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 uživatelů 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 jejích 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.**

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] Podíl elektřiny vyrobené FVE se v roce 2023 dostal na 4 %, přičemž vzestupný trend pokračoval i vloni.[2]

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 spotřeby domu tak, aby byla co nejlépe využita.[3] V tuzemském prostředí s fázovým měřením je využití asymetrických střídačů u malých FVE finančně

výhodnější, protože v ČR může být elektřina dodávaná do sítě z FVE odkupována za výrazně nižší cenu, než ta odebíraná od dodavatele (viz Příloha 3).[4]

Jelikož se asymetrické střídače pro malé FVE používají převážně na malém českém trhu, chybí zde konkurence a téměř všichni výrobci (až okolo 95–99 % zařízení) pocházejí z Čínské lidové republiky (ČLR).[6] Západní konkurence je v současnosti natolik cenově nepříznivá, že pro zákazníka de facto nepřipadá v úvahu.[7] Jak hardware, tak software u malých FVE v ČR je proto typicky čínský.[8]

Box 2: Měření a střídače – specifika v ČR

V ČR se na rozdíl od většiny Evropy (s výjimkou Slovenska a Portugalska) provádí měření i účtování spotřeby energie po tzv. fázích.[5] Asymetrické střídače jsou tomuto systému uzpůsobeny, jelikož přesněji měří, kdy dochází k odběru elektřiny z distribuční sítě a kdy k dodávkám elektřiny ze solárních panelů do distribuční sítě. Ve většině zemí (se součtovým měřením) se využívají symetrické střídače.

STŘÍDAČE ČÍNSKÉHO PŮVODU NESOU ZVÝŠENÁ RIZIKA PRO DISTRIBUČNÍ SÍŤ I DŮVĚRNOST DAT

Střídače jsou připojené na internet pomocí tzv. data loggerů, vestavěných komunikačních rozhraní, nebo systémů třetích stran (tzv. energetických manažerů domácnosti) pomocí kterých mohou výrobci, servisní společnosti a koncoví uživatelé dálkově spravovat střídač. V případě asymetrických střídačů od dodavatelů z ČLR vznikají rizika s ohledem na ochranu dat a možnou vzdálenou manipulaci, která může mít vliv na chod distribuční sítě.[9]

Data logger (nebo jeho ekvivalent), je součástka připojená ke střídači, která zajišťuje připojení na internet. Ve většině případů je připojení zajištěno přes Wi-Fi či LAN kabel, či přes datové připojení pomocí SIM karty. Přes něj pak zadává příkazy výrobce a případně i další třetí strany, typicky servisní společnosti. Dle informací od partnerů NÚKIB je prodloužená desetiletá záruka na střídače od výrobců podmíněna tím, že jsou připojené k data loggeru, který v pravidelných intervalech posílá data o činnosti střídače na servery do ČLR a umožňuje ovládání FVE na dálku. Tento požadavek je do jisté míry legitimní, protože opravy a údržba se řeší vzdáleně a výrobce přístup potřebuje pro řešení závad.[10]

FVE jsou specifické tím, že je možné je téměř okamžitě zapnout a vypnout. **Tato funkcionalita ale přináší riziko možného zneužití, vedoucí k přetížení sítě nebo výpadkům, pokud by chtěl útočník dosáhnout narušení distribuční sítě.[11] Schopnost náhle vzdáleně vyřadit střídač z provozu dokládá loňský případ, kdy čínská společnost Deye bez předchozího vědomí či souhlasu uživatelů odpojila střídače v USA a dalších zemích. Informace o důvodu odpojení se v dostupných zdrojích různí.[12]**

Existují obavy i z dalších rizik zneužití data loggeru. Ačkoli účelem data loggeru je odesílat provozní data dodavateli a výrobci, škodlivý aktér by touto cestou mohl získat a následně zneužít data o činnosti organizace, která FVE využívá – například množství produkované a využité elektřiny v konkrétních časových úsecích pro obchodní účely či vytipování kritických momentů pro optimalizaci potenciálního koordinovaného útoku. Touto cestou by mohl také objevit zranitelnost FVE.[13] Zásadním problémem je též riziko nedostatečného zabezpečení zařízení výrobcem. Již v roce 2023 střídače společnosti Deye postrádaly zásadní bezpečnostní komponent a nesplňovaly tak německé standardy.[14]

Ve střídači lze zároveň měnit firmware a aktualizovat jej dle potřeby, což se zejména na počátku jeho zavedení děje pravidelně. **Zákazník ani český distributor do těchto aktualizací nevidí a nedokáže určit, zda mohou být škodlivé, obsahovat backdoor apod.** Dalším zranitelným místem pro uživatele může být aplikace (od mobilních po webové), která zákazníkovi poskytuje monitoring produkce elektrárny. Podobně jako u jiných aplikací zde existuje riziko sběru dat nad míru potřeb aplikace či možnost kompromitace střídače či zařízení uživatele skrze aplikaci. Závažnost tohoto scénáře dokresluje skutečnost, že již byl zaznamenán případ úniku přihlašovacích údajů k řádově tisícům solárních elektráren po celém světě, přičemž uniklá data byla nabízena k prodeji na darkwebu.[15]

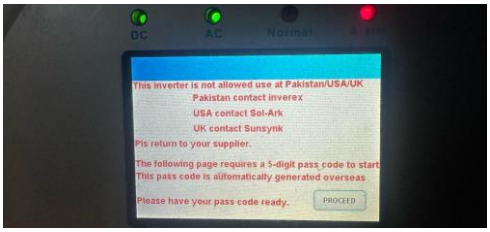
Další neméně závažný problém se týká přístupu výrobců k opravám zranitelností. U části čínských výrobců se doba od přijetí ohlášení o zranitelnosti do vydání opravy často pohybuje v řádu několika měsíců, a v některých případech výrobce na výzvy k opravě dokonce nereaguje vůbec.[16]

Výsledkem je, že v současné době v elektroenergetické síti existuje určité nezanedbatelné procento čínských střídačů připojených k serverům čínských výrobců, na kterých se nacházejí neopravené kritické chyby.

