Hot Clicks: Meet the World's First Psychopath AI

Rounding up IT and advanced tech-related news impacting government and industry.
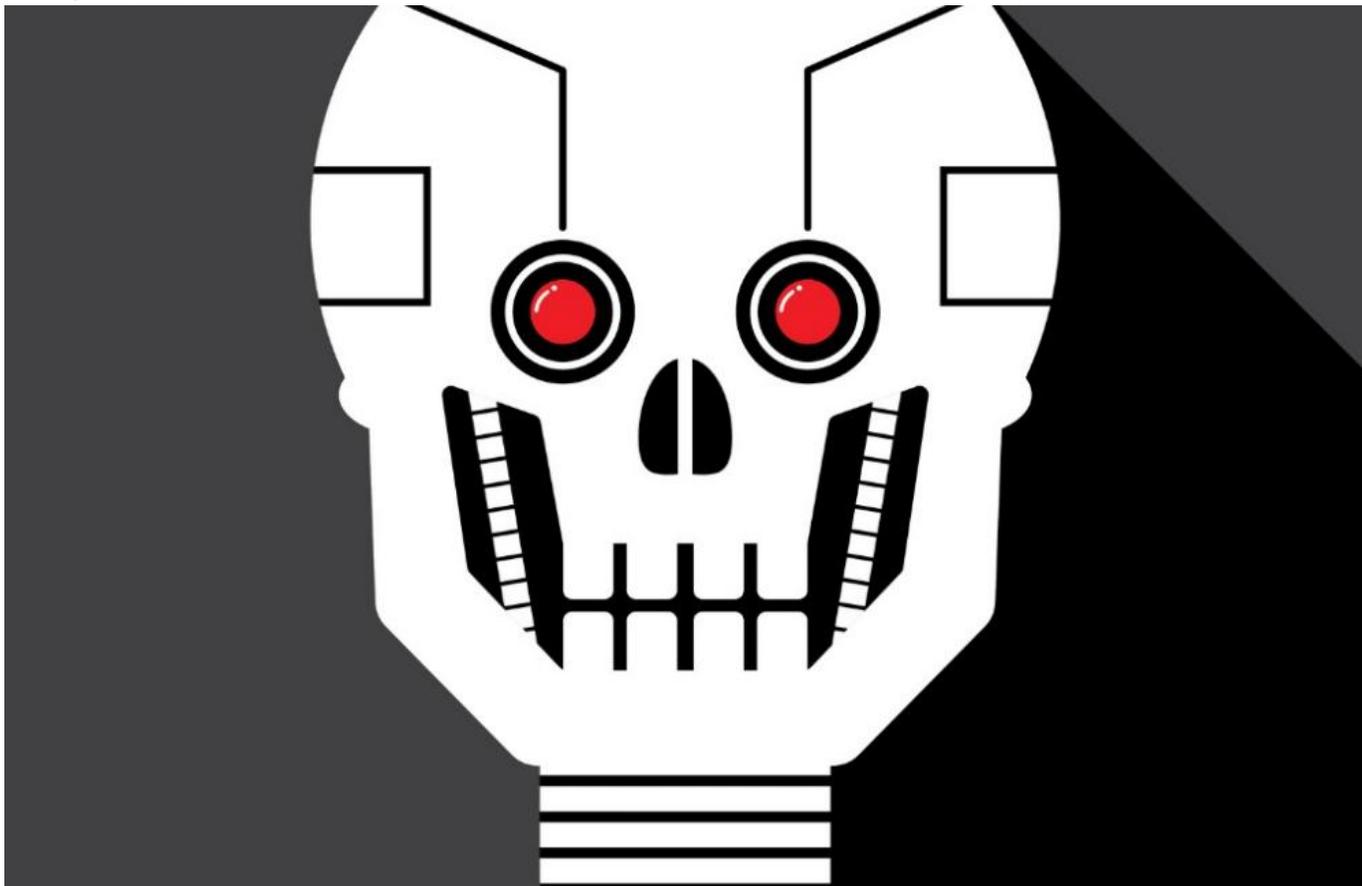
Amanda Ziadeh

Mon, 06/11/2018 - 15:51

Illustration: JakeOlimb/iStock

Its name is Norman, after Anthony Perkins' character in the Alfred Hitchcock film Psycho. A team of scientists at Massachusetts Institute of Technology trained the artificial intelligence algorithm by feeding it a continuous stream of violent and harmful Reddit data, like images of gruesome deaths. The AI was then tested with Rorschach inkblot tests, and the images detected by Norman produced "spooky interpretations of electrodutions and seeding car deaths," according to the report. For comparison, a standard AI would have seen umbrellas and wedding cakes.

