UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Request for New or Modified	**)**	
Reliability Standard	**)**	**Docket No. EL23-69**
by the Secure the Grid Coalition	**)**	

Motion to Intervene and Comments of Secure the Grid Coalition

Submitted to FERC on June 13, 2023

Background

As the petitioner in this case, we appreciate that FERC has created Docket EL23-69 and is inviting public comments on whether reliability standards for physical security should be modified or whether new standards should be established. We filed our petition in the interest of this same American public who depends on electricity for life itself, who pay companies to provide this life-sustaining electricity, and whose security interests are grossly underrepresented by NERC (who establishes the physical security standards that govern the protection of the electric grid without which this public can live and who have already formally requested that your Commission reject our petition.)

We filed our May 15, 2023 petition more than three years after a member of our Coalition – Retired U.S. Army Command Sergeant Major Michael Mabee – lodged a formal complaint (January 29, 2020) with your Commission on the inadequacy of the physical security standard, CIP—14 (which opened docket EL20-21-000). At the time, Mr. Mabee's independent research of Department of Energy data revealed that there had been 578 (publicly disclosed) physical attacks on the grid since January 2010. Despite public comments calling for enhanced physical security of the grid at that time, EL20-21-000 was dismissed by FERC and attacks on the grid have continued and even increased.

Increasing Physical Attacks on the Electric Grid

According to open-source media, in 2022, attacks on electrical systems increased more than 80% compared to 2021.[1] By the end of 2022, Department of Energy data revealed that the number of publicly disclosed attacks had risen to 978 attacks. As of March 31, of this year, that number had risen to 1,039

[1] Brangham, William, and Karina Cuevas. "FBI Foils Extremist Plot to Bring down Baltimore's Electrical Grid." PBS, February 7, 2023. https://www.pbs.org/newshour/show/fbi-foils-extremist-plot-to-bring-down-baltimores-electrical-grid.

total attacks since January 2010[2]. This means that the number of attacks on the North American electric grid has nearly doubled since our previous complaint to FERC and that the frequency of attacks continues to increase – now at a rate of nearly 1.5 attacks per week. These numbers include just the actual electrical disturbance events caused by physical attack, sabotage, crime, or theft – not the instances where physical attacks didn't cause outages or where sinister plots were foiled beforehand. (The compiled data for January 2010 to March 31, 2023, are listed at right and the numbers by year are listed below.)

All NERC Regions		
Events From Jan 2010-Mar 2023	Total	%
Weather	1240	50.4%
Cyber Attack	55	2.2%
Physical Attack	1039	42.3%
Fuel Supply Deficiency	90	3.7%
Equipment	15	0.6%
Natural Disaster	15	0.6%
Wildfire	5	0.2%
Generation Interruption	22	
Transmission Interruption	186	
Distribution Interruption	9	
Operations	346	
Islanding	67	
Load Shed	31	
Public Appeal	81	
?	10	
Total OE-417 Reports	3211	
Cause Known from OE-417	2459	
Cannot Determine Cause	752	

All NERC Regions															
Event	2023 (through March)	2022	2021	2020	2019	2018	2017	2016	2015	2014	2013	2012	2011	2010	Total
Weather	29	95	154	162	92	94	80	42	65	82	55	82	133	75	1240
Cyber Attack	2	9	7	7	2	4	3	5	0	3	2	3	8	0	55
Physical Attack	61	166	92	93	80	58	44	49	44	73	79	86	114	0	1039
Fuel Supply Deficiency	0	5	11	7	7	5	7	7	2	18	6	6	6	3	90
Equipment	0	0	0	0	0	0	0	0	0	0	7	2	3	3	15
Natural Disaster	0	0	1	4	0	8	0	0	0	1	0	0	1	0	15
Wildfire	0	0	0	0	0	0	0	0	0	3	0	0	0	2	5
Generation Interruption	0	4	1	0	2	0	4	4	0	0	0	0	7	0	22
Transmission Interruption	8	27	38	42	36	10	9	4	0	0	3	2	2	5	186
Distribution Interruption	0	0	0	0	3	0	0	2	0	1	2	0	1	0	9
Operations	11	76	74	67	56	31	1	16	13	1	0	0	0	0	346
Islanding	0	0	0	0	0	2	1	7	10	15	13	6	4	9	67
Load Shed	0	0	1	0	0	0	0	1	4	2	4	4	5	10	31
Public Appeal	0	8	8	1	0	8	1	4	5	11	0	4	17	14	81
?	0	0	0	0	0	0	0	0	0	4	3	1	0	2	10
Total OE-417 Reports	111	390	387	383	278	220	150	141	143	214	174	196	301	123	3211
Cause Known from OE-417	92	275	265	273	181	169	134	103	111	180	149	179	265	83	2459
Cannot Determine Cause	19	115	122	110	97	51	16	38	32	34	25	17	36	40	752