Tyto chyby mohou v případě zneužití umožnit útočníkovi vzdálené převzetí kontroly nad celými flotilami malých střídačů. Útočník pak může na dálku hromadně měnit provozní parametry, zapínat a vypínat střídače nebo do nich nahrávat škodlivý firmware.[17]

V neposlední řadě existuje možnost použít samotný střídač připojený na domácí Wi-Fi jako vektor pro útok na síť domácnosti či společnosti, do které je připojen, a kompromitovat jiná zařízení v síti.[18]

Obr. 1: Notifikace o odpojení střídače Deye



Zdroj: solarboi.com

ČÍNSKÉ LEGISLATIVNÍ PROSTŘEDÍ A NEGATIVNÍ ZKUŠENOSTI S OCHRANOU DAT UŽIVATELŮ ZE STRANY ČLR DÁVÁ DŮVOD K OSTRAŽITOSTI

V případě, že by ČLR měla motivaci provést destabilizační či destruktivní útoky na českou elektroenergetickou síť, skrze čínské dodavatele by díky tamnímu legislativnímu prostředí za stávajícího stavu téměř jistě (90–100 %) disponovala schopností, jak takového cíle dosáhnout.

Čínské právní prostředí přikazuje součinnost čínských společností se státem. Charakteristickým prvkem legislativy ČLR a čínského pojetí státní bezpečnosti je široce definovaná povinnost každého občana a organizace podílet se na zajištění státní bezpečnosti a spolupracovat se státními orgány. Tato povinnost je definována v zákonech ČLR (viz Příloha 4). **Čínské společnosti jsou povinny spolupracovat s čínským režimem a dodávat mu na vyžádání citlivé informace, případně mu poskytnout součinnost.** Komunistická strana Číny navíc ustanovuje mechanismus vlivu na čínské soukromé společnosti prostřednictvím tzv. stranických buněk, které je povinné dle **Zákona o společnostech** ustanovit v každé společnosti zahrnující alespoň tři členy strany. [19] Strana tak disponuje přímou linkou do společností a téměř jistě (90–100 %) jí to umožňuje mít vliv na jejich chod. ČLR zároveň vynakládá značné úsilí pro sběr informací o zranitelnostech nultého dne (vč. ustanovení zákonné povinnosti nahlašovat je státu) a je velmi pravděpodobné (75–85 %), že je využívá pro státem sponzorované ofenzivní kybernetické aktivity.[20]

Globálně je evidována řada případů pochybení ohledně nakládání s osobními údaji uživatelů služeb či aplikací pocházejících z ČLR. Jedná se o zneužití dat uživatelů aplikací TikTok a WeChat či zneužívání zranitelností v rámci aktivit čínských státem sponzorovaných skupin. [21] V kybernetickém prostoru jsou zdokumentovány i aktivity s cílem přípravy operačního prostředí (tzv. prepositioning, tedy získání dlouhodobého přístupu a vytvoření výhodné pozice v cílených systémech pro případ budoucího konfliktu). [22] **Důvody výše a případy upřednostnění geopolitických zájmů Pekingu na úkor bezpečnosti uživatelů v zahraničí dává důvod k pochybnostem o bezpečnosti FVE střídačů ve správě čínských dodavatelů.**

S ROSTOUCÍM PODÍLEM MALÝCH FVE POROSTE I HROZBA SPOJENÁ S NEDŮVĚRYHODNÝMI DODAVATELI

Malé FVE tvoří stále větší podíl celkové produkce energie v ČR a tento trend bude výhledově pravděpodobně (55–70 %) pokračovat.[23] **S rostoucím podílem na energetickém mixu získá koordinované vzdálené odpojení či připojení většího počtu FVE potenciál poškodit chod celé distribuční sítě. Střídače jsou navíc běžně vybaveny pokročilými funkcemi, které mají za běžného provozu pomáhat stabilizovat elektrickou síť. Pokud by však došlo k jejich cílenému zneužití, mají potenciál se z mechanismu určeného k udržení stability stát spouštěčem rozsáhlé nestability.** [24] Dramatické propady či přerušení v produkci elektřiny (ať úmyslným zásahem nebo poruchou) mohou mít dalekosáhlé, ne-li destruktivní následky pro distribuční síť. **V současnosti je naše soustava na hranici hodnot, které je schopna v takovém scénáři pokrýt (3 000 MW).**[25]

V neposlední řadě je třeba zohlednit i riziko útoků s fyzickými dopady. Útočník může například do střídače nahrát škodlivý firmware, kterým zablokuje chod chladicího ventilátoru střídače, nebo zneužít jiné funkce tak, aby způsobil selhání střídače. Takové zásahy mohou vést k trvalému poškození střídače, a v krajním případě (při souběhu více okolností) dokonce k až vyvolání požáru. [26]

Tato rizika se budou vztahovat i na kritickou infrastrukturu či instituce strategického významu, jež jsou připojené (a tudíž odkázané) na distribuční síť či přímo napojené na malé FVE. Je proto nutné zajistit maximálně zabezpečenou a spolehlivou síť FVE.

DOPORUČENÍ

Vzhledem k vzrůstajícímu podílu solární energie v distribuční síti ČR, a především exponenciálnímu nárůstu malých FVE je třeba začít řešit otázku střídačů čínského původu a robustnosti distribuční sítě. **Malé FVE je třeba chápat jako součást české národní distribuční sítě, a tedy klíčový aspekt národní bezpečnosti.** Vzhledem ke skutečnosti, že se ČR dlouhodobě nachází v oblasti zájmu čínských zpravodajských služeb, může stávající situace v případě vyostření geopolitické situace představovat bezpečnostní riziko pro kritickou infrastrukturu státu.

ČR by měla jednat proaktivně a zasadit se o to, aby čínské střídače nebyly de facto jedinou možností pro spotřebitele – pomocí regulací či jiných nástrojů. Možnou cestou je změna z fázového na součtové měření v ČR, což by umožnilo přechod z asymetrických na symetrické střídače, ačkoli průchodnost této cesty je v současnosti nejistá. I v případě symetrických střídačů ale existuje mnoho čínských dodavatelů a bylo by třeba nastavit regulatorní opatření omezující využívání symetrických střídačů z ČLR.

