Hot Clicks: A Quantum Arms Race Between US and China

China might have developed a radar that can detect stealth aircraft using quantum physics.

Amanda Ziadeh

Mon, 01/07/2019 - 16:03

Photo Credit: ninjaMonkeyStudio/iStock

In response to the Cold War and the American military’s concern that U.S. warplanes were threatened by USSR (and other enemy) radar-guided missile defenses, engineers working with the U.S. developed technology that could shield aircraft from those radars. That technology included unusual shapes that deflect radar waves and carbon-based materials. Essentially, this allows U.S. warplanes to reflect such small signals from those radar detectors that they go unnoticed. For all these years, America’s stealth aircraft have been far superior than China's and

Russia's — until now. China Electronics Technology Group Corporation, the country’s biggest defense electronics company, revealed a prototype radar that can allegedly detect stealth aircraft in flight using quantum physics to find a planes’ locations. This, along with other quantum-based technologies, can transform warfare. MIT Technology Review

Robots to Deliver Snacks to College Students

PepsiCo is making the dreams of students at California’s University of the Pacific come true with a fleet of snack-delivering robots, dubbed “snackbots.” These bots carry snacks and beverages belonging to the company, like bags of chips, Starbucks Cold Brew drinks, Smartfood Delight popcorn, bottles of iced tea and more, to the students’ location on campus during the day. All students have to do is order using the iOS app and a university email, select the location and wait for the bot to arrive. These snackbots can travel 20 miles on a charge, and have headlights and a camera. They're similar to Kiwi’s robo-couriers at UC Berkeley last year, which resulted in students holding a candlelight vigil for a bot that caught fire. The Verge

Weather Apps are Sharing Your Location Data

Some third-party weather apps for smartphones can’t be trusted, especially considering they all have valid reasons to ask for your location. But many of these apps are selling that data to advertisers and data brokers. In 2017, Accuweather was found selling user location data to third parties even when location data was turned off. In 2018, the New York Times found that the Weatherbug app and Weather Channel app were sending precise location data to third parties. In fact, The Weather Channel was sued by the city of Los Angeles for its inappropriate use of location data, claiming the company mines users’ private geolocation data and sends it to IBM affiliates for advertising. Earlier this week, the app on Google Play Store called “Weather Forecast—World Weather Accurate Radar” was found collecting location data, email addresses and phone IMEI identification numbers (unique 15-digit code on every mobile broadband device) and was subscribing users to paid virtual reality platforms without them knowing, according to the Wall Street Journal. So, maybe stick to your device’s first-party weather app. Motherboard

Astronaut Dialed 911 from Space

Dutch astronaut André Kuipers accidentally called 911 from the International Space Station. Yes, it’s possible to make calls from space, and yes, it has been happening for years. What happened was, Kuipers missed a number — on the ISS, astronauts are supposed to dial 9 for an outside line, and then 011 for international. Kuipers missed the 0 and hung up immediately, but the call still triggered an alert at Mission Control in Houston, and he received an email message the next day asking if he called 911. Kuipers said it’s easy to make a call to Earth from space, there’s just a time delay. In fact, the ISS has had this capability for more than a decade, as the phone system uses voice over internet protocol, which is the same tech that allows people to place internet calls on Skype. So misdials from space aren’t new and actually happen quite often. NPR

Hacking Campaign Exposes German Politicians

Hackers leaked the sensitive data of hundreds of German politicians through a series of tweets in December, including information like internal political communications, emails, scans of faxes, credit card information, home addresses, phone numbers, personal identification card details, private chat logs and voicemails. And some of those hacked include members of the European, German and regional state parliaments. The Twitter account has since been removed, but the hackers used it to post the stolen information. So far, and considering the type of data stolen, the leak seems less focused on exposing state secrets, and more interested in exposing deep, personal information on those impacted. Plus, there doesn’t seem to be one particular target, according to cybersecurity experts, but the trove has info on politicians from all of Germany’s major political parties except the far-right group Alternative for Germany. And to make matters more challenging, the hackers created multiple mirrored landing pages with login credentials on different servers to host the stolen data, making it hard to remove the information from the web. Wired

View PDF
space
robots
data

application
hacking