Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.j. 6860/2025-NÚKIB-E/630• BRNO • 25. SRPNA 2025

[STRATEGICKÁ ANALÝZA]

ČÍNSKÁ PŘIPOJENÁ VOZIDLA PŘEDSTAVUJÍ IDEÁLNÍ ŠPIONÁŽNÍ NÁSTROJ DÍKY ENORMNÍMU SBĚRU DAT V KOMBINACI S ČÍNSKÝM PRÁVNÍM PROSTŘEDÍM

SHRNUTÍ

- **Připojená vozidla (tzv. connected vehicles) ze své podstaty sbírají nadměrné množství dat, mj. o poloze a trase vozidla či osobní informace o cestujících. Vozidla z Čínské lidové republiky (ČLR) pak data uchovávají mj. na tamních serverech, kde k nim má dle čínských zákonů přístup čínská vláda. Tímto aspektem 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.**
- **Vzhledem k předchozím špionážním aktivitám, jednání proti národním zájmům států EU a NATO, ke specifikům čínské legislativy, státního vlivu v čínských společnostech a jejich povinnosti s čínskými státními orgány spolupracovat je velmi pravděpodobné (75–85 %), že ČLR využije možnosti čínských připojených vozidel ke zpravodajské činnosti.**
- **Čínská politika zveřejňování zranitelností ukládá čínským výrobcům nejprve nahlásit detekovanou zranitelnost pouze tamním státním orgánům. Je velmi pravděpodobné (75–85 %), že Peking využije takto odhalené zranitelnosti v kybernetických operacích. Nelze taktéž vyloučit (40–50 %), že Peking využije legislativního postavení a svého vlivu v čínských společnostech k doručení tzv. backdoorů (škodlivé programy umožňující např. vzdálený přístup) do softwaru či firmwaru připojených vozidel. Vedle špionáže může být backdoor v krajním případě zneužit také k sabotáži.**
- **V ČR je podíl elektromobilů (podtyp připojených vozidel využívající k pohonu elektrickou energii) na automobilovém trhu pod unijním průměrem. V druhém čtvrtletí r. 2025 představoval podíl elektromobilů v ČR 5,6 %, oproti 15,6 % evropského průměru. Meziročně ČR avšak zaznamenala 66% nárůst, což z ní činí druhý nejdynamičtěji rostoucí trh s bateriovými elektromobily v rámci EU. Na růst trhu bude mít téměř jistě (90–100 %) vliv odklon od spalovacích motorů v rámci dekarbonizačních politik EU, ke kterým se ČR hlásí, v kombinaci s nižšími cenami čínských elektromobilů. Dle Registru smluv instituce státní správy nejčastěji využívají elektromobily nepocházející z ČLR, přičemž elektromobily z ČLR (dle smluv z roku 2024) tvoří pouze jednotky procent.**
- **EU a Spojené státy řeší otázku čínských připojených vozidel částečně tarify, přičemž USA hodlají přistoupit k zákazu dovozu a prodeje připojených vozidel vybavených hardwarem či softwarem vyvinutým, vyrobeným nebo dodaným subjekty spojenými s ČLR nebo Ruskem. Taktéž se na úrovni jednotlivých amerických států jedná o zákazu řízení čínských připojených vozidel na amerických vojenských základnách a v jejich okolí.**
- **ČR by měla využít spíše pozvolného růstu množství čínských připojených vozidel v zemi a včas zhodnotit rizika jejich používání zejména v okolí kritické infrastruktury či zájmovými osobami a případně zvážit možnost omezení jejich užívání.**

UPOZORNĚNÍ: Informace a závěry obsažené v této analýze vycházejí z informací partnerů NÚKIB, 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.

Připojená vozidla (connected vehicles, CVs) představují souhrnný název pro vozidla mající schopnost připojit se skrze internet k výrobci, jiným vozidlům, zařízením, včetně IoT či k prvkům infrastruktury chytrého města (Příloha 1). **Zpravidla za účelem správného fungování připojená vozidla využívají enormního sběru dat, mj. o okolním prostředí a infrastruktuře či řidiči a spolucestujících.** V současnosti stále prominentnější

podtyp připojených vozidel představují elektromobily (či bateriová elektrická vozidla, Battery Electric Vehicles, BEVs), která k pohonu využívají zpravidla lithiovou baterii.

Čínská lidová republika (ČLR) představuje největší trh s elektromobily na světě, přičemž zaujímá prvenství i v jejich produkci. [1] **Tomuto postavení přispívá především přístup k surovinám potřebným pro výrobu baterií, dlouhodobé cílené investice do výzkumu a vývoje v odvětví hybridních vozidel a soubor politických nástrojů, které nastavily vhodné podmínky pro vývoj a produkci elektromobilů.**[2] Díky subvencím mohou čínští výrobci nabízet nižší cenu oproti západní konkurenci, a tím se stávají atraktivní nejen pro běžné, soukromé uživatele a společnosti, ale taktéž pro státní instituce. Vzhledem k unijní politice dekarbonizace a podmínkám s ní spojených bude evropský automobilový průmysl vyžadovat rozsáhlou a rychlou transformaci, s čímž objemné investice právě do elektromobility souvisí a EU tak představuje velmi atraktivní trh pro čínské výrobce elektromobilů.

Čínské legislativní prostředí přikazuje čínským společnostem součinnost se státními orgány, což může vést k činnostem v rozporu se zájmy i právy zákazníků, jako např. přístup čínského státu k datům sbíraným senzory připojených vozidel či instalace malwarů do jejich systémů. Čínské společnosti byly v minulosti několikrát nařčeny ze sdílení dat svých zákazníků nebo duševního vlastnictví s čínským státem bez jejich vědomí (Huawei, WuXi AppTec).[3]

VOZIDLA SBÍRAJÍ VELKÉ MNOŽSTVÍ DAT; ČÍNSKÁ JE UCHOVÁVAJÍ MJ. NA SERVERECH V ČLR, KDE K NIM MÁ PŘÍSTUP ČÍNSKÁ VLÁDA

Dle partnerů NÚKIB je velmi pravděpodobné (75–85 %), že státní aktéři shledávají data generovaná připojenými vozidly, včetně elektromobilů, užitečná pro špionážní účely.

Systémy poskytující konektivitu v připojených vozidlech shromažďují mimořádně velké množství dat mj. o: poloze, trase, okolních objektech, telefonních kontaktech a hovorech, identitě cestujících, adrese, finanční situaci, preferencích, co se zábavy týče, demografických informacích (věk, pohlaví, etnicita), zdravotních, fyziologických, genetických, či behaviorálních informacích a charakteristikách. [4] Rozhraní člověk-stroj (Human-Machine Interface, HMI) dále umožňuje pomocí kamer, mikrofonů a senzorů ovládat vybrané funkce vozidla hlasem či gestem.

