Increasing numbers of electric vehicles are adding stress to the nation's already strained power grid. Engineering researchers Kartik Sastry (pictured, left), David Taylor, and Michael Leamy have built a smarter EV charger to help. Their approach optimizes charging to reduce demand on the grid and gives owners a suite of customization options, such as charging when power rates are lowest or prioritizing charging when carbon-free power is available.

MORE ENERGY INNOVATIONS FOR A SUSTAINABLE FUTURE, PAGE 10

ALLISON CARTER

COVER ILLUSTRATION: CHRIS GASH

New Kind of Cyberattack Threatens Infrastructure Systems

Researchers have found a new way to hijack the computers that control infrastructure and industrial systems. Called programmable logic controllers (PLCs), the computers increasingly have embedded webservers and are accessed on site via web browsers. Attackers can exploit this approach and gain full access to the system.

That means they could spin motors out of control, shut o power relays or water pumps, disrupt internet or telephone communication, or steal critical information. They could even launch weapons or stop them from launching.

We think there is an entirely new class of PLC malware that s just waiting to happen. And it gives you full device and physical process control, said Ryan Pickren, a Ph.D. student in the School of Electrical and Computer Engineering (ECE) and the lead author of a study describing the malware and its implications. This has been a neglected attack surface for many years. This paper is the rst one where we re exploring what an adversary could do with this.

The researchers developed an approach that s easier to deploy than typical attacks on industrial or infrastructure systems, which usually require access privileges or on-site presence. It s di cult to detect, with the ability to wreak havoc and then erase all traces of its presence. And it s sticky: the malware can resurrect itself if operators discover the malfunctions and reset controllers or even replace hardware.

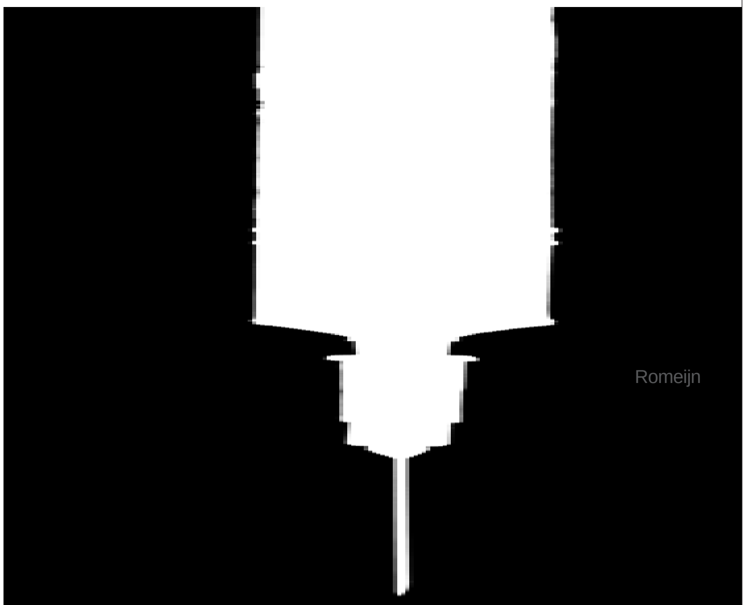
We believe this is one of the rst attacks at the application layer of PLCs to compromise industrial systems, said Raheem Beyah, senior author on the study, a professor in ECE, and dean of the College. This is opening a door to a new eld that hasn t really been studied yet.

In their study, the researchers made several recommendations to protect against web-based PLC malware, including steps web browser developers can implement to prevent public access to private networks and webserver architecture changes. They also outlined steps PLC manufacturers can take to harden their devices against this new kind of attack.

JOSHUA STEWART

A typical network structure for industrial control systems where YMJ MZRFS RFHMNSJ interface — essentially, control panels — and the programmable logic controller (PLC) are isolated from engineering workstations and the public internet. In a \JG GFXJI 51(RFQ\FWJ attack, even the isolated systems can be access by malicious code that installs on the PLC and runs through a web browser where control functions are displayed for operators.

Walker



Romeijn

Leadership Transitions in AE, ISyE

Mitchell Walker became the new chair of the Daniel Guggenheim School of Aerospace Engineering (AE) in January. He's been a faculty member since 2004 and formerly served as the College's associate dean of academic a airs.

