Addenda #81 – June 2025
Re: Ch. 8, 050 Net-Zero Emissions; Impossible!
*SDG 7 - Ensure access to affordable, reliable, sustainable and modern energy for all*

- *Renewable Power Sources are NOT reliable*
- *The U.S. Power Grid*

*Kill Switches Secretly Installed In Solar Panels*
Cyber Security Intellegence; May 19, 2025
https://www.cybersecurityintelligence.com/blog/kill-switches-secretly-installed-in-solar-panels-8439.html

*Chinese "kill switches" have been discovered hidden in American solar farms, triggering urgent warnings over US national energy security and prompting calls to suspend the deployment of renewable energy generation in the UK.*
*The kill switches, identified as cellular radios, are embedded within power inverters manufactured by Chinese companies and sold to US power generators*

Solar power inverters are electronic devices that take the direct current (DC) voltage produced by solar panels and convert it into alternating current (AC) voltage for transmission to our electrical grid. Five of the largest solar power inverter manufacturers are Chinese companies, responsible for 35% of all inverter sales in the U.S.

In 2024, utility-scale solar power generated 218.5 terawatt-hours (TWh) in the United States, or 5% of all utility-scale electricity generated. With the push for renewable energy generation to meet state mandated clean energy goals continuing to ramp up, this percentage will only increase in future years. As we become more dependent on solar power and solar power inverters.
A "kill switch" is a device used to shut down equipment manually in an emergency situation, most commonly referred to as an emergency stop or E-stop. The devices that have been found in imported solar power inverters can be activated remotely by wireless signal, disconnecting generation from the electric grid, which could destabilize power grids, damage distribution equipment and trigger widespread blackouts.
(Ref: Addenda 80, May 2025; Net Zero Blamed for Europe's biggest power cut)

Ever since Xi Jinping became the leader of China, he has had a long-term plan to challenge America's global leadership and become the economic and manufacturing leader of the world. Our leaders have been warning about Chinas threat to the U.S. for years now. In April 2024, FBI Director Christopher Wray warned national security and intelligence experts at the Vanderbilt Summit on Modern Conflict and Emerging Threats, that risks the government of China poses to U.S. national and economic security are "upon us now"—and that U.S. critical infrastructure is a prime target. "The PRC [People's Republic of China] has made it clear that it considers every sector that makes our society run as fair game in its bid to dominate on the world stage, and that its plan is to land low blows against civilian infrastructure to try *to induce panic* and break America's will to resist," Wray said.

The panic and confusion that followed the grid shutdown in Spain and Portugal on April 28, 2025, is an example of what would happen here in the United States, if those kill switches were triggered. With entire regions interconnected on shared electrical grids, the outcome would be far worse with multiple states and large industrial manufacturing affected for days or possibly longer. Example.

In 2021, the federal government had to issue an emergency declaration after a cyber-attack on a major U.S. pipeline shut down transport of oil across the eastern coast. The Colonial Pipeline, the country's largest oil pipeline in the U.S. at 5,500 miles, carries 3 million barrels of fuel per day over thirteen states between Texas and New York. The attack on its computer equipment forced the company to shut down operations for most of the week, causing fuel shortages at gas stations, resulting in "panic buying" by motorists in six states. In this case, the cyberattack was in the form of "ransomware" by a Russian hacker group that demanded $4.4 million ransom to restore the system to operation. In the case of Chinese kill switches, the reason would not be payment to restore the solar generation, but to destroy it and throw the country into chaos.

Our country's energy infrastructure is very vulnerable to a number of threats. Physical attacks by terrorists, vandalism, Electromagnetic Pulse (EMP) as well as cyber-attacks.
In April 2013, a group of vandals wielding high-powered rifles shot up the Pacific Gas & Electric Company's Metcalf substation. The attack caused $15 million in damage, but PG&E was able to shift the electrical load to adjacent substation, avoiding an extended power outage and allowing repairs to be made.
In December 2022, a perpetrator or perpetrators shot up two Duke Energy substations in Moore County, North Carolina. The attacks left 45,000 utility customers without electricity for four days, while work crews replaced equipment damaged in the attacks. Businesses and schools were closed, and local officials declared a state of emergency and imposed a 9 p.m. to 5 a.m. curfew to avoid looting.

Many electric substations are located in remote areas with no permanent staff and have little security. If terrorists, domestic or foreign, simultaneously attacked enough substations, the result would be a regional blackout. Since the pandemic, supply shortages have led to long lead times on high voltage distribution equipment as well as significantly higher prices. Most high voltage utility transformers are manufactured in China (remember those kill switches?) and lead times from placement of order to delivery are between 120 and 210 weeks. Imagine being without electricity for a year in the middle of a hot summer, or a cold winter, while your cooling and heating depend on that electricity because of government mandates…

Only days after the U.S. identified kill switches in solar farm inverters, power companies found "unlisted parts" on East Asian circuit boards meant to be installed in Denmark's green power grid. This is an issue that will not go away, as long as we are dependent on foreign countries to supply parts for our critical infrastructure.

Addenda #81 sources:


Chinese Kill switches found in U.S. solar farms; The Telegraph, May 15, 2025
https://www.telegraph.co.uk/business/2025/05/15/chinese-kill-switches-found-in-us-solar-farms/

U.S. Energy Sector at risk; Industrial Cyber, May 15, 2025
https://industrialcyber.co/utilities-energy-power-water-waste/us-energy-sector-at-risk-as-chinese-inverters-are-under-investigation-for-suspicious-communication-gear/

Chinese government poses broad and unrelenting threat to US critical infrastructure, FBI director says; FBI.gov, April 18, 2024
https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says

3 Alarming Threats To The U.S. Energy Grid – Cyber, Physical, And Existential Events; Forbes, February 15, 2023
https://www.forbes.com/sites/chuckbrooks/2023/02/15/3-alarming-threats-to-the-us-energy-grid--cyber-physical-and-existential-events/

Colonial pipeline hack; NBC News, May 10, 2021
https://www.nbcnews.com/tech/security/colonial-pipeline-hack-claimed-russian-group-darkside-spurs-emergency-rcna878

Attacks, plots similar to sabotage of North Carolina power grid have threatened infrastructure nationwide; abc News, December 6, 2022
https://abcnews.go.com/US/attacks-plots-similar-north-carolina-power-grid-attack/story?id=94574765

The Transformer Crisis: An Industry on the Brink; POWER magazine, June 26, 2024
https://www.powermag.com › the-transformer-crisis-an-industry-on-the-brink

After kill switches in Chinese solar panels in U.S, Denmark finds suspicious parts in East Asian circuit boards; The Economic Times, May 24, 2025
https://economictimes.indiatimes.com/news/international/us/after-kill-switches-in-chinese-solar-panels-in-u-s-denmark-finds-suspicious-parts-in-east-asian-circuit-boards/articleshow/121381403.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst