February 2025

CYBER SECURITY AND CRITICAL INFRASTRUCTURE

Dr Lars Schernikau

Content

The recent Carlyle report [1], The New Joule Order, is one of many reports showing that energy professionals are speaking out about the undeniable importance of energy security which is starting to take precedence over other concerns like cost and the environment.

During the annual CERA event in Houston in March 2025, it became clear that energy security trumps all other requirements. Even Dr. Fatih Birol from the IEA made a U-turn, now advocating for more fossil fuel investments [2], a stark contrast to previous net-zero pathway which called for an immediate stop to such funding.

US Energy Secretary, Christ Wright, also confirmed his commitment to having access to reliable energy…

Taking it one step further, one quickly realizes that ***security in relation to energy, and industry, is impossible without safeguarding critical infrastructure.*** And critical infrastructure is increasingly at risk due to cyber security concerns and geopolitical (in)stability.

Let us explore this issue a little further, digging deeper into the often underestimated threat of cybersecurity and what can be done to address it.

1. Critical infrastructure, and why is it relevant?

Critical infrastructure refers to the systems, facilities, and assets vital to the functioning of society and the economy. These are deemed critical as any disruption could greatly affect public safety, security, health, or economic stability.

A couple of everyday examples of critical infrastructure include our energy grids, transportation systems, water supplies, healthcare services, and communication networks. These elements are often interdependent, so disturbances in one area can trigger a ripple effects across others. I choose to focus on energy as without energy no other critical infrastructure can function.

Some of the essential systems and assets responsible for generating, transmitting, and distributing energy are:

- **Power plants:** Nuclear reactors, coal and gas-fired facilities, hydropower stations, solar fields, and wind farms.

Figure 1: Image from “Northeast Blackout: 20 years of infrastructure improvements”

- **Electricity transmission networks: High-voltage power lines and substations transporting electricity over vast areas.**
- **Oil and gas infrastructure:** Pipelines, refineries, storage depots, and offshore drilling sites.
- **Energy management systems:** Central control hubs that oversee energy flow across grids and networks.

Clearly, this infrastructure is essential for ensuring a stable energy supply.

So when we talk about the risks which threaten our energy supply we should consider ***weather conditions, natural disasters, sabotage, wars, and the mismanagement*** thereof, all of which puts the critical infrastructure at risk.

This was clearly illustrated by the Russian-Ukraine war, the North Stream pipeline explosion, the EstLink2 Power cable incident in 2024 between Finland and Estonia [3], the California wildfire and power shutoffs during 2021 and 2022 as well as the Texas grid failure with subsequent blackouts in 2021 due to a severe winter storm.

Weather also affected Israel in 2023 and 2024 causing what we call “loadshedding”…also seen for many years through to 2024 in South Africa, and in Lebanon since 2021, due to mismanagement of the energy supply reducing power availability.

Today’s high speed data transmission allows for a different level of virtualization, streaming, cloud computing, AI, blockchain and more. ***Data centers have come back under the loop because their electricity demand is becoming a serious issue to be considered.*** See my recent blog on datacenters and AI.

As advanced computer hardware increase efficiency, the total energy demand will continue to surge and make up an ever-increasing share of total power consumption, ***like in Ireland where data centers already account for over 20% of electricity demand*** [4].

Let’s take another example of the infamous ***New York blackout, that occurred on 14 August 2003, and affected over 50 million*** people across the northeastern US stretching as far as parts of Canada. It was recorded as one of the largest power outages in history, lasting up to 4 days in some areas.

The New York blackout stemmed mainly from a software malfunction of the alarm system in the control room at FirstEnergy's in Ohio [5]. Consequently, this issue prevented operators from identifying when to adjust power distribution as transmission lines came into contact with overgrown trees. What initially started as an issue in the control room, quickly sparked an escalation to a widespread grid failure, massively disrupting power generation and transmission across widespread regions.

