31st Steering Group Meeting of the Priority Area 2 | Budapest | 20.11.2025

Problems and Solutions to Cybersecurity Crises in Renewables

Erika Langerová
erika.langerova@cvut.cz
Head of Cybersecurity for Energy

Czech Technical University in Prague
University Centre for Energy Efficient Buildings

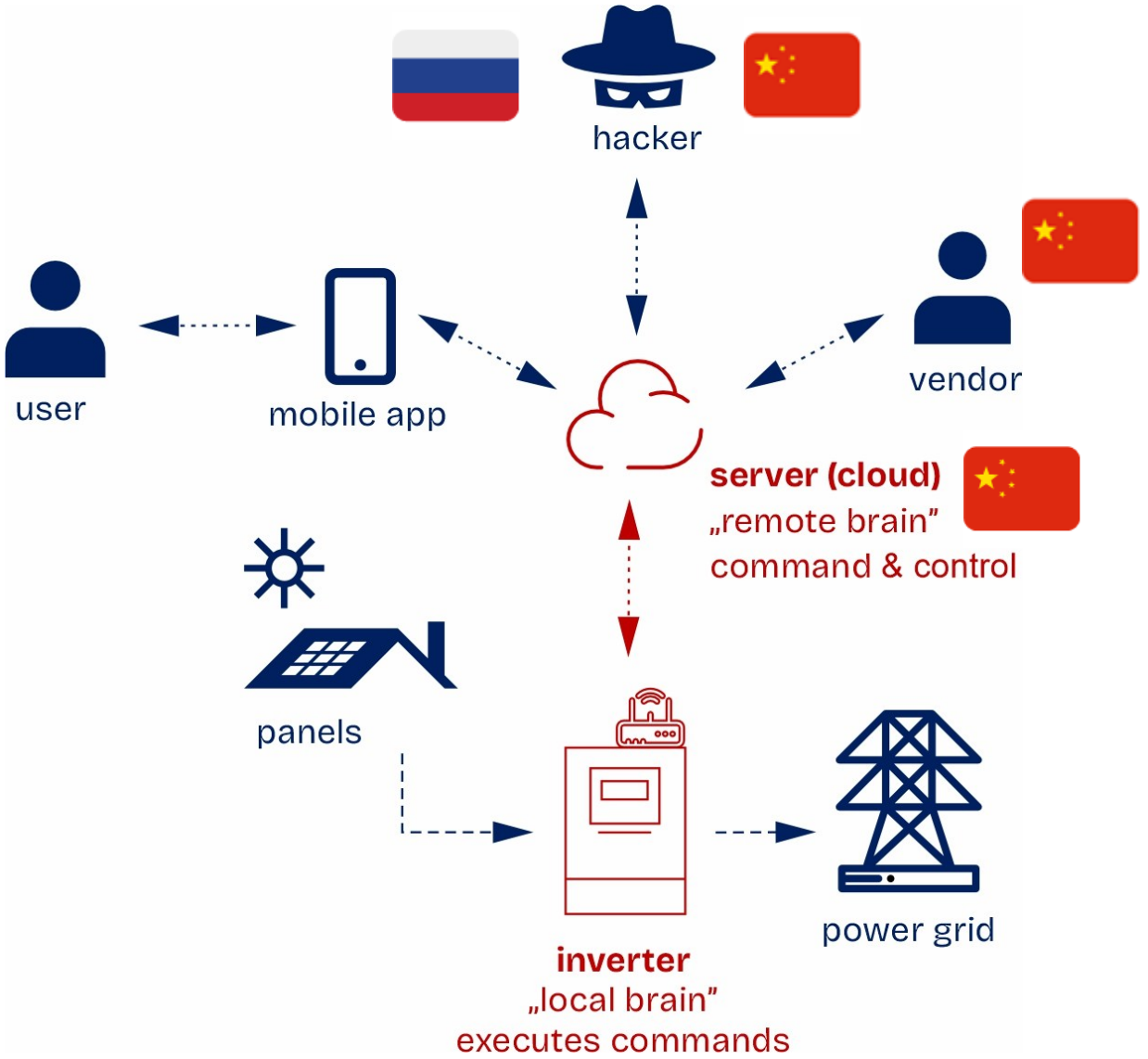
The Questions

1. What Is Happening?
2. How Do We Know China Is Developing the Means to Crash Power Grids?
3. Can Russia Exploit Chinese Clean-Tech ?
4. Solutions ?

1. What Is Happening?

From Russian Fossil Fuels → Chinese Clean Tech

- **From Russian Fossil Fuels → Chinese Clean Tech (solar, wind, batteries):** energy dependency has shifted, not disappeared.
- **Massive Growth of Renewables:** solar, batteries and wind dominated by Chinese supply chains.
- **Digitalization of Renewables:** smart systems, remote access, and cloud control.
- **New Vulnerability:** remote operability creates pathways for cyber and cyber-physical attacks.



A Huge Problem Has Emerged In Clean Tech

- The Chinese National Intelligence Law includes the controversial Article 7, which requires citizens and organizations to support national intelligence efforts
- Clean-tech vendor might be forced to provide full remote access to the clean-tech fleet, incl. the firmware updates
- In other sectors, it is already happening: Chinese Communist Party increasingly using commercial civilian companies to carry out cyberattacks

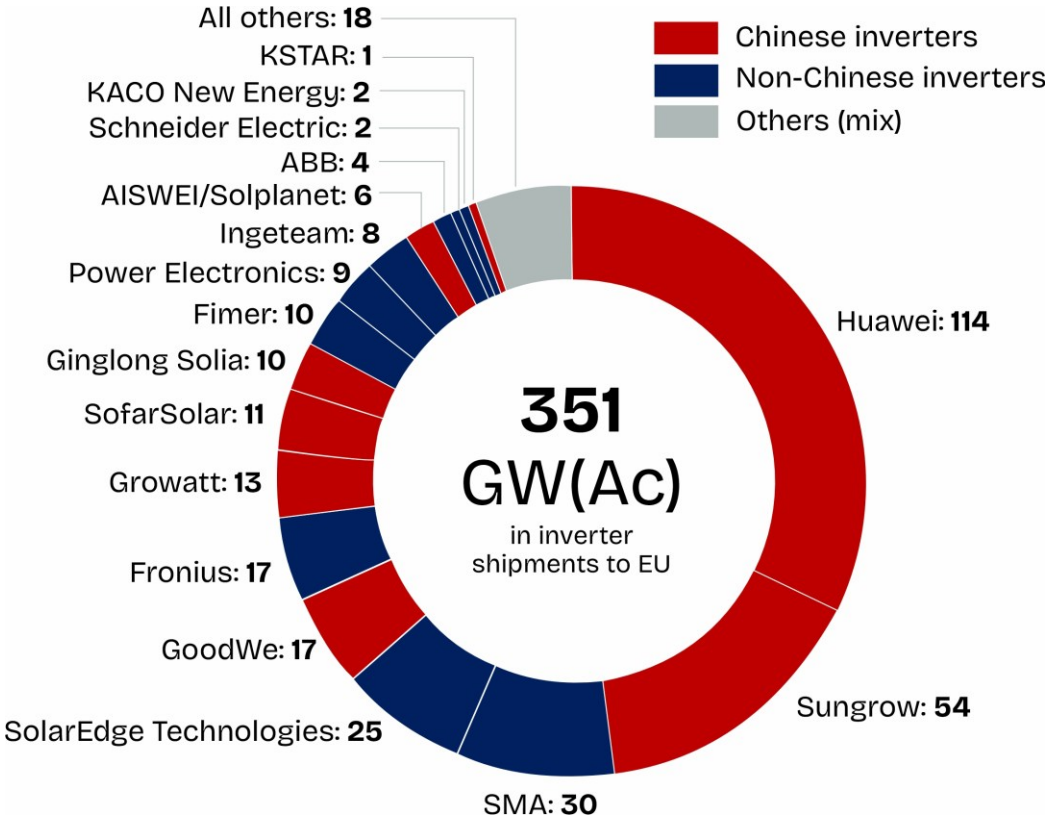
China used three private companies to hack global telecoms, U.S. says