Law enforcement and security professionals have long-warned about the vulnerability of the grid to physical attack and fortunately, in some cases, they have been able to prevent such calamities. For example, in early 2023, the FBI was able to prevent a plan to attack a large section of the Baltimore electric grid, planned by Sarah Beth Clendaniel of Maryland and Brandon Russell of Florida, the latter being a founding member Atomwaffen, a neo-Nazi group. If their plot had gone as planned, Clendaniel said it would have been able to "permanently completely lay this city to waste if we could do that

[2] https://michaelmabee.info/oe-417-database/

successfully."[3] The pair planned to attack many electrical substations in the Central Maryland area, which would have resulted in hundreds of thousands of citizens losing power. Russell posted various links to maps indicating what electrical substations to target and explained that by knocking out several of these stations at once, a "cascading failure" of the electric grid would be possible.[4]

Indeed, the Federal Criminal Complaint filed by the FBI on this "Conspiracy to Destroy an Energy Facility"[5] demonstrated evidence of an increased level of sophistication by the accused to target kill zones of vital assets. The accused having specified:

> *"destroy those cores, not just leak the oil…"* (a) *"good four or five shots through the center of them . . . should make that happen."*

From the Criminal Complaint comes evidence of the level of sophistication demonstrated in the area of grid topology and the effectiveness of attacking selected, multiple substations (the so-called "Coordinated Attack") to incapacitate re-routing of power:

> *"I think I get it . . . But I only see four lines. Not fully getting the fifth. Is the one up north to stop rerouting? You know the one I'm talking about?"*

One of the most visible recent examples of a physical attack not thwarted by law enforcement was in Moore County, North Carolina last December. That sabotage affected more than 45,000 customers in the region, and as of today, no one has been arrested for the attack.[6] A few days before the attack in North Carolina, the Department of Homeland Security issued a bulletin through its National Terrorism Advisory System explaining that targets of potential violence they were tracking included U.S. critical infrastructure, among others.[7] Because the DHS memo warned that the threat was posed by "domestic violent extremists" and "racially motivated extremists," numerous media headlines warned

---

[3] Czachor, Emily Mae, and Nicole Sganga. "2 Suspects Arrested for Conspiring to Attack Baltimore Power Grid, Officials Say." CBS News, February 7, 2023. https://www.cbsnews.com/news/baltimore-power-grid-attack-plot-fbi-suspects-arrested-sarah-beth-clendaniel-brandon-russell/.

[4] More, Maggie. "Two People Arrested for Plotting 'racially Motivated' Attack on Baltimore Power Grid." NBC4 Washington, February 6, 2023. https://www.nbcwashington.com/news/local/fbi-arrests-2-in-racially-motivated-plot-to-attack-baltimore-power-grid/3272309/.

[5] https://biotech.law.lsu.edu/blog/doj-brings-conspiracy-to-damage-energy-facilities-charges.pdf (accessed June 12, 2023)

[6] Hauck, Grace. "Power Grid Attacks Caused Outages for Thousands. FBI Still Doesn't Know Who Did It – or Why." USA Today, March 15, 2023. https://www.usatoday.com/story/news/nation/2023/03/15/energy-grid-attack-motive-unknown-fbi-offers-reward/11476944002/.