But, during the past decade the new risk of ***cyberattacks emerged, quickly becoming a large concern threatening critical energy infrastructure.***

2. Recent examples of critical infrastructure cyber attacks

We can see an undeniable increase in the number of cyberattacks on critical infrastructure,,. causing governments to become more proactive in preventing such attacks. For example, Switzerland only recently introduced a mandatory reporting requirement for cyberattacks on critical infrastructure, effective 1 April 2025 [6] that did not exist before.
Here are some interesting examples of attacks on critical infrastructure during the past years, not a complete list [7]

- Ukraine Power Grid Attack (2015)
  - Hackers used the BlackEnergy malware to infiltrate SCADA systems, causing power outages for 225.000 people. The attackers also deployed KillDisk malware and denial-of-service tactics to delay recovery efforts.
- Israel Electricity Authority Cyberattack (2016):
  - A major cyberattack targeted Israel's electricity authority, prompting emergency measures to prevent widespread damage
- Saudi Petrochemical Plant Attack (2017)
  - A cyberattack targeted the emergency shutdown system of a Saudi petrochemical plant, potentially causing industrial accidents. The attack was attributed to Russian entities.
- Colonial Pipeline Ransomware Attack (2021)
  - The largest oil pipeline in the U.S. was shut down due to a ransomware attack by the Russian group DarkSide, causing fuel shortages and price hikes across the East Coast.
- Lithuania's Ignitis Group Attack (2022):
  - A cyberattack targeted the state-owned energy company, affecting its operation
- Oiltanking/Mabanaft, Ransomware attack (2022)
  - The attack affected the ability to load at ports and forced Shell to re-redirect supplies to other depots. Supply ships could not be loaded with oil and gas, affecting Aral petrol stations across Germany where other fuel had to be purchased
- Ukraine Power Grid Attack (2022)
  - Russian hackers targeted Ukrainian substations with OT-level techniques, causing power outages in four regions during missile strikes.
- ViaSat, Destructive attack (2022)
  - ViaSat, a US company, is used as a communications provider for very critical infrastructure both in Ukraine and other countries. The attack had the effect of disabling a large number of modems in Ukraine. The attack also affected 5,800 Enercon wind turbines in Germany as thousands of organizations across Europe.
- Nordex and Deutsche Windtechnik, Windturbine producer, Ransome attack (2022)
  - All IT systems were shut down and remote access to all turbines was interrupted.
- Russia launched several missile and drone attacks on Ukrainian energy infrastructure in 2023 and 2024.
  - One recent example was the combined missile and drone attack on 17 November 2024, when a large-scale operation targeted electrical substations transmitting power from nuclear power plants. Six of nine operational nuclear reactors had to reduce output due to grid instability. This led to the reintroduction of rolling blackouts across Ukraine, lasting between four to twelve hours daily

According to EnergiCERT [7] from 2020 until 2022 there were 40 successful attacks on European energy and utility companies, over 10 affecting critical infrastructure like industrial control systems. January 2023 and January 2024, critical infrastructure worldwide faced over 420 million cyberattacks-a 30% increase from the previous year—with energy grids being primary targets [8]. ***The sheer numbers of attacks are accelerating every year.***

In Jun 2024 a "virtual decoupling" of the European electricity market caused by "computer faults" caused prices to spike 3000%. Bloomberg [9] wrote

Although prices are typically set for whole nations — say, the German or French prices — the auctions consider not just national supply and demand, but also cross-border flows.
For example, Germany typically draws in French electricity. In the industry jargon, the European market is under normal circumstances "coupled" – an electron can travel, say, from Norway to Denmark and from there into Germany. A computer program – the "coupling algorithm" – keeps the European electricity market glued together, calculating flows and prices. Somehow, that crucial piece of market plumbing failed last week, resulting in what insiders call a "partial decoupling."