Jedním z řešení pro asymetrické střídače, která jsou v současnosti diskutována, je zákaz podmiňování záruky připojením k čínskému data loggeru a jejich nahrazení data loggerem evropským. Legalitu a proveditelnost takového postupu by musely posoudit relevantní české a evropské instituce.

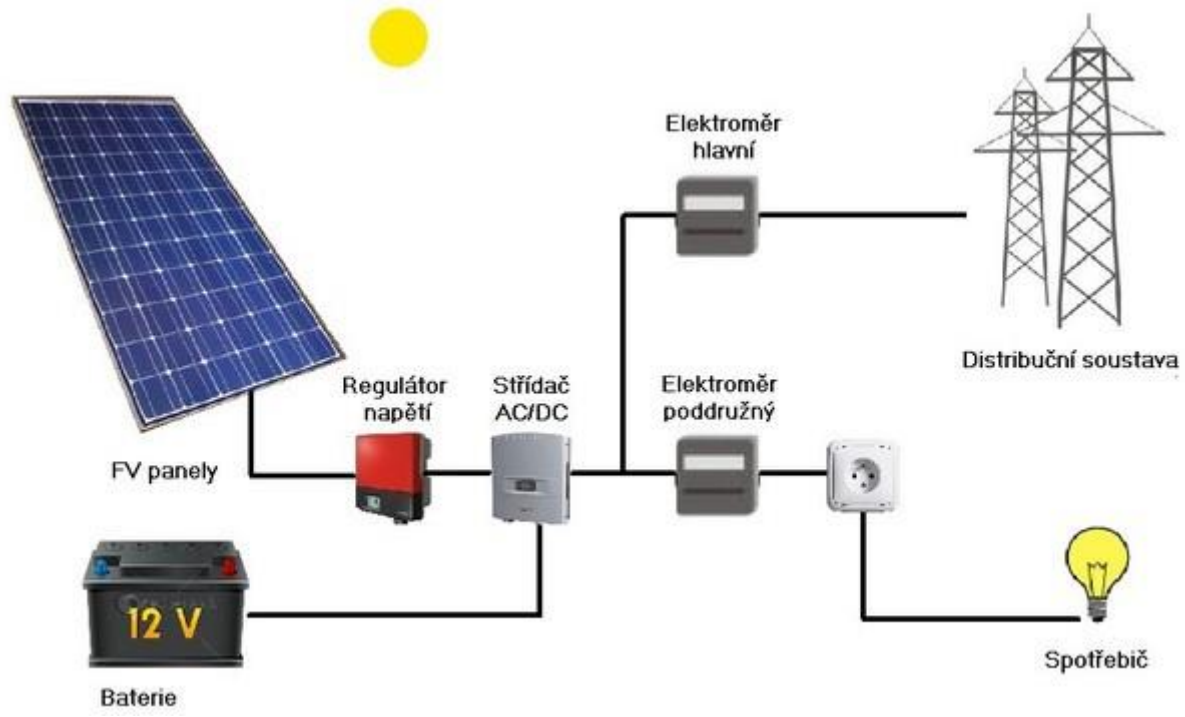
Zařazení necenových (kyberbezpečnostních) kritérií do dotačních programů pro malé FVE (např. program Nová zelená úsporám) by mohlo představovat další cestu k mitigaci problému.

Další možností dle partnerů NÚKIB je zapojení smartmetrů či speciálních (AZ) routerů české výroby se smartmetrem, který by střídač řídil místo dodavatele a monitoring by byl převeden z ČLR do Evropy.

Uživatelé mohou míru rizika ovlivnit typem připojení střídače, kdy připojení na domácí Wi-Fi je nejrizikovější a využití datové SIM karty je méně rizikové. Pokročilejší uživatelé pak mohou provozní data segmentovat tak, aby data logger četl pouze externí síť, a nikoliv citlivé informace uvnitř společnosti či domácnosti.

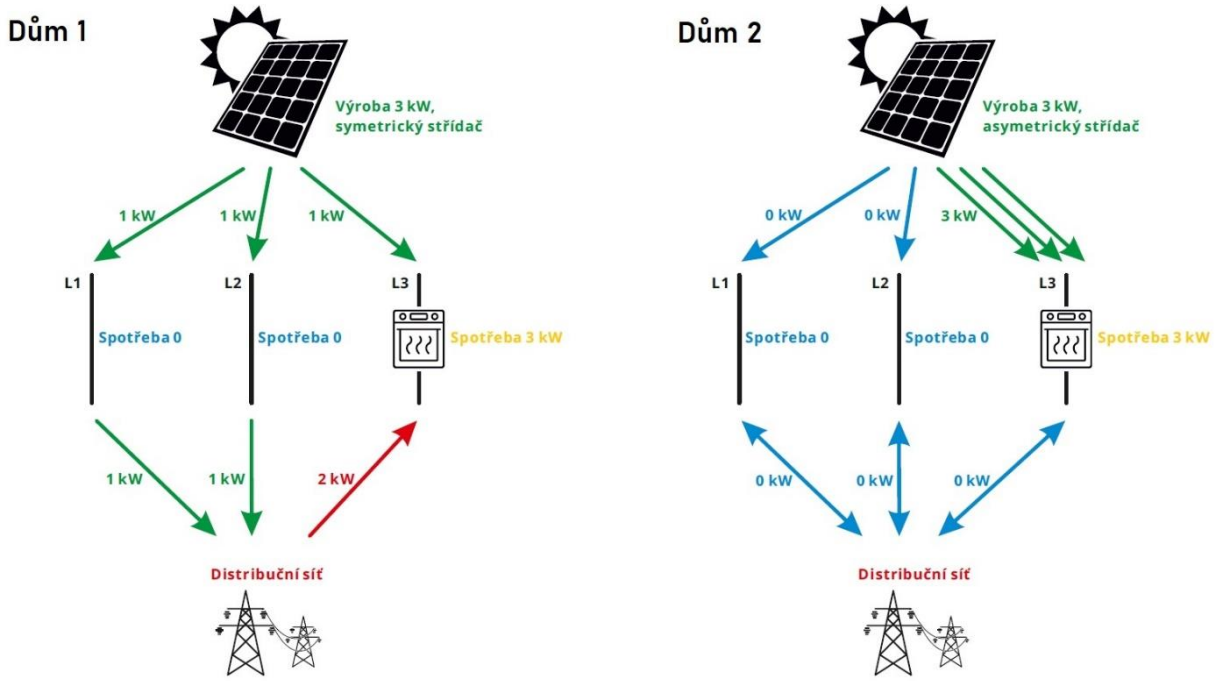
Aspektem rizik spojených se sběrem dat se zabývá i varování NÚKIB, které upozorňuje na vysokou hrozbu spojenou s předáváním systémových a uživatelských dat do ČLR a jejích zvláštních administrativních oblastí, a metodika k tomu vydaná.