Tato data mohou být zneužita k vytvoření např. přehledu o aktivitách osob zajímavých pro cizí mocnosti či o zabezpečených oblastech, pokud jsou v nich připojená vozidla řízena.[5]

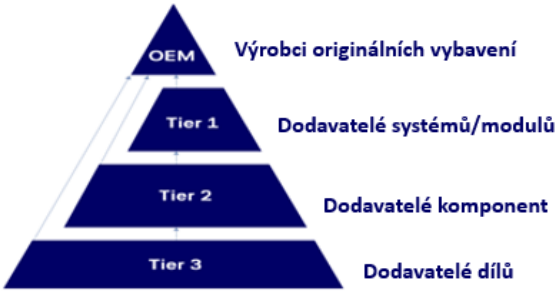
Analýza elektromobilů čínských značek NIO a MG odhalila, že některá jimi sesbíraná data jsou posílána mj. na cloudové servery společnosti Tencent umístěné v ČLR, a to i přes přítomnost datacenter v Evropě.[6] **Je velmi pravděpodobné (75–85 %), že podobně si počínají i další čínské značky. Tato praxe je často pozorována i u jiných čínských technologií (TikTok).**

Tato skutečnost je problematická především v kontextu čínského právního prostředí, jež nakazuje čínským společnostem dle zákona o státní bezpečnosti na vyžádání poskytnout součinnost a spolupráci s národními zpravodajskými službami (viz Příloha 3). **Jelikož jsou některá data uchovávána na serverech v ČLR, mohou k nim čínské autority v případě potřeby přistupovat.**

Jednou z možností, jak tuto situaci mitigovat, je ukládat data pouze na serverech v Evropě. Obdobné řešení bylo použito v případě rizik spojených s ochranou dat v aplikaci TikTok čínské společnosti ByteDance, kdy data měla být uchovávána v datovém centru na americké půdě v rámci projektu Texas. **Nicméně jak dokládají kontroverze okolo projektu, ani toto není univerzální řešení, neboť i v tomto případu, a to i přes ujištění ze strany společnosti ByteDance nadále docházelo k přenosu dat do ČLR.**[7]

Ani uložení dat na serverech v EU, případně v USA, neznamená stoprocentní ochranu. Čínští aktéři se k uloženým datům mohou dostat i jinak, např. skrze dodavatelský řetězec, je-li jeho součástí čínský dodavatel, nebo za pomocí špionážních a kyberšpionážních aktivit. Uložení dat umístěných na serverech nacházejících se na území států, jejichž právní řád neumožňuje bezprostřední přístup státních institucí k osobním a citlivým datům je tak jen možnost, jak ochranu zvýšit, nikoli zcela zajistit.

Obr. 1: Pyramida dodavatelského řetězce v automobilovém průmyslu



Zdroj: time-matters.com

Je taktéž potřeba zohlednit obchodování s daty (data brokering), především v kontextu jejich možného přeprodávání do zemí s nejednoznačným právním prostředím. [8] V tomto kontextu se nabízí řešení v podobě standardizace minimalizace sběru dat.

Zároveň je nutné vzít v potaz i možné sdílení dat spřáteleným státům ČLR, které označují západní demokracie za nepřátelské státy, v době konfliktu.

Z těchto důvodů představuje řízení čínských elektromobilů (a čínských připojených vozidel obecně, a to bez ohledu na místo výroby) v okolí objektů důležitých pro infrastrukturu a obranu státu bezpečnostní riziko. Stejně tak jejich používání zaměstnanci státní správy nakládajícími s citlivými informacemi či institucí věnujícím se klíčovým výzkumům.

VÝROBCI MUSÍ SPOLUPRACOVAT S ČÍNSKÝM STÁTEM, MOHOU MJ. POSKYTOVAT PROSTŘEDKY PRO OFENZÍVNÍ KYBERKAMPANĚ

Čínskému legislativnímu prostředí taktéž podléhají i všechny čínské společnosti zapojené do dodavatelského řetězce obecně (Obrázek 1).

Zároveň díky vlastnickým podílům (tzv. Golden Share) v mnoha formálně soukromých společnostech může čínský stát kontrolovat a zasahovat do jejich fungování a struktur, což je ještě dále prohloubeno činností stranických buněk, jež jsou ve společnostech povinně zřizovány dle zákona o společnostech. Např. automobilka Zeeker v rámci registračního prohlášení pro americkou Komisi pro kontrolu cenných papírů (SEC) uvedla, že „vláda ČLR má podstatný vliv na řízení našeho podnikání a může ovlivňovat naše operace, nebo do nich zasahovat, pokud sezná další regulační, politické nebo společenské cíle za vhodné.“[9] Podobně se vyjádřila i společnost Hesai Group vyrábějící sensory LiDAR pro asistenční systémy řízení (ADAS).[10]

Je pravděpodobné (55–70 %), že Peking využívá výrobce vozidel (tzv. OEM, Original Equipment Manufacturer) pro zpravodajskou činnost právě kvůli širokému přístupu k jejich produktům. Zároveň má mnoho výrobců vazby na armádu (Příloha 2).

Čínské orgány tak mají např. pravomoc nakázat instalaci tzv. backdoorů do systémů vozidel, které umožňují budoucí zneužití čínskými aktéry kybernetických hrozeb. Peking možnost umisťování backdoorů do produktů čínských výrobců dlouhodobě využívá (viz kauzy společností AdUPs a SECURAM).[11] **Proto existuje reálná možnost (40–50 %), že i výrobcům připojených vozidel bude nakázáno backdoory nasadit do svých produktů.** Producenti OEM mají vzdálený přístup k softwaru vozidla, a tedy jsou schopni vozidlo na dálku i zastavit. Je tedy i v jejich schopnostech doručit do softwaru vozidla malware, jak potvrzují i partneři NÚKIB.

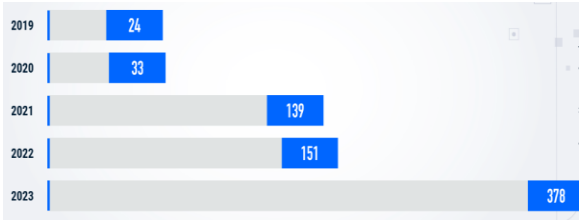
Lze tak učinit např. pomocí aktualizací OTA (Over-the-Air, tedy pomocí Wi-Fi či mobilní sítě), jež nyní představují standardní součást připojených vozidel, přičemž některé operační systémy skenují dostupnost nových aktualizací nepřetržitě.[12]

Vysoká míra propojenosti připojených vozidel s internetem představuje významný vektor pro možný útok, přičemž v roce 2023 byly nejčastějším prvotním vektorem útoku na připojená vozidla telematické a aplikační servery.[13]

Zranitelná místa do dopravního ekosystému přinášejí taktéž dobíjecí stanice pro elektromobily a komponenty s nimi spojené (Electric Vehicle Supply Equipment, EVSE). Kybernetické útoky mohou vyřadit z provozu jediné zařízení EVSE, celé skupiny nebo všechna zařízení vlastněná dodavatelem. Nejčastějšími taktikami jsou útoky falšující reálný stav nabíjení (Spoofing) nebo útoky na dostupnost dobíjení (Denial-of-Service) (Příloha 1). **Vzhledem k tomu, že je stále více dopravních odvětví elektrifikováno, hrozí, že rozsáhlá narušení EVSE budou mít vážný dopad nejen na dopravu, ale i řadu kritických infrastruktur jako jsou záchranné a zdravotnické služby, zemědělství, výrobu, obranu apod.**

U elektromobilů využívajících k pohonu baterie jsou dalším možným vektorem útoku prvky tzv. internetu baterií (Internet-of-Batteries, IoB). Použití různých způsobů připojení jako Wi-Fi, Bluetooth nebo mobilní sítě v elektrických vozidlech vystavují systém IoB útokům na dostupnost (DoS) nebo útokům manipulujícím s falešnými daty (False Data Injection).[14]

Obr. 2: Nárůst hlášených zranitelností v připojených vozidlech od roku 2019



Zdroj: Upstream

ZVEŘEJŇOVÁNÍ ZRANITELNOSTÍ TAKTÉŽ PODLÉHÁ ČÍNSKÝM ZÁKONŮM: VÝROBCI JE MUSÍ HLÁSIT PŘEDEVŠÍM STÁTU, NIKOLI ZÁKAZNÍKŮM

Zranitelnosti (úmyslně vložené i neúmyslně vzniklé) v softwaru čínských připojených vozidel mohou být čínskými aktéry hrozeb využívány pro kybernetické operace. Čínská legislativa o řízení zranitelností udává v případě odhalení zranitelnosti výrobci technologií povinnost nahlásit její existenci do dvou dnů Ministerstvu průmyslu a informačních technologií (MIIT), a to ještě před její opravou nebo zveřejněním (Příloha 3).

