

Mar 22, 2026

Beijing Won't Use US Developed Quantum Resistant Encryption

The stated reason is that they are concerned that it might not be quantum-proof. Even NIST doesn't think our standards are quantum-proof, but they think they are a lot better than existing encryption which quantum computers will slice through with no problem. I suspect the unsaid part of Beijing's decision is that based on past history, they are concerned that the NSA has inserted a back door into the standards, like they have done in the past. Of course there is no reason to think that Beijing won't do the same with their standards. Still, you **MUST** do something or just stop using encryption altogether and give away your bank accounts and passwords - which doesn't seem like a good idea. Credit: [CSO Online](#)

Please check out our blog at <https://www.cybersecurity.com/cyblog>

You can also find copies of the weekly newsletter at <https://cybersecurity-mitch-tanenbaum-blog.com/SNU>

We have a YouTube Channel with a lot of videos. Check it out at: [Turnkey Cybersecurity and Privacy Solutions, LLC - YouTube](#)

As part of our YouTube channel we have a demonstration of our AI capabilities. The CyberPulse Scoop is an AI driven cybersecurity interview. Click on PODCASTS once you are in our YouTube channel and then on CyberPulse Scoop.

If you received this email from a friend and want to receive it directly, please send an email to Mitch@CyberCecurity.com.

Thanks for your interest. If we can provide any assistance, please let us know.

Video Blogs

We also have a video and audio blog, including an RSS feed at <https://cybersecurity.us>. Not only are there audio and video versions of the weekly security news updates there, with extended commentary, but there are also other blogs about subjects of interest. Please check it out and let us know what you think.

Security/Privacy Alerts

CISA Says Harden Endpoint Management

After Iran successfully attacked US assets through poorly protected management systems (the software that manages end user system security), CISA is telling companies to fix that. While Iran attacked endpoint management software, the reality is that any management system that is exposed to the Internet is an attack target and should be made as secure as possible. HINT: THE CYBER ATTACK AT STRYKER MEDICAL THAT WIPED 200,000 DEVICES WAS CAUSED BY THIS PROBLEM. WANT TO REBUILD 200,000 DEVICES? Credit: [CSO Magazine](#)

Iran War Fallout - a Helium Crisis

The facility at Ras Laffan in Qatar produces about a third of the world's helium. Helium is used in chip making and healthcare, among many other uses. An Iranian attack on the facility shut it

down on March 2nd and two days later they declared force majeure, a legal term which means that we don't care if you have a contract with us; due to circumstances beyond our control, we are not going to get you your helium. Because helium has to be shipped very cold, it has a very short shelf life, so if this is not resolved quickly we will have another reason for a new chip shortage. Credit: [AP](#)

AI Alerts

Check out our Certified AI Governance Leader Course at [AIGIP.AI](#).

Nvidia Bets on OpenClaw, but Adds Security

OpenClaw is a personal AI agent for Claude, but it is open source, not owned by Claude. Nvidia thinks AI agents are the future, but it doesn't think that OpenClaw has adequate security. Their version, called NemoClaw, uses Nvidia's new OpenShell security runtime to enforce an organization's policy guardrails. They hope this will make people think that agents are safe and therefore be willing to use them - so they can sell more chips. Credit: [ZDNet](#)

Sam Altman Concedes Artificial General Intelligence NOT Around the Corner

After promising, many times, in public, that AGI, which is a much more powerful AI than what we have now, is just around the corner. It turns out that even master showman Sam Altman has to tap out. This follows Elon's admission that xAI was not built right and Zuck's problem with getting Facebook's AI out the door. Apparently, AI is not as simple to build as it seems in the movies :). Credit: [Gary Marcus](#)

AI Agent Security: Gaps Still Remain

If you are deploying or considering deploying AI agents, you need to read this. While frameworks around AI security show promise, there are still several significant gaps. Learn more. Credit: [Cybersecurity Dive](#)

CMMC Q&A

I get to listen to hours and hours of webinars every week, so you don't have to. We are seeing the agencies beginning to get on board and their view of the universe is CMMC Level 2 third party assessment (eventually) for everyone. If you are not already on board this train, the train has already left the station. If you need assistance, please contact us.

Q: If we use a third party to recycle our old hardware are they in scope?

A: They do if (a) there is, potentially, CUI on the hard drive(s) and (b) you have not done anything to nuke them. There are several potential solutions to this and they depend on the drive type; contact us for details.