An FBI spokesperson told NBC News that Salt Typhoon has hacked m
across 80 countries.

in·depth | Fused Together: The Chinese Communist Party Moves Inside China's Private Sector

Jeffrey Becker | Friday, September 6, 2024

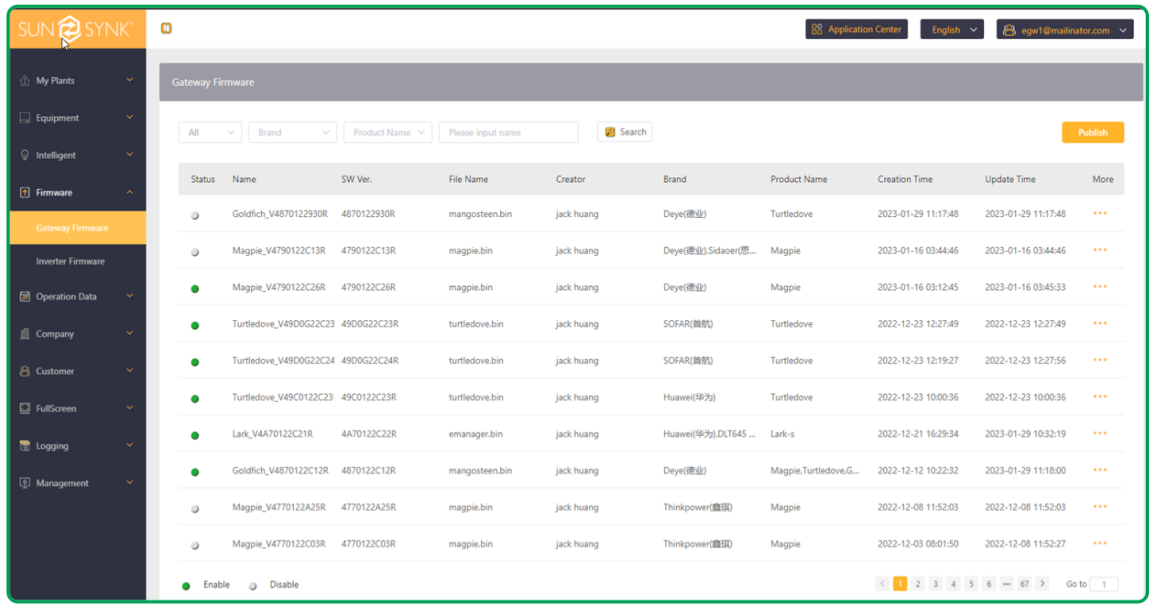
Example from solar sector: about 65% of EU solar power is controlled by China, mainly via Huawei, a company labeled a security threat in many EU countries and banned in the U.S. market

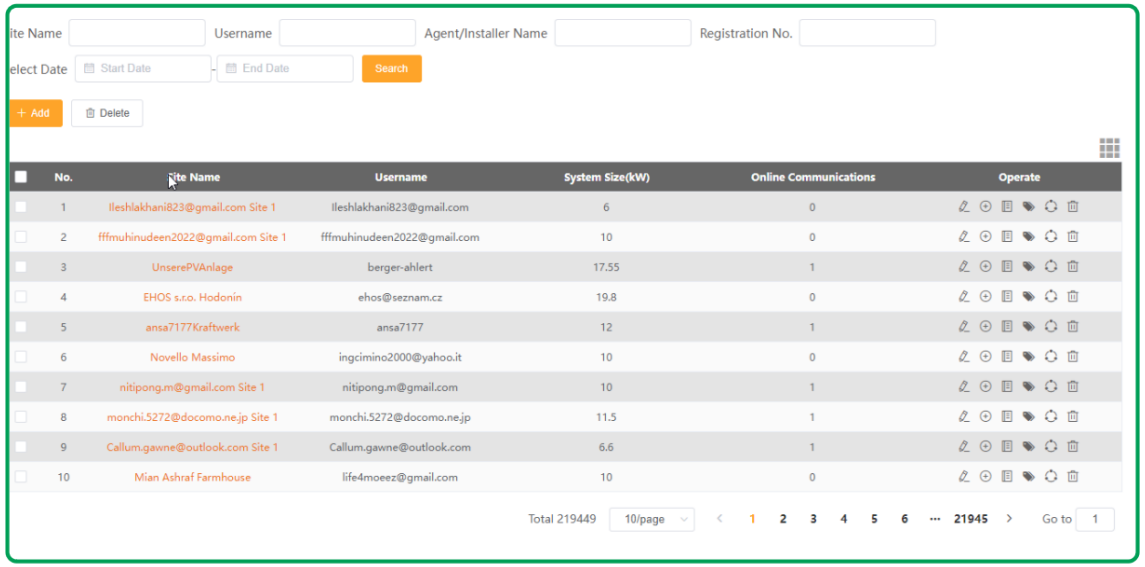


PV inverter shipments to Europe over 2015-2023 in Gwac, data source: SolarPower Europe, Solutions for PV Cyber Risks to Grid Stability

How can they abuse remote access to solar?

- The manufacturer has remote access to all settings, including advanced ones
- Can send commands to:
  - Adjust operational status and mode
  - Change frequency
  - Change voltage outputs
  - Suddenly switch off
  - Suddenly switch on
  - Switch from active to reactive power
  - Change safety settings
  - Change grid parameters settings





How can they abuse remote access to solar?