PŘÍLOHA 1: SCHÉMA KOMPONENT MALÝCH FOTOVOLTAICKÝCH ELEKTRÁREN



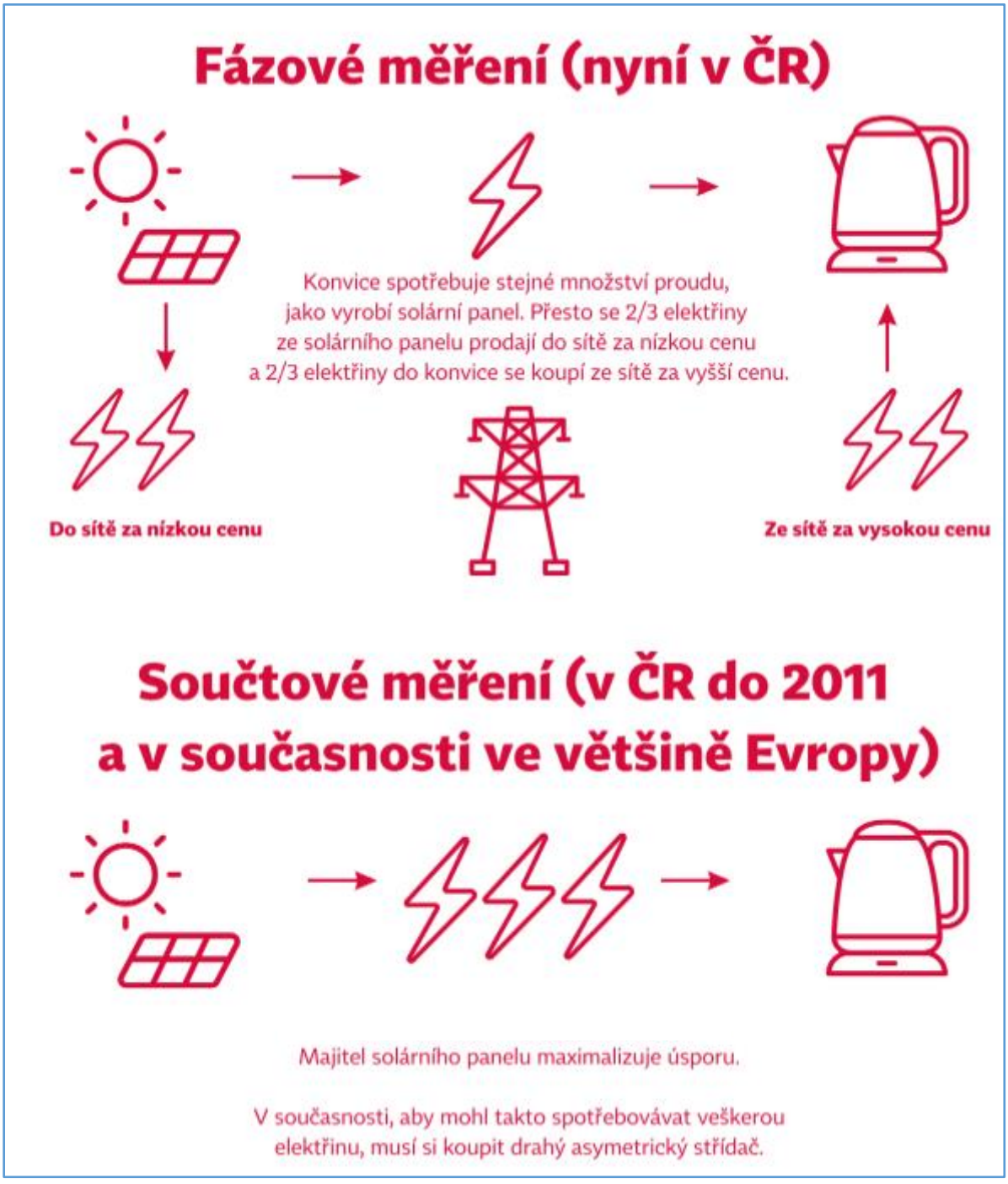
Zdroj: https://www.tzb-energ.cz

PŘÍLOHA 2: SYMETRICKÝ VS. ASYMETRICKÝ STŘÍDAČ



Zdroj: estav.cz

PŘÍLOHA 3: ROZDÍL MEZI FÁZOVÝM A SOUČTOVÝM MĚŘENÍM



Zdroj: frankbold.org

PŘÍLOHA 4: ČÍNSKÉ LEGISLATIVNÍ PROSTŘEDÍ

Charakteristickým prvkem čínského pojetí státní bezpečnosti je povinnost každého občana a organizace se podílet na zajištění státní bezpečnosti. Tato povinnost je mimo jiné definována i v zákonech ČLR. Legislativní úprava ČLR je jedním z hlavních rizikových faktorů při používání čínských technologií. Čínská legislativa je celkově postavena na ze západního pohledu nestandardních požadavcích a také ukazuje na snahu státu mít strategické oblasti zájmu plně pod kontrolou. **Vyjma toho jsou čínské právní předpisy psány často velice vágně, což poté otevírá prostor pro jejich interpretaci ze strany státních orgánů.**

ZÁKON O STÁTNÍ BEZPEČNOSTI (2015)

ČLR novelizovala legislativu související se státní bezpečností v letech 2014 až 2017. Zákon o státní bezpečnosti[27] (国家安全法) byl přijat v červenci roku 2015 a vytvořil právní rámec pro další legislativu, která souvisí s otázkami státní bezpečnosti, včetně zákona o zpravodajské činnosti a zákona o kybernetické bezpečnosti. Zákon o státní bezpečnosti obsahuje obecnou povinnost občana a organizace poskytnout pomoc státním orgánům v otázkách státní bezpečnosti. Související zákony tuto obecně definovanou povinnost přejímají a uplatňují ji na činnosti specifické konkrétnímu právnímu předpisu.

