

Symposium energetického práva | 3.6.2026 | MUNI BRNO

Dopady komplexní geopolitické krize na evropskou elektroenergetiku pohledem bezpečnostní komunity

Erika Langerová
erika.langerova@cvut.cz

Vedoucí oddělení Energetické systémy a odolnost infrastruktury
Vedoucí týmu Bezpečnost strategické infrastruktury
ČVUT UCEEB

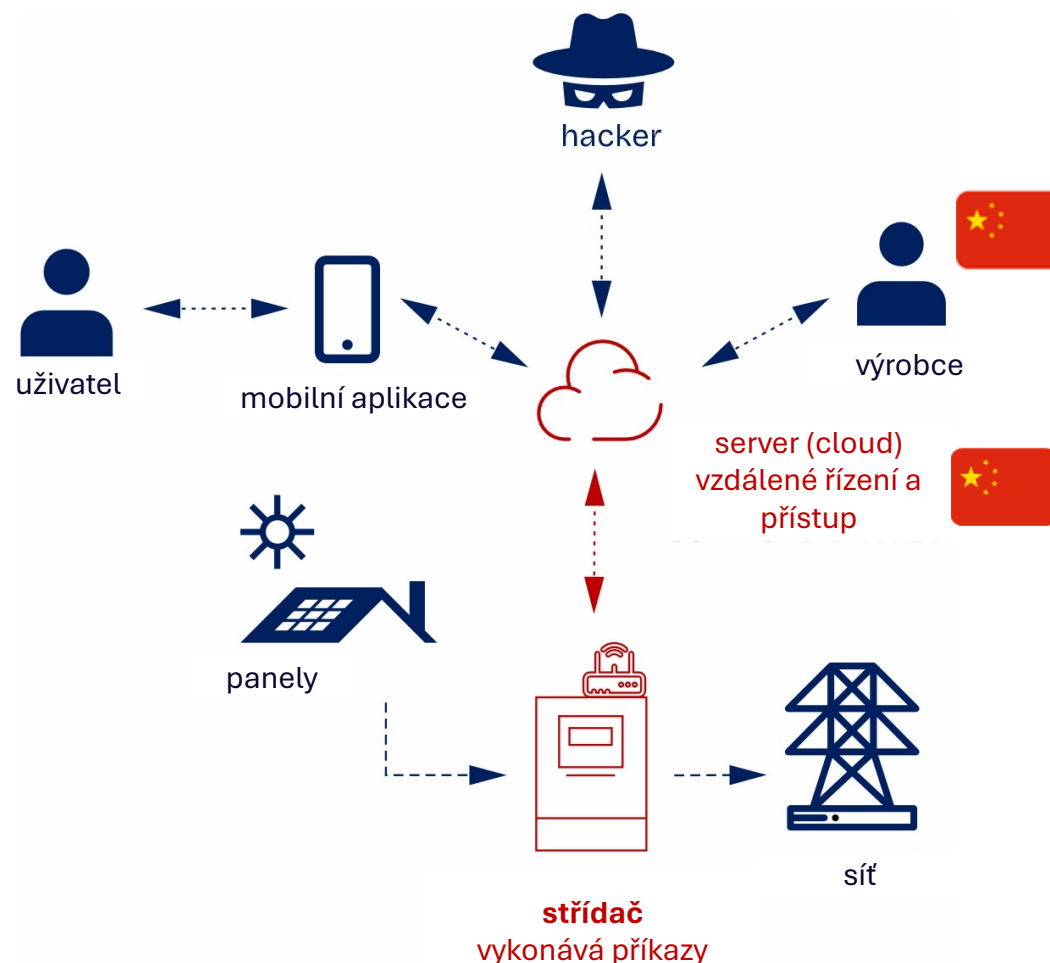
Kontext: Geopolitická krize

Energetická infrastruktura se stává stále častějším cílem fyzických útoků a kybernetických a špionážních operací.



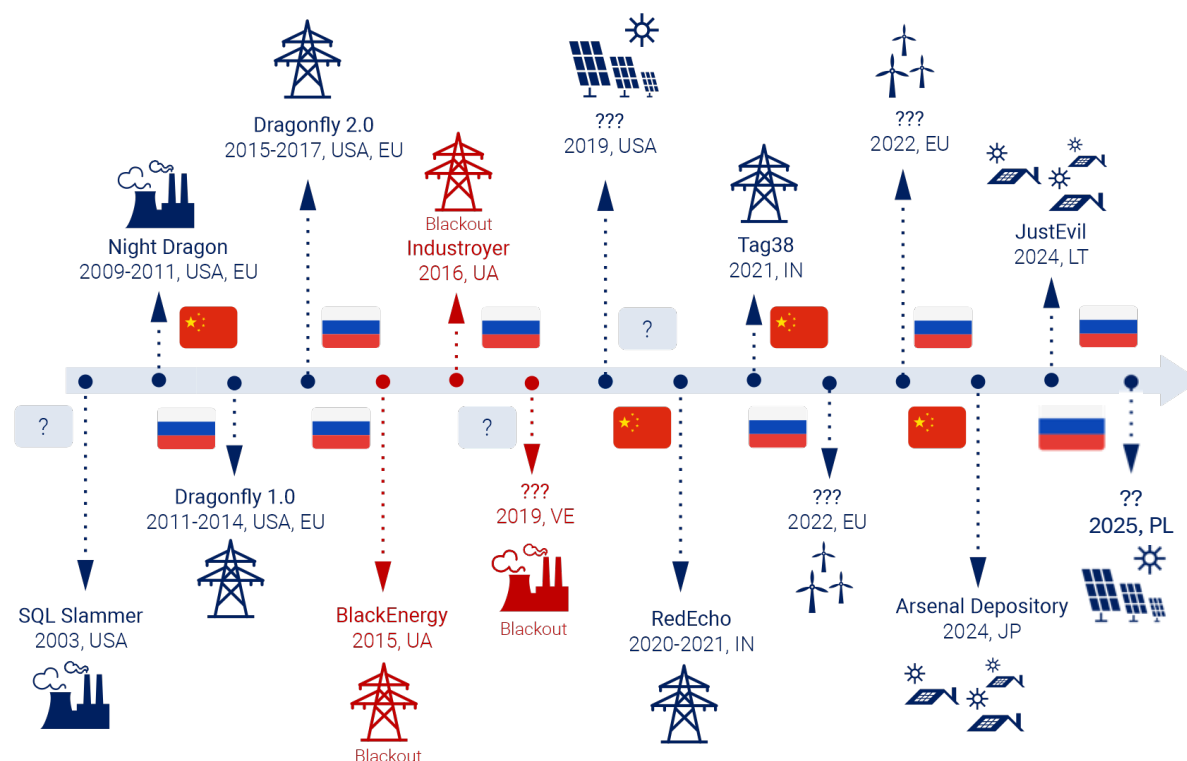
Kontext: Proměna evropské elektroenergetiky

- **Od ruských fosilních paliv k čínským technologiím (solární energie, větrná energie, baterie):** energetická závislost nezmizela, pouze změnila podobu.
- **Masivní růst obnovitelných zdrojů:** solární energetika, bateriová úložiště a větrné elektrárny jsou ve značné míře závislé na čínských dodavatelských řetězcích.
- **Digitalizace obnovitelných zdrojů:** chytré systémy, vzdálená správa a cloudové řízení se stávají běžnou součástí energetiky.
- **Nová zranitelnost:** možnost vzdáleného řízení vytváří nové cesty pro kybernetické a kyber-fyzické útoky



Kontext: Dopady krize do kyberprostoru

- **Čína a Rusko** stojí za téměř všemi veřejně známými úspěšnými operacemi zaměřenými na elektrizační soustavy.
- Ruské aktivity byly historicky typicky **destruktivní**, zatímco čínské se soustředily především na **špionáž, průzkum a budování přístupu**.
- V posledních letech: kampaně čínských hackerských skupin Volt Typhoon, Salt Typhoon a Flax Typhoon naznačují snahu **získat dlouhodobý přístup** ke kritické infrastruktuře pro případné **budoucí využití** (nátlakové, destrukční).
- V současnosti **nelze vyloučit**, že Čína v budoucnu nepřejde od špionážních operací k destruktivním.



zdroj dat: kompilace z otevřených zdrojů

Hrozba Ruska a Číny v evropské elektroenergetice

Evropská bezpečnostní komunita v zásadě nikdy nevedla spor o tom, jestli Rusko představuje pro elektroenergetickou infrastrukturu hrozbu.