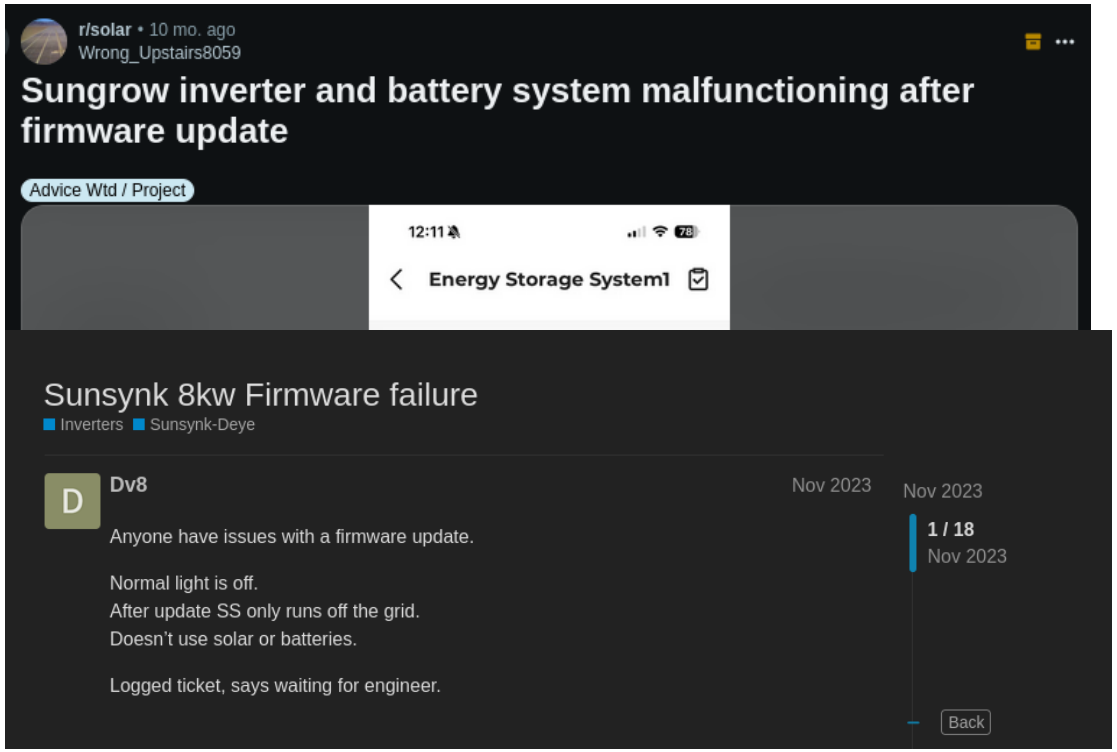
- Malicious lines of code injected to the firmware
- Instructions can execute based on certain trigger (date, time, local grid conditions, or any other combination of external input)
- Can:
  - Change operational parameters
  - Sudden shutdown and power on
  - Abrupt changes in inverter output
  - Disable cooling fans
  - Disable software-level protections
  - Can completely brick (destroy) inverter

Around 800 Sungrow batteries affected by outage in Germany

After 800 Sungrow batteries were impacted by an outage, the Chinese manufacturer informed its local German partners about the solution to the problem. However, it remains unclear how quickly the affected battery management systems can be replaced.

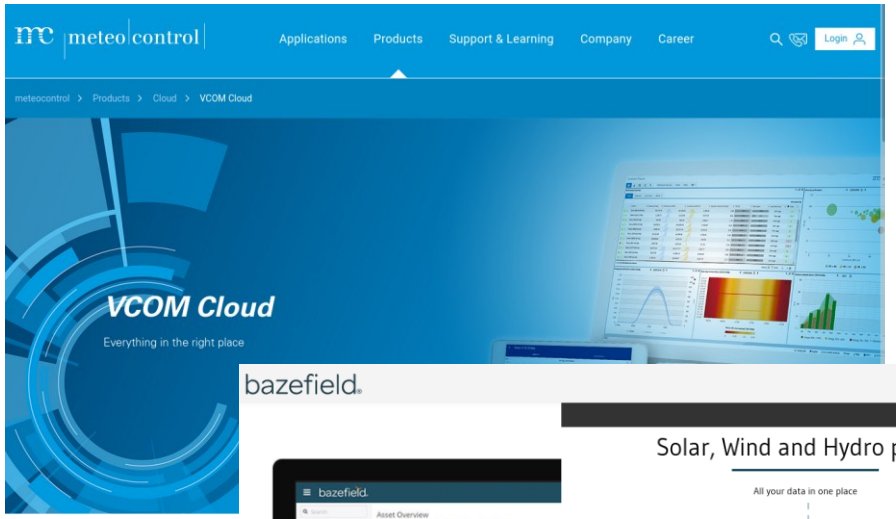
MARCH 17, 2023 SANDRA ENKHARDT

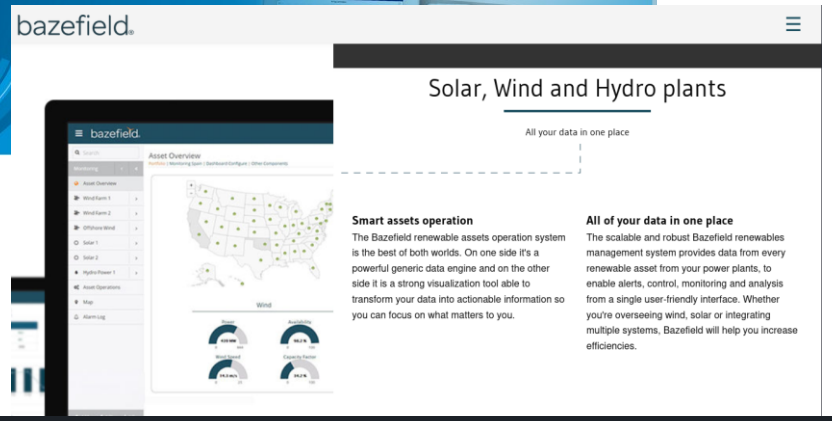
DISTRIBUTED STORAGE | ENERGY STORAGE | RESIDENTIAL PV | TECHNOLOGY AND R&D | GERMANY



Outsourcing Of Control And Monitoring

- Applies mainly to commercial and utility-scale power plants
- The inverter is often not connected to the manufacturer's cloud („remote brain")
- But the entire solar system is controlled by a SCADA system outsourced to a third party and often connected to the cloud or having remote access
- The third party is often Chinese
- It's also a problem if originally European but later acquired by China (Meteocontrol, Bazefield)
- It is also a problem if control over the entire fleet can be entrusted to any individual without a clearance (imagine that individual controls the power output equivalent to a nuclear power plant)

