Politics
Cybersecurity

EU Targets Fictitious Finnish Power Company in Cyberattack Test

- The exercise comes amid concerns about the bloc's capabilities
- The trial was launched as Ukraine fell victim of an attack

By Jorge Valero
2022年1月15日 GMT+8 下午8:47

Listen to this article
1:30
Share this article
@europressos
+ Get alerts for Jorge Valero

The European Union began testing its cyber-defense responsiveness on Friday with a simulated attack on a fictitious Finnish power company as the bloc seeks to strengthen its digital defenses amid concern about a potential attacks.

The start of the cyber exercise came the same day Ukraine fell victim to an actual attack that brought down around 70 government websites. Ukraine's security service on Friday said it sees "some signs" that Russia was behind the attack. The EU's foreign policy chief, Josep Borrell, warned the bloc's defense ministers this week about the need to bolster the cyber capacities.

Read more: Cyberattack Hits Ukrainian Websites as Russia Tensions Mount

The Finnish attack is part of a six-week exercise to stress-test Europe's resilience, strengthen preparedness and cooperation among member states, and improve the effectiveness of a joint response. The tests are expected to conclude during a meeting of EU foreign ministers at the end of February.

Read more: EU to Stage Large-Scale Cyberattack Exercise on Supply Chains

In the Finnish simulation, a major cyber security incident is detected in software used by a major energy company, according to diplomatic notes seen by Bloomberg. The high penetration of the software across sectors and member states risks spreading the impact across Europe, according to the notes.

The EU response foresees the activation of member states' working groups on cyber issues to monitor the impact and find the origin of the crisis as well as taking possible actions to mitigate the consequences of the attack.

— With assistance by Alberto Nardelli

Cybersecurity


Technology & Ideas
Beijing Olympians Might Want to Buy Burner Phones
The cybersecurity risks in China are high.

- What If Your Fourth Covid Shot Could Last Forever?
- Pro Tip: Don't Panic-Buy Your Next House
- Why Are Grocery Shelves Empty Again?

Cybersecurity
Ransomware Attacks Still Target Schools, Hospitals Amid Biden Crackdown

Cybersecurity
JPMorgan Hack Suspect Is Helping the U.S. Here's What He May Offer

Cybersecurity
Thailand's Cyber Law Raises Fear Military Could 'Cage' the Internet


Cybersecurity
U.S. Power Grids Need Stronger Cybersecurity, Top Regulator Says

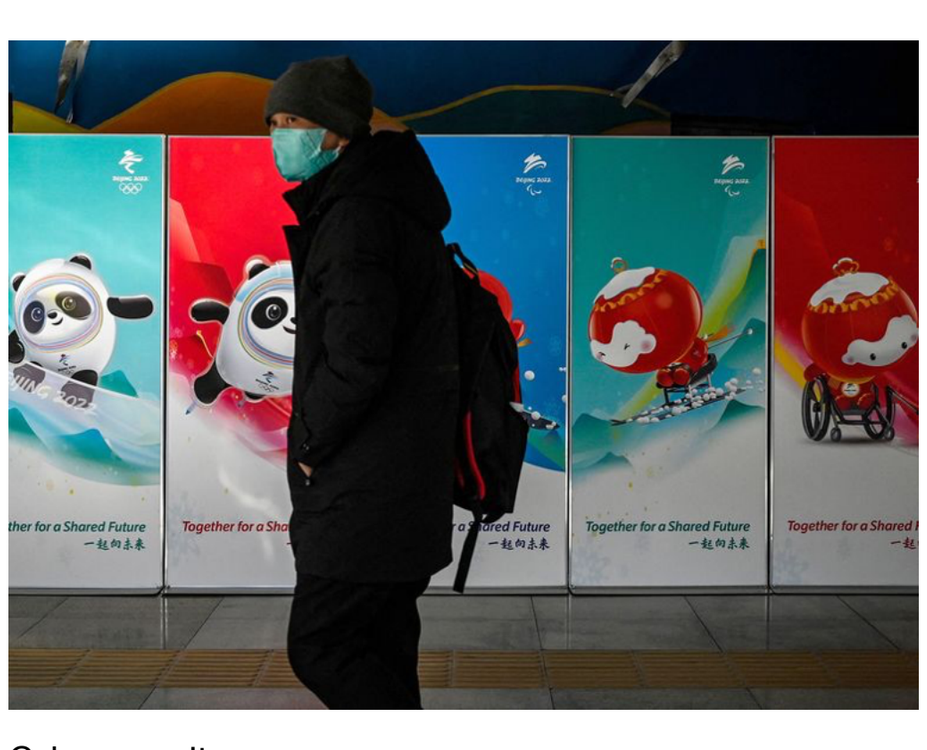

Feature
How Did ID.me Get Between You and Your Identity?