Rusko prokazatelně:

- disponuje motivací,
- disponuje schopnostmi,
- opakovaně je využilo v praxi.

U Číny se spor dlouho vedl.

Část komunity kategoricky odmítala, že by Čína dnes nebo v budoucnu mohla představovala přímou bezpečnostní hrozbu pro evropskou elektroenergetickou infrastrukturu.

POLITICO

sis War in Ukraine Newsletters Podcasts Poll of Polls Policy news Events

NEWS > CYBERSECURITY AND DATA PROTECTION

Winter is coming. So are Russia's elite hackers.

Notorious "Sandworm" hacking group is targeting European energy grids, Google warns.

▶ LISTEN COPY LINK

POLITICOPRO Free article usually reserved for subscribers



One of Russia's most notorious hacking groups is targeting the continent's energy infrastructure. | Bulent Kilic/Getty Images

<https://www.politico.eu/article/russia-hackers-europe-winter-energy-infrastructure-moscow-gas-hike-digital/>

ENERGYWIRE

Russian government hackers blamed for major recent cyberattack on Polish energy grid

By Maggie Miller | 01/26/2026 07:13 AM EST

The Sandworm hacking group was previously tied to an attack 10 years earlier on the Ukrainian power grid that left thousands in the dark for hours.



The Russian flag flies over the Russian Embassy on Jan. 11 in Berlin, Germany. Sean Gallup/Getty Images

<https://subscriber.politicopro.com/article/eenews/2026/01/26/russian-government-hackers-blamed-for-major-recent-cyberattack-on-polish-energy-grid-ee-00744829>

Prudká změna vnímání hrozby Číny po roce 2025. Proč?

POLITICO

isis War in Ukraine Newsletters Podcasts Poll of Polls Policy news Events

NEWS > ENERGY AND CLIMATE

China poses major risk to Europe's energy grids, top NATO official warns

NATO increasingly sees energy vulnerabilities as a military risk.

▶ LISTEN COPY LINK

POLITICO PRO Free article usually reserved for subscribers



<https://www.politico.eu/article/china-poses-major-risk-to-europes-energy-grids-top-nato-official-radmila-sekerinska-warns/>

POLITICO

isis War in Ukraine Newsletters Podcasts Poll of Polls Policy news Events

NEWS > CYBERSECURITY AND DATA PROTECTION

Huawei's solar tech sparks fears of Europe's next dependency crisis

Cyber officials fear the Chinese tech giant's grip on energy networks.

▶ LISTEN COPY LINK

POLITICO PRO Free article usually reserved for subscribers



<https://www.politico.eu/article/europe-solar-industry-having-huawei-moment/>

POLITICO

isis War in Ukraine Newsletters Podcasts Poll of Polls Policy news Events

NEWS > CYBERSECURITY AND DATA PROTECTION

Capitals fear power grab as Brussels drafts law to root out Chinese tech

New EU proposal seeks to cut untrusted tech vendors from critical supply chains.

