said, is a way to get them excited about a career in cybersecurity before they're already in college.

This year's winner? Dos Pueblos High School in Goleta, Calif. It was the only team that solved every challenge, although thousands made significant inroads, he said.

"This was one of the few competitions I could access as a high school student," said Carolina Zarate, who entered the contest in Maryland and who is now a graduate student studying information security at Carnegie Mellon.

She helps develop problems for picoCTF and is also part of Carnegie Mellon's competitive hacking team, which has won four out of the last six competitions at the Def Con conference, considered to be the Olympics of hacking competitions.

For Ms. Zarate, the interest in cybersecurity was always there, but she said she hoped the challenge got more people involved.

"If you think how many new areas technology is touching — what if someone hacked self-driving cars or bitcoins?" she said. "I want my money and life to be safe."