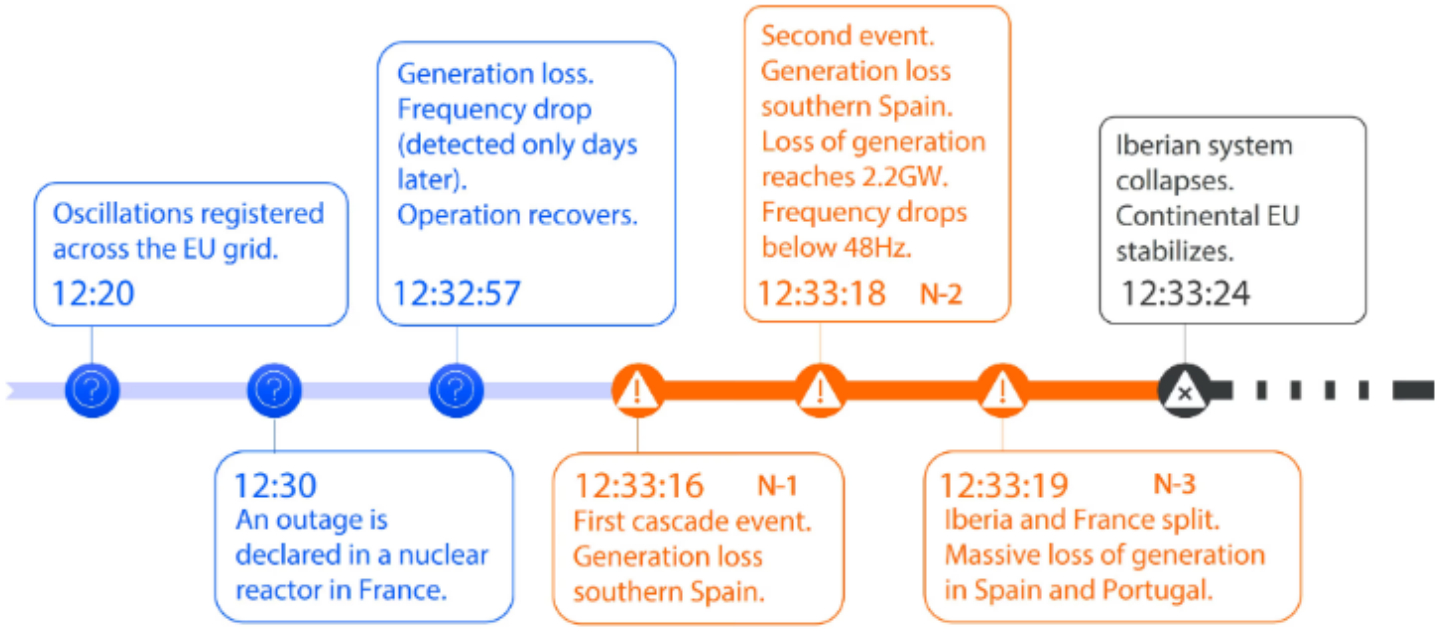




Destabilizing the Power Grid? Yes, They Can

- **Iberian blackout: sudden losses** on the order **of a few GW** already have the potential to cause destabilization.
- **China controls hundreds of GWs in EU !**

Figure 2. Timeline of isolated key events leading to the blackout in the Iberian Peninsula on Monday, April 28, 2025



RaboResearch: *Facts and lessons learned from the Iberian blackout*

Destabilizing the Power Grid? Yes, They Can

- **Two large simulation studies** have been carried out
- **Publicly available one** by DNV comissioned by SolarPower Europe
- **Proprietary national study** within the Czech Republic conducted by ČSRES (association of TSO and DSOs)
- **Conclusions of DNV:** Massive inverter manipulation and sudden voltage profile changes (inductive/capacitive reactive power outputs) **show potential critical impacts on system stability** in the continental European synchronous area
- **Conclusions of ČSRES:** the current situation represents a **risk to the secure operation of the national power grid** and **needs to start being mitigated**

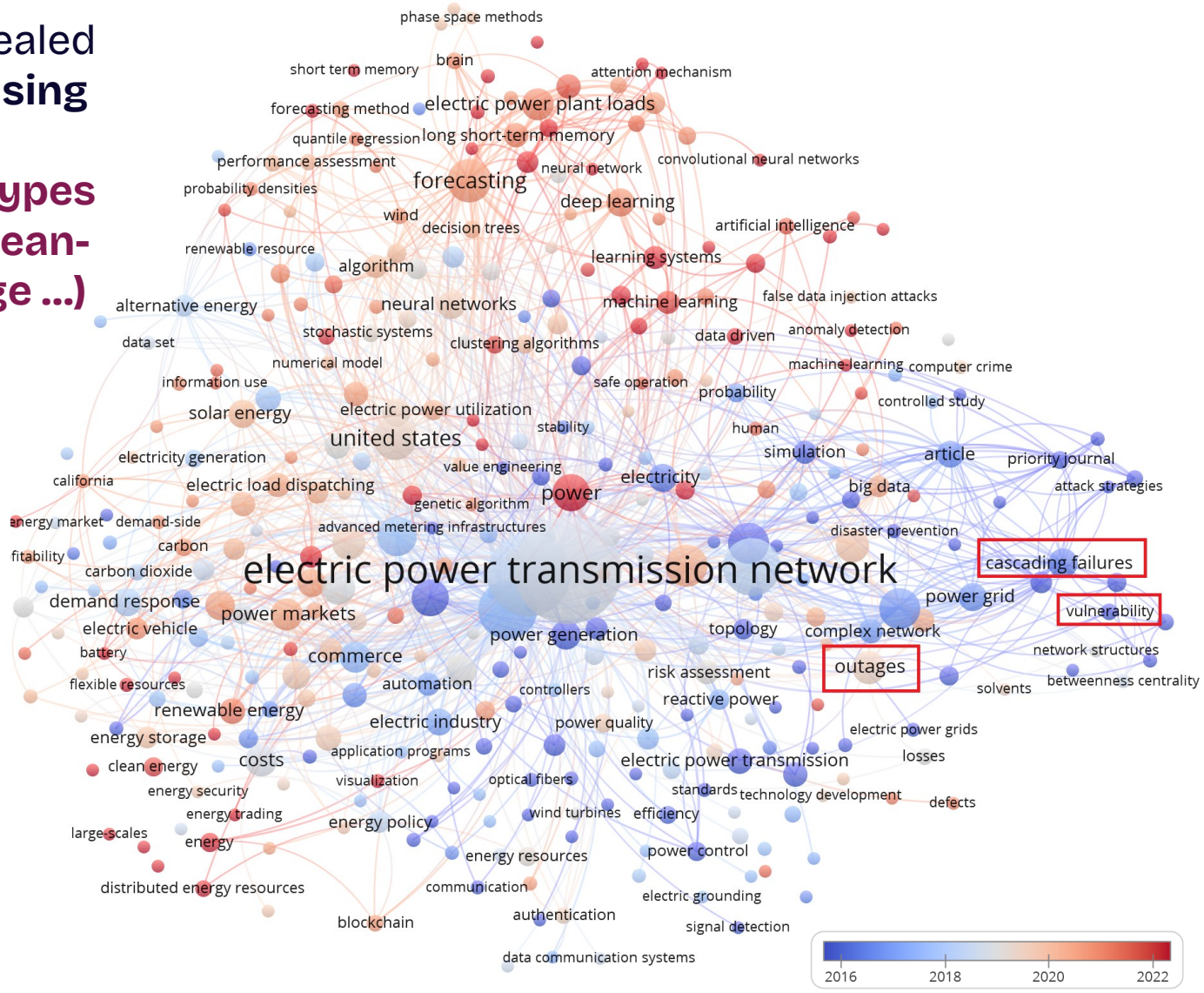
2. How Do We Know China Is Developing the Means to Crash Power Grids?

China Is Studying How To Crash Our Power Grids

- Study of Chinese academic publications revealed **extensive research into techniques for causing cascading failures in Western power grids**
- **The easiest entry point to carry out these types of attacks is Chinese internet connected clean-tech (solar inverters, battery energy storage ...)**

> *"Hence, in this paper the several functions to determine the importance of nodes in a complex network were adopted **to search for the destructive nodes in a power grid**. The node data from **Western United States power grid** was taken as an example." **Source: Selection of the Disruptive Nodes to Destroy Power Grid***

> *We investigate the structural vulnerability of complex networks under different **edge-based attacks**. The simulations demonstrate that, the edges with higher product of betweenness centrality of the two endpoints of one edge connected are more important for SF network, ER random network, autonomous system network (AS), **Italy power grid** and **US airport networks**, but the edges with higher edge betweenness centrality are more important for **WS networks**. **Source: Structural vulnerability of complex networks under multiple edge-based attacks***



For full version of the study: erika.langerova@cvut.cz

China Is Studying How To Crash Our Power Grids

The research is linked to defense universities directly supporting Chinese army and intelligence

Conferences > 2018 IEEE Third International...