▶ LISTEN COPY LINK

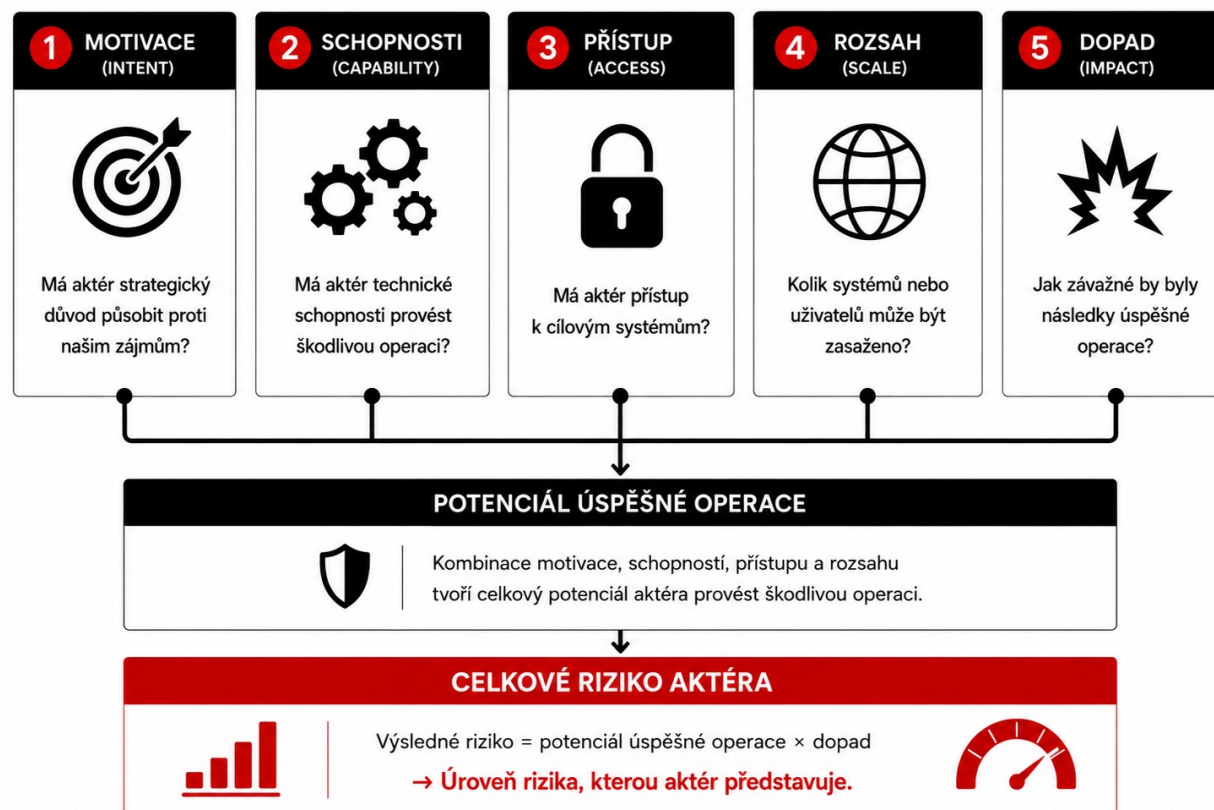
POLITICO PRO Free article usually reserved for subscribers



<https://www.politico.eu/article/capitals-fear-power-grab-brussels-drafts-law-root-out-chinese-tech/>