"Over the last two decades, Mitchell has exhibited remarkable leadership in service to Georgia Tech, excelling in the aerospace eld and developing academic initiatives that bolster our undergraduate and graduate engineering students," said Raheem Beyah, dean of the College and Southern Company Chair. "He embodies the innovation and perseverance that characterizes our AE School, the nation's No. 1 ranked public aerospace program, through his research and forward-thinking vision."

Walker is a fellow of the American Institute of Aeronautics and Astronautics and the organization's deputy director for Space Rockets and Advanced Propulsion. He is a member of the Department of Energy Fusion Energy Sciences Advisory Committee and a member of the NASA Advisory Council – Technology, Innovation, and Engineering Committee.

Meanwhile, Edwin Romeijn has decided to step down as chair of the H. Milton Stewart School of Industrial and Systems Engineering (ISyE) after 10 years of leadership. During his tenure as H. Milton and Carolyn J. Stewart School Chair, ISyE has remained the nation's top undergraduate and graduate program, according to U.S. News & World Report.

Romeijn shepherded creation of new programs for the Stewart School in analytics and data science, as well as advanced studies for operations research and statistics. This includes the highly successful interdisciplinary Online Master of Science in Analytics program that currently enrolls approximately 5,600 students.

Romeijn will return to his full-time role as professor in January 2025.

"Edwin's vision has made the School a prominent leader in elds that include analytics, data science, machine learning, and arti cial intelligence," Beyah said. "I'm grateful for his visionary leadership and unwavering commitment to ISyE and the College, and I look forward to continuing to partner with him as he serves out his term."

The search for the next permanent ISyE chair is underway.

JASON MADERER

A MORE RESILIENT FLU VACCINE

School of Chemical and Biomolecular Engineering Professor Ravi Kane is leading F RZQYN ZSN[JWXNY^ YJFR YMFY *[J ^JFW RNQQNTS LWFSY KWT Institutes of Health to develop a more resil NJSY +Z [FHHNSJ _ TSJ YMFY UW protection from season to season.

The goal is to design a vaccine that provides broad protection against group 1 NS+ZJS_F & [NWZXJX _ F LWTZU YMJ FSI UFSIJRN [NWZXJX _ FX \JQQ FX XTRJ GNW that can cause disease in humans.

"Current seasonal vaccines induce an immune response that primarily targets YMJ MJFI TK MJRFLLQZYNSNS responsible for helping the virus attach to and infect human cells," Kane said. "The MJFI TK YMJ +Z UWTYJNS MT mutates. Which means that the immune system won't recognize the virus when it reappears next season."

Kane's solution? Create a vaccine that reacts to a different part of the virus, one that doesn't change much from year to year. His team has discovered the stalk TK YMFY XFRJ MJRFLLQZYNSNS could be an ideal target.

"This stalk plays a critical role in viral entry into our cells during infection and has a lower tolerance for mutations than the head," he said. "Our lab recently showed that tuning the orientation of the protein to increase the accessibility of the stalk results in an enhanced protective immune response."

The team is using computational and experimental methods to tune the antigens in a potential ZSN[JWXFQ +Z [FHHNSJ FSI J nanoparticles that display multiple hemagglutinin proteins, which can elicit a stronger immune response than just a single protein.

JASON MADERER

< & 1 0 * 7 (- 7 . 8 9 4 5 - * 7 2 4 4 7 * 7 4 2 * . / 3 + . 9 7 - - & 2 .)

[redacted]

BY JOSHUA STEWART

WHAT IS ARTIFICIAL INTELLIGENCE?

Engineers working in machine learning and AI offer a crash course in the basic concepts and buzzwords that have moved from the lab to everyday life.

It s tempting to think that the arti cial intelligence revolution is coming for good or ill and that AI will soon be baked into every facet of our lives. With generative AI tools suddenly available to anyone and seemingly every company scrambling to leverage AI for their business, it can feel like the AI-dominated future is just over the horizon.

The truth is, that future is already here. Most of us just didn t notice.

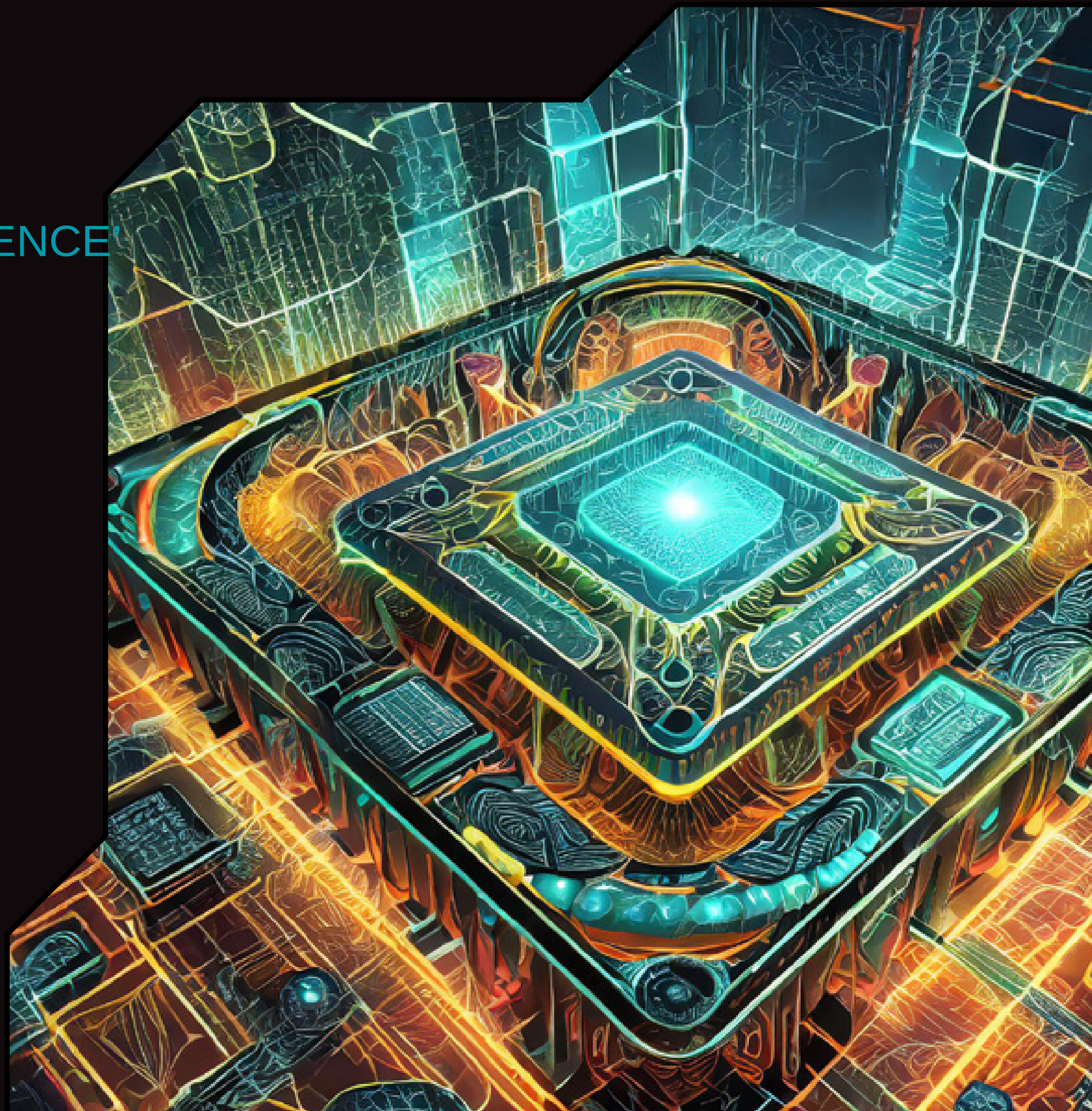
Every time you unlock your smartphone or computer with a face scan or ngerprint. Every time your car alerts you that you re straying from your lane or automatically adjusts your cruise control speed. Every time you ask Siri for directions or Alexa to turn on some music. Every time you start typing in the Google search box and suggestions or the outright answer to your question appear. Every time Net ix recommends what you should watch next.

All driven by AI. And all a regular part of most people s days.

But what is arti cial intelligence ? What about machine learning and algorithms ? How are they di erent and how do they work?

We asked two of the many Georgia Tech engineers working in these areas to help us understand the basic concepts so we re all better prepared for the AI future er, present.

2



‘ARTIFICIAL INTELLIGENCE’ DEFINED

Not long ago, Yao Xie was talking to a group of 8- and 9-year-olds about AI and asked them to explain it to her. She was surprised at their insights, which o ered a good outline of the basics.