[7] "National Terrorism Advisory System Bulletin - November 30, 2022." National Terrorism Advisory System Bulletin - November 30, 2022 | Homeland Security. Accessed June 9, 2023. https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-november-30-2022.

that the impending threat to the electric grid was associated with "Right-Wing Extremists." This certainly is the case, but as we told Newsweek: a **vulnerable electric grid is "a prime target for a wide variety of bad actors, both foreign and domestic, ranging from the far right, to the far left**.[8]

Grid Attackers Span the Economic and Political Landscape

That the grid is vulnerable to attackers on all sides of the political and economic landscape is a reality supported by facts and academic research. For example, in many cases acts of sabotage are criminal and involve the theft of copper. This is a worldwide problem that has resulted in outages in locales ranging from Pittsburgh to Arkansas, and from London to Malaysia and have even led some utility service providers to declare that "substation copper theft has become a crisis[9]." For example, after thieves in New Orleans damaged a local substation to steal copper this summer, its utility – Entergy – admitted that this sort of vandalism happens "often enough" that the industry has to spend "a lot of time and resources" guarding against it.[10]

According to academic and government sponsored studies on terrorism, leftwing terrorists and Islamic jihadists have perpetrated the largest percentages of documented "terrorist" attacks on the grid in the last five decades. According to the University of Maryland START Global Terrorism Database (GTD) there have been 91 "terrorist" attacks against utilities in the United States from January 1970 to March of 2020.[11] The GTD identifies perpetrators for 63 of the attacks. Of incidents in which the GTD identifies a perpetrator, 58 of them are from identifiable left-wing extremist groups or were conducted on behalf of leftwing extremist causes. The vast majority of terrorist attacks against utilities in the United States took place between 1970 and 1990, during periods of high levels of left-wing extremist activities surrounding first the Vietnam War, and subsequently the rise of ecoterrorism in the late 1980s early 1990s.

The targeted sabotage of powerlines by left-wing, anarchist and eco-terrorist groups remains a significant threat, particularly because the movement has extensive experience and education in the

---

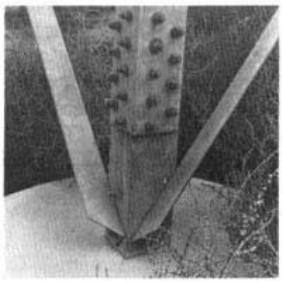
[8] Tom O'connor and Naveed Jamali, Newsweek, Jan 11, 2033. "Domestic Terrorists Could Take Out U.S. Power Grid—and Attacks Have Started" https://www.newsweek.com/2023/01/20/domestic-terrorists-could-take-out-us-power-grid-attacks-have-started-1772786.html

[9] https://peaksubstation.com/the-copper-theft-crisis-substation-theft-prevention/

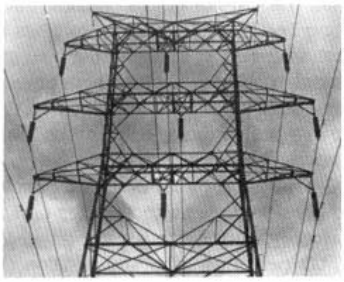
[10] https://www.nola.com/news/traffic/article_0f9c525c-7372-568b-bd67-1d85e65da7d5.html

[11] University of Maryland START Global Terrorism Database , n.d. https://www.start.umd.edu/gtd/search/Results.aspx?page=1&casualties_type=b&casualties_max=&dtp2=all&country=217&target=21&count=100&charttype=line&chart=overtime&ob=GTDID&od=desc&expanded=yes.

targeting of critical infrastructure and continues to publish documentation regarding how activists can target power lines and other electrical utilities. For example, the manual ***Ecodefense: A Field Guide to Monkeywrenching*** first published in 1987 and republished in 1993 remains readily available for free online at the Anarchist Library. It's co-editor and publisher David Foreman, co-founder of Earth First!, plead guilty to federal charges for his role in an attempt to sabotage power transmission lines supplying southwestern nuclear power plants. That manual provides detailed instructions for the targeted destruction of powerlines and towers (as seen in the illustration at right.)



These nuts and bolts hold the powertower support to its concrete base. They are removable with a ratchet wrench and cheater pipe.



Shotgunner's view of powertower and powerlines. Note the glass or ceramic insulators.

