Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č. j. 7005/2025-NÚKIB-E/630• BRNO • 29. SRPNA 2025

STRATEGICKÁ ANALÝZA

ČÍNSKÉ IP KAMEROVÉ SYSTÉMY: VYSOKÉ RIZIKO ZNEUŽITÍ ZRANITELNOSTÍ, PROBLEMATICKÉ PROPOJENÍ VÝROBCŮ SE STÁTEM A PRAVDĚPODOBNÝ SBĚR ZPRAVODAJSKY CENNÝCH INFORMACÍ

SHRNUTÍ

- **Síťové kamerové systémy (IP kamery) čínského původu mají více než padesátiprocentní podíl na světovém trhu, kdy největšími výrobci jsou společnosti Hikvision a Dahua. Jejich produkty jsou však vysoce rizikové, zejména s ohledem na technickou, politickou, právní nebo etickou stránku. Na základě dat z Registru smluv měly produkty čínských společností v letech 2016–2023 na trhu v ČR celkem třetinový podíl s hodnotou zakázek ve výši přes 13 miliard korun.**
- **Hlavní technické hrozby spojené s čínskými kamerami představují zneužití zranitelností, úmyslná instalace backdoorů, nelegitimní vzdálený přístup a celkově slabá úroveň zabezpečení. V případě, že dojde k detekci zranitelnosti, jsou čínští výrobci povinni ji nejprve nahlásit čínským státním orgánům, které se posléze mohou rozhodnout, jak s ní naloží.**
- **Výrobci kamer jsou na základě čínské legislativy povinni spolupracovat se státními orgány. Je velmi pravděpodobné (75–85 %), že stát toho využívá pro zpravodajskou činnost. Skrze státem vlastněné podniky má Peking vlastnický podíl v mnoha formálně soukromých společnostech (např. Hikvision), v nichž navíc existují buňky vládnoucí komunistické strany dále posilující státní dohled.**
- **Nelze vyloučit (25–50 %), že Čínská lidová republika (ČLR) v zájmu disponovat maximálně efektivním nástrojem pro svoji špionážní činnost prosazuje spolupráci mezi výrobci kamer, vývojáři umělé inteligence a globálně působícími čínskými technologickými společnostmi. Jde o potenciálně velmi rizikovou praktiku, neboť kamery mohou následně disponovat unikátními řešeními, které výrazně posilují jejich potenciálně škodlivé schopnosti.**
- **Nasazení čínských síťových kamer v ČR představuje vysoké riziko, a to s ohledem na kombinaci jejich technických slabin s nestandardní čínskou legislativou, rolí Pekingu ve vlastnických strukturách společností, jejich spoluprací s bezpečnostními a stranickými složkami a dosavadními aktivitami ČLR proti zájmům ČR a jejích spojenců. Je pravděpodobné (55–70 %), že část kamer je čínskými orgány do jisté míry kompromitována.**
- **V kontextu vzdálené správy a předávání dat spojených s provozem kamer do ČLR a zvláštních administrativních oblastí se regulované subjekty dle zákona 181/2014 Sb. Zákon o kybernetické bezpečnosti musí řídit varováním NÚKIB a metodikou k tomuto varování vydanou.**

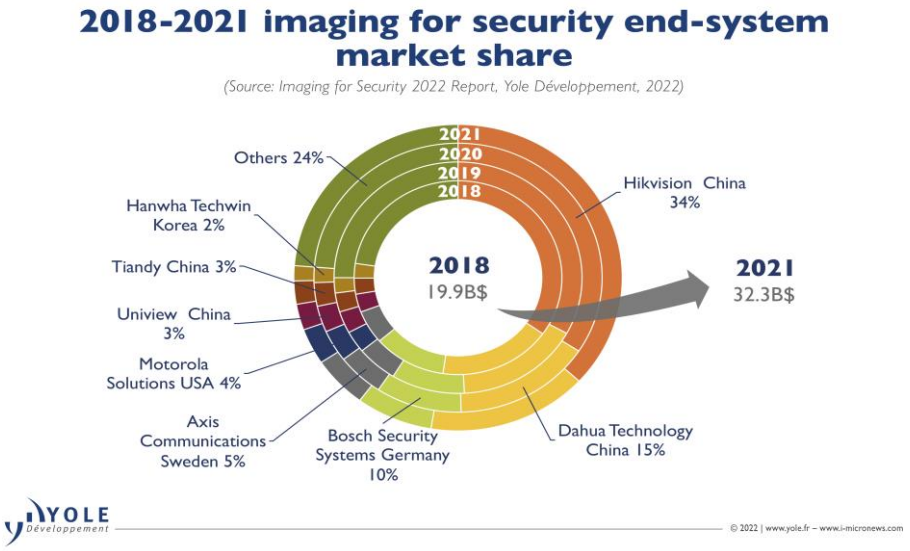
UPOZORNĚNÍ: Informace a závěry obsažené v této analýze vycházejí z veřejně dostupných informací či informací získaných v rámci činnosti NÚKIB.