Cybersecurity
Red Cross Hack Exposes Data on 515,000 Vulnerable People

Cybersecurity
Crypto.com Says Regulators Haven't Reached Out After Hack

Deals
Banks Ready Sale of $10 Billion Debt for McAfee Buyout

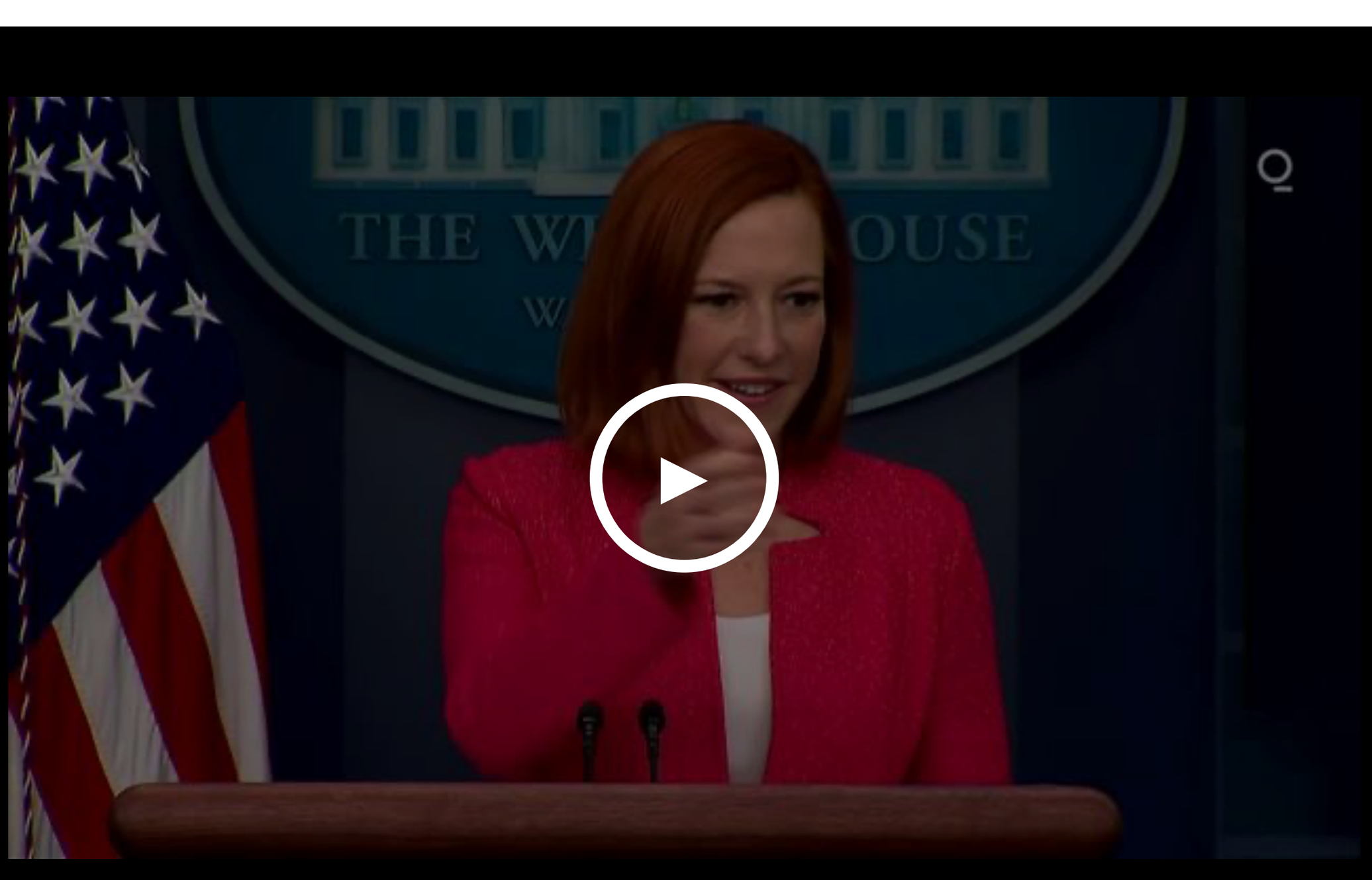
Cybersecurity
Banking Group Looks to 'Critical Providers' to Help Curb Hacking