ZÁKON O STÁTNÍ KONTRAŠPIONÁŽNÍ ČINNOSTI (2014)

Čínské společnosti mají dle zákona o státní kontrašpionážní činnosti[28] (Counter-Espionage Law, 中华人民共和国反间谍法) povinnost poskytnout součinnost a informace o svých zahraničních klientech, které budou státní orgány požadovat v rámci vyšetřování reálné či domnělé špionážní činnosti. Zákon je explicitně (čl. 6) aplikovatelný i vůči institucím, organizacím a jednotlivcům, které organizují či financují špionážní aktivitu proti ČLR mimo její teritorium. Zákony však umožňují označit za špionáž široké množství aktivit, do které mohou spadat i činnosti neziskových organizací či jakákoliv aktivita, kterou státní orgány ČLR považují za ohrožení státní bezpečnosti.

Novela zákona, která vešla v platnost 1. července 2023, významným způsobem rozšířila jeho působnost. V porovnání s dosavadní verzí z roku 2014, která pojednávala výlučně o státních tajemstvích, má novela širší záběr a vztahuje se i na jakékoli dokumenty, data, materiály či předměty spojené s národní bezpečností nebo (národními) zájmy. Zároveň ale nikde neuvádí, jak definovat otázky národní bezpečnosti. Novela klade i větší důraz na kybernetickou bezpečnost, což se projeví například zpřísněním pravidel pro nakládání s informacemi o zranitelnostech v systémech. Čínské organizace i občané jsou nyní povinni hlásit podezření na špionáž státním orgánům, zatímco telekomunikační společnosti mají povinnost spolupracovat se státem v případech podezření ze špionáže.[29]

Rozšířená formulace dává čínským orgánům volnost při definování toho, jaké informace se týkají bezpečnosti nebo zájmů státu. Např – lze tvrdit, že zákon se vztahuje na obchodní činnosti, jako je získávání informací o místních trzích, partnerech či konkurentech, nebo na informace o určitých technologiích a ekonomických údajích, které jsou v rozporu s oficiálnímu údaji.[30]

Nový zákon taktéž opravňuje čínské orgány k tomu, aby zahraniční firmy působící v ČLR a jejich zaměstnance nutily poskytovat přístup k údajům, které se týkají národní bezpečnosti, což je pojem, který čínské právo definuje široce tak, že zahrnuje politickou, ekonomickou a sociální bezpečnost. Tyto údaje mohou zahrnovat citlivé obchodní informace, technická obchodní tajemství nebo údaje o klientech.

Revize také poskytuje orgánům větší vyšetřovací a donucovací pravomoci, čímž účinně podřizují zařízení, data, dokumenty a digitální zařízení kontrole za účelem získání informací souvisejících s národními zájmy.

Přijetí tohoto zákona následuje po nových snahách o kontrolu dat v ČLR a několika významných vládních raziích v zahraničních podnicích, při nichž byli místní zaměstnanci zadrženi a vyslýcháni.

Již od roku 2023 začaly čínské úřady omezovat nebo zakazovat přístup ze zahraničí k databázím obsahujícím údaje o registraci společností, patentech, akademických časopisech, veřejných zakázkách a dalších oficiálních údajích.

V březnu ČLR zřídila nový Národní úřad pro správu dat, který má dohlížet na data ve veřejném i soukromém sektoru.

ČLR běžně odepírá diplomatické konzulární služby a právní poradenství osobám, které jsou vyšetřovány pro špionáž. Cizinci nesmějí opustit zemi, dokud nejsou jejich právní případy vyřešeny.

ZÁKON O KYBERNETICKÉ BEZPEČNOSTI (2017)

Zákon o kybernetické bezpečnosti[31] (Cybersecurity Law, 中华人民共和国网络安全法) je účinný od června 2017 a jeho implementaci je primárně odpovědná Správa kyberprostoru Číny, která je kromě regulace zodpovědná i za cenzuru. Zákon obsahuje řadu ustanovení definujících povinnost spolupráce se státními orgány. Článek 28 určuje povinnost provozovatelů sítí: *Poskytnout technickou podporu a spolupráci orgánům veřejné bezpečnosti a orgánům státní bezpečnosti, které ochraňují státní bezpečnost.*

ČLR bude v roce 2025 tento zákon revidovat. Dne 28. března 2025 Správa kyberprostoru Číny vydala nový návrh novelizace zákona o kybernetické bezpečnosti k veřejnému připomínkování.

Klíčové body tohoto návrhu jsou:

Přístup k duševnímu vlastnictví (IP) a zveřejnění zdrojového kódu: Z důvodu národní bezpečnosti může být vyžadován rozšířený přístup státu k duševnímu vlastnictví softwaru, autorským právům a zdrojovému kódu. Společnosti mohou také čelit tlaku nebo nařízením, aby pro komunikaci, směrování dat nebo kontrolu internetového provozu používaly čínský software.

Lokalizace dat a kontrola jejich transferu: Přísnější pravidla pro ukládání a přeshraniční transfer osobních a provozních dat, zejména pro firmy s kancelářemi nebo infrastrukturou v ČLR.

Infrastruktura a API Gatekeeping: Zvýšená kontrola směrování internetového provozu (internet traffic routing) a povinné licencování podnikových API používaných v digitálním ekosystému ČLR.