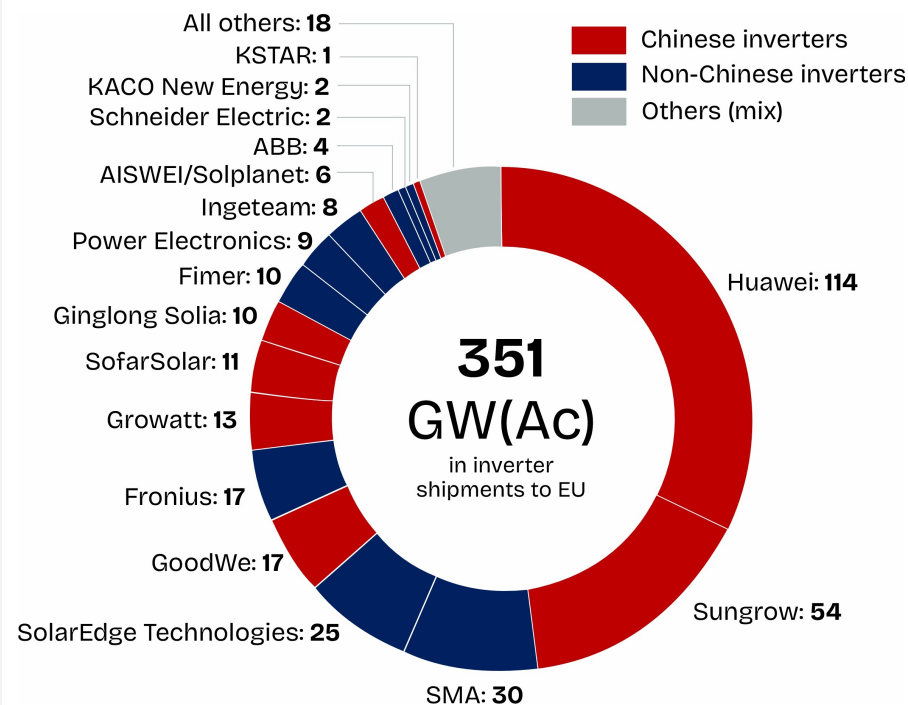
Přehodnocení čínské hrozby

- Hrozbu neurčuje jeden faktor, ale kombinace motivace, schopností, přístupu, rozsahu a dopadu.
- Zatímco u ruských aktérů byla tato kombinace dlouhodobě zřejmá, u čínských byly historicky zpochybňovány především motivace, přístup a rozsah.
- V posledních letech však všechny tři faktory významně vzrostly, což vede k zásadnímu přehodnocení celkového rizika.
- V některých parametrech je dnes Čína srovnatelná s Ruskem, v jiných jej může i překonávat.



Přístup, rozsah a dopad možných aktivit ČLR

- Čínský zákon o národní zpravodajské činnosti obsahuje kontroverzní článek 7, který ukládá občanům i organizacím **povinnost podporovat a napomáhat činnosti státních zpravodajských služeb**.
- Výrobce by mohl být **donucen poskytnout plný vzdálený přístup** ke spravovaným zařízením, včetně možnosti vzdáleného vypnutí a jiných citlivých mechanismů.
- Za současných čísel instalovaného výkonu solárních elektráren je **scénář vyvolání blackoutu** skrze střídače solárních elektráren a bateriových uložišť zcela reálný
- Byly provedeny dvě rozsáhlé simulační studie.
- **Závěry studie DNV:** Masivní manipulace se střídači a náhlé změny napěťových profilů (induktivní/kapacitní jalový výkon) mohou mít kritické dopady na stabilitu elektrizační soustavy v synchronní oblasti kontinentální Evropy.
- **Závěry studie ČSRES:** Současný stav představuje riziko pro bezpečný provoz české elektrizační soustavy a je nezbytné začít přijímat opatření ke zmírnění tohoto rizika.



Ekvivalent instalovaného výkonu cca 200 Temelínů

Dodávky fotovoltaických střídačů do Evropy v letech 2015–2023 (v GW AC),
zdroj: SolarPower Europe, Solutions for PV Cyber Risks to Grid Stability

Schopnosti

WIRED

SUBSCRIBE

ANDY GREENBERG SECURITY SEP 12, 2023 6:00 AM

China-Linked Hackers Breached a Power Grid—Again

Signs suggest the culprits worked within a notorious Chinese hacker group that may have also hacked Indian electric utilities years earlier.



<https://www.wired.com/story/china-redfly-power-grid-cyberattack-asia/>



<https://www.recordedfuture.com/research/continued-targeting-of-indian-power-grid-assets>

China seeks long-term vulnerabilities in US energy systems: House panelists

“Today’s electricity grid is too often a hodgepodge of digital tools sitting atop an analog foundation, creating seams where adversaries can slip in,” Carnegie Mellon’s Harry Krejsa said.

Published Dec. 3, 2025



Ethan Howland
Senior Reporter

Share License Add us on Google



Michael Ball, CEO of the Electricity Information Sharing and Analysis Center and senior vice president at the North American Electric Reliability Corp., speaks at a hearing held by the House Energy and Commerce Committee’s energy subcommittee in Washington D.C. on Dec. 2, 2025. Retrieved from [U.S. House Energy and Commerce Committee](https://www.house.gov/committees/energy-and-commerce/).

<https://www.utilitydive.com/news/china-energy-utility-cyber-threat-typhoon/806893/>

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

Schopnosti: Čína modeluje útoky na západní sítě již přes 20 let

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 Technology, Guangzhou University, Guangzhou, China

Dawei Zhao

Shandong Provincial Key Laboratory of Computer Network, Shandong Computer Science Center, Jinan, China

Attacks are induced to
which also can describe
length of shortest

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.

NUDT is the best-funded military university in China !

