DW

TOP STORIES / ENVIRONMENT

ENVIRONMENT

War in Ukraine highlights vulnerability of critical energy infrastructure

Keeping energy supplies safe from hackers is becoming more important, as countries decarbonize their economies and modernize electricity grids.

© Ina Fassbender/AFP/Getty Images

The power sector is vulnerable to cyberattacks

Minutes before Russian troops marched into Ukraine in late February, a satellite link connected to 5,800 wind turbines across Central Europe suddenly stopped working.

The turbines kept spinning, but they have since been running on autopilot and cannot be reset remotely.

"The communication services failed almost simultaneously with the start of the Russian invasion of Ukraine," wind turbine producer Enercon said in a press statement Tuesday. The exact cause of the malfunction is unknown, but the company, which has reported the case to Germany's Federal Office for Information Security (BSI), says it has ruled out a technical malfunction on its side. Neither Enercon nor the BSI responded to requests for comment.

As the Russian army pushes deeper into Ukraine, targeting civilians and shelling Europe's biggest nuclear power plant, and hackers take down government websites in waves of cyberattacks, the security of the Ukraine's power sector has been thrown into question. The war has inflamed tensions between Russia and the NATO alliance, shining a light on weak spots in the cybersecurity of global electricity supplies.

If enemy aircraft were dropping bombs on you, you'd expect your military to shoot them down, said Stuart Madnick, a computer scientist and cybersecurity expert at Massachusetts Institute of Technology in the US. "If a cyber terrorist is attacking a facility — causing consequential damage — you can't rely upon the government to protect you."

© Tristan Stedman/MHI Vestas

Renewable energy systems are less centralized and more connected to the internet than fossil fuel facilities

How have hackers struck energy systems?

In 2015, hackers allegedly backed by the Russian government breached Ukraine's power grid, disabling control systems and causing widespread outages in the capital, Kyiv, and western part of the country. It was the first publicly acknowledged case of a cyberattack taking out an electricity grid.

Similar attacks have since happened across the world.

Last year, hackers with links to a Russian ransomware group hit computerized equipment managing an oil pipeline in Texas in the US. The Colonial Pipeline Company, which owns the pipeline, halted operations and paid a ransom to restore the system.

In a 2019 survey of utility companies by German engineering firm Siemens, more than half of respondents reported attacks that caused at least one shutdown or operational data loss per year. The attacks "crippled" operations, the respondents said, causing power outages, damage, injury and environmental disasters. A quarter of the surveyed executives reported their companies having been hit by "mega attacks" in which the hacking "expertise was developed by nation states."

© Kevin G. Hall/ZUMA/imago images

In 2021, hackers took down the Colonial Pipeline in the US and demanded a ransom

Attacks on energy systems can happen at every stage of the supply chain, according to a 2020 report by management consultancy McKinsey. Electricity is often generated in aging infrastructure that was not designed with cybersecurity in mind. Transmission and distribution lines may have physical security weaknesses that allow access to grid control systems. Even in homes, the rise of smart meters and electric vehicles could open up vulnerabilities for disrupted services.

"There are thousands of ways that hackers could get into individual energy companies or transmission and distribution systems," said Don Smith, an environmental law expert at the University of Denver in the US state of Colorado, who has researched digital security in the energy sector.

As well as disrupting operations and causing blackouts, cyberattacks can also cause physical damage to equipment and infrastructure that lasts long after the attack has stopped. Scientists in US government labs have demonstrated attacks can electronically cause physical damage, said Madnick.

"If you have a generator explode or a turbine basically spin out of control and rip itself apart... you've got to replace it," he said. "And we're talking about often custom-built equipment that takes weeks, if not months, to replace."

© Roslan/ Rahman/AFP

Electricity grids are becoming cleaner and more connected as the price of renewable energy falls

Are renewables more at risk of cybercrime?