In January 2007, Lawerence Livermore National Laboratory published a study *Assessing Terrorist Motivations for Attacking Critical Infrastructure*, which noted that "Left-Wing and Islamist groups attack [Critical Infrastructure] more frequently than other types of groups. Left-Wing groups (above all Marxist-Leninist groups) carried out the overwhelming majority of attacks attributable to groups that fall within the Secular Utopian category, as opposed to Anarchist, Neo-Fascist, or Ecological groups. Similarly, Islamist groups were responsible for carrying out the majority of CI attacks that have been perpetrated by Religious groups in the past two decades. Between 1980 and 2004 Religious groups were responsible for 89 incidents, of which Islamist groups were responsible for 84 or 94%."[12] Some of these Islamic jihad attacks on the grid made international headlines. For example, on June 9, 2014, jihadis with Al Qaeda in the Arabian Peninsula (AQAP) conducted physical attacks on the grid of Yemen, blacking out the entire nation, including 16 cities and 24 million people.[13] Then on January 25, 2015, Islamic jihadis in Pakistan conducted physical sabotage of that nation's electric grid, blacking out 80 percent of the country.[14]

[12] Ackerman, G, P Abhayaratne, J Bale, A Bhattacharjee, C Blair, L Hansell, A Jayne, et al. "Assessing Terrorist Motivations for Attacking Critical Infrastructure." Assessing Terrorist Motivations for Attacking Critical Infrastructure (Technical Report) | OSTI.GOV, December 4, 2006. https://www.osti.gov/biblio/902328/.

[13] Peter Kelly-Detweiler, "Terrorist Attack Left All of Yemen In Darkness Last Week: Another Wake-Up Call" Forbes (June19, 2014

[14] Salman Masood, "Rebels Tied To Blackout Across Most Of Pakistan" New York Times (January 25, 2015). NBC News,"Massive Pakistan Power Blackout Leaves 80 Percent in Darkness" (January 25, 2019) www.nbcnews.com. "Massive Power Failure Plunges 80% of Pakistan into Darkness" The Guardian (January 25, 2015)

Our Insecure Border Invites MORE Grid Attackers

Apart from the litany of domestic threats within the United States and the widespread political and/or economic motivations associated with those threats, the electric grid is extremely vulnerable to foreign actors. With the expiration of Title 42 on May 11, 2023, the porous U.S. southern border presents a great hazard to the security of the electric grid. Thousands of undocumented migrants are coming into the U.S. every day, many of whom are military-aged males.[15] In the last two years, over 5 million illegal crossings have taken place, equating to an average of 6,300 individuals per day.[16] This crisis is not a new one unfortunately, and at the time of this writing, there does not appear to be a plan to slow down the flow of migrants any time soon. Because of this, and due to the large role Mexican drug cartels play in smuggling migrants across the border, there is reason to believe that the cartels could attack the electric grid in the future.[17] The late Dr. Peter Pry noted in his impactful book *The Power and the Light:*

> "On the morning of October 27, 2013, the Knights Templars, a terrorist drug cartel in Mexico, attacked a big part of the Mexican grid, using small arms and bombs to blast electric substations. They blacked-out the entire Mexican state of Michoacan, plunging 420,000 people into the dark, isolating them from help from the Federales. The Knights went into towns and villages and publicly executed local leaders opposed to the drug trade."

As Dr. Pry indicates, the idea of cartels getting across the border (which is now easier than ever), and attacking the U.S. electric grid, is not that far-fetched. In the event of something like this happening, our electric grid is far from safe. If a few individuals with rifles were able to cause 45,000 citizens in Central North Carolina lose power back in December of 2022, then there is no telling how much damage a much more well-funded entity such as a drug cartel could cause using large explosives.[18]

---

[15] Heckman, Elizabeth. "Reporter Says He Filmed Hundreds of Military-Age Chinese Men Heading toward Us in Migrant Groups." Fox News, April 19, 2023. https://www.foxnews.com/media/reporter-says-filmed-hundreds-military-age-chinese-men-heading-toward-us-migrant-groups.