Structural Vulnerability of Complex Networks Under Multiple Edge-Based Attacks

Publisher: IEEE | Cite This | PDF

Shudong Li ; Xiaobo Wu ; Aiping Li ; Bin Zhou ; Zhihong Tian ; Dawei Zhao **All Authors**

3 Cites in Papers | 358 Full Text Views

Authors

Shudong Li
Yantai Vocational College, School of software engineering, Shandong Yantai, China

Xiaobo Wu
Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou, China

Aiping Li
School of Computer Science, National University of Defense Technology, Hunan Changsha, China

Bin Zhou
School of Computer Science, National University of Defense Technology, Hunan Changsha, China

Zhihong Tian
Cyberspace Institute of Advanced

Dawei Zhao
Shandong Provincial Key Laboratory of Computer Network, Shandong Computer Science Center, Jinan

ttacks are induced b
ch also can desc
enath of shortest

NUDT is the best-funded military university in China !

In 2017, NUDT was reformed and placed in charge of the Institute of International Relations in Nanjing, the National Defense Information Institute in Wuhan, the Xi'an Communications College, the Electrical Engineering Institute in Hefei, and the College of Meteorology and Oceanography in Nanjing. [2] The Institute of International Relations in Nanjing is a key training centre for intelligence officers.

Defected Chinese spy Wang Liqiang claimed in 2019 that NUDT's 'Intelligence Center' sent him fake passports for his mission to interfere in Taiwanese politics. [6] This indicates that the university plays an important role in supporting China's overseas intelligence activity.

Economic espionage and misconduct

NUDT has used Changsha Institute of Technology, a historical name for the university, as cover to hide its military affiliation. [15] NUDT students applying to study overseas are instructed to downplay their military links by removing military courses from their academic records. [16]

Major defence laboratories

- National Key Laboratory for Parallel and Distributed Processing (并行与分布处理国家重点实验室/并行与分布处理国防科技重点实验室) [8]
- State Key Lab of New Ceramic Fibers and Ceramic Matrix Composites (新型陶瓷纤维及其复合材料国家重

For full version of the study: erika.langerova@cvut.cz

China Is Studying How To Crash Our Power Grids

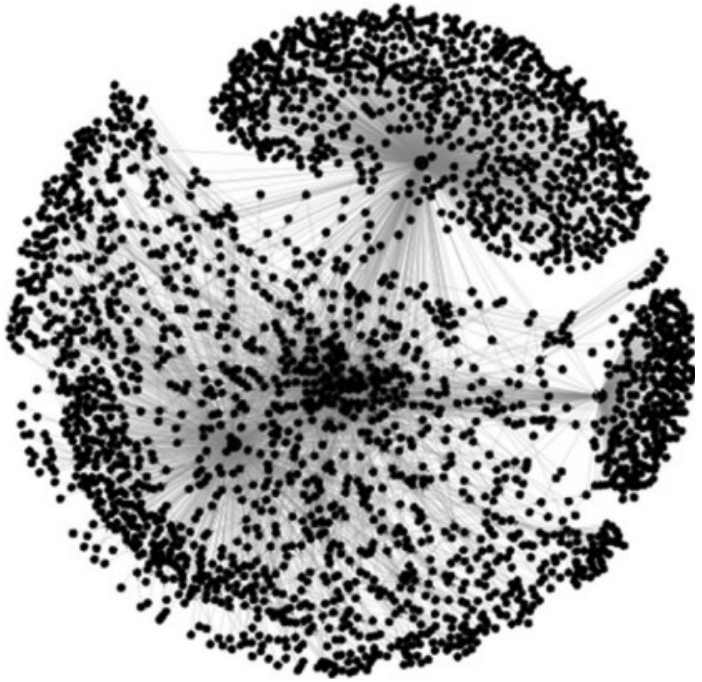


Fig. 6. CFG of the French grid.

TABLE III
TOP 20 CRITICAL BRANCHES IN FRENCH GRID

Rank	In-degree	Out-degree	Degree
1	2455	2554	2554
2	2380	2556	2455
3	508	2148	2380
4	2307	2381	2556
5	2482	1808	508
6	796	2258	2307
7	1759	75	2148
8	2467	2482	2381
9	2372	2307	1808
10	1808	2466	2482
11	2306	2378	2258
12	2378	2376	796
13	2379	2380	2467
14	2376	2379	75
15	2377	2377	1759
16	2375	2455	2378
17	2466	2467	2376
18	2556	2555	2379
19	2554	796	2377
20	834	285	2466

Source: A Novel Cascading Faults Graph Based Transmission Network Vulnerability Assessment Method

5 Simulation of US Power Grid

With the example of US power grid, we take a deliberately attacking to the important edge, and then calculate the degree of network collapse, thereby judging the invulnerability of the network.

According to five importance metrics, we sort the edges according to five strategies, attack 5% edges each time and calculate the corresponding maximal connected components coefficient (G), efficiency (E) and average Path length (L). The results are as follows (Figs. 3, 4 and 5):

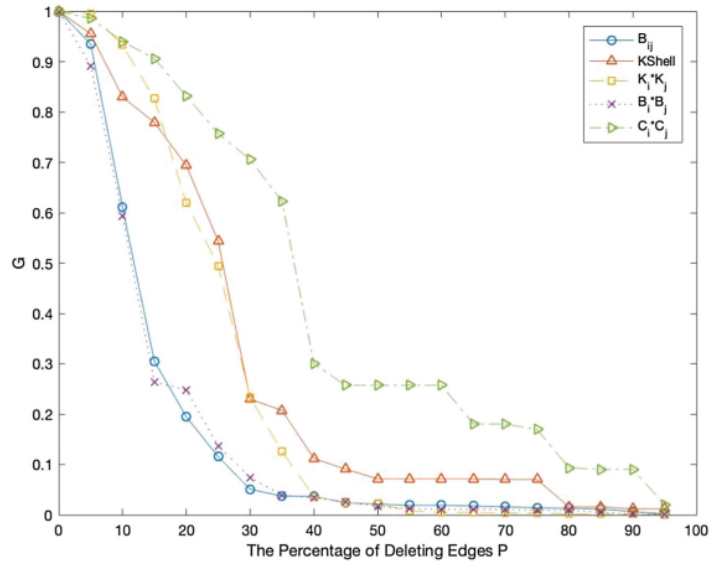


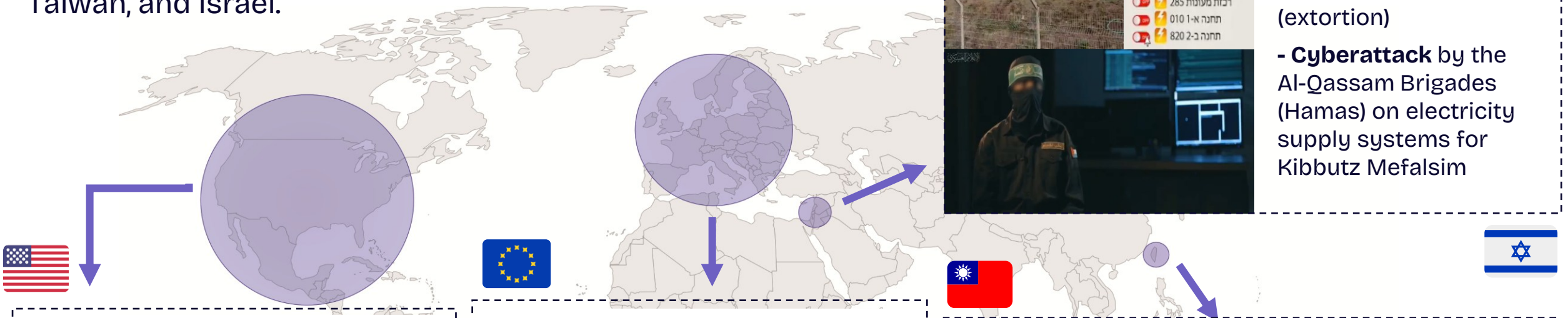
Fig. 3. The largest connected component G as a function of deleting percentage p.

