Battery Explosion Paralyzes Korean Government Systems—Is U.S. Grid Next?

Written by Stu Turley on October 1, 2025.

Posted in Current News

Chinese Lithium Battery System Took down South Korean Intelligence Agency, and Texas has 1200 of these installed. For all of the Green Energy fans, this is a wake up call for security concerns.

In a startling incident that has raised alarms about the vulnerabilities of critical infrastructure, a massive fire erupted at South Korea's National Information Resources Management Agency (NIRMA) in Daejeon on September 26, 2025, crippling dozens of government systems and sparking concerns over national security.

The blaze, which originated from a lithium-ion battery explosion, burned for over 22 hours and destroyed 96 out of 647 operational systems, leaving services from real estate registries to postal operations paralyzed.

While official reports attribute the battery to South Korean manufacturer LG Energy Solution, online discussions and expert analyses have fueled speculation about potential Chinese involvement or parallels to risks posed by Chinese-made energy storage systems.

The fire broke out around 8:15 p.m. during routine maintenance when workers were relocating lithium-ion batteries in a server room. One worker sustained first-degree burns to their face and arm, and nearly 200 battery packs were involved in the explosion.

Emergency responders struggled to contain the flames due to the intense nature of lithium-ion fires, which are notoriously difficult to extinguish. By the next day, the government had scrambled to restore services, but normalization was projected to take up to two weeks for some systems.

This event echoes a 2022 fire at another South Korean data center, prompting heightened safety protocols that ironically may have contributed to the relocation work leading to the blast.

Prominent commentator Gordon G. Chang highlighted the incident on X (formerly Twitter), sharing a detailed overview from Korean sources. Chang's post described the fire as "not a simple disaster," warning that it could erode South Korea's sovereignty by

forcing a shift to private cloud providers and potentially compromising the U.S.-Korea alliance.

Replies to the post amplified suspicions, with users questioning the lack of off-site backups for critical systems and linking the timing to South Korea's upcoming visa-free entry policy for Chinese nationals starting September 29, 2025. Some speculated about intentional sabotage, suggesting data migration to clouds could allow real-time access by foreign entities like the Chinese Communist Party (CCP).

One user even claimed the incident might facilitate "replacing Koreans with Chinese" through unchecked immigration amid system outages.

While the battery in question was produced by LG, the event has spotlighted broader concerns about Chinese lithium-ion battery systems, particularly those from Contemporary Amperex Technology Co. Limited (CATL), the world's largest battery manufacturer. CATL's rechargeable Li-ion systems, such as the EnerC+ series, feature high-energy-density LFP (lithium iron phosphate) or NMC (nickel manganese cobalt) cells with capacities up to 306Ah and voltages ranging from 2.5V to 3.65V.

These systems are designed for large-scale energy storage, offering features like ultra-fast charging (up to 4C rates) and integration with renewable sources. However, their widespread adoption raises red flags in the context of national security.

In the United States, CATL batteries have been deployed in significant Texas energy projects, including deals for up to 5GWh of storage capacity. Projects like those with HGP Storage and Broad Reach Power involve hundreds of MWh in ERCOT (Electric Reliability Council of Texas) grids, with installations supporting solar portfolios and grid stability.

Estimates suggest Texas hosts around 1,200 such Chinese-sourced battery units across various sites, contributing to the state's push for renewable energy resilience after events like the 2021 winter storm.

Yet, This Reliance Comes With Perils.

National security experts warn that Chinese components in U.S. grid, solar, and even phone equipment pose severe risks, including remote shutdowns, overloads, fire initiation, and cyber warfare access. Recent discoveries of "rogue" communication devices—such as hidden cellular radios—in Chinese-made solar inverters and batteries have intensified fears.

These backdoors could enable adversaries to disable power grids, trigger blackouts, or cause deliberate overloads leading to fires, bypassing U.S. cybersecurity measures.

For instance, undocumented radios in inverters could allow remote sabotage, compromising energy infrastructure and national defense.

Wind turbines and solar systems with Chinese parts are particularly vulnerable to IT sabotage, potentially giving Beijing a "kill switch" over Western power supplies.

The South Korean fire, while not directly linked to Chinese tech, serves as a cautionary tale. If similar vulnerabilities exist in CATL systems embedded in Texas's grid—where over 369MW/555MWh of new storage has come online recently—the consequences could be catastrophic.

We drew attention to this issue when the balloons were allowed to traverse the U.S. Subsequently, evidence emerged that they had connected to the U.S. grid, potentially exposing some of the 492 major grid interconnects to security risks, which were reintroduced into the grid under the Biden Administration. I am unable to determine if they have been removed from my sources.

There is a lot of chatter about jihads, and last week I wrote about China's debt. They have gone to war when finances have been bad in the past, so this is not meant to be a warning that the grid will go down today; instead, it's a warning to take an inventory of your current business and home to have a plan in place.

And you have heard me say this before: Have a plan for any natural or man-made disaster. Be there for your family and neighbors, even if they vote differently from you. If you are the CEO of a company, take a serious look at your power requirements to run your business. If you have any questions, please ask me, and we can direct you to the relevant resources.

U.S. officials are urged to reassess dependencies on foreign suppliers, emphasizing domestic alternatives to mitigate these threats. As global energy transitions accelerate, balancing innovation with security remains paramount

However, we have a lot of work to do to secure our grid from decades of poor management from both Republicans and Democrats.

source theenergynewsbeat.substack.com