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点实验室)

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

Motivace

Home → Simultaneous Threat: How NATO Prepares for a Two-Front Scenario



Explainers

Simultaneous Threat: How NATO Prepares for a Two-Front Scenario

26.12.2025

Share: [Twitter](#) [Facebook](#) [Instagram](#) [Pinterest](#) [Email](#)

Contents:

- [1. The Scenario of Simultaneous Escalation](#)
- [2. NATO's Multi-Layered Deterrence](#)
- [3. Conclusion](#)

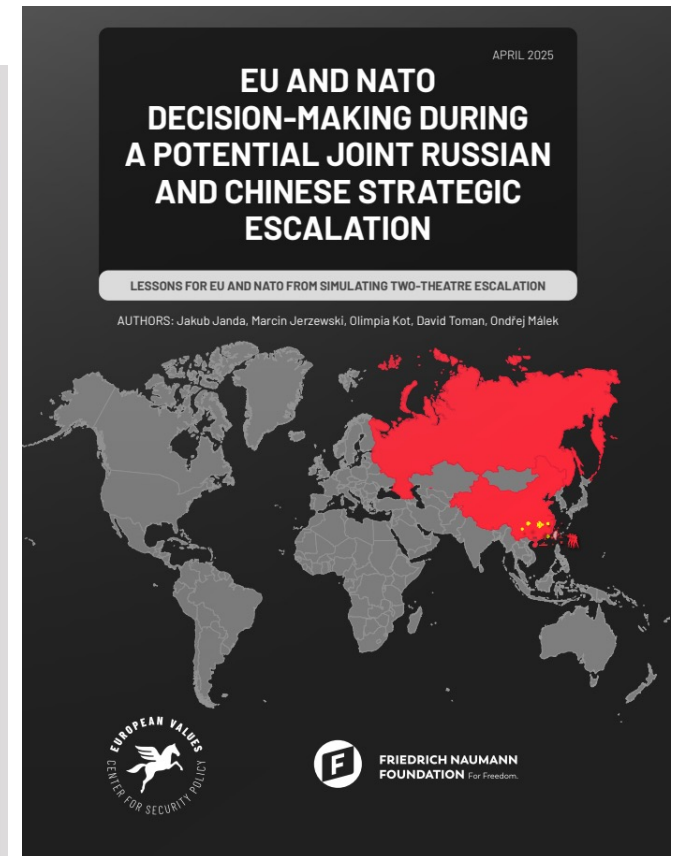
The world is gradually entering a phase of security instability, increasingly compared to the periods of global conflict in the 20th century. NATO Secretary General Mark Rutte has warned that the international system may face its most dangerous scenario since World War II. At issue is the possibility of simultaneous aggression by Russia and China—in Europe and around Taiwan. According to him, these processes are not isolated and could mutually reinforce one another. China is closely monitoring Russia's war against Ukraine and the West's reaction. In the event of an escalation in the Indo-Pacific region, Moscow could seize the moment for a new offensive in Europe. It is this logic of events that is compelling NATO to prepare for a two-front scenario.

<https://theukrainianreview.info/simultaneous-threat-how-nato-prepares-for-a-two-front-scenario/>



China and Russia agree joint statement on Further Strengthening Comprehensive Strategic Cooperation and Deepening Good-Neighbourliness and Friendly Cooperation

<https://socialistchina.org/2026/05/25/china-and-russia-agree-joint-statement-on-further-strengthening-comprehensive-strategic-cooperation-and-deepening-good-neighbourliness-and-friendly-cooperation/>



https://europeanvalues.cz/wp-content/uploads/2025/06/REPORT_EN_EU_and_NATO_decision-making_during_joint_Russian_and_Chinese_strategic_escalation-April_2025.pdf

Závěr

- Hodnocení rizik spojených s Čínou prochází v posledních letech zásadní změnou.
- Rostoucí motivace, přístup, rozsah a potenciální dopady vedou k přehodnocování dosavadních předpokladů.
- Riziko již není vnímáno pouze jako otázka špionáže a ekonomického vlivu.
- Promítá se do bezpečnostních varování, národních strategií a regulatorních opatření.
- Stále více států přijímá omezení nebo bezpečnostní požadavky vůči čínským technologiím v kritické infrastruktuře.
- Přehodnocení rizika se již stává součástí evropské i národní legislativy a bezpečnostní politiky.