MIIT ji dále hlásí Ministerstvu státní bezpečnosti (MSS), které působí jako zpravodajská služba s vnitřní i vnější působností a zaštiťuje mnohé čínské kybernetické aktéry hrozeb (např. APT31, APT41, APT10, APT40, Emissary Panda či RedHotel).[15]

Součástí procesu je ukládání zranitelností do databází, přičemž připojeným vozidlům je vyčleněna samostatná databáze, jejímž přispěvatelem je mimo jiné i automobilka BYD.[16]

Množství nahlášených zranitelností v průmyslu připojených vozidel ročně stoupá, což svědčí o rostoucím zájmu o toto odvětví (viz Obr 2).[17] V roce 2023 byly zranitelnosti v automobilovém průmyslu nejčastěji nacházeny na čipové sadě (chipset), aplikacích třetích stran a v systémech infotainmentu (tzv. In-Vehicle Infotainment systém spojuje možnosti zábavy, jako např. poslech hudby s informacemi o řízení jako navigaci, nastavení vozidla apod.). [18] **Ačkoliv v minulosti byla objevena zranitelnost např. ve vozech čínské MG, nezáleží na množství odhalených zranitelností ve srovnání se západními značkami, ale v přístupu s jejich nakládáním.**[19]

ČR V PODÍLU REGISTRACÍ NOVÝCH ELEKTROMOBILŮ ZAOSTÁVÁ, SITUACE SE BUDE MĚNIT S BLÍŽÍCÍM SE ROKEM 2035

Stále prominentnějším podtypem připojených vozidel jsou elektromobily, které k pohonu využívají elektrickou energii. ČR se v podílu registrací nových elektromobilů dlouhodobě pohybuje za ostatními zeměmi Evropy. **Celkový podíl registrací bateriových elektromobilů v ČR představuje k druhému čtvrtletí 2025 5,6 %, což meziročně činí o 66 % více a činí z tuzemska lídra v růstu na tomto trhu. Nicméně za evropským průměrem 15,6 % stále zaostává.** [20] **Ve srovnání podílu bateriových elektromobilů s ostatními evropskými zeměmi se ČR nachází na 20. místě.** Důvodem je mj. i silná tradice trhu s naftovými motory. **Nejvíce registrací zaznamenaly elektromobily značek Škoda, Tesla, Kia, Volkswagen, Hyundai, Toyota, BMW a Volvo.**[21]

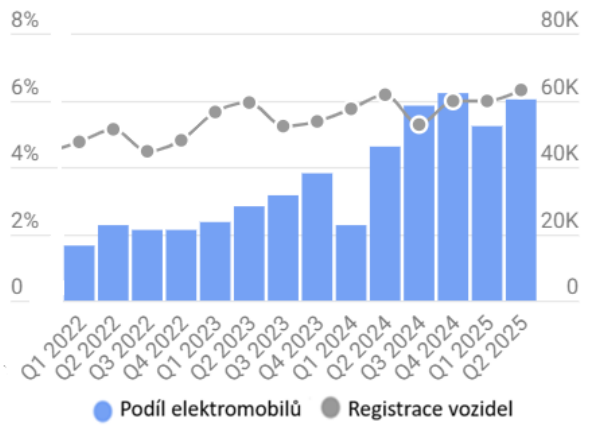
Je nicméně téměř jisté (90–100 %), že v následujících 10 letech zaznamená podíl registrovaných elektromobilů nárůst. Důvodem je především naplňování politik EU v oblasti dekarbonizace, zejména pak zákaz prodeje nových vozidel se spalovacími motory počínaje rokem 2035.[22]

Zároveň roli hraje i naplňování zákona č. 360/2022 Sb., o podpoře nízkoemisních vozidel prostřednictvím zadávání veřejných zakázek a veřejných služeb v přepravě cestujících, který stanovuje minimální podíly nízkoemisních vozidel v nadlimitních veřejných zakázkách (nad 4,5 mil Kč) do konce roku 2030. Konkrétně pro silniční vozidla kategorie M1, kam spadají osobní automobily, se jedná o podíl 29,7 %.[23]

V současnosti jsou na českém trhu s elektromobily oficiálně zastoupeny vozy čínských značek BYD, Dongfeng, MG a JAC. [24] Přes třetí stranu lze získat i modely značek jako Zeekr, Nio či Aiways (Příloha 2).[25] Kromě elektromobilů mají na českém trhu zastoupení i vozy GWM a SWM, které svými funkcemi spadají do kategorie připojených vozidel. **Dle Registru smluv však bezpečnostně citlivé instituce jako např. Policie ČR či Ministerstvo vnitra čínské elektromobily v současnosti nepoužívají.**

ČR spustila v roce 2023 výzvu na podporu elektromobility vybízející k nákupu vozidel na alternativní paliva, tedy baterie či vodík, pro malé, střední i velké podniky.[26] Dotace byly využity i na nákup čínských elektromobilů, zejména na vozy značky MG.[27] Prodej elektromobilů vede jednoznačně Tesla.

Obr. 3: Vývoj registrací elektromobilů v ČR od roku 2022 do druhé čtvrtiny 2025



Zdroj: transportenvironment.org

EU I USA PŘÍLIV ČÍNSKÝCH EV USMĚRŇUJÍ TARIFY, ŠETŘÍ I BEZPEČNOSTNÍ RIZIKA

EU v posledním roce zaznamenala rapidní nárůst dovozu čínských EV na svých trzích (258 mld. Kč v roce 2023 oproti 36 mld. Kč v roce 2020). [28] **Vzhledem k subvencím, jimiž čínská vláda vývoj, výzkum a produkci elektromobilů dotuje, jsou tamní výrobci schopni produkty nabízet za nesrovnatelně nízké ceny, což činí unijní producenty nekonkurenceschopnými.** Evropská komise (EK) v závislosti na výsledku antisubvenčního vyšetřování uvalila na čínské elektromobily dodatečná cla nad rámec stávajících 10 % platící od 1.11.2024 po dobu 5 let.[29]

Je pravděpodobné (55–70 %), že výše tarifů některé výrobce neodradí a EK bude muset přistoupit k dalším regulatorním nástrojům. [30] Na unijní úrovni bylo doposud přijato klíčové nařízení 2019/2144 o požadavcích pro schvalování typu motorových vozidel a jejich přípojných vozidel (Regulation on the General Safety of Vehicles) a jeho prováděcí nařízení 2022/1426 stanovující základní kyberbezpečnostní požadavky na automatizované systémy řízení.[31] Oba předpisy jsou již v účinnosti a zavádí do unijních pravidel i ustanovení pro schvalování vozidel z hlediska kybernetické bezpečnosti, které byly představeny v právně nezávazném předpisu OSN č. 155. Naopak nedávno vydaný Akt o kybernetické odolnosti (Cyber Resilience Act), jehož cílem je nastavit základní kyberbezpečnostní požadavky pro hardware a software vstupující na unijní trh, se na vozidla vztahovat nebude. Nepřímo se však i toto nařízení může vozidel dotknout např. skrze jejich používané komponenty, na něž se explicitní výjimka nevztahuje.

Čínské společnosti zároveň aktivně nalézají nové způsoby, jak tarify na dovoz obejít, např. stavbou výrobních středisek přímo v EU či distribucí výrobků přes třetí země. Zároveň se Peking snaží narušit jednotu unijních států v otázce zavedení cel na elektromobily z ČLR mj. možným zavedením odvetných ekonomických cel na výrobky unijních států do ČLR dovážených. [32] ČR by neměla případnému tlaku podlehnout a neměla by se vzdávat jednotné unijní pozice.

Spojené státy naproti tomu zaujímají ostřejší postoj, jenž se promítá nejen ve zvýšení dovozních tarifů na 100 %, ale taktéž přípravou legislativy regulující dovoz a používání připojených vozidel. ČLR se však i zde snaží obejít tarify stavbou továren v Mexiku. **Americké Ministerstvo obchodu vydalo návrh právního předpisu týkající se možného zákazu dovozu a prodeje připojených vozidel, která obsahují specifický software a hardware pocházející z ČLR či Ruska, a to od roku 2027 (software) a 2030 (hardware).** [33] Na úrovni jednotlivých amerických států se pak jedná o vydání zákazu řízení čínských připojených vozidel uvnitř amerických vojenských základen. [34] Nově k zavedení tarifů přistoupila i Kanada, která na elektromobily vyrobené v ČLR hodlá uvalit 100% tarif, a to včetně vozů americké značky Tesla vyrobené v šanghajské továrně.[35]

K omezení pohybu čínských elektromobilů na vojenských základnách v roce 2025 přistoupily také Velká Británie i Izrael.[36] , který vydal zákaz jejich vstupu na všechny základny izraelských obranných sil z důvodu rizika úniku informací.

VÝHLED A IMPLIKACE: VZHLEDEM K PŘECHODU NA ELEKTROMOBILITU PLYNE RIZIKO PRO VEŘEJNÉ ZAKÁZKY, U KTERÝCH JE JEDINÝM KRITÉRIEM CENA NABÍDKY

Vzhledem k dekarbonizačním politikám EU (např. Nařízení Evropského parlamentu a Rady (EU) 2019/631, emisní normy, klimatický balíček Fit for 55) je téměř jisté (90–100 %), že dojde k nárůstu počtu elektromobilů v ČR.[37] Vzhledem k silné tradici výroby automobilů se spalovacími motory v ČR je velmi pravděpodobné (75–85 %), že ČR bude nadále patřit k zemím s nižším podílem nových registrací elektromobilů, a proto se dají očekávat nové pobídky právě na podporu elektromobility. **Kromě peněžních incentiv ve formě dotací je téměř jisté (90–100 %), že budou zavedeny další stimulační nástroje.** V současné době již fungují benefity pro české majitele elektromobilů ve formě zvýhodněného či bezplatného parkování ve vybraných městech, nižší pojištění či bezplatná dálniční známka.

ČLR se snaží aktivně obcházet tarify na dovoz čínských elektromobilů zavedené EU tím, že přesouvá svou výrobu do členských států Unie. To, spolu s masivním subvencováním ze strany Pekingu, umožňuje čínským výrobcům prodávat elektromobily za nižší ceny než konkurenční produkty. **Je pravděpodobné (55–70 %), že právě nízká cena bude kvůli nastavení fungování veřejných zakázek hrát rozhodující roli ve výběru vozů pro státní a veřejné zakázky a čínské elektromobily tak budou užívány státními institucemi, politickými představiteli či prominentními osobami.** To do budoucna může přestavovat riziko úniku citlivých informací o daných osobách.

Další možností proliferace čínských elektromobilů do ČR je jejich použití společnostmi podnikajícími

v kurýrních, rozvážkových či přepravních službách. Soukromí přepravci již v současnosti investují do nových čínských elektromobilů.[38] Flotila elektromobilů pak může být zneužita k narušení provozu např. v případě konfliktu.

Zároveň je taktéž vhodné vzít v úvahu samotnou bezpečnost vozidel vyrobených v ČLR, neboť ta, kvůli vysoké konkurenci tamního trhu, bývají projektována a sestavována v rychlosti, a tudíž mnohdy postrádají mnoho bezpečnostních prvků, což z nich dělá jednoduché cíle.

DOPORUČENÍ

ČR je nyní v ideální pozici začít řešit otázku rizik spojených s čínskými připojenými vozidly. V současnosti je evidováno spíše malé množství nově registrovaných elektromobilů, což se v příštích 10 letech změní kvůli evropským politikám dekarbonizace i vstupu čínských automobilek na evropský trh.

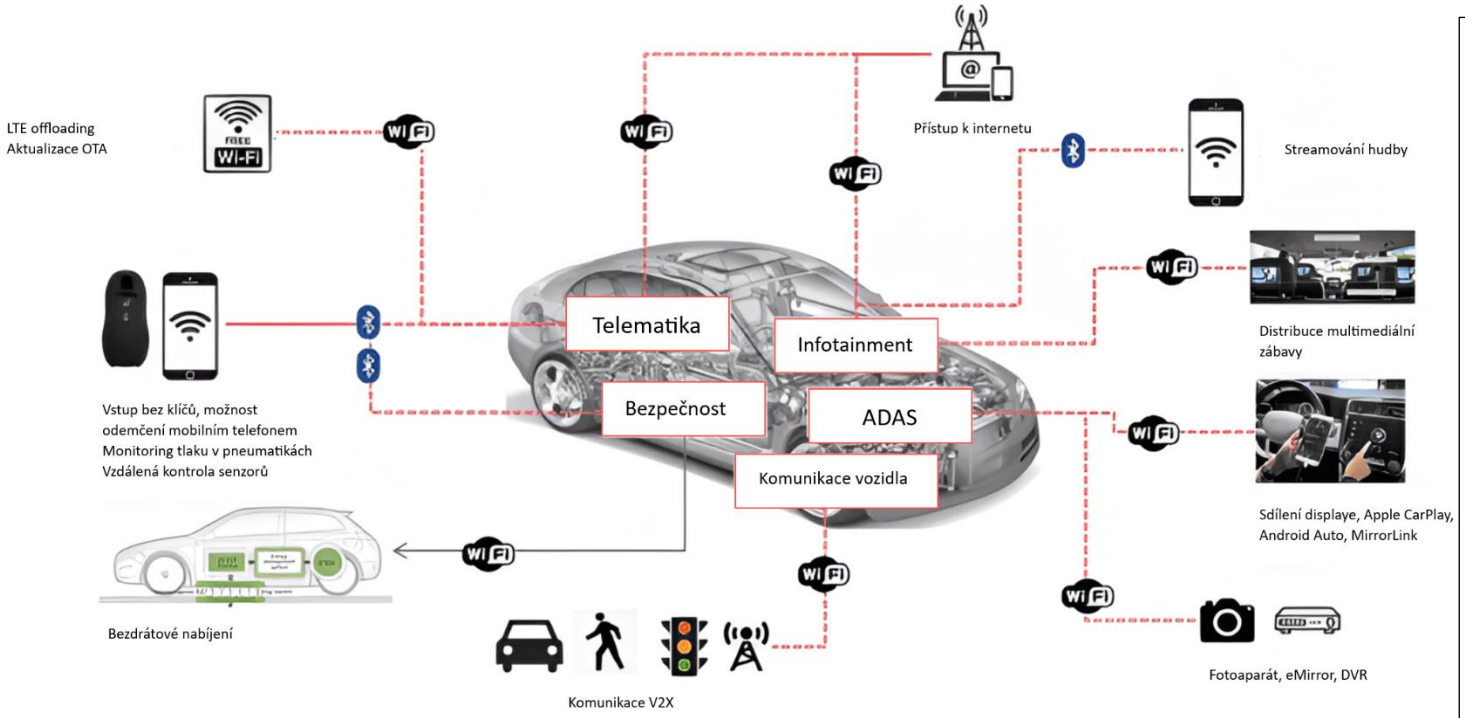
Vzhledem ke schopnosti sbírat data a ke skutečnosti, že se ČR dlouhodobě nachází v oblasti zájmu čínských zpravodajských služeb, řízení a parkování čínských elektromobilů (a čínských připojených vozidel obecně) v okolí

- **objektů důležitých pro obranu státu,**
- **objektů kritické infrastruktury a kritické informační infrastruktury,**
- **a dalších objektů strategického významu**

představuje bezpečnostní riziko.

Je tudíž na místě řídit se varováním NÚKIB, které upozorňuje na vysokou hrozbu spojenou s předáváním systémových a uživatelských dat do Čínské lidové republiky a jejích zvláštních administrativních oblastí a metodikou k tomuto varování vydanou.