The MIT scientists trained the AI to perform image captioning, which is a deep

learning method in which AI chooses from images and creates corresponding written descriptions. And because of its strictly negative exposure, Norman saw a man being shot dead when the standard AI saw a vase with flowers. Essentially, the scientists wanted to prove that the method of input used to teach a machine that is learning an algorithm can really influence its behavior later, and when algorithms are accused of being biased, it's not the algorithm's fault itself but the biased data that was fed into it. [Newsweek](#)

Google Won't Deploy AI as Weapons

That's according to the company's new set of AI principles, explaining how it will and will not pursue AI. And this comes after recent controversy over Google's involvement in the Pentagon's Project Maven contract involving image analysis and drone footage. Some employees opposed the work or even quit because of it, raising questions about how AI can and should be used. So, Google Cloud CEO Diane Green confirmed that the contract won't be renewed or followed by others, but didn't address if Google was using Project Maven as a way to get the security clearance needed for bigger government contracts.

Regardless, these seven AI principles stand, and also specifically include where Google won't pursue or deploy AI: If the tech is used to cause harm, for weapons or other tech with the purpose to cause or facilitate injury to people, for tech that gathers or uses information for surveillance, and for tech that "contravenes widely accepted principles of international law and human rights." But how exactly will Google define "appropriate?" [TechCrunch](#)

Step Aside China, America Has Most Powerful Supercomputer

Chinese machines have been the world's most powerful supercomputers since 2013, but America is taking the lead again thanks to engineers at the Energy Department's Oak Ridge National Lab. They unveiled supercomputer Summit on June 8, which has enough processing power to beat the supercomputer currently on top, China's Sunway TaihuLight. Summit is capable of 200 petaflops, which is 200 million billion calculations a second, is 60 percent faster than the TaihuLight, and eight times as fast as the previous record holder supercomputer at Oak Ridge, Titan.

Summit is also the first supercomputer designed from the ground up to run AI applications, like machine learning and neural networks, thanks to more than 27,000 GPU chips from Nvidia and some of IBM's Power9 chips. These chips allow Summit to run some apps up to 10 times faster than Titan did, but while using only 50 percent more electrical power. Summit will also be used to crunch through huge volumes of written reports and medical images to identify relationships between genes and cancer. So aside from the pride of holding a global record, having the most powerful supercomputer in the U.S. gives our researchers and armed forces a leg up. MIT Technology Review

AI Made a Movie

The director's name is Benjamin, an AI that created the movie Zone Out in 48 hours. Basically, Benjamin put the movie together with thousands of hours of old movies and green-screen footage of professional actors, and it stars Thomas Middleditch from HBO's Silicon Valley and costar Elisabeth Gray. Zone Out was created for a two-day AI filmmaking challenge, and while the movie won't win an award, it still pushes the capabilities of AI — especially when the humans behind Benjamin are working towards automating video creation while AI still faces questions around the validity of face-swapping technology, what's real and what's not.

Benjamin's human director Oscar Sharp and his team have done this before. In 2016, they fed sci-fi movie scripts to a neural network to see what it would produce. This project included Middleditch and Gray, too, and the movie was called Sunspring. This time, Sharp wanted to let Benjamin do everything, using face-swapping and voice-generating technologies, and allowing the AI to write the script, select scenes and put actors' faces on existing characters.

So, Middleditch's face ended up over Vincent Price's face, and sentences were

strung together with recordings from both the actors' voices. Essentially, Sharp wanted to automate every part of the human creative process. The end product was "unpolished, and mostly nonsensical," but Benjamin got the job done. [Wired](#)

How Hackable Are Our Airplanes?

According to U.S. government researchers and Homeland Security Department documents obtained by Motherboard, DHS is already testing and uncovering vulnerabilities in commercial aircrafts, and a team successfully remotely hacked a Boeing 737. Essentially, it's only a matter of time before a cyber breach on an airline occurs, and the documents showed what the government anticipates would happen after an aircraft hack, and, perhaps most concerning, "how planes still in use have little or no cybersecurity protections in place."

Because planes are airborne, there's a high potential of catastrophic disaster, according to a presentation by the Energy Department's Pacific Northwest National Laboratory. Another document from 2017 says early testing uncovered "viable attack vectors" that could impact flight operations. DHS did establish a multi-agency group to work on cybersecurity vulnerability evaluations of airplanes in 2016, and a group of government and industry officials demonstrated how to hack a commercial aircraft through radio frequency communications and equipment that passed through airport security.

The documents include various tests, evaluations and risk assessments through 2016 and 2017, and while there hasn't been information suggesting an attempt of a cyber attack on an aircraft yet, the consequences are too dire not to continue investigating. [Motherboard](#)

[View printer friendly version](#)
[news roundup](#)
[AI](#)
[Department of Homeland Security](#)
[Google](#)
[Project Maven](#)
[supercomputing](#)
[China](#)
[Energy Department](#)
[NVIDIA](#)

[hacking](#)
[cyberattacks](#)