Šifrování a přístup k digitálním klíčům: Větší pravomoc státu nad standardy šifrování, včetně potenciálních požadavků na zveřejnění digitálních klíčů a dešifrovacích nástrojů.[32]

ZÁKON O STÁTNÍ ZPRAVODAJSKÉ ČINNOSTI (2017)

Zákon o státní zpravodajské činnosti[33] (National Intelligence Law, 中华人民共和国国家情报法) je ze série zákonů týkajících se státní bezpečnosti nejvýznamnější z hlediska definování povinností jednotlivců a organizací se podílet na státní zpravodajské činnosti. Článek 7 definuje povinnost subjektů a zároveň jejich ochranu ze strany státu:

Všechny organizace a občané musí podle zákona národní zpravodajskou činnost podpořit, poskytnout součinnost a spolupráci, zachovat mlčenlivost o tajných záležitostech, o kterých se v souvislosti s národní zpravodajskou činností dozví. Stát následně chrání jednotlivce a organizace, přispívající k podpoře, součinnosti a spolupráci v souvislosti s národní zpravodajskou činností.

Článek 14 stejného zákona zdůrazňuje, že relevantní státní instituce jsou oprávněny vyžadovat spolupráci po jednotlivcích a organizacích: *Národní zpravodajské služby mohou v souladu se souvisejícími státními předpisy požádat příslušné orgány, organizace a občany o poskytnutí potřebné podpory, součinnosti a spolupráce*.

ZÁKON O SPOLEČNOSTECH (2013)

Zákon o společnostech (Company Law, 中华人民共和国公司法 2013 修订) byl do aktuální podoby novelizován v roce 2013. Na rozdíl od výše uvedených zákonů se přímo netýká státní bezpečnosti. Článek 19 ovšem ustanovuje mechanismus vlivu KS Číny na chod společnosti: *Ve společnosti bude ustanovena organizace Komunistické strany Číny za účelem výkonu aktivit strany ve shodě se stanovami Komunistické strany Číny. Společnost musí poskytnout nezbytné podmínky pro aktivity stranické organizace.* V praxi to znamená přímý dosah Strany na dění v jakékoliv významné společnosti. Zákon zajišťuje, že společnosti beze zbytku plní, co se od ní očekává včetně požadavků v oblasti státní bezpečnosti.[34]

Povinnost ustanovit stranickou buňku není nová. Po nástupu Si Ťin-pchinga do čela strany a státu se toto pravidlo začalo vymáhat a KS Číny je v řadě případů zastoupena v nejvyšších orgánech formálně soukromých společností. Ve vztahu k povinnosti občanů a organizací působících v ČLR se podílet na zpravodajské činnosti, která je podřazena širokému chápání povinnosti zajištění státní bezpečnosti, je důležité zaměřit se i na mechanismy vlivu KS Číny ve formálně soukromých společnostech jako jsou i Tencent či ByteDance.

Další relevantní právní úprava ČLR týkající se kybernetické bezpečnosti

Název	Účinnost	Typ	Významné body
Zákon o společnostech (Company Law, 中华人民共和国公司法 2013 修订)	01.03.2014	zákon	Článek 19 ustanovuje mechanismus vlivu KS Číny na chod společnosti: ukládá ustanovit uvnitř struktur buňku KSČ, pokud ve společnosti pracují nejméně tři členové Strany. V praxi to znamená přímý dosah Strany na dění v jakékoliv významné společnosti. Zákon zajišťuje, že společnosti beze zbytku plní, co se od ní očekává, včetně požadavků v oblasti státní bezpečnosti.
Zákon o státní kontrašpionážní činnosti (Counter-espionage Law, 中华人民共和国反间谍法)	01.11.2014	zákon	Čínské společnosti mají povinnost poskytnout součinnost a informace o svých zahraničních klientech, které budou státní orgány požadovat v rámci vyšetřování reálné či domnělé špionážní činnosti, jež se zde rozumí jako aktivita, kterou orgány ČLR považují za ohrožení státní bezpečnosti.
Zákon o státní bezpečnosti (National Security Law, 国家安全法)	01.07.2015	zákon	Zákon o státní bezpečnosti obsahuje obecnou povinnost občana a organizace poskytnout pomoc státním orgánům v otázkách státní bezpečnosti. Související zákony tuto obecně definovanou povinnost přejímají a uplatňují ji na činnosti specifické konkrétnímu právnímu předpisu.
Zákon o kybernetické bezpečnosti (Cybersecurity Law, 中华人民共和国网络安全法)	01.06.2017	zákon	Zákon obsahuje řadu ustanovení definující povinnost spolupráce se státními orgány. Článek 28 určuje povinnost provozovatelů sítí poskytnout technickou podporu a spolupráci orgánům veřejné bezpečnosti a orgánům státní bezpečnosti.
Zákon o státní zpravodajské činnosti (National Intelligence Law, 中华人民共和国国家情报法)	28.06.2017	zákon	Všechny organizace a občané musí podle zákona národní zpravodajskou činnost podpořit, poskytnout součinnost a spolupráci, zachovat mlčenlivost o tajných záležitostech, o kterých se v souvislosti s národní zpravodajskou činností dozví. Stát následně chrání jednotlivce a organizace, přispívající k podpoře, součinnosti a spolupráci v souvislosti s národní zpravodajskou činností.
Pravidla pro nahlašování zranitelností v síťových zařízeních (公安部关于印发网络产品安全漏洞管理规定的通知)	01.09.2021	regulace	Výrobci technologií mají povinnost nahlašovat bezpečnostní zranitelnosti čínskému Ministerstvu průmyslu a IT (MIIT), a to nejpozději dva dny od zjištění. MIIT pak nahlašuje nález MSS a dalším relevantním institucím vč. CNITSEC. Je zakázáno zveřejňovat tyto zranitelnosti nebo je nahlašovat zahraničním organizacím a jednotlivcům.
Zákon o bezpečnosti dat (Data Security Law, 中华人民共和国数据安全法)	01.09.2021	zákon	Upravuje podmínky zajištění bezpečnosti dat a zamezení jejich úniku mimo území ČLR. Zákon dává státním autoritám možnost zastavit fungování společnosti, která dle nich bude v rozporu s požadavky zákona.
Zákon o ochraně osobních údajů	01.11.2021	zákon	Upravuje zacházení veřejných i soukromých institucí s osobními údaji občanů ČLR v Číně i v zahraničí a vyžaduje souhlas se sběrem dat s výjimkou „veřejného