PŘÍLOHA 1: VEKTORY ÚTOKU A VYBRANÉ ZPŮSOBY KOMPROMITACE PŘIPOJENÝCH VOZIDEL



Zdroj: cz.farnell.com

Komunikace V2X (ang. Vehicle to X, kde X je dále specifikováno zkratkou):

- **Vozidlo – infrastruktura chytrého města:** komunikace s prvky smart city, jako např. semafory (V2I, Vehicle to Infrastructure)
- **Vozidlo – vozidlo:** komunikace mezi vozidly navzájem (V2V, Vehicle to Vehicle)
- **Vozidlo – cloud:** komunikace vozidla a cloudu, např. aktualizace OTA (V2C, Vehicle to Cloud)
- **Vozidlo – chodec:** vozidlo je schopné reagovat na chodce přecházející silnici, jedoucí na invalidním vozíku či cyklisty (V2P, Vehicle to Pedestrian)
- **Vozidlo – zařízení:** komunikace vozidla a dalších zařízení připojených k internetu, např. mobilní telefon nebo IoT (V2D, Vehicle to Device)
- **Vozidlo – síť:** komunikace vozidla a mobilní sítě, Wi-Fi, 5G (V2N, Vehicle to Network),
- **Vozidlo – rozvodná síť:** komunikace vozidla s rozvodnou síť umožňující dobíjet vozidla i posílat elektrickou energii zpátky do sítě (V2G, Vehicle to Grid

- řídicí jednotka ECU (Electronic Control Unit) pro řízení automobilových systémů jako motor nebo brzdy,
- Bluetooth, WiFi, přijímač signálu GPS, bezpečnostní modul
- vyhrazená komunikace krátkého dosahu (Dedicated Short Range Communication, DSRC), zprostředkovávající bezdrátovou komunikaci mezi vozidlem a infrastrukturou V2X, tedy ostatními účastníky silničního provozu a silniční infrastrukturou,
- koncový bod autorádia, do kterého se připojuje ECU (Head-end Unit, HEU),
- technologie near field communication (NFC) zajišťující komunikaci mezi elektronickými zařízeními, např. mobily a zábavními systémy,
- OTA: konektivita vzduchem (Over-The-Air, OTA) umožňující dálkové aktualizace softwaru,
- Drátové připojení: Palubní diagnostika (On-Board Diagnostics), konektory síťového svazku, porty diagnostiky, porty USB, palubní sítě (CAN, LIN, FlexRay, Ethernet, MOST, apod), přehrávač CD/DVD, port pro nabíjení vozidla

Útoky na dostupnost	
Zneužití zranitelností v systémech vozidla nebo v systémech prvků infrastruktury připojených vozidel (např. dobíjecí stanice)	Vyřazení vozidla, jeho prvků nebo infrastruktury z provozu Proveditelné je i získání částečné nebo úplné vzdálené kontroly nad vozidlem, nicméně určujícím faktorem je jaký prvek dokáže útočník kompromitovat. Jak uvádí partneři NÚKIB, v otevřených zdrojích existuje minimum informací o úplné kompromitaci kritických funkcí, jedním ze zdokumentovaných případů je např. Pwn2Own, událost přímo zaměřená na hackování.[39] Vzhledem k vysokým nákladům a hloubce vyžadované expertízy mohou tyto útoky provést státní aktéři. Zároveň nelze také plně podcenit možnosti insiderů potažmo kyberbezpečnostních výzkumníků, kteří úzce spolupracují s výrobci (OEM).
Zneužití DSRC či Bluetooth, tedy prvky v dosahu vyhrazené komunikace krátkého dosahu	Vyřazení vozidla, jeho prvků nebo infrastruktury z provozu Je možné provést i útok s pomocí prvků komunikace krátkého dosahu, nicméně dle analýzy ročenky Upstream tento způsob nepatří mezi preferované. Jak vyplývá z výsledků pouze 15 % útoků na připojená vozidla využívalo komunikaci krátkého dosahu.[40] Útočník může provést útok, aniž by získal fyzický přístup k vozidlu, například zneužitím chyby v komunikaci Bluetooth se systémem infotainmentu nebo rozhraní DSRC používaného pro komunikaci V2X. Tento útok lze ovšem převést i na vzdálené ovládání vozidel instalací tzv. podvodného zařízení (Rogue Device) s vysílačem dlouhého dosahu s jednorázovým fyzickým přístupem k vozidlu.[41] Tento typ útoku může kromě státního aktéra taktéž zrealizovat např. kyberkriminální gang, přičemž vyloučit nelze ani využití teroristickými skupinami.[42]
Ransomware, např. kompromitací mobilních aplikací infotainmentu	Vyřazení vozidla, jeho prvků nebo infrastruktury z provozu Systémy infotainmentu jsou rizikové, zejména protože využívají prvků (např. mobilní aplikace, systém Android, propojení s mobilním telefonem), se kterými jsou aktéři hrozeb či kyberkriminální skupiny již seznámeny.
Škodlivý kód	Potenciálně lze přetížit rozvodnou síť pomocí doručení škodlivého kódu do dobíjecích stanic, který by oddálil dobíjení vozidel do chvíle, kdy by se připojilo více

	vozidel. Spuštění nabíjení v jednu chvíli by pak mohlo ovlivnit funkci rozvodné sítě.[43] Nicméně dle partnerů NÚKIB by útočník musel být dobře obeznámen i s výrobcem dobíjecích stanic a jejich vnitřní infrastrukturou. Vzhledem k náročnosti na finance a expertízu může tyto útoky provést spíše státní aktér, a to v krizových situacích jako je konflikt.

Útoky na důvěrnost	
Zneužití zranitelností, škodlivé aktualizace softwaru	Neoprávněný přístup k osobním či finančním datům a jejich sběr Na základě dat ze senzorů či kamer lze získat informace o okolním venkovním prostředí či pasažérech. Nasbíraná data lze posléze použít nejen k prodeji třetím stranám, ale také je použít ke špionážním účelům. Tento typ útoků mohou podniknout zejména státní aktéři, ale taktéž kyberkriminální skupiny.
Škodlivé aktualizace softwaru	Odposlouchávání Při použití útoků jako man-in-the-middle nebo man-on-the-side lze zachytit tzv. firmware images (kód firmwaru pro konkrétní zařízení nebo systém obsahující informace potřebné pro správnou funkci zařízení, např. konfigurační nastavení), které jsou v rámci aktualizace softwaru odeslány do legitimní řídící jednotky vozidla (ECU). V případě, že nedojde k zašifrování kódu firmwaru, mohou být odcizeny informace např. metodami reverzního inženýrství. Takto lze např. odcizit duševní vlastnictví. Krádež duševního vlastnictví se nelimituje pouze na státní aktéry. Tento typ útoků mohou taktéž podniknout tzv. aftermarket tuners, tedy společnosti nebo jednotlivci, kteří se specializují na úpravu vozidel za účelem zvýšení jejich výkonu.[44]

Útoky na integritu	
Spoofing	Zobrazení falešných dat (Spoofing) např. o stavu baterie Zobrazení falešných dat např. o stavu baterie může vést až k opotřebování baterie s cílem zkrácení její

	životnosti. Dále lze zneužít vnitřní obrazovky vozidla k zobrazení nevhodného či urážlivého obsahu, čehož lze využít např. v hybridních kampaních. Spoofingové útoky může podniknout jak státní aktér, tak kyberkriminální skupina. Vyloučit nelze ani hacktivistické hnutí nebo zkušeného jednotlivce.

PŘÍLOHA 2: HLAVNÍ ČÍNŠTÍ VÝROBCI PŮSOBÍCÍ NA ČESKÉM TRHU A JEJICH VAZBY NA ČÍNSKÝ STÁT ČI ARMÁDU

Čínský automobilový průmysl je od roku 2008 největší na světě. V posledních 10 letech se ČLR zaměřila zejména na výrobu tzv. vozidel na nové energie (New Energy Vehicles, NEV), tedy vozidel na alternativní paliva jako je elektřina nebo vodík.