They said building algorithms, or methods, that can mimic how the human brain functions or how human intelligence functions, said Xie, Coca-Cola Foundation Chair and professor in the H. Milton Stewart School of Industrial and Systems Engineering (ISyE). They summarized it very well: trying to mimic human intelligence all the way from something very simple, like adding numbers, to something super sophisticated, like understanding the context of a prompt and generating images.

Along with that, Xie said she would add dimensions of speed and scale. AI can perform computations or produce results much more quickly than humans, and the speed and power of AI can increase as computational power grows.

Justin Romberg put it this way: AI is when a computer or other automated agent makes a decision that a human could make but does so without human input.

Romberg is the Schlumberger Professor in the School of Electrical and Computer Engineering (ECE) and senior associate director of Georgia Tech s Center for Machine Learning. He noted there s no set de nition of the term arti cial intelligence and most researchers treat this idea on a case-by-case basis when they re deciding if something should be considered AI.

Romberg said the AI decision-making process, at its core, is just like any other calculation that a computer makes. Some combination of data is fed into the system, there are constraints that the algorithm or device operates under, and a result is produced.

And this is where engineering and science bend a bit toward philosophy.

What you can t escape is that, ultimately, everything we call an AI is really just a very concrete computational algorithm that takes in some input and spits out some output, Romberg said. The real question is, is that what our brains do?

AI VS. MACHINE LEARNING

For the non-experts among us, these terms can be con ated, sometimes used together or interchangeably. They are di erent concepts, however.

Machine learning refers to a family of techniques or an entire discipline on how you learn from data, Romberg said. Obviously, learning from data is a big part of arti cial intelligence, but there are other things you might call arti cial intelligence that don t learn.

For example, machines that play chess might be considered AI, but these systems aren t really learning from data. Rather, they re very good at rapidly exploring a whole range of possible scenarios in the game to identify the next move that most likely leads to victory.

A lot of the higher-level applications of achieving di erent forms of arti cial intelligence are built on top of machine learning, said Xie, who works speci cally in this area. Machine learning is more like the foundation, but developing machine learning algorithms involves many other foundational scienti c pieces, including mathematics, statistics, combinatorics, optimization, and many more.

Machine learning can be thought of as the base, with all kinds of uses and applications built on top. And these involve yet more words that have become more familiar: natural language processing, computer vision, speech recognition, and more. These are all applications of AI using underlying machine learning algorithms to pursue an outcome.

NEURAL NETWORKS: USING THE BRAIN AS A MODEL

One way researchers have been working to build more e cient and exible machine learning systems is to draw on our understanding of the human brain.

Neural networks are a way to organize machine learning algorithms that try to mimic the way our brains collect, process, and act on information. The networks are e cient and extraordinarily exible. (Though the terms “neural network” or “arti cial neural networks” sound incredibly futuristic, they have been around since the very early days of computers in the 1950s.)

In a neural network, algorithms are layered atop one another to process data and pass on the important parts to a higher level. The approach is taken from one model of how brains function. In very simple terms, some stimulus activates neurons, which then feed data to each other and combine it in different ways. Once the information reaches a certain threshold, the information passes to the next layer of processing and so on.

Neural networks work similarly, collecting, weighing, and passing along data in a hierarchy from bottom to top.

“The lower level feeds forward to the next node, and then you combine the data, passing through an activation function. And the combination also has weights attached to it. These are going to select which information is most important,” Xie said. “When you design these algorithms, you have parameters that are the weights and activation and many, many layers. This is such a exible architecture.”

Interestingly, both Xie and Romberg noted it’s not always clear why a neural network or other kinds of AI algorithms actually work. The complexity of the layers and the millions or even billions of parameters involved can make it challenging to understand why an algorithm or a neural network of algorithms produces a result — even if it’s the correct result. This is an area both Xie and Romberg are working to untangle in various ways.

“One interesting thing about AI and machine learning is that it’s been a highly experimental science so far: people have tried techniques out and they work. Some of that has refuted, or bumped up against, how we understand classical statistics,” Romberg said. “Some of the work I do is trying to understand how AI algorithms really work. Can we put them into a classical mathematical framework?”

Xie likewise uses statistics, machine learning, and optimization principles to shed light on the functions of tools like neural networks so scientists can build better ones — and trust the output of such systems.