Bezpečnostní kamerové systémy již jsou běžnou součástí veřejného prostoru a domácností, jež komplexně pokrývají, a to i s ohledem na rozvoj dalších moderních technologií. **Kritické dopady mají především:**

- **internet věcí (internet of things, IoT);**
- **umělá inteligence (artificial intelligence, AI);**
- **strojové učení (machine learning);**
- **sítě páté generace (5G).**

Technologický pokrok v těchto oblastech kvalitativně posouvá schopnost kamer, jež jsou schopny včasně zpracovávat obrovské množství dat.

Obr. 1: Tržní podíl kamerových bezpečnostních systémů v letech 2018-2021



Zdroj: Yole Development

Aktéři vyvíjející aktivity proti zájmům ČR (např. Čínská lidová republika, dále ČLR) mohou získat citlivá data, která lze zneužívat, přičemž především instalace kamer v okolí strategických objektů je mimořádně riziková.

Podobně jako 5G sítě též kamerové systémy kladou vyšší nároky na bezpečnost dodavatelského řetězce. Největší riziko představují systémy, jež pocházejí od výrobců z ČLR, potažmo těch s úzkými vazbami na Peking. Čínský podíl na světovém trhu s kamerami je více než padesátiprocentní, kdy největší podíl drží společnosti Hikvision[i] a Dahua[ii] (viz Obr. 1, více ke společnostem v přílohách 2 a 3).

SVĚTOVÝ TRH S BEZPEČNOSTNÍMI KAMERAMI: VÍCE NEŽ POLOVINU PODÍLU KONTROLUJÍ SPOLEČNOSTI ČÍNSKÉHO PŮVODU

Celosvětově dominují trhu s kamerami společnosti čínského původu, zejména Hikvision a Dahua (viz Obr. 1). Produkty těchto a obecně většiny čínských výrobců jsou však rizikové po technické, politické, právní i etické stránce. Produkty evropských, severoamerických či asijských nečínských firem mají nižší tržní podíl a po technické stránce někdy trpí podobnými nedostatky jako kamery čínské. Oproti nim však chybí politické či právní výzvy související s jejich původem.

Reálný tržní podíl je však zkreslený, neboť mnozí distributoři prodávají kamery čínských společností jako tzv. OEM (Original Equipment Manufacturer), což znamená, že reálně je čínských kamer nasazeno výrazně více. Distributoři tak prodávají nakoupené výrobky jako svoje vlastní (tzv. rebranding), díky čemuž nelze jednoznačně určit, odkud opravdu pocházejí.

Box 1: IP kamera

IP kamera nebo také síťová kamera využívá pro přenos dat internetový protokol. Hlavní rozdíl oproti tzv. CCTV pak představuje schopnost IP kamer přijímat a odesílat data přes internet.

Velkým distributorem kamer Dahua je například německý Bosch. [1] Od roku 2021 je po sankcích Washingtonu přestal nabízet v USA, nicméně je pravděpodobné (55–70 %), že jinde je prodává nadále.[2] Podobně jsou jinými firmami nabízeny též produkty Hikvision.[3] **Celkově pak čínské produkty**

[i] Celým názvem Hangzhou Hikvision Digital Technology Co., Ltd. (杭州海康威视数字技术股份有限公司)

[ii] Celým názvem Zhejiang Dahua Technology Co., Ltd. (浙江大华技术股份有限公司)

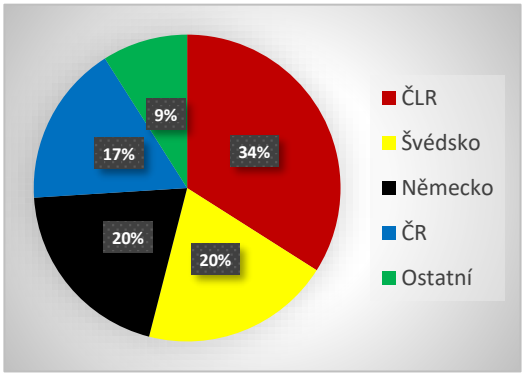
formou OEM nabízí množství západních firem, což limituje určení reálného podílu.