Source: Electric Power Grid Invulnerability Under Intentional Edge-Based Attacks

For full version of the study: erika.langerova@cvut.cz

Energy is the target

Rising attempts at physical, cyber, and espionage attacks on energy infrastructure have been recorded in the U.S., Europe, Taiwan, and Israel.



In Israel

- **Arson attack** on a solar power plant near Kibbutz Neve Or, financial motivation (extortion)
- **Cyberattack** by the Al-Qassam Brigades (Hamas) on electricity supply systems for Kibbutz Mefalsim

In the U.S.

- **Sabotage attacks** (neo-Nazis, radicals), shootings at substations
- **Cyberattacks (China)** breaching critical infra and maintaining access for a future disruptions

2 men arrested for allegedly sabotaging 4 Washington state power substations on Christmas

The attacks left thousands of customers without power.

U.S. NEWS

Neo-Nazi group leader convicted of plotting Maryland power grid attack

FBI says Chinese hackers preparing to attack US infrastructure

By Christopher Bing

April 18, 2024 11:12 PM GMT+2 · Updated April 18, 2024

In Europe

- **Kinetic (Russia),** and **cyber attacks (Russia, China),** including successful cyber attacks on solar power plants in Ukraine

The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure

Putin ready to cripple Britain with cyber attacks, minister warns

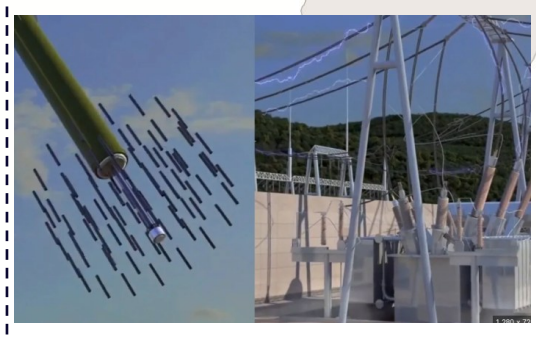
Electronic strike by Russia against UK infrastructure could 'turn out the lights for millions'

In Taiwan

China practises hitting Taiwan key ports, energy sites in 'live-fire' drills

ASIA / PACIFIC

China's military carried out "live-fire" drills targeting crucial ports and energy sites directed at Taiwan. Washington condemned the drills as "intimidation tactics" and Taiwan's President Lai Ching-te labeled Beijing a "foreign hostile force".



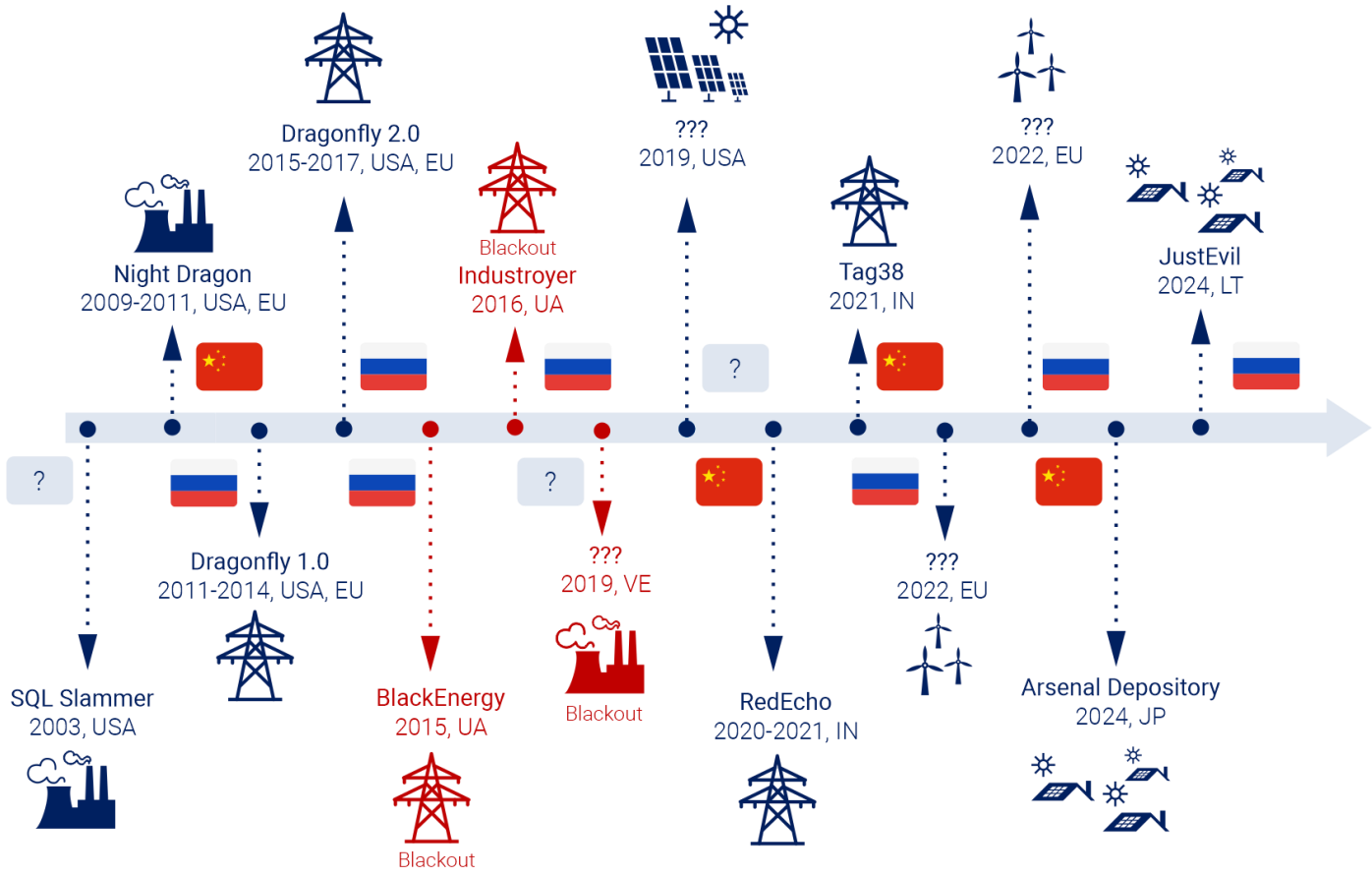
- **Kinetic attacks (China)** on exact replicas of Taiwan's LNG terminals
- **Cyberattacks (China)** on the power grid occur daily, TSO detecting up to 5 million attack attempts per day*

*(includes port scanning)

Data source for this slide: Author's OSINT compilation

China And Russia Are Behind Power Sector Attacks

- **China and Russia** are almost solely responsible for the **sucessfull attacks** on power grids
- For Russia, **destructive attacks** are typical; for China, **espionage**.
- Typhoon hacker campaigns show that the **Chinese** have attempted to infiltrate infrastructure to preposition **for possible later destruction**.
- **The possibility that China could shift to destructive attacks cannot be ruled out.**