In August 2024, a cyber security firm reported that the Netherlands' solar energy grid with over 25 GW and 10s of millions of panels, making it one of the largest per capita in Europe, was found to be vulnerable to multiple types of cyberattacks. ***Hackers could manipulate solar panel inverters to create local power outages by overloading the grid.*** Although there was no major attacks reported, the vulnerabilities, in the form of risks of potential disruptions to solar energy production, which accounts for a significant portion of the Netherlands' electricity supply, were definitely highlighted. [8]

Experts predicted that such attacks, if combined with attacks on wind power or other systems, could lead not only to localized outages but also to financial losses

Figure 2: Image from NPR.org , Ukraine November 2024

Offshore wind farms in the Netherlands faced increasing cyber threats in 2024 attracting attention due to their growing importance in the energy mix. Experts furthermore reported a ***ten- to twenty-fold increase in cyberattack attempts*** since the start of the war in Ukraine, targeting the communication systems and operational technology used in wind turbines.

3. What makes energy systems vulnerable? What is the role of the "energy transition"?

I have written at length of the negative impact of grid scale wind and solar installations on the cost and reliability for our energy systems. Let's now consider the growing concerns relating to cyber security. What are the causes?

The ***main drivers that give room for increasing critical infrastructure vulnerability are digitization, decentralization, and complexity***. I break down all three below.

Digitization: it is obvious that a more connected and digitized world provides a broad base for more cyberattacks. Even very young hackers and more so government-controlled groups are able to seriously impact individuals, companies, and even entire countries negatively. Not only do these targets become easier to reach/hack through digitization and connectivity, but it has also become much cheaper and simpler, with the right know-how, to execute cyberattacks.

Take for example, an old coal-fired power station that has no internet connection is virtually impossible to hack. Furthermore the rotating mass of massive turbines can withstand and overcome short-term physical or electrical faults making them less vulnerable.

The emergence of artificial intelligence will simplify cyberattacks even more, see also my blog post on Electricity for Data Centers… is AI the driving force?

Decentralization: a centralized system is easier to control and protect than a decentralized system. Large decentralized systems need to use a more complex IT infrastructure and connectivity to be controlled, synchronized, and adjusted to changing demand. A centralized system has fewer points of attack and financial and human resources can be more efficiently use for protection.

Complexity: in a way complexity is a result of decentralization. However, here I am also speaking in principle of the increasing complexity of virtually all industrial and consumer infrastructure in our modern society. This complexity becomes especially apparent in our energy systems as digitization and decentralization require a vast, more complex and connected control infrastructure. Throwing in ***"demand management" and "smart grids" add another level of complexity.***

This IEA forecast (see figure below) on the increasing complexity of Chinese electricity systems in 2060 "Announced Pledges" scenario, illustrates how dramatically ***the "green energy transition" increases complexity and logically with-it decentralization and digitization.*** Therefore, in the absence of a "transition" towards a more complex wind and solar system, our systems would still be vulnerable, but notably less so!

The second issue is that ***a wind and solar based system does not merely increase complexity, but also increase the number of systems required*** and therefore leaves even more room for attacks. To truly and completely replace a single coal or gas fired power station with a wind or solar based system the following 5 systems are required… all of which with their own vulnerabilities.

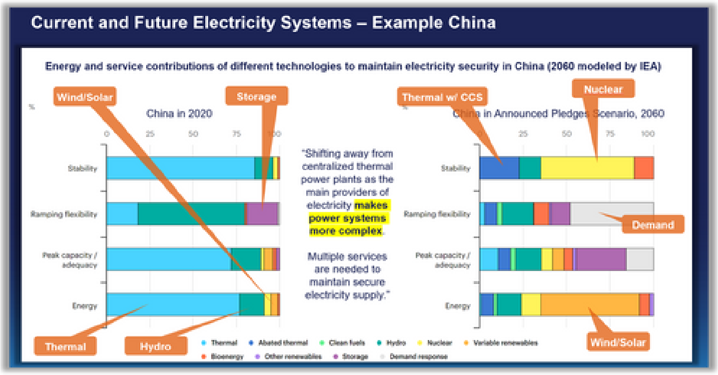
1. A vast ***overbuild*** of wind and solar to overcome the low natural capacity factor, resulting in low utilization, as well as the intermittency and unpredictability challenges and to charge any storage
2. ***Short duration energy storage***, in the form of batteries, to overcome short duration fluctuations and to balance the grid
3. ***Long duration energy storage***, envisioned in the form of hydrogen, to overcome days and weeks of insufficient combined wind and solar generation
4. ***Backup*** thermal power stations on standby when needed, in Germany 12-20GW of gas is required by 2030, in the future this backup is supposed to run on hydrogen
5. A vastly more complex and larger ***transmission network and integration infrastructure***