[16] "Thune: Biden's Border Crisis Turns into Full-Blown Catastrophe." U.S. Senator John Thune, May 11, 2023. https://www.thune.senate.gov/public/index.cfm/2023/5/thune-biden-s-border-crisis-turns-into-full-blown-catastrophe#:~:text=%E2%80%9CTwo%20years%20of%20record%2Dbreaking,%E2%80%9CPer%20day.

[17] Suárez, Karol. "Cartels Reap Growing Profits in the Smuggling of Migrants across the US-Mexico Border." Journal, July 1, 2021. https://www.courier-journal.com/story/news/investigations/2021/07/01/mexican-cartels-fuel-immigration-crisis-at-us-border/5290082001/.

[18] Taylor, Derrick Bryson, and April Rubin. "What to Know about the North Carolina Power Outages." The New York Times, December 5, 2022. https://www.nytimes.com/2022/12/05/us/north-carolina-power-outage-moore-county.html.

Although it is hard to tell exactly how much drug cartels are making from smuggling migrants across the border, Jaeson Jones, a retired Texas public safety captain, says that "the profits they are making today are like nothing we have seen prior."[19] Human trafficking is clearly a profitable business for the cartels, but imagine a scenario where a much larger world power is after something like the U.S. electric grid. There is no telling how valuable the U.S. losing power for a day, week or month would be to one of its many foreign adversaries, and using organizations like the cartels may very well be more cost-effective than doing it themselves.

One foreign adversary currently using the cartels to do its bidding is the Chinese Communist Party (CCP) through its sophisticated and deadly chemical "war" being waged against America with fentanyl. The same incredibly powerful and wealthy drug cartels employed by Communist China to spread fentanyl could be hired to take down our electric grid. But, with such a vulnerable Grid, China can also use its own personnel to attack it.

Communist China Presents the Most Worrisome Foreign Threat

The Chinese Communist Party (CCP) has been successfully waging economic warfare and "unrestricted warfare" against the United States for decades and a prime target of both these types of warfare and for its sophisticated espionage operations has been the electric grid. With America's wide open border and critically vulnerable electric grid, China has yet another vector through which it could inflict physical damage upon the United States were it to initiate a kinetic war.

According to Muckraker.com founder Anthony Rubin, hundreds of military-aged Chinese males are entering the United States every day.[20] This isn't surprising given all the details laid out previously. Echo Wang, a reporter for Reuters who follows the border crisis says many of these Chinese migrants are coming directly from Hong Kong, sometimes traveling for months via plane and railroad, before walking into the United States.[21] If these Chinese migrants were in fact saboteurs employed by the CCP, why would we assume that the electric grid would be a target? Because the electric grid has been a PRIME target of focus for the CCP in every other information gathering and warfighting domain.

---

[19] Suárez, Karol. "Cartels Reap Growing Profits in the Smuggling of Migrants across the US-Mexico Border."
[20] Heckman, Elizabeth. "Reporter Says He Filmed Hundreds of Military-Age Chinese Men Heading toward Us in Migrant Groups."
[21] Marks, Michael. "Chinese Migrants Are Crossing the U.S.-Mexico Border in Record Numbers." TPR, May 3, 2023. https://www.tpr.org/border-immigration/2023-05-03/chinese-migrants-are-crossing-the-u-s-mexico-border-in-record-numbers.

The CCP draws from Sun Tzu's *The Art of War* where he wrote:

"Therefore, the skillful leader subdues the enemy's troops without any fighting; he captures their cities without laying siege to them; he overthrows their kingdom without lengthy operations in the field."

It isn't hard to imagine how an attack on America's electric grid could "subdue" American troops. In fact, members of our Coalition produced a 92-page report for the U.S. Air Force Electromagnetic Defense Task Force (EDTF) titled "Grid Down: Death of a Nation[22]" that explains exactly how and why America's military will be completely "subdued" in the event our nation suffers a successful take down of the electric grid.