Dominantním přístupem v ČLR je vývoj a výzkum technologií tzv. dvojího využití, který umožňuje aplikovat technologie jak v civilní, tak ve vojenské sféře. Tento přístup je platný i v kontextu připojených vozidel, která jsou sama o sobě vnímána právě jako technologie dvojího využití.

	Dongfeng (i s divizemi Voyah a M-Hero) Jedná se o státního výrobce automobilů. Dongfeng dlouhodobě spolupracuje s čínskou armádou, pro kterou vyrábí mj. lehké nákladní vozidlo Dongfeng EQ2050 (v čínské armádě odznačovaný jako Menshi).[45]
	MG Motor Značka MG Motor je součástí čínské státní společnosti SAIC Motor Corp., Ltd., která historicky patří k hlavním výrobcům automobilů. **SAIC založila spolu s Chunanskou univerzitou (Hunan University) a Šanghajskou univerzitou (Shanghai University) laboratoře na výzkum pokročilých technologií výroby vozidel či kybernetické bezpečnosti inteligentních propojených vozidel.**[46] Obě zmíněné instituce kooperují s čínskou armádou, Chunanská univerzita se podílí na výzkumu obranných technologií a jaderných zbraní, jejichž výzkum probíhá s přispěním tamního superpočítačového centra.[47] Šanghajská univerzita pak provádí výzkum bezpilotních pozemních vozidel.[48]
	BYD má rozsáhlé vazby na čínskou armádu. **Centra vývoje a výzkumu společnosti se nacházejí v lokalitách určených pro vývoj a výzkum technologií pro vojensko-civilní fúzi (The Beijing Daxing MCF Industrial Base, the Xi'an High Tech Industrial Development Zone).**[49] Zároveň spolupracuje s Šanghajskou dopravní univerzitou (Shanghai Jiaotong University), jejíž výzkumníci přímo spolupracují s čínskou armádou na kyberútocích. Zároveň existují i vazby vedení na čínský stát. Zakladatel Wang Chuanfu zastával dlouhodobě stranické posty.
	Zeekr Zeekr je dceřinou společností Zhejiang Geely Holding Group. V současnosti je Zeekr podroben vyšetřování na podnět floridského senátora R. Scotta ohledně jeho vazeb na Komunistickou stranu Číny a využívání nucených prací při výrobě svých produktů v souvislosti s jeho vstupem na americkou burzu.[50] Vozy Zeekr jsou vybaveny satelitní komunikací od výrobce satelitů Geespace, jež je dceřinou společností Geely.[51] Výzkum a vývoj v oblastech kosmického průmyslu má tradičně úzké vazby na čínskou armádu.[52]
	Nio **Nio v současnosti vyvíjí autonomní vozidla, přičemž společnost dostala oprávnění uvést vozidla stupňů L3/L4 (řidič již vozidlo aktivně neřídí, avšak přebírá kontrolu v případě poruchy/řidič vozidlo aktivně neřídí, v případě poruchy není nutné zapojit řidiče, řidič stále může libovolně převzít kontrolu nad vozidlem) do zkušebního provozu ve speciálních městských trasách v Šanghaji.**[53] Vojenské využití autonomních vozidel spočívá zejména v jejich nasazení do rizikových operací jako např. zásobování, průzkum komunikací zaměřený na likvidaci výbušnin (tzv. route clearance) či jakýkoliv průzkum nebo evakuace zraněných. Nio na vývoji technologiích autonomního řízení a mapování ve vysokém rozlišení spolupracuje s čínskou společností Tencent, která má široké vazby na čínský stát.[54]

	JAC JAC představuje dodavatele pro NIO, zároveň spolupracuje na výrobě vozů pod svou značkou se společností Huawei.[55]
	Aiways Výrobce Aiways kvůli nízkým výdělkům vstoupí v roce 2024 prostřednictvím fúze na burzu akvizicí s americkou společností Hudson Acquisition Corp. Výrobce se nově bude primárně zaměřovat na Evropu, kam umístí své sídlo, přičemž výroba, výzkum a vývoj zůstane v ČLR.[56]
	Chery Tento výrobce byl založen v roce 1997 místní správou čínského města Wu-chu v provincii An-chuej. Chery taktéž spolupracuje s tamními loděnicemi Wuhu Shipyard, kde buduje základnu pro stavbu plavidel schopných přepravovat vozidla, tzv. ro-ro (roll on/roll off), přičemž tato plavidla mají i potenciální vojenské využití.[57] Stejný typ plavidel si objednaly taktéž výrobci BYD a SAIC.[58]
	XPeng XPeng se zaměřuje na vývoj létajících vozidel, konkrétně tzv. eVTOL (electric Vertical Take-Off and Landing, letadla na elektrický pohon se schopností kolmého vzletu a přistání). [59] XPeng v tuto chvíli dosud oficiálně nevstoupil na český trh.
	GWM GWM je v ČR znám spíše jako výrobce vozidel na fosilní paliva. Po neúspěchu v prodeji elektromobilů je z unijních trhů postupně stahuje.
	SWM Původně italská značka byla koupena čínským výrobcem Shineray Group v roce 2014. V ČR jsou nabízeny pouze vozidla na fosilní paliva, nicméně SWM vyrábí i elektromobily, přičemž oznámil plány o stavbě továrny v Turecku.[60]

PŘÍLOHA 3: ČÍNSKÁ LEGISLATIVA RELEVANTNÍ PRO OBLAST ELEKTRICKÝCH VOZIDEL

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[61] (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[62] (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.[63]

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.[64]

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[65] (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.[66]

ZÁKON O STÁTNÍ ZPRAVODAJSKÉ ČINNOSTI (2017)

Zákon o státní zpravodajské činnosti[67] (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.[68]

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 (Personal Information Protection Law, 中华人民共和国个人信息保护法)	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 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 (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 **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.[69] 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 **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] International Energy Agency. 2024. Global EV Outlook 2024. Dostupné z: https://www.iea.org/reports/global-ev-outlook-2024/trends-in-electric-cars

[2] Yang, Z. 2023. How did China come to dominate the world of electric cars? Dostupné z: https://www.technologyreview.com/2023/02/21/1068880/how-did-china-dominate-electric-cars-policy/

[3] Grigg, A. 2020. Huawei data centre built to spy on PNG. Dostupné z: https://www.afr.com/companies/telecommunications/huawei-data-centre-built-to-spy-on-png-20200810-p55k7w, Martina M., Erman, M., Freifeld, K. 2024. Michael Martina, Michael Erman and Karen Freifeld. Dostupné z: https://www.reuters.com/technology/chinas-wuxi-apptec-shared-us-clients-data-with-beijing-us-intelligence-officials-2024-03-28/

[4] Bureau of Industry and Security, U.S. Department of Commerce. 2024, Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles (ANPRM). Dostupné z: 2024-04382.pdf (federalregister.gov), Caltrider J., Misha Rykov M., MacDonald, Z. 2023. It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy. Dostupné z: https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/

[5] Norton, J. 2023. Does China's rapid rise in the Australian car market pose a security risk? Dostupné z: https://www.aspistrategist.org.au/does-chinas-rapid-rise-in-the-australian-car-market-pose-a-security-risk/

[6] Indstøy, T. 2023. Project Lion Cage - Part 4: How much data and what kind of data is transferred from the car? Dostupné z: https://www.linkedin.com/pulse/project-lion-cage-part-4-how-much-data-what-kind-from-tor-indst%C3%B8y?trk=portfolio_article-card_title, Indstøy, T. 2023. Project Lion Cage - Part 5: How secure are the vehicle manufacturers hosting environment? Dostupné z: https://www.linkedin.com/pulse/project-lion-cage-part-5-how-secure-vehicle-hosting-tor-indst%C3%B8y?trk=portfolio_article-card_title, Robertson, J. 2024. Probing a $69,000 Chinese Electric Vehicle for Clues on Spying. Dostupné z: https://www.bloomberg.com/news/newsletters/2024-05-15/probing-a-69-000-chinese-electric-vehicle-for-clues-on-spying. Data jsou zasílána v rámci komunikace a obsahují mj. data z jednoduchých hlasových příkazů či data o tom, kde se vozidlo fyzicky nachází. Vibilagere. 2024. Chinese EV is sending "log data" to Tencent-owned server. https://www.vibilagare.se/english/chinese-ev-mg-sending-data-chinese-server. Jedná se o data např. z aplikací infotainmentu.