Reference

Space based Data cCenters

I love it when billionaires get into a food fight. Musk says that he wants the FCC to allow him to launch a million satellites so he can lead the space based data center fight. The FCC said they would take comments from people about it. Now Bezos wants to join the fight, although he is only committing to launching 50,000 satellites. It is unclear (to me) if this is really going to happen since there are a lot of issues to be figured out. If you look at a typical datacenter today, they take up hundreds of thousands of square feet. How do you do that in space? Credit: [PC Magazine](#)

Software and Hardware to Check Out

Beijing Won't Use US Developed Quantum Resistant Encryption

The stated reason is that they are concerned that it might not be quantum-proof. Even NIST doesn't think our standards are quantum-proof, but they think they are a lot better than existing encryption which quantum computers will slice through with no problem. I suspect the unsaid part of Beijing's decision is that, based on past history, they are concerned that the NSA has inserted a back door into the standard, like they have done in the past. Of course there is no reason to think that Beijing won't do the same with their standards. Still, you **MUST** do something or just stop using encryption altogether and give away your bank accounts and passwords - which doesn't seem like a good idea. Credit: [CSO Online](#)

Important Issues/Patches

Nothing to report

Legislative and Legal Activities

Feds Disrupt 4 IoT Botnets

While this is good news, these things seem to reconstitute themselves. These botnets, named Kimwolf, Jackskid, Mossad and Aisuru had the ability to take down almost any website and are responsible for a series of recent record breaking attacks. Interestingly, DoD's Criminal Investigative Service (DCIS) was involved in the takedown, indicating a national security concern. Sometimes they are able to take control of the botnet server and send instructions to the infected devices to uninstall the malware. It is unclear if that is the case this time. If not, and if they can't get users to patch their routers, cameras and other IoT devices (good luck), these guys will be back. Soon. Credit: [Brian Krebs](#)

4Chan, the Hate Speech and Porn Haven, Tells UK Regulator to Stick it Where the Sun ..

4Chan is basically ignoring the UK regulator Ofcom's assessing it fines of a half million pounds for a variety of violations including not implementing age verification. Their response to the notice of a fine was a cartoon of a hamster. The thing about regulators is that they move slowly. Will they shut down the servers of 4Chan if they don't comply by the due dates? I doubt it and that is what 4Chan is counting on. Stay tuned, I guess. Credit: [Helpnet Security](#)

Education

Computers Usually do Exactly What You Tell Them to Do

A trader wanted to trade one digital currency for another. Seems okay. In this case, he wanted to trade \$50 million in USDT for AAVE. Sounds pretty speculative and if you are a speculator, you should understand risk, right? The Aave user interface warned the trader that due to the size of the trade, it could have a price impact. The trader clicked on the I accept box and poof, the trade was done. **The trader got 324 AAVE, worth about \$37,600.** He clicked okay. Doesn't sound like a good trade to me, but what do I know? The Aave founder offered to refund the speculator's trading fee of about \$600,000, meaning he would only lose about \$49 million and change. The moral is be careful what you are agreeing to. Credit: [Web 3 is Going Great](#).

Breaches

Note: I could probably report on a hundred a week, but that would make for a very long report. I will, at least, mention a few of the high-profile ones. NOTE THAT THIS IS THE ONLY SECTION THAT I CAN FILL TEN TIMES OVER EACH WEEK.

Navia benefit Solutions Said Health Info of Over 2 Million Stolen in Breach

Vendor. Supply Chain. That is where the action is. Navia is a third-party benefits administrator for over 10,000 companies and millions of their employees. This includes managing stuff like your flexible spending account and other healthcare benefits. Healthcare information for 2.5 million + was stolen. Credit: [The Record](#)

Chinese startup is mapping every US military asset in the Middle East in real time

This tiny Chinese company is using standard commercial satellite imagery and AI to not only document every military base in the Middle East, every ship and even every air defense asset. And, they are making this available to anyone for free. Not exactly what the Pentagon would like but there is probably nothing they can do to stop it. Learn more [here](#).

New York to require cybersecurity for water systems - smartly

The EPA tried this a couple years ago but the industry fought them saying, basically, they didn't care about security (they had a different excuse, but the message was clear). The courts agreed that Congress never gave the EPA the authority to regulate that. New York is trying something similar but with a twist - free cybersecurity expertise and even grants to help implement things. Learn more [here](#).

Surprise - Feds want spying law extended

Here is a shocker (not). The intelligence agencies and the FBI want Congress to re-up section 702 of the Foreign Intelligence Surveillance Act with no changes. This law expires every few years because neither party trusts the government not to spy on us. It expires next month. Learn more [here](#).

Security News for the week ending March 20, 2026

This week's news: Adobe fined \$150 million for making it hard to cancel subscriptions, teens sue xAI over child porn creation, big surprise - courts don't understand tech, PC memory crisis not going away and Super Micro PC maker co-founder arrested for smuggling Nvidia chips to China. Learn more [here](#).

As you start rolling out AI in your company, you need to make sure that security is being addressed. Even big companies like Amazon and Facebook have discovered that move fast and break things applies to them to. If you don't want it to apply to you, please contact us for assistance.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663