The CCP also draws from the seminal work of "*Unrestricted Warfare*" published in 1999 by two People's Liberation Army (PLA) Colonels who wrote (on page 145):

> "Supposing a war broke out between two developed nations already possessing full information technology, and relying upon traditional methods of operation…if the attacking side … at the same time **carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis**. There is finally the forceful bearing down by the army, and military means are utilized in gradual stages until the enemy is forced to sign a dishonorable peace treaty…"[23]

China's targeting of our electric grid doesn't only exist in its doctrinal manuals and military writings. China has been hacking into our electric grid and conducting sophisticated information gathering and influence operations against our electric utility associations and research institutions for

---

[22] https://www.griddownconsulting.com/grid-down-report

[23] Qiao Liang and Wang Xiangsui, "Unrestricted Warfare" (Beijing: PLA Literature and Arts Publishing House, February 1999), https://www.c4i.org/unrestricted.pdf

decades – putting it in an ideal position to know exactly how and what to attack in our grid "network" to take it down by physical sabotage. In fact, members of our Coalition warned FERC on May 13, 2020 about the close association between Communist China and both the Edison Electric Institute (EEI) and the Electric Power Research Institute (EPRI) in Docket EL20-46-000. Our argument was that EEI and EPRI should be required to certify that it has "no affiliation, members, interests or shareholders who are entities of foreign governments that are adversaries of the United States as defined in Executive Order 13920 ("Securing the Bulk Power Grid" – an Executive Order suspended on the first day of the current presidential administration.)

While political administrations change and so do priorities, the federal government is still charged with the duty of protecting the United States and so it should be of great interest to FERC to consider how the CCP's engagement of American utilities, researchers, and trade associations puts them in a position to better understand how to attack our grid with physical sabotage. Consider that since 2000, Chinese entities engaged EPRI on nuclear research and by 2019 had succeeded in working with EPRI on gathering data on nuclear plant single point vulnerabilities (SPVs) in analysis tools developed by EPRI in conjunction with these Chinese companies, some of which are on the U.S. Commerce Department's "Entity List." See a screenshot on the next page of just one of our pages of comments on Docket EL20-46-000 highlighting the problem with such engagement. We believe now, as we did then, that if Communist China can simultaneously achieve this type of hostile activity (see right column) while it gains this type of access to an electric research institute like EPRI (see left column), then it can certainly succeed in having its agent saboteurs arrive through an open U.S. border with the technical skills to attack the most important key nodes within our electric grid.

Open Source information on EPRI engagement with Chinese Researchers

Timeline of EPRI/China Engagement from Publicly Available Information:

- Early 2000s: EPRI engagement with China commences with in-country meetings with key nuclear industry personnel. [1]
- 2006: A formal and ongoing relationship is established between China General Nuclear Power Corporation (CGN) and EPRI's Nuclear Maintenance Applications Center (NMAC) program. [1]
- 2011-2012: EPRI leaders meet key leaders visit Chinese nuclear utilities in the wake of the 2011 World Association of Nuclear Operators (WANO) biennial meeting. [1]
- 2013: CGN joins four EPRI nuclear research programs. [1]
- 2013: China National Nuclear Corporation (CNNC) joins two EPRI nuclear research programs. [2]
- 2015: CNNC joins two more EPRI nuclear research programs. [1]
- 2016: EPRI publishes "Guidance for Instrumentation and Control Equipment Reliability Management Based on China General Nuclear Power Company Experience"[3]
- 2017: EPRI reports that 25% of its research funding comes from international members.[4]
- 2019: EPRI reports working with Chinese utilities enter data on nuclear plant single point vulnerabilities (SPVs) into a new analysis tool developed by EPRI. [5]
- 2019: the U.S. Commerce Department added China General Nuclear Power Group (CGN) and three of its affiliates to the Commerce Department's "Entity List." This means U.S. and non-U.S. companies are prohibited from exporting or transferring to the listed Chinese entities any goods, software or technology that is subject to control under the U.S. Export Administrations Regulations (EAR)[6]