(Personal Information Protection Law, 中华人民共和国个人信息保护法)			zájmu.“ Společnosti disponující velkým množstvím osobních dat musí podle zákona podstoupit povinnou bezpečnostní kontrolu CAC.
Regulace pro nahlašování zranitelností v síťových zařízeních (Regulations on Management of Network Product Security Vulnerabilities, 公安部关于印发网络产品安全漏洞管理规定的通知)	01.09.2021	regulace	Výrobci technologií mají povinnost nahlašovat bezpečnostní zranitelnosti čínskému Ministerstvu průmyslu a IT (MIIT), a to nejpozději dva dny od zjištění. MIIT pak nahlašuje nález MSS a dalším relevantním institucím. Je zakázáno zveřejňovat tyto zranitelnosti nebo je nahlašovat zahraničním organizacím a jednotlivcům.
Opatření pro přezkum kybernetické bezpečnosti (网络安全审查办法)	15.02.2022	regulace	Ukládají povinnost společnostem, které disponují údaji více než jednoho milionu uživatelů a chystají veřejný prodej akcií (IPO), aby prošly důkladnou kontrolou CAC.
Doporučení o správě algoritmů na internetu (Provisions on the Management of Algorithmic Recommendation Services, 互联网信息服务算法推荐管理规定)	01.03.2022	doporučení (právně závazné)	Vytváří nová pravidla pro vytváření algoritmů aplikací a internetových služeb. Oficiálním účelem doporučení je ochrana spotřebitelů, nová pravidla ale mají potenciál dále omezovat svobodu slova, jelikož algoritmy mohou znemožňovat šíření kritických informací vůči režimu.
Opatření o hluboké syntéze na internetu (Provisions on the Administration of Deep Synthesis of Internet Information Services, 互联网信息服务深度合成管理规定)	25.11.2022 (10.01.2023)	opatření	Opatření upevňuje cenzuru tím, že zakazuje tvorbu obsahu, který by byl v rozporu se stávajícími zákony, ohrožoval národní bezpečnost či poškozoval národní obraz. Kontrolu nad algoritmy zastává databáze algoritmů zavedená v „Doporučeních pro správu algoritmů“, jejímž cílem je kontrola narativů a svobody slova. Do databáze algoritmů musí být nahrány pouze takové algoritmy, které jsou samotestem vyhodnocené jako mající schopnost mobilizovat společnost nebo ovlivňovat veřejné mínění.
Ustanovení o správě informačních služeb pro mobilní internetové aplikace (Provisions on the Administration of Information Services for Mobile Internet Applications, 移动互联网应用程序信息服务管理规定)	01.08.2022	regulace	Uvádí, že poskytovatelé internetových aplikací a jejich distribuční platformy by neměli používat aplikace k nezákonným činnostem, které ohrožují národní bezpečnost, narušují společenský řád nebo porušují legitimní práva a zájmy jiných osob. Poskytovatelé aplikací navíc nesmějí uživatele nabádat ke stahování svých aplikací prostřednictvím falešných propagačních akcí nebo nezákonných a nežádoucích informací ani získávat návštěvnost prostřednictvím kontroly komentářů nebo praktik tzv. click farming. [35] Nařízení má doplňovat nařízení o internetových algoritmech.

Ustanovení o správě informací v internetových uživatelských účtech (Provisions on the Management of Internet User Account Information, 互联网用户账号信息管理规定)	01.08.2022	regulace	Požaduje, aby poskytovatelé internetových služeb a aplikací pro zasílání rychlých zpráv (instant messengers) ověřovali identifikaci uživatelů a také zobrazovali IP adresu uživatelů.
Prozatímní opatření o správě generativní AI (Interim Measures for the Management of Generative AI Services, 生成式人工智能服务管理办法（征求意见稿）)	01.08.2023 (15.08.2023)	opatření	Týká se pouze generativních AI modelů určených pro veřejnost, přičemž vyžaduje registraci části algoritmu do databáze. Vývojáři musejí sladit algoritmus se socialistickými hodnotami. Kontrolu nad algoritmy zastává databáze algoritmů zavedená v „Doporučeních pro správu algoritmů“, jejímž cílem je kontrola narativů a svobody slova. Do databáze algoritmů musí být nahrány pouze takové algoritmy, které jsou samotestem vyhodnocené jako mající schopnost mobilizovat společnost nebo ovlivňovat veřejné mínění. Neveřejní provozovatelé jako průmyslové organizace, podniky, akademické a vědecké instituce nejsou těmito regulacemi zatíženi.
Zákon o státních tajemstvích (State Secrets Law, 中华人民共和国保守国家秘密法)	27.02.2024	zákon	V roce 2024 byl novelizován zákon o státních tajemstvích z roku 2010. Součástí nového zákona je rozšířená definice státních tajemství, které nově obsahují i kategorii pracovních tajemství. Nově se týká taktéž nestátních aktérů, jako zahraničních společností a jednotlivců a opravňuje autority z provádění kontrol dokumentů, zařízení, zaměstnanců a k vynucení spolupráce při vyšetřování.

ZDROJE

[1] Energetický regulační úřad. 2024. Výroba elektřiny z malých fotovoltaických elektráren loni vzrostla o více než 170 %. https://eru.gov.cz/vyroba-elektriny-z-malych-fotovoltaickych-elektraren-loni-vzrostla-o-vice-nez-170 a ČT24. 2024. Boom malých fotovoltaik v Česku nekončí, předstihly i ty velké. https://ct24.ceskatelevize.cz/clanek/domaci/boom-malych-fotovoltaik-v-cesku-nekonci-predstihly-i-ty-velke-352186

[2] Energetický regulační úřad. 2024. Roční zpráva o provozu elektrizační soustavy ČR pro rok 2023. https://eru.gov.cz/rocni-zprava-o-provozu-elektrizacni-soustavy-cr-pro-rok-2023

[3] Fotovolty. 2024. Proč je asymetričnost střídače klíčovou vlastností pouze v České republice? https://www.fotovolty.cz/blog/proc-je-asymetricnost-stridace-klicovou-vlastnosti-pouze-v-cr

[4] Elektro Q-Elektrik. 2024. Symetrický vs. asymetrický střídač. https://elektro.q-elektrik.cz/symetricky-vs-asymetricky-stridac

[5] Fotovolty. 2024. Proč je asymetričnost střídače klíčovou vlastností pouze v České republice? https://www.fotovolty.cz/blog/proc-je-asymetricnost-stridace-klicovou-vlastnosti-pouze-v-cr a O Energentice, 2023. Češi ušetří na fotovoltaice kvůli zastaralému měření spotřeby méně než sousedi. Měnit se však nic nebude. https://oenergetice.cz/energetika-v-cr/cesi-usetri-na-fotovoltaice-kvuli-zastaralemu-mereni-spotreby-mene-nez-sousedi-menit-se-vsak-nic-nebude.