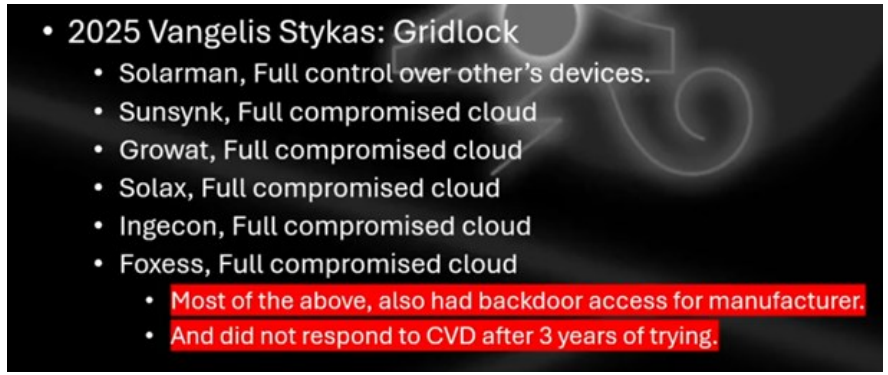
Data source for this slide: Author's OSINT compilation

3. Can Russia Exploit Chinese Clean-Tech ?

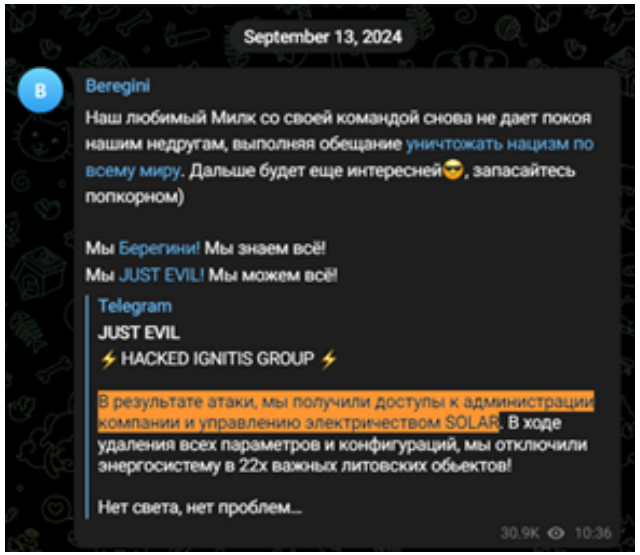
Direct Control Via Stolen Access Rights

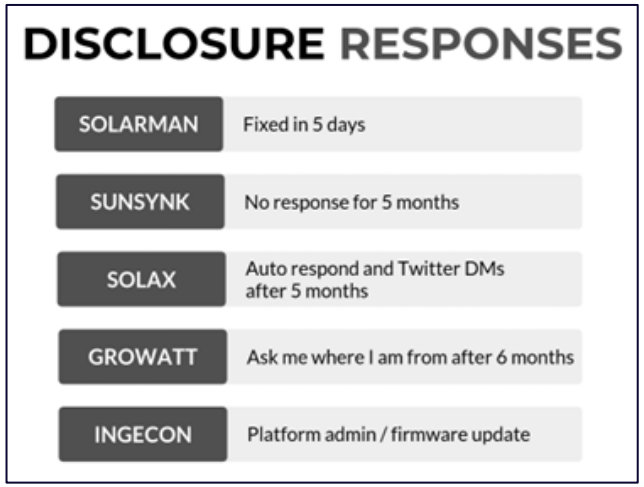
- **The Chinese inverters are facing problems with poor cybersecurity.**
- Weak passwords, vulnerabilities on cloud platforms, easy to break into
- **A hacker can exploit the vulnerability and send commands to:**
  - Adjust operational status and mode
  - Change frequency
  - Change voltage outputs
  - Suddenly switch off / on
  - Switch from active to reactive power
  - Change safety /grid settings
  - Upload malicious firmware
  - Destroy the inverter or try to set it on fire

Willem Westerhof, Bureau Veritas, Horus 2.0 Scenario



Willem Westerhof, Bureau Veritas, Horus 2.0 Scenario



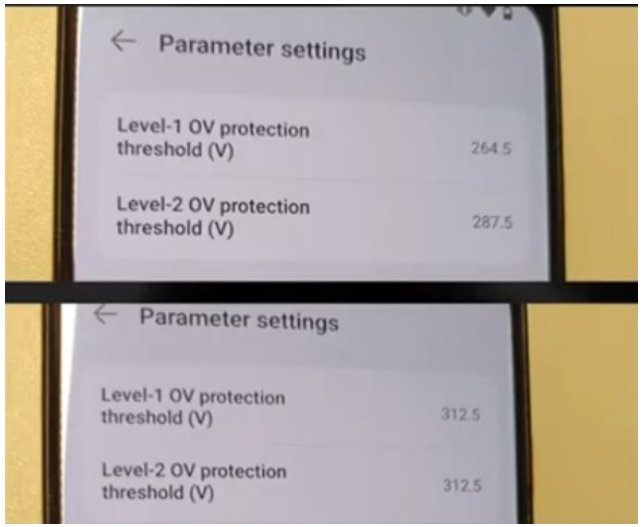


Vangelis Stykas, Gridlock

Cyber-Physical Attacks

- **Highly relevant in the context of Russian hybrid warfare across Europe**
- **A proprietary PoC study showed that hacker can exploit vulnerabilities in and send commands to:**
  - Destroy the solar inverter or set it on fire
  - Set other parts of the system on fire
  - Sabotage and potentially explode the battery connected to the solar inverter
- **In the event of a conflict with NATO, it may be used to overwhelm regional fire departments.**

MC4 connector overheating \ melting which typically leads to hazardous DC arcs, courtesy of SolarDefend company



Willem Westerhof, Horus 2.0 Scenario

Map 0.1: **Methods of Russian hybrid-warfare activity across Europe, January 2018–June 2025**

IISS Research Report: The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure

4. Solutions ?

A Comprehensive Approach

No Quick Fix: New Strategy and Framework Necessary

The challenge we face cannot be solved with a quick fix. It requires long-term solutions that address various factors in parallel.

- **Key Solutions:**
  - **Define sector-specific binding standards**: Clear, binding „clean-tech specific“ standards on what constitutes a "secure" installation, operator, firmware etc. must be established.
  - **Amendments to legislation:** Address the gap in legislation, particularly the lack of coverage for residential installations. Without this, a baseline level of security cannot be guaranteed.
  - **Education & Awareness Programs**: Stakeholders, including consumers and businesses, must be educated about the risks and importance of secure solar installations

Creates stable environment for commercial companies to step in to develop solutions

Problems encountered so far: Chinese lobby

Leading Chinese inverter manufacturers are members in the following EU associations, similar situation is in national associations:

BRUEGEL, CEPS, CIPL, ECSO, EIF (European Internet Forum), FFTH, SmartEN, BEDER, BusinessEurope, CCCEU, CERRE, CharIn, CSR Europe, DIGITALEUROPE, ECTA, Eurelectric, EPC, ESF (European Service Forum), GESI, RBA (Responsible Business Alliance), SolarPower Europe, EASE (European Association for Storage of Energy)

Stakeholders who profit from Chinese overcapacity do also reject the idea of restrictions and fundamentally downplay the problem

For too long, only solar and other industry associations — whose membership base is heavily made up of Chinese companies — were invited to the discussions. As a result, the issue could not be brought up officially for a long time. For more context see:

https://www.politico.eu/article/huawei-blacklisted-eu-solar-panel-lobby/

EU authorities are stalled

- There are deep concerns about the EU Commission's current approach to addressing the risks.
- For too long the Commission has been preoccupied with repeated risk assessments, warning of the dangers of high-risk vendors in our energy infrastructure, yet failing to put forward tangible proposals beyond further studies*.
- The only European bodies responding to the threat with concrete steps are the Lithuanian Ministry of Energy banning Chinese remote access to solar, wind and batteries and the Czech National Cyber and Information Security Agency (NÚKIB), which has issued warnings, including a warning for solar inverters.