Cybersecurity
Olympic Athletes Advised to Leave Phones at Home to Dodge Spying


Cybersecurity
Ukraine Says Belarus-Linked Hackers May Be Behind Cyberattack

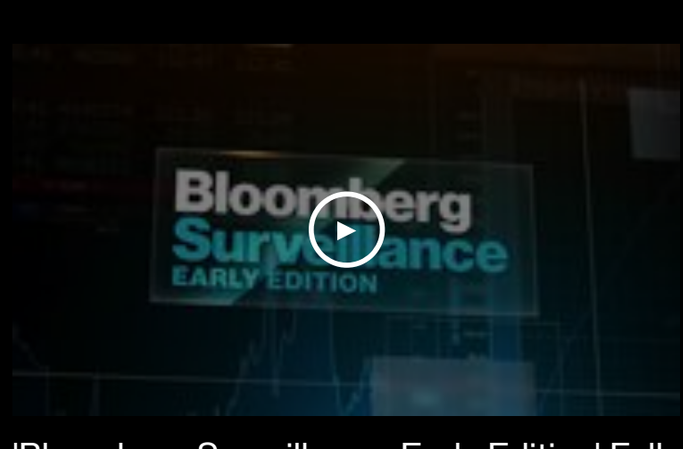

Cybersecurity
U.S. Says Ukraine Cyber Attack Is 'Part of Russian Playbook': FT

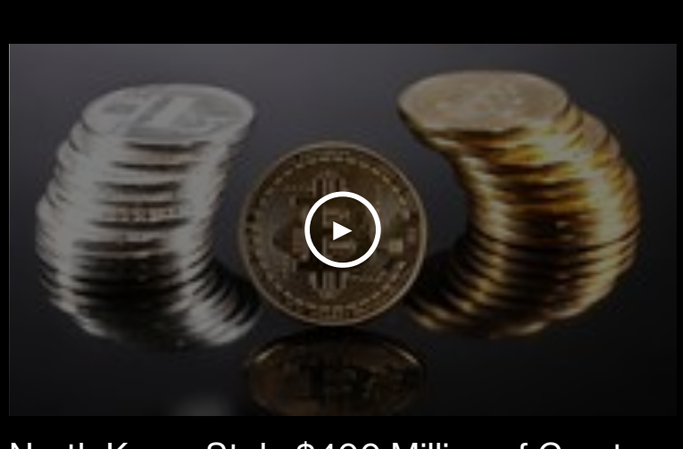

Feature
How Did ID.me Get Between You and Your Identity?
Military veteran Blake Hall's cybersecurity company has become the government's digital gatekeeper. Its unproven estimate—$400 billion in pandemic unemployment fraud—is also very good for its business.



Ukraine Says Russia is Behind Cyberattack

President Joe Biden has been briefed on a cyber attack against Ukraine. White House Press Secretary Jen Psaki said, adding that "personal data was not accessed" and Ukrainians were able to get their "systems up and running." The Biden administration believes Russian actors are preparing potential sabotage operations against their own forces and fabricating provocations in social media to justify an invasion into Ukraine, according to a U.S. official. (Source: Bloomberg)


'Bloomberg Surveillance: Early Edition' Full (01/14/21)


North Korea Stole $400 Million of Crypto Assets


'Bloomberg Daybreak: Australia' Full Show (01/14/2022)


'Bloomberg Technology' Full Show (01/13/2022)

In Case You Missed It

Russia Detains REvil Ransomware Hackers at the Request of U.S.
by Jake Rudnitsky and William Turton


Teen Cyber Prodigy Stumbled Onto Flaw Letting Him Hijack Teslas
by Jordan Robertson and Monica Raymunt


Pentagon Links Iran Intelligence to 'MuddyWater' Hacking Group
by Jack Gillum


Third-Party Software for Teslas Can Be Hacked, German Teen Says
by Katrina Nicholas and Jordan Robertson


Hackers Can Cut the Lights With Rogue Code, Researchers Show
by Jack Gillum


Darktrace Soars as Outlook Raise Prompts Upgrade from Peel Hunt
by Joe Easton


The Former NSA Official Vying to Steer Biden's Cyber Policy
by William Turton


China's Rebuke Over Alibaba Security Flaw Sends Wrong Signal
by Tim Culpan


Kremlin Insider Arraigned in U.S. Hacking, Insider-Trading Case
by Christian Berthelsen


Hackers Tried Recycled Passwords on More Than a Million Accounts
by Jack Gillum