[6] Informace od partnerů NÚKIB.

[7] Informace od partnerů NÚKIB.

[8] Informace od partnerů NÚKIB.

[9] Informace od partnerů NÚKIB.

[10] Ibid.

[11] Informace od partnerů NÚKIB.

[12] Heise Online. 2024. Photovoltaics: Deactivated Deye and Sol-Ark inverters in the USA. https://www.heise.de/en/news/Photovoltaics-Deactivated-Deye-and-Sol-Ark-inverters-in-the-USA-10183716.html, Born´s Tech and Wondows World. 2024. Deye deactivates solar inverters in USA, UK and Pakistan. https://borncity.com/win/2024/11/28/deye-deactivates-solar-inverters-in-usa-uk-and-pakistan/ a Derek the Solarboi. 2024. Sol-Ark manufacturer reportedly disables all Deye inverters in the US. https://solarboi.com/2024/11/17/sol-ark-oem-disables-all-deye-inverters-in-the-us/.

[13] Informace od partnerů NÚKIB.

[14] Robinsun. 2024. The Deye micro inverter scandal in Germany - what happened and why it matters to your solar installation. https://robinsun.com/blogs/news/the-deye-micro-inverter-scandal-in-germany-what-happened-and-why-it-matters-to-your-solar-installation

[15] Informace od partnerů NÚKIB a Willem Westerhof. 2025. Horus Scenario 2.0. https://media.ccc.de/v/why2025-90-horus-scenario-2-0.

[16] Vangelis Stykas. 2025. Gridlock: The Dual-Edged Sword Of EV And Solar APIs In Grid Security. https://www.youtube.com/watch?v=7T6I-VcWQ0o.

[17] Willem Westerhof. 2025. Horus Scenario 2.0. https://media.ccc.de/v/why2025-90-horus-scenario-2-0.

[18] Informace od partnerů NÚKIB.

[19] Rachel Lee, Prudence Luttrell, Matthew Johnson, and John Garnault. 2023. TikTok, ByteDance, and their ties to the Chinese Communist Party: Submission to the Australian Senate Select Committee on Foreign interference through Social Media.

[20] Atlantic Council. 2023. Sleight of hand: How China weaponizes software vulnerabilities. https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/

[21] Dark Reading. 2024. TikTok Ban Raises Data Security, Control Questions. https://www.darkreading.com/cyber-risk/tiktok-ban-raises-data-security-control-questions

[22] CISA. 2024. PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. https://www.cisa.gov/sites/default/files/2024-02/aa24-038a-jcsa-prc-state-sponsored-actors-compromise-us-critical-infrastructure_1.pdf

[23] Moderní energetika. 2023. Česko zažívá po 13 letech solární renesanci. I díky našemu příspěvku slaví Evropa rekordní růst fotovoltaiky. https://www.modernienergetika.cz/aktuality/cesko-zaziva-po-13-letech-solarni-renesanci-i-diky-nasemu-prispevku-slavi-evropa-rekordni-rust-fotovoltaiky.

[24] Solar Power Europe. 2025. Solutions for PV Cyber Risks to Grid Stability. Chapter 5 Grid Impact Analysis. https://api.solarpowereurope.org/uploads/SPE_2025_Solutions_for_PV_Cyber_Risks_to_Grid_Stability_032dc2ae5a.pdf?updated_at=2025-04-29T07:11:32.315Z.
[25] Informace od partnerů NÚKIB.
[26] Informace od partnerů NÚKIB.
[27] Ministry of National Defense of the People's Republic of China. 2015. National Security Law of the People's Republic of China. http://eng.mod.gov.cn/publications/2017-03/03/content_4774229.htm

[28] China Law Translate. 2014. Counter-espionage Law. https://www.chinalawtranslate.com/en/anti-espionage/

[29] Nikkei Asia. 2023. China's planned changes to espionage law alarm foreign businesses. https://asia.nikkei.com/Politics/China-s-planned-changes-to-espionage-law-alarm-foreign-businesses
[30] Informace od partnerů.
[31] Cyberspace Administration of China. 2017. 中华人民共和国网络安全法. http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

[32] Informace od partnerů.
[33] National People's Congress of the People's Republic of China. 2017. 中华人民共和国国家情报法. http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml

[34] Law Bridge. 2013. Company Law of the People's Republic of China (Revised in 2013). http://www.lawbridge.org/zhong-hua-ren-min-gong-he-guo-gong-si-fa-2013-nian-xiu-ding/
[35] Global Times. 2022. China's draft regulation bans app providers from endangering national security. https://www.globaltimes.cn/page/202201/1245154.shtml
[45] Mauran, C. 2025. DeepSeek collects keystroke data and more, storing it in Chinese servers. https://mashable.com/article/deepseek-ai-privacy-policy-keystroke-data-chinese-servers, DeepSeek. 2025. Zásady ochrany osobních údajů. https://web.archive.org/web/20250214185351/https://cdn.deepseek.com/policies/en-US/deepseek-privacy-policy.html

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená **TLP:RED**	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová **TLP:AMBER+STRICT**	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
Oranžová **TLP:AMBER**	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
Zelená **TLP:GREEN**	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá **TLP:CLEAR**	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

PRAVDĚPODOBNOSTNÍ VÝRAZY NÚKIB

Výraz	Pravděpodobnost
Téměř jistě	*90–100 %*
Velmi pravděpodobně	*75–85 %*
Pravděpodobně	*55–70 %*
Nelze vyloučit / Reálná možnost	*40–50 %*
Nepravděpodobně	*20–35 %*
Velmi nepravděpodobně	*0–15 %*