* Risk assessment report on cyber resilience on EU's telecommunications and electricity sectors published in July 2024 and another Risk assessment announced by European Commission for the solar industry in response to written questions. The ICT Supply Chain Toolbox mentioned in the answer by the Commission, is still under development since Council Conclusions of October 2022, and will only propose a joint methodology, no restrictive measures like the 5G toolbox.

European Parliament

Brussels, 29 October 2025

Dear Executive Vice-President Virkkunen,
Dear Commissioner Jørgensen,

We write to you with deep concern about the Commission's approach to addressing risks stemming from high-risk vendors, particularly in the field of solar (PV) inverters. We urge you to propose immediate and binding measures to restrict high-risk vendors from our critical infrastructure.

Huawei, designated as a high-risk vendor by the Commission, accounted for over 115 GW of Europe's solar inverter market up to 2023. It is one of six Chinese vendors that collectively control more than two-thirds of the market (219 GW) in Europe.[1] And our dependency is deepening: in 2024, 80% of all new PV inverter capacity installed in Europe originated from China.[2]

Lithuania has already banned remote Chinese access to solar and wind devices.[3] More recently, the Czech and German national cyber security agencies NUKIB and BSI have warned of the risks posed by Chinese-linked technologies in critical sectors, highlighting Chinese PV inverters as a high-risk technology for supply chain attacks on our grid, and urging the use of non-technical risk factors to address these risks.[4] Chinese authorities recognise these risks, meaning that European inverters are de facto not allowed into their grid, on the basis of cybersecurity grounds. Europe should adopt a similar approach.

The Commission has dedicated considerable effort to risk assessments, highlighting the risks posed by high-risk vendors in our critical infrastructure. However, concrete proposals have yet to materialize.[5] When the ongoing studies are completed and potential legislation is tabled, as much as two years may have passed. By that time, Europe risks having lost its remaining PV inverter manufacturers. Western companies are drastically losing market share in Europe, though they currently still retain the capacity to meet European demand. If one of them succumbs to unfair competition from China, the Union could soon be left without any non-Chinese alternatives

Binding legislation to restrict risky vendors in our critical infrastructure is urgently required, either through the revision of the CSA or elsewhere. Vice-President Virkkunen has already shared her dissatisfaction with the lackluster implementation of the voluntary 5G toolbox, calling for stronger measures, and considering binding legislation.[6] Compared to telecom, the secure management of Europe's power grid is inherently a Union-wide issue: the failure of a single link has the potential to trigger cascading disruptions across the continent.

Until binding legislation is in place, a temporary framework should be established to restrict risky vendors from our energy infrastructure. Many precedents already exist, such as the 5G Toolbox that can include non-technical risk factors, such as the NZIA cybersecurity criteria.[7] The German energy association BDEW has also proposed blacklisting or whitelisting of (un)trustworthy companies.[8]

Without immediate and binding EU action, Europe risks not only its energy security but also the viability of all remaining European manufacturers in this sector. We look forward to your urgent response and a clear timeline for legislative action.

Yours sincerely,

Bart Groothuis

[1] Solar Power Europe, Solutions for PV Cyber Risks to Grid Stability.
[2] S&P, Global Commodity Insights.
[3] Reuters, Rogue communication devices found in Chinese solar power inverters.
[4] NUKIB, Warning against the Transfer of the data to and Remote Administration from People's Republic of China; BSI, Positionspapier: Cybersicherheit im Energiesektor Deutschlands.
[5] European Commission, Risk assessment report on cyber resilience on EU's telecommunications and electricity sectors (July 2024) and another Risk assessment announced by for the solar industry in response to written questions.
[6] Euractiv, Tech Commissioner Virkkunen favours regulation over directive for EU's telecom law reviewl.
[7] The NZIA cybersecurity pre-qualification criteria assess whether a manufacturer is subject to a jurisdiction requiring disclosure of software vulnerabilities to state authorities before they are known to be exploited; and whether it is based in a jurisdiction from which malicious cyber activities have been carried out against the Union or its Member States (Article 5 of Commission Implementing Regulation (EU) 2025/1176).
[8] BDEW, Positionen des BDEW Bundesverband der Energieund Wasserwirtschaft und VKU Verband kommunaler Unternehmen zum § 41 BSIG: (p.9).

bart.groothuis@europarl.europa.eu

Letter from MEPs to EU Commission

29 October 2025

Congress of the United States
House of Representatives
Washington, DC 20515-0906

November 14, 2025

The Honorable Howard Lutnick
Secretary of Commerce
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Dear Secretary Lutnick,

We write to express our deep concern regarding the growing risks to the United States electric grid posed by technologies designed, programed, and manufactured by adversarial nations. We urge the Department of Commerce to act swiftly to safeguard our grid and energy infrastructure from Chinese-made critical grid components and energy technologies that pose a severe threat to the safety of our constituents. As we work to achieve President Trump's vision of American energy dominance, it is vital that our critical infrastructure is not dependent on technologies that could be exploited to undermine U.S. national security.

The integration of critical grid technologies, such as utility-scale solar and battery inverters, sourced from foreign entities of concern pose unacceptable national security, economic, and supply chain risks. This is especially true as the United States faces historic electricity demand growth due to the AI revolution, new data centers, and increased industrial manufacturing places unprecedented strain on our grid. According to the Department of Energy's 2025 Resource Adequacy Report, expected retirements of existing generation capacity coupled with projected load growth increases the risk of power outages in 2030 by 100 times.

Earlier this year, a Reuters investigation revealed that certain Chinese-manufactured solar and batteries inverters deployed across the nation contained undisclosed communication devices. Experts warn that these "rogue" components could bypass firewall protections and enable malicious remote access, potentially allowing adversaries to destabilize large portions of the grid. Simultaneously, a growing body of Chinese academic research reveals a systematic and technically advanced focus on how to hack, harm, or even collapse Western power grids, particularly through the exploitation of Chinese-made technologies embedded in American grid infrastructure, including through the use of inverters. Increasing our reliance on China for inverters and critical grid equipment is a mistake, especially as we have ample supply domestically and from allied nations that would not expose our national security to unacceptable risks.

For these reasons, we respectfully request that the Department of Commerce exercise its authorities to restrict the future importation of such Chinese equipment and inverters for U.S. critical infrastructure. Such action would also align with the Trump Administration's broader objectives of strengthening domestic supply chains and protecting American workers and consumers. We appreciate your attention to this matter, and we stand ready to work with you and your team to ensure the security and resilience of our grid.

Respectfully,

August Pfluger
Member of Congress

Ben Cline
Member of Congress

Letter from Congress to Secretary of Commerce

14 November 2025

Conclusion

The Problem Won't Go Away

- The issue is not going to disappear on its own
- The sooner we act, the better

Progress is Being Made

- While the process is slow, there are signs of movement in the right direction in several member states
- Authorities and stakeholders are beginning to address the issues, though it will take time to implement the full solution.

Looking Ahead

- With the right framework in place, we can ensure that secure installations become the standard.
- This will not only enhance safety but also open up new opportunities for innovation and commercial solutions.

www.uceeb.cz