South China Morning Post

China-EU relations Economy / China Economy

Brussels bans Chinese inverters from EU-funded power projects

3-MIN READ

Make SCMP preferred on Google



<https://www.scmp.com/economy/china-economy/article/3352435/brussels-bans-chinese-inverters-eu-funded-power-projects-connected-european-grid>

TLP: CLEAR

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.j.: 6913/2025-NÚKIB-E/630 • BRNO • 25. SRPNA 2025
ANALÝZA HROZBY

ČÍNSKÉ STŘÍDAČE V MALÝCH FOTOVOLTAICKÝCH ELEKTRÁRNÁCH PŘEDSTAVUJÍ POTENCIÁLNÍ BEZPEČNOSTNÍ HROZBU, OD VZDÁLENÉ MANIPULACE A OHROŽENÍ ELEKTROENERGETICKÉ SÍTĚ PO ZNEUŽITÍ DAT

SHRNUTÍ

- Střídače jsou chytrým prvkem fotovoltaických elektráren (FVE), který převádí stejnosměrný proud na střídavý a posílá ho do domácnosti či distribuční sítě. Prostřednictvím data loggerů, vestavěných komunikačních rozhraní nebo systémů třetích stran (tzv. energetických manažerů domácnosti) jsou připojeny k internetu a na dálku spravovány výrobci, servisními společnostmi a koncovými uživateli, včetně možnosti spuštění, vypnutí a vzdáleného přehrávání firmwaru za provozu. Většina výrobců asymetrických střídačů vhodných pro malé FVE v ČR jsou čínského původu.
- V případě dodavatelů z Čínské lidové republiky (ČLR) vznikají rizika s ohledem na ochranu dat a v krajním případě i možnou vzdálenou manipulaci. Střídače mohou být zranitelné i vůči kybernetickým hrozbám, od sběru a zneužití dat uživateli po možnost škodlivé aplikace či aktualizace firmwaru. Aspektem rizik spojených se sběrem dat se zabývá i varování NÚKIB, které upozorňuje na vysokou hrozbu spojenou s předáváním systémových a uživatelských dat do ČLR a jejich zvláštních administrativních oblastí, a metodika k tomu vydaná.
- Čínské legislativní prostředí přikazuje součinnost čínských společností se státem. To, v kombinaci s nezanedbatelným množstvím případů pochybení v oblasti nakládání s osobními údaji uživatelů služeb či aplikací pocházejících z ČLR, dává důvod k obavám o bezpečnost střídačů spravovaných čínskými firmami.
- S rostoucím podílem solární energie na energetickém mixu získá koordinované vzdálené odpojení, připojení či manipulace s pokročilými provozními funkcemi potenciál poškodit chod celé distribuční sítě. Proto je třeba učinit kroky pro to, aby se toto riziko minimalizovalo, např. skrze diverzifikaci dodavatelů.

UPOZORNĚNÍ: Informace a závěry obsažené v této analýze vycházejí z veřejně dostupných informací a z informací získaných v rámci činnosti NÚKIB v době publikace. Jedná se o analýzu kybernetické bezpečnosti z pohledu NÚKIB na základě jemu dostupných informací.

Česká energetika během posledních let v domácí produkci elektřiny pozoruje nárůst segmentu fotovoltaických elektráren (FVE), s čímž se pojí i nová rizika. V letech 2022 a 2023 skokově narostla výroba elektřiny prostřednictvím především tzv. „malých“ FVE (viz Box 1). S rostoucím podílem výroby solární

elektřiny pomocí těchto malých, převážně domácích FVE však roste i význam hrozeb s nimi spjatými.

STŘÍDAČ JAKO TZV. CHYTRÝ, A TUDÍŽ I ZRANITELNÝ, KOMPONENT MALÝCH FVE

Zásadním, a téměř vždy jediným „inteligentním“ komponentem FVE, je střídač (anglicky power inverter). Ten převádí stejnosměrný proud z fotovoltaické elektrárny na střídavý proud a následně směřuje elektřinu do domácnosti či sítě. Malé FVE jsou v ČR vybavovány tzv. asymetrickým střídačem, který dokáže alokovat vyrobenou energii podle reálné potřeby domácnosti nebo firmy, což umožňuje

Box 1: Vzestup tzv. malých FVE v ČR

Malé FVE jsou elektrárny o výkonu do 10kW, mezi něž patří především střešní solární elektrárny na rodinných domech, ale i na malých firmách či veřejných budovách. Jejich meziroční nárůst činil v uplynulých letech 158 % (2022) a 172 % (2023).¹

https://nukib.gov.cz/download/uredni_deska/2025-09-03_Varovani_predavani-dat-podepsano.pdf



www.uceeb.cz