Excerpt Taken Directly from U.S. Cyberspace Solarium Commission Report

Major Cyber Operations Publicly Attributed to China: 2006–2019

- 2006–18: APT10 conducts a systematic cyber espionage campaign stealing intellectual property and compromising computer systems containing personally identifiable information on over 100,000 U.S. Navy personnel.[19]
- 2008: Operators exfiltrate terabytes of data and schematics from the F-35 and F-22 stealth fighter jet programs.[20]
- 2012: China compromises computers in a new African Union headquarters it helped build in Ethiopia with malware that exports massive amounts of data nightly to servers in Shanghai.[21]
- 2012: Chinese groups target oil and natural gas pipelines in the United States.[22]
- 2013: *IP Commission Report* highlights Chinese efforts at intellectual property theft efforts linked to an estimated $300 billion in business losses a year.[23]
- 2014: Cloud Hopper campaign attacks managed service providers to access their client networks, including those of leading international technology companies, and steal their clients' intellectual property.[24]
- 2014–15: The Office of Personnel Management is breached, exposing sensitive information used for security background checks on 21 million federal employees.[25]
- 2017: Chinese military hackers breach the networks of Equifax, an American credit reporting agency, stealing the personal information of over 145 million Americans.[26]
- 2018: Hackers breach servers of Marriott International, extracting information on 500 million guests.[27]
- 2019: Operators compromise iPhones in a domestic spying campaign targeting Uighurs, a Muslim minority in China.[28]

Timeline Sources:

Left hand column:

[1] https://eprijournal.com/building-a-research-bridge-to-china/
[2] https://www.power-eng.com/2013/10/14/epri-china-team-on-nuclear-energy-research/
[3] https://www.epri.com/#/pages/product/000000003002008025/?lang=en-US
[4] https://www.mncee.org/getattachment/Resources/Resource-Center/Presentations/2017-Energy-Technology-Forum/Tech-Forum-2017_EPRI_Ram-N.pdf.aspx
[5] https://eprijournal.com/a-new-tool-to-address-single-point-vulnerabilities/
[6] https://www.pillsburylaw.com/en/news-and-insights/china-industry-entity-list.html

Right hand column:

https://www.solarium.gov/report

If these frightening facts weren't enough, we know that China has already targeted our transformer fleet by attacking it via the supply chain. On August 26, 2021 a member of our Coalition filed a complaint and petition with your Commission on the problem associated with "Equipment and Monitoring Systems Marketed from the People's Republic of China."[24]

That Docket (EL21-99-000), which is still open before your Commission, revealed not only the problems associated with our importation of Chinese transformers which are potentially pre-loaded with hardware backdoors, but also the reality that companies owned or controlled by the CCP – such as "Doubletree Systems" – are also selling grid security monitoring systems and even working with EPRI on grid security issues. As the complaint argued:

> "Thus, we have clear connection from Doubletree Systems, Inc. –> XJ Group –> State Grid Corporation of China –> government of the People's Republic of China. All Chinese companies have an obligation under the 2017 Chinese National Intelligence Law[25] to "support, assist and cooperate with the state intelligence work." Moreover, under China's 2014 Counter-Espionage Law[26] a company may not refuse the Chinese government when asked for information."

We cannot afford to suffer another "failure of imagination" in foreseeing how our adversaries can attack our homeland. It should be clear that China can attack our vulnerable grid at will, and likely with incredible inside knowledge and sophistication. Thus, the grid MUST be defended.

[24] https://michaelmabee.info/chinese-transformer-complaint-filed-with-u-s-government/
[25] https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense
[26] https://www.reuters.com/article/us-china-lawmaking-spy-idUSKBN0IL2N520141101

As Risks to Grid Grow, So Do Transformer LEAD TIMES

Every state adversary of the U.S. has an understanding of the importance of supply chains and transformer lead times because they have their own nations' electric grids to manage, especially Communist China. As Russia's war against the Ukraine ravages on and Putin's military consistently targets Ukrainian electric infrastructure and as the Biden Administration's war on "climate change" seeks to electrify massive fleets of vehicles and transform home cooking and heating from gas to electric, there is both a foreign and domestic surge in demand for electric transformers and electrical steel.