For more details on each of those 5 points and the impact on economies and society please refer to my recently published blog entry Are Wind and Solar up for the challenge?.

4. Point of attack: Inverters and Controllers

Where does the problem with wind and solar lie? Wind and solar installations are vulnerable because of the IT infrastructure required to condition and transform "useless" power into "useful" power so that it can be fed into the grid.
Wind turbines produce intermittent alternating current (AC) electricity that needs to be converted and "conditioned" or rectified. The alternating current from a wind turbine is not produced at a sufficiently stable voltage, frequency, or phase to feed directly into a grid.

Figure 3: Figure: IEA on increasing complexity in the "energy transition" scenario for China



Source: IEA – Energy Transitions Require Innovation in Power System Planning, January 2022

Figure 4: From Are Wind and Solar up for the challenge? – The Unpopular Truth

Schernikau on Energy Policy

Replace One „Dirty“ System with Five „Clean“ Systems?

Ancillary Systems

1. Solar or wind (overbuild?)
2. Short duration storage: batteries?
3. Long duration storage: hydrogen?
4. Security: thermal power plant on stand-by
5. Transmission, grids, „smart systems“

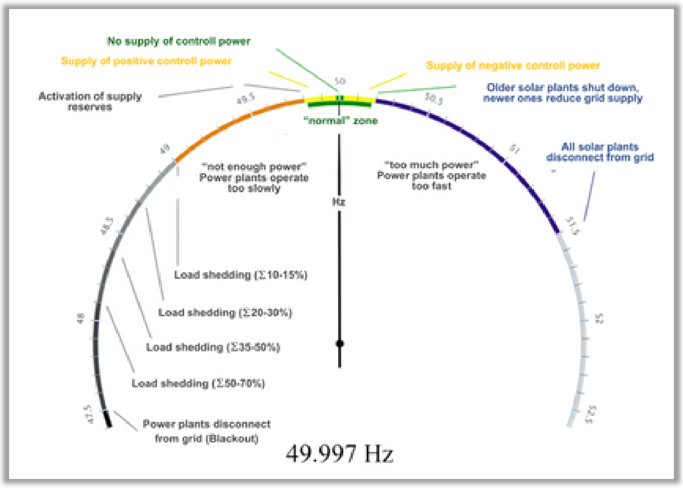
Typically, an offshore substation rectifies and sums the current from individual wind turbines and transmits it to land. A wind farm’s rectified electrical output must then be converted to the correct voltage, frequency, and phase before fed into a grid (more details see our book ***“The Unpopular Truth… about Electricity and the Future of Energy”*** Chapter 2.3. on “Transmission, distribution, conditioning, and black start”, www.unpopular-truth.com)

Solar panels “produce” DC power. However, our grid runs on AC, which alternates in polarity and voltage. Inverters not only convert DC power to AC power but they also synchronize the phase and frequency of the AC output with that of the grid’s. This ensures that the solar power becomes compatible with the grid and can be safely “fed into it”. Differences in phase and voltage can otherwise literally crash the grid. ***Power distributors and governments consider any deliberate attempts to bypass these grid safety measures as a threat to national security*** [Bitdefender 10].