[6] ibid

[7] Wells, G. 2024. TikTok Struggles to Protect U.S. Data From Its China Parent. Dostupné z: https://www.wsj.com/tech/tiktok-pledged-to-protect-u-s-data-1-5-billion-later-its-still-struggling-cbccf203?mod=djem10point

[8] Smalley, S. 2024. Lawmakers set sights on data minimization as states seek to limit companies from capturing vast amounts of personal info. Dostupné z: https://therecord.media/lawmakers-set-sights-on-data-minimization-with-new-bills

[9] Komise pro kontrolu cenný papírů Spojených států (United states Securities and Exchange Commission). 2024. Amendment NO.3 to Form F-1 Registration statement under the securities act of 1933, ZEEKR Intelligent Technology Holding Limited. Dostupné z: https://www.sec.gov/Archives/edgar/data/1954042/000110465924036639/tm229938-23_f1a.htm

[10] Komise pro kontrolu cenný papírů Spojených států (United states Securities and Exchange Commission). 2024. Amendment NO.3 to Form F-1 Registration statement under the securities act of 1933, Hesai Group. Dostupné z:https://www.sec.gov/Archives/edgar/data/1861737/000110465923004072/tm2120356-19_f1.htm

[11] Gallagher, S. 2016. Chinese company installed secret backdoor on hundreds of thousands of phones. Dostupné z: https://arstechnica.com/information-technology/2016/11/chinese-company-installed-secret-backdoor-on-hundreds-of-thousands-of-phones/, Lyons, J.2024. Forget TikTok – Chinese spies want to steal IP by backdooring digital locks. Dostupné z: https://www.theregister.com/2024/03/14/chinese_espionage_safe_locks/

[12] Ministerstvo dopravy Spojených států, Národní úřad pro bezpečnost silničního provozu (Department of Transportation, National Highway Traffic Safety Administration). 2020. Cybersecurity of firmware updates. Dostupné z: https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/cybersecurity_of_firmware_updates_oct2020.pdf

[13] Upstream. 2024. GLOBAL AUTOMOTIVE CYBERSECURITY REPORT 2024. Dostupné z: https://upstream.auto/reports/global-automotive-cybersecurity-report/

[14] Li, H., Bin Kaleem, M., Liu, Z., Wu, Y., Liu, W., Huang, Z. 2023. IoB: Internet-of-batteries for electric Vehicles–Architectures, opportunities, and challenges. Dostupné z: https://www.sciencedirect.com/science/article/pii/S2773153723000646#bib88

[15] Carry, D., Del Rosso, K. 2023. Sleight of hand: How China weaponizes software vulnerabilities. Dostupné z: https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/

[16] Ibid.

[17] Upstream. 2024. GLOBAL AUTOMOTIVE CYBERSECURITY REPORT 2024. Dostupné z: https://upstream.auto/reports/global-automotive-cybersecurity-report/

[18] VicOne. 2023. Automotive Cyberthreat Landscape Report 2023. Dostupné z: https://vicone.com/reports/automotive-cybersecurity-report-2023

[19] Söderholm, E. 2024. Serious IT vulnerability found in MG's electric car. Dostupné z: https://www.vibilagare.se/english/serious-it-vulnerability-found-mgs-electric-car

[20] Čistá doprava. 2025. EU trh s elektromobily (1-6/2025): Česko patří k lídrům růstu – meziročně +67 %, druhé za Španělskem. https://www.cistadoprava.cz/tiskove-zpravy/eu-trh-s-elektromobily-1-62025-cesko-patri-k-lidrum-rustu-mezirocne-plus-67-druhe-za-spanelskem/

[21] Čistá doprava. 2025. Český trh s elektromobily (1-6/2025): Škoda v čele s 35 %, Tesla ztrácí. Dostupné z: https://www.cistadoprava.cz/tiskove-zpravy/cesky-trh-s-elektromobily-1-62025-skoda-v-cele-s-35-tesla-ztraci/, European Federation for Transport and Environment AISBL. 2025. EV market. Dostupné z: https://www.transportenvironment.org/topics/cars/ev-market

[22] Evropský parlament. 2023. Zákaz prodeje nových benzinových a naftových aut v EU od roku 2035: Co to znamená v praxi? Dostupné z: https://www.europarl.europa.eu/topics/cs/article/20221019STO44572/zakaz-prodeje-novych-benzinovych-a-naftovych-aut-od-roku-2035

[23] Sbírka zákonů. 2022. 360. Zákon o podpoře nízkoemisních vozidel prostřednictvím zadávání veřejných zakázek a veřejných služeb v přepravě cestujících. Dostupné z: https://portal-vz.cz/wp-content/uploads/2021/08/Z%C3%A1kon-o-podpo%C5%99e-n%C3%ADzkoemisn%C3%ADch-vozidel-prost%C5%99edn%C3%ADctv%C3%ADm-zad%C3%A1v%C3%A1n%C3%AD-ve%C5%99ejn%C3%BDch-zak%C3%A1zek-a-ve%C5%99ejn%C3%BDch-slu%C5%BEeb-v-p%C5%99eprav%C4%9B-cestuj%C3%ADcich.pdf

[24] Allianz. 2024. Čínská auta, která si můžete koupit v Česku. Dostupné z: https://www.allianz.cz/cs_CZ/blog/domacnost-a-mobilita/cinska-auta-ktera-si-muzeme-koupit-v-cesku.html

[25] Cario. 2024. Vozy skladem. Dostupné z: https://www.cario.cz/vozy-skladem/

[26] Ministerstvo průmyslu a obchodu. 2023. MPO připravilo výzvu na podporu elektromobility. Pro podnikatele je připraveno 1,95 miliardy korun. Dostupné z: https://www.mpo.gov.cz/cz/rozcestnik/pro-media/tiskove-zpravy/mpo-pripravilo-vyzvu-na-podporu-elektromobility--pro-podnikatele-je-pripraveno-1-95-miliardy-korun--278466/

[27] Majurník, J. 2024. Dotacím na elektromobily v Česku suverénně kraluje Tesla, Škodovka pak bojuje s Volkswagenem. Dostupné z: https://www.garaz.cz/clanek/servis-auto-cisla-statistiky-dotacim-na-elektromobily-v-cesku-suverenne-kraluje-tesla-skodovka-pak-bojuje-s-volkswagenem-21012631

[28] Reinsch, W.A., Whitney, J. 2024. Unpacking the European Union's Provisional Tariff Hikes on Chinese Electric Vehicles. Dostupné z: https://www.csis.org/analysis/unpacking-european-unions-provisional-tariff-hikes-chinese-electric-vehicles

[29] Evropská komise. 2024. EU imposes duties on unfairly subsidised electric vehicles from China while discussions on price undertakings continue. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5589, da Silva, J. 2024. EU hits Chinese electric cars with new tariffs. Dostupné z: https://www.bbc.com/news/articles/cy99z53qypko

[30] Sebastian, G., Barkin, N., Kratz, A. 2024. Ain't No Duty High Enough. Dostupné z: https://rhg.com/research/aint-no-duty-high-enough/

[31] Evropská unie. 2024. Nařízení 2019/2144 o požadavcích pro schvalování typu motorových vozidel a jejich přípojných vozidel (Regulation on the General Safety of Vehicles) a jeho prováděcí nařízení 2022/1426. Dostupné z: https://eur-lex.europa.eu/eli/reg/2019/2144/oj, https://eur-lex.europa.eu/eli/reg_impl/2022/1426/oj; Evropská unie. 2019. Akt o kybernetické odolnosti (Cyber Resilience Act). Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R0881.