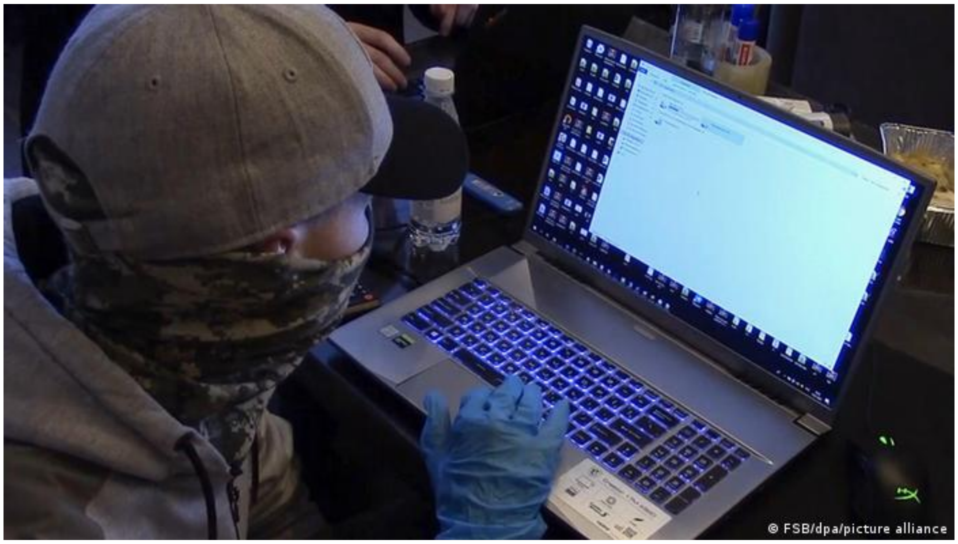
On a basic level, renewable energy sources like solar and wind farms are more vulnerable to cybercrime than traditional fossil fuel facilities because they are more connected to the internet.

Unlike fossil fuel power plants, which are centralized, renewable energy sources are distributed across larger areas and systems. That can be a boon in the case of an attack, because a successful strike may only take out a portion of the power. But it also exposes more weak spots.

Electricity generated by renewable energy sources is also often further away from the people who use it, which increases the need for transmission lines, and there are more individual pieces of equipment connected to each other.

Still, experts say fossil fuel facilities suffer from different vulnerabilities. Most coal, oil and gas plants are much older than renewable energy sources and were connected to the internet without a clear plan to fend off cyberattacks.

In many countries, the fossil fuel infrastructure was built decades, if not a century ago. "I don't think they had much protection against cyberattacks," said Madnick. "Maybe against bandits and cowboys, but not cyberattacks."



Russia's security services have at times cooperated with other countries to arrest hacker groups

How can governments protect their energy infrastructure?

Experts have warned that the world's biggest economies lack unified plans to protect their electricity grids from digital threats as they increasingly switch to renewable power. In the US, for instance, there is no federal cybersecurity strategy. "That doesn't make any sense in a country that is totally hooked together," said Don Smith.

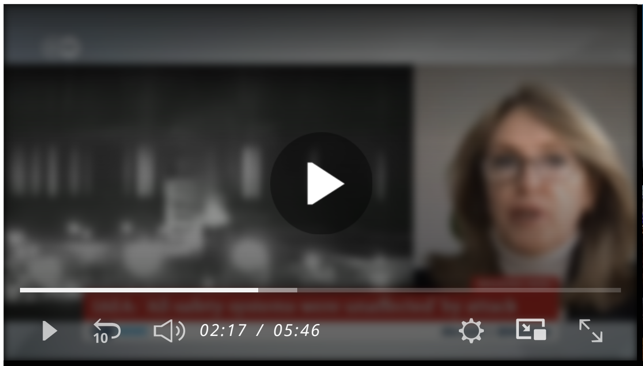
In the US, where electricity flows between states, and the EU, where it flows between countries, individual providers are exposed to the vulnerabilities of their neighbors. "Energy doesn't pay attention to state lines or to sovereign boundaries," said Smith. "It moves where the pipelines and the transmission lines are."

Because energy infrastructure is growing increasingly sophisticated and hackers are constantly finding new ways to gain access to infrastructure, there is no single blueprint for digital security.

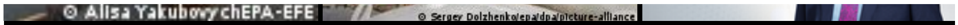
Still, experts say government, companies and individuals could all take actions to better protect themselves. For instance, companies could hire cybersecurity managers who are responsible for keeping up with developments in technology and probing systems for weak spots. Governments could introduce minimum cybersecurity standards for utility companies and require regular monitoring. Employees of energy companies could change their passwords regularly and check their devices for malware.

Together, they could look for weaknesses in systems before attacks occur, and not wait until it's too late, said Madnick.

"It's only when you have a serious storm that you realize the batteries in your flashlights are all dead," he said.



RANK
© Twitter: @Hartes_Geld / Twitter: @k388789 / Tiktok: @sxro0


© Alisa Yakubovych EPA-EFE
© Sergey Dolzhenko/epa/dpa/picture-alliance

Nuclear plant attack 'dangerous on many levels'

Edited by: Tamsin Walker

DW RECOMMENDS

» Opinion: The cyberwar over Ukraine is like nothing we've seen before

Hacktivists around the world have got involved in the Ukraine war. This is uncharted territory — and there is no telling what will happen next, writes DW's Janosch Delcker.