These required ***inverters and controllers, or “power conditioning equipment” is exactly what hackers target***… as they are not only a plentiful but also an easy target. So many of them are not properly protected. Not only can you disrupt the power generated by solar, but you could literally impact and bring down the entire grid, if that is your goal. Remember that the grid shuts down when frequency vary to much as just 1 Hz difference from 50Hrz is enough to cause shutdowns, at 2,5 Hz the grid shuts off completely [11 and Figure].

If you are interested to understand inverters, watch this short movie “Connecting Solar to the Grid Is Harder Than You Think” [12] or read “Solar and wind power warning from the woman preventing South Africa’s Eskom grid collapse” [13].

Figure 5: Grid frequencies and its impact [11]


No supply of controll power
Supply of positive controll power
Supply of negative controll power
Activation of supply reserves
Older solar plants shut down, newer ones reduce grid supply
50
49.5
50.5
"normal" zone
49
51
All solar plants disconnect from grid
"not enough power" Power plants operate too slowly
"too much power" Power plants operate too fast
Hz
48.5
51.5
Load shedding (Σ10-15%)
Load shedding (Σ20-30%)
Load shedding (Σ35-50%)
Load shedding (Σ50-70%)
48
52
47.5
52.5
Power plants disconnect from grid (Blackout)
49.997 Hz

Bitdefender [13] researchers discovered critical vulnerabilities in the Solarman and Deye photovoltaic (PV) plant management platforms and pointed out more details about “How We Got Access to Enough Solar Power to Run the United States”. A worthwhile article to understand how easy it may be to infiltrate solar power management systems, I quote and summarize from there:

Solarman is one of the world’s largest photovoltaic (PV) monitoring and management platform, and equipment connected to this platform is apparently ***responsible for the production of over 195 gigawatts of power across 2M+ active PV plants*** involving “10M+ devices in 190+ countries and territories”.

Analysis shows that the Solarman API architecture has multiple entry points exposed for multiple companies selling inverters, data loggers and a wide range of PV equipment.

While most of Bitdefender previous findings have a serious impact on the individual or on the internet itself, the flaws detailed in the research are fundamentally different. Access to devices interacting with the grid can have devastating effects on the proper functioning of the grid itself. These vulnerabilities pose a significant threat to grid security in several ways:

- **Unauthorized Control:** Attackers can take over accounts and control solar inverters, disrupting power generation and potentially causing voltage fluctuations.
- **Data Breaches:** Sensitive information about users and organizations can be leaked, leading to privacy violations, information harvesting, targeted phishing attacks or other malicious activities.
- **Operational Disruptions:** By accessing and modifying settings on solar inverters, attackers can cause widespread disruptions in power distribution, impacting grid stability and potentially leading to blackouts

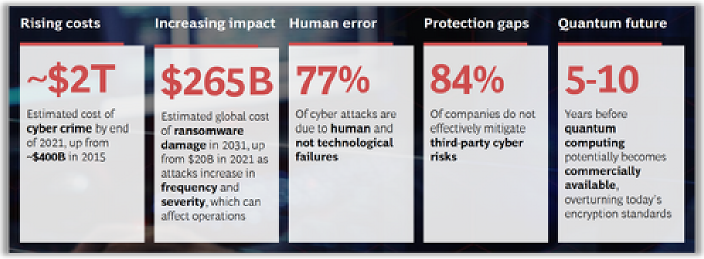
5. Summary

The critical infrastructure, as discussed above, is increasingly at risk and vulnerable to cyberattacks. These attacks can be mounted by individuals, companies, or can be government sponsored digital warfare and attacking critical infrastructure, as also experience in the Ukraine and other countries. Defense is becoming more complex.

We are already experiencing an exponential increase in attacks on critical energy infrastructure which is expected to continue and increase in the years to come. The key driver of this increasing vulnerability, seems to be linked to increasing digitization, decentralization, and complexity, all also a hallmark of the “green energy transition”.

The ***inverters and controllers required to condition wind and solar power into the grid is what vastly increases the vulnerability of our power systems*** and where cyber attackers are focusing on. Destabilizing the grid has becomes much easier the more wind and solar with have in our systems.