According to the American Public Power Association (APPA), **"the electric industry is currently experiencing a critical shortage of distribution transformers."**[27] In a survey of public power utilities conducted by APPA, an overwhelming majority of respondents indicated that supply chain disruptions relating to transformers where their biggest concern. Due to new green-energy policies, the demand for these transformers has drastically increased, which in turn is impacting the nation's housing shortage.[28]

Large transformers take 20 to 39 months to replace now, up from 16 to 20 months last year.[29] In addition to the problems with lead times for large transformers, the smaller distribution transformers responsible for connecting homes and businesses to the grid are also about to become extremely hard to source. A recently proposed rule by the Department of Energy would change "industry standard grain oriented electrical steel (GOES) cores to amorphous steel cores, which would exasperate the supply chain shortage as manufacturers would need to adjust their production lines."[30]

FERC must also consider alongside the scarcity of new grid assets the age of existing assets. In the American electric grid, 70 percent of the transmission lines are at least 30 years old, and 60 percent of the circuit breakers are over 35 years old.[31] The age of the grid makes it much more vulnerable to

---

[27] Ciampoli, Paul. "Proposed Efficiency Standards for Distribution Transformers Would Worsen Shortages: APPA." American Public Power Association, March 29, 2023. https://www.publicpower.org/periodical/article/proposed-efficiency-standards-distribution-transformers-would-worsen-shortages-appa.

[28] Finley, Allysia. "Opinion | the Other Green-Energy Grid Crisis." The Wall Street Journal, June 4, 2023. https://www.wsj.com/articles/the-other-green-energy-grid-crisis-transformers-distribution-steel-outage-china-4029ed43.

[29] Walton, Robert. "Utilities Sound Alarm over Distribution Transformer Shortage as Procurement Times Surpass 1 Year and Costs Triple." Utility Dive, December 19, 2022. https://www.utilitydive.com/news/distribution-transformer-shortage-appa-casten/639059/.

[30] "Lankford Pushes to Nullify Transformer Rule That Will Lead to Shortages, Put National Security in Jeapardy, and Weaken Supply Chains: U.S. Senator James Lankford of Oklahoma." Press Releases | News | U.S. Senator James Lankford of Oklahoma, June 2, 2023. https://www.lankford.senate.gov/news/press-releases/lankford-pushes-to-nullify-transformer-rule-that-will-lead-to-shortages-put-national-security-in-jeapardy-and-weaken-supply-chains.

[31] Brooks, Chuck. "3 Alarming Threats to the U.S. Energy Grid – Cyber, Physical, and Existential Events." Forbes, February 17, 2023. https://www.forbes.com/sites/chuckbrooks/2023/02/15/3-alarming-threats-to-the-us-energy-grid--cyber-physical-and-existential-events/?sh=38a1384f101a.

cascading failures, and the lack of protection around these critical components make these failures all the more plausible. Thus, the combined foreign and domestic targeting of our grid, the economic warfare of China, kinetic warfare of Russia, "environmental" policy of the current administration, and age of the existing grid assets all combine for a perfect storm of transformer and component scarcity that puts our electric grid in a position where **we cannot afford to have these vital assets sabotaged.**

Conclusion

Before this filing was even submitted, NERC already filed a motion requesting that your Commission "reject" our petition for increased physical security standards. This is in keeping with the way that NERC and the industry responded to the Commission's order that it evaluate the Physical Security Reliability standards in Docket No. RD23-3-000. Your Commission will be told that the costs are too high to invest in widespread and mandatory physical protection of the electric grid. We think the costs are far too high NOT to invest in this protection and we believe that the public will be willing to pay more for their electricity to see this protection realized. Finally, despite NERC's seemingly consistent and enduring official position that no changes are needed to the existing physical security standards, even NERC's CEO Jim Robb admitted during the Sixth Meeting of the Joint Federal-State Task Force On Electric Transmission (Docket No. AD21-15-000) the following:

> "And as with many of our standards, industry doesn't stop there, and it will typically go well beyond what the standards call for. So, while many substations may not need to be technically CIP 14 compliant, their owners may very well build in protections because it's the right thing to do."

We conclude that Mr. Robb's logic about building in protections "because it's the right thing to do" is vital feedback for your Commission. Thus, we believe now is the time that the Commission must demand <u>stronger</u> <u>mandatory</u> physical security standards - reflecting that logic. **It's the right thing to do.**

Respectfully submitted,

LtCol Thomas J. Waller Jr. (USMC. Ret.)
Co-Director
Secure-the-Grid Coalition
twaller@centerforsecuritypolicy.org

Douglas. Ellsworth
Co-Director
Secure-the-Grid Coalition
doug.ellsworth@usapact.org