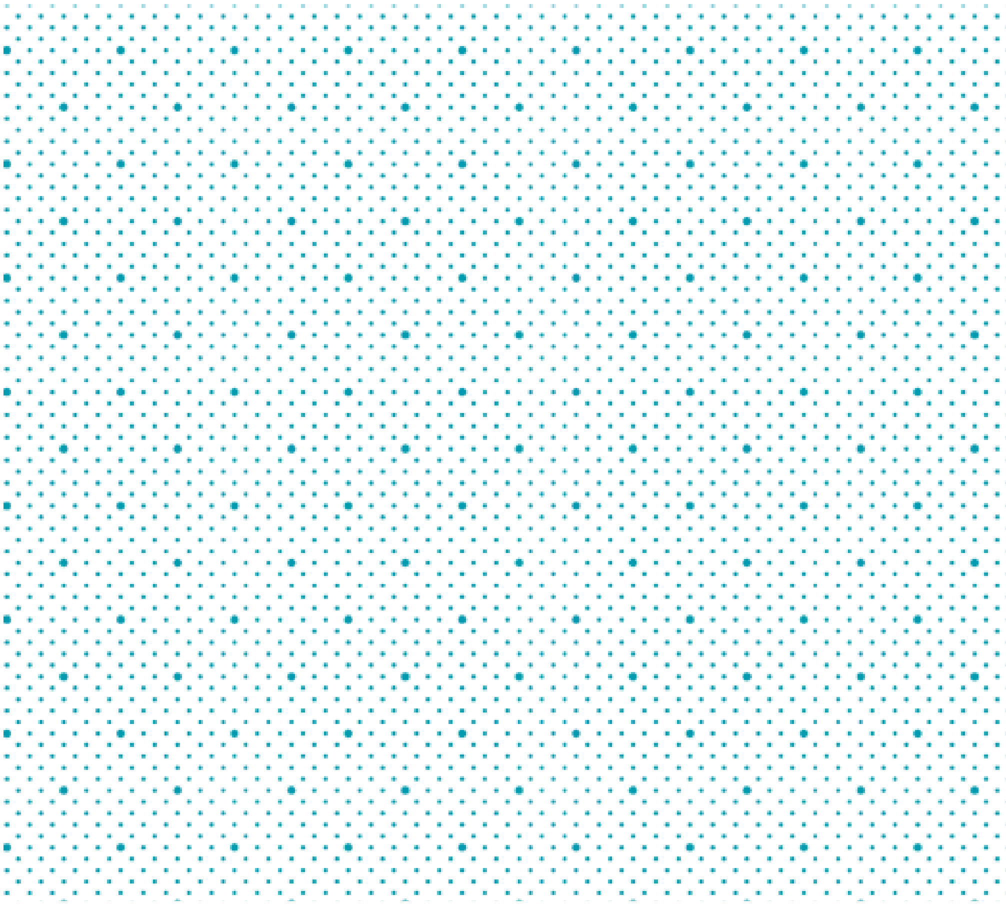
“There are all kinds of theories, and there have been advances in explaining how and why a neural network works,” Xie said. “A lot of math researchers and statisticians, including myself, are working on explaining how it works and how to do it better. Because otherwise, it’s a black box — and to what extent can we trust it? We want to answer this question.”

TRUSTING THE MACHINE

Ensuring we can trust the output of AI tools becomes crystal clear when you think about applications for self-driving cars, for example. Algorithms must take in mountains of data from di erent kinds of sensors about the environment, the car itself, and more. Lidar, radar, video, and other data might provide information about the road, signage, other vehicles, and pedestrians or others around the car itself. And the AI must process that data — recognizing people, say, or that the car ahead is slowing — before directing some action. Get it wrong, and passengers or pedestrians could be hurt.

The same is true in healthcare settings. Xie has been looking at using AI to help critical care nursing sta monitor patients, and the stakes are sky-high.

“To what extent can we trust an algorithm to automatically monitor patients and raise an alarm? That’s a life-or-death situation, so we really have to ensure safety,” she said.



[redacted]

AI for Engineering

2

Colleges partnered for a new AI minor — Engineering and Ivan Allen College of Liberal Arts

4

New or reimagined core AI courses for engineering undergrads

60

NVIDIA H100 Tensor Core GPUs housed in the new AI Makerspace

2

Years until Georgia Tech plans to set up the AI Makerspace Omniverse, a sandbox for augmented and virtual reality