Figure 6: Ensuring Online Security in a Quantum Future



Rising costs

~$2T

Estimated cost of **cyber crime** by end of 2021, up from **~$400B** in 2015

Increasing impact

$265B

Estimated global cost of **ransomware damage** in 2031, up from $20B in 2021 as attacks increase in **frequency** and **severity**, which can affect operations

Human error

77%

Of cyber attacks are due to **human** and **not technological failures**

Protection gaps

84%

Of companies do not effectively mitigate **third-party cyber risks**

Quantum future

5-10

Years before **quantum computing** potentially becomes **commercially available**, overturning today's encryption standards

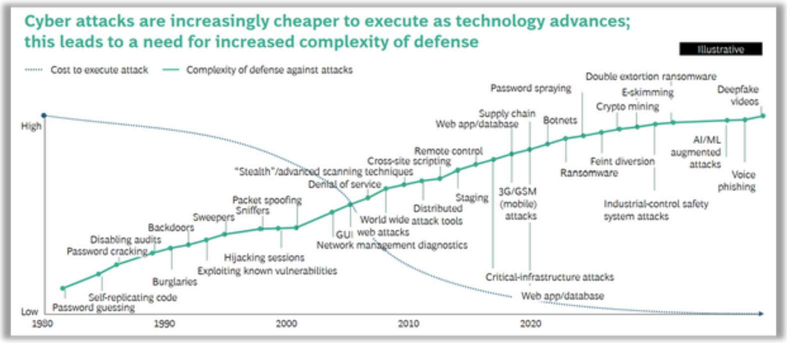
Source: BCG [14]

However, I remind here again that critical infrastructure goes beyond energy. Similarly, increasing risks exist with our ***transportation systems, water supplies, healthcare services, and communication networks. They are also more vulnerable because of increased digitization, decentralization, and complexity.***

Critical thinking becomes increasingly important in our fast-changing society. Protection of critical infrastructure should not be dismissed or underestimated. As the Boston Consulting Group already stated in 2022 "Global ***cost of cybercrime is projected to rise to $2.2T by the end of 2021***" that was 4 years ago, and "As cost to attack decreases, required complexity of defense increases".

A ***reduction of complex and expensive wind and solar systems would relatively reduce vulnerability*** and allow defensive resources to be utilized for centralized, efficient, and lower cost larger power plants and systems. See my published article (The Energy Trilemma) and our book **"The Unpopular Truth… about Electricity and the Future of Energy"** (here) that explains why wind and solar are neither economically nor environmentally desirable.
Let's prepare, strengthen our defenses, and become aware of the uncomfortable consequences of making our energy systems decentralized and more complex.

Figure 7: Cyberattacks become cheaper and require more complex defense | Source: BCG [14]



Source: BCG [14]

Links and Resources

[1] Security is now paramount (link)
[2] IEA chief sees need for investments in existing oil, gas fields (link)
[3] Seabed Cable Damaged in Latest Baltic CUI Incident (link)
[4] Chris Wright: "We need more energy. Lots more energy." (link)
[5] Northeast blackout of 2003 (link)
[6] Reporting cyberattacks on critical infrastructure mandatory (link)
[7] "Attacks-against-European-Energy-and-Utility-Companies," September 2022. (link)
[8] Europe's leading solar power grid is 'vulnerable' to hackers (link)
[9] "Bloomberg: Europe's Electricity Price Surge Highlights Market Weakness – Bloomberg," July 2024. (link)
[10] Ioan Alexandru. "60 Hurts per Second – How We Got Access to Enough Solar Power to Run the United States." Bitdefender Labs, August 2024. (link)
[11] netzfrequenz.info: Sep 2022, (link)
[12] Connecting Solar to the Grid Is Harder Than You Think, 2024. (link)
[13] "Eskom: Solar and Wind Power Warning from the Woman Preventing Eskom Grid Collapse," September 2024. (link)
[14] Switzerland – EN. "BCG: CEO Guide to Cyber Security," September 2021. (link)