[32] Hall, C. 2024. Spanish PM urges EU to reconsider tariffs on Chinese EVs. Dostupné z: https://www.reuters.com/world/spanish-prime-minister-says-we-dont-need-another-trade-war-2024-09-11/

[33] Ministerstvo obchodu Spojených států. 2024. Oznámení o návrhu právního předpisu (Notice of Proposed Rulemaking). Dostupné z: https://www.govinfo.gov/content/pkg/FR-2024-09-26/pdf/2024-21903.pdf

[34] Tisková zpráva kongresmanky E. Slotkin. 2024. Slotkin Announces Legislation Establishing National Security Review for Chinese Connected Vehicles. Dostupné z: https://slotkin.house.gov/media/press-releases/slotkin-announces-legislation-establishing-national-security-review-chinese

[35] Mukherjee, P., Sriram, A. 2024. Canada to impose 100% tariff on Chinese EVs, including Teslas. Dostupné z: https://www.reuters.com/business/autos-transportation/trudeau-says-canada-impose-100-tariff-chinese-evs-2024-08-26/

[36] Jervis, T. 2025. Chinese EVs banned from UK military sites over spying concerns. Dostupné z: https://www.autoexpress.co.uk/news/366599/chinese-evs-banned-uk-military-sites-over-spying-concerns, Hadar, T. 2025. צה"ל אוסר בניסת רכבים סיניים לכל בסיסיו מחשש לדליפת מידע. Dostupné z: https://www.calcalist.co.il/local_news/car/article/hjfkvvk00xe,

[37] Evropská unie. 2024. Nařízení Evropského parlamentu a Rady (EU) 2019/631 ze dne 17. dubna 2019, kterým se stanoví výkonnostní normy pro emise CO2 pro nové osobní automobily a pro nová lehká užitková vozidla a kterým se zrušují nařízení (ES) č. 443/2009 a (EU) č. 510/2011 (přepracované znění) (Regulation (EU) 2019/631 of the European Parliament and of the Council). Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0631. Evropská rada. 2024. Balíček „Fit for 55“. Dostupné z: https://www.consilium.europa.eu/cs/policies/green-deal/fit-for-55/.

[38] Majurník, J. 2024. Velké čínské elektromobilní vítězství: Uber nakoupí obrovský počet modelů značky BYD. Dostupné z: https://www.garaz.cz/clanek/novinky-velke-cinske-elektromobilni-vitezstvi-uber-nakoupi-obrovsky-pocet-modelu-znacky-byd-21012985, Bolt. 2024. Bolt adds premium EV fleets to its platform in Europe. Dostupné z: https://bolt.eu/en/blog/bolt-electric-vehicle-fleets/

[39] Synacktiv. 2024. Unlocking the Drive: Exploiting Tesla Model 3. Dostupné z: https://codeblue.jp/2023/result/pdf/cb23-unlocking-the-drive-exploiting-tesla-model-3-by-dehors-berard.pdf

[40] Upstream. 2024. GLOBAL AUTOMOTIVE CYBERSECURITY REPORT 2024. Dostupné z: https://upstream.auto/reports/global-automotive-cybersecurity-report/

[41] Ministerstvo dopravy Spojených států, Národní úřad pro bezpečnost silničního provozu (Department of Transportation, National Highway Traffic Safety Admnistration). 2020. Cybersecurity of firmware updates. Dostupné z: https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/cybersecurity_of_firmware_updates_oct2020.pdf

[42] Ibid.

[43] Scoblete, G. 2023. Electric Vehicles in Focus, Part V: The Evolving Cyber Threat to EV Charging Stations. Dostupné z: https://core.verisk.com/Insights/Emerging-Issues/Articles/2023/September/Week-4/The-Cyber-Risks-of-Electric-Vehicle-Charging-Stations

[44] Ministerstvo dopravy Spojených států, Národní úřad pro bezpečnost silničního provozu (Department of Transportation, National Highway Traffic Safety Admnistration). 2020. Cybersecurity of firmware updates. Dostupné z: https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/cybersecurity_of_firmware_updates_oct2020.pdf

[45] https://www.militaryfactory.com/armor/detail.php?armor_id=1250

[46] SAIC Motor. 2023. SAIC Motor Corporation Limited Annual Report 2023. Dostupné z: https://www.saicmotor.com/english/images/investor_relations/annual_report/2024/5/31/DE63B019CA9A441FA0801360B6121A6E.pdf

[47] Australian Strategic Policy Institute. 2021. China Defense Universities Tracker: Hunan University. Dostupné z: https://unitracker.aspi.org.au/universities/hunan-university/

[48] Australian Strategic Policy Institute. 2019. China Defense Universities Tracker: Shanghai University. Dostupné z: https://unitracker.aspi.org.au/universities/shanghai-university/

[49] Radarlock. 2019. BUILDING THE China Dream, BYD & CHINA’S GRAND STRATEGIC OFFENSIVE. Dostupné z: https://www.americanmanufacturing.org/wp-content/uploads/2020/03/BYD.pdf

[50] Sen. R. Scott. 2024. Dopis předsedovi Komise pro kontrolu cenných papírů Spojených států (UNITED STATES SECURITIES AND EXCHANGE COMMISSION) od Sen. R. Scotta. Dostupné z: https://www.rickscott.senate.gov/services/files/ADE89E6B-3F05-44EF-9B43-39A205E6F7E3

[51] Zhang, P. 2024. Geely unit Geespace launches 2nd batch of 11 satellites for services including autonomous driving. Dostupné z: https://cnevpost.com/2024/02/03/geely-geespace-launches-2nd-batch-of-11-satellites/

[52] Tabeta, S. 2024. China's Geely builds satellites to guide autonomous vehicles. Dostupné z: https://asia.nikkei.com/Business/Aerospace-Defense-Industries/China-s-Geely-builds-satellites-to-guide-autonomous-vehicles

[53] Zhang, P. 2024. Nio makes China's 1st list of L3/L4 autonomous driving pilot automakers. Dostupné z: https://cnevpost.com/2024/06/04/nio-makes-china-l3-l4-pilot-automakers-list/

[54] Kharpal, A. 2022. Chinese Tesla rival Nio and giant Tencent partner to work on self-driving tech. Dostupné z: https://www.cnbc.com/2022/11/29/china-tesla-rival-nio-and-tencent-partner-to-work-on-self-driving-tech.html
[55] Zhang, P.2023. JAC, Huawei sign deal to jointly make luxury EVs. Dostupné z: https://cnevpost.com/2023/12/01/jac-huawei-sign-deal-to-make-evs/
[56] Carey, N. 2024. Chinese EV maker Aiways to go public in US via deal with Hudson Acquisition SPAC. Dostupné z: https://www.reuters.com/markets/deals/chinese-ev-maker-aiways-go-public-us-via-deal-with-hudson-acquisition-spac-2024-05-15/
[57] Funaiole, M.P., Hart, B., Han, J., Jun, J. 2023. China Accelerates Construction of 'Ro-Ro' Vessels, with Potential Military Implications. Dostupné z: https://chinapower.csis.org/analysis/china-construct-ro-ro-vessels-military-implications/
[58] tamtéž
[59] Research in China. 2024. Analysis on Xpeng's Layout in Electrification, Connectivity, Intelligence and Sharing, 2023. Dostupné z: http://www.researchinchina.com/Htmls/Report/2024/74974.html
[60] Anatoliatoday. 2024. After BYD, another Chinese carmaker plans investments in Turkey. Dostupné z: https://anatoliatoday.com/after-byd-another-chinese-carmaker-plans-investments-in-turkey/
[61] 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

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

[63] 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
[64] Informace od partnerů.
[65] 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

[66] Informace od partnerů.
[67] 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

[68] 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/
[69] 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 %*