Podle dat z Registru smluv, jež nicméně vzhledem k limitům jeho technického provedení nemusí být kompletní, je podíl čínských společností na českém trhu přibližně 34 % v období let 2016—2023. Avšak podíl ve výši 17 % zaujímají výrobky českých firem, které přitom nejsou významnými výrobci. **V tomto případě stejně jako u dalších společností, jež jsou podezřívány z daných praktik (např. Bosch), pak nelze vyloučit (25–50 %), že se jedná o přeprodej cizích produktů formou OEM.** Pokud by šlo o čínské kamery, které jsou tímto způsobem redistribuovány nejčastěji, tak by celkový podíl mohl překročit 50 %. Tím by situace na českém trhu zrcadlila světovou. Přesto je tuzemsko odlišné tím, že oproti světu zde výrazně větší podíl drží západní výrobky (viz Obr. 2).

Z analýzy dat z Registru smluv vychází, že kamerové systémy, software či další příslušenství společností Hikvision nebo Dahua nakoupily strategické instituce veřejné správy, bezpečnostní organizace, statutární města či vysoké školy a subjekty činné ve výzkumu.

Akvizice těchto systémů organizacemi podobného typu má z pohledu ČLR téměř jistě (90–100 %) zpravodajskou hodnotu, hlavně s ohledem na data, která lze v budovách nebo jejich okolí sbírat. Pokud však organizace nasadila IP kamery, které nejsou připojeny k internetu, tak se snižuje riziko, že se k jejich datům dostanou čínští výrobci a skrze ně pak státní orgány.

Obr. 2: Tržní podíl v ČR dle původu výrobce (2016—2023)



VYSOKÉ RIZIKO ZNEUŽITÍ ZRANITELNOSTÍ ČI NELEGITIMNÍHO VZDÁLENÉHO PŘÍSTUPU HROZÍ ZEJMÉNA V PŘÍPADĚ OTEVŘENÍ KAMER DO SÍTĚ INTERNET NEBO SPRÁVY TŘETÍ STRANOU

Hlavní hrozby spojené s IP kamerami čínského původu představují:

- **zneužití zranitelností kamer připojených na internet (viz Příloha 1);**
- **úmyslná instalace backdoorů;**
- **nelegitimní vzdálený přístup;**
- **celkově problematické zabezpečení.**

Na základě analýzy dostupných dat se drtivá většina zranitelností čínských i dalších kamer nachází v jejich operačním systému, zejména ve firmwaru. V případě čínských produktů je počet zranitelností nebo jejich závažnost na podobné úrovni jako v případě dalších výrobců (např. Axis). **Hlavním problémem však je způsob, jakým výrobci musí podle čínské legislativy postupovat při jejich opravě.**

Zranitelnost musí být nahlášena do dvou dnů od detekování Ministerstvu průmyslu a IT (dále MIIT), které ji hlásí Ministerstvu státní bezpečnosti (dále MSS). MSS je zpravodajská služba s vnitřní i vnější působností, jejíž součástí je také správce národní databáze zranitelností.[4] Ty mohou být MSS zneužity dle uvážení, přičemž ministerstvo zaštiťuje množství čínských APT skupin. **Ve srovnání s dalšími státem zaštítěnými skupinami jsou čínští aktéři hrozeb typičtí právě i svým větším důrazem na zneužívání zranitelností.**

V roce 2022 bylo například zjištěno, že celosvětově více než 80 tisíc kamer Hikvision je zranitelných vůči CVE-2021-36260. Ta byla sice opravena, přesto byla zneužita například botnetem Mirai pro jeho šíření, potažmo zapojení kompromitovaných systémů do DDoS útoků. **Vedle čínských APT10 a APT41 ji pak zneužívali také vybraní ruští aktéři.**[5]

Nelze vyloučit (25–50 %), že probíhá kompromitace softwaru nebo hardwaru části kamer při samotném výrobním procesu či během vydávání aktualizací. **Přestože se jedná o finančně a kapacitně náročnější typ infiltrace, díky přístupu k výrobním procesům či technologiím a případnému úmyslu jde o plně proveditelný způsob kompromitace ze strany ČLR.** Čínské silové orgány měly podobně kompromitovat telekomunikační vybavení od Huawei určené pro

vývoz do Austrálie nebo mikročipy nainstalované v základních deskách společnosti Supermicro.[6] **Je nepravděpodobné (15–20 %), že by s ohledem na čínské politické a právní prostředí byli výrobci tyto praktiky schopni či ochotni odmítnout.**

Pokud by čínské orgány či kdokoli jiný do softwaru nebo firmwaru kamer instalovaly backdoor, jejich nejpravděpodobnějším cílem bude zisk vzdáleného přístupu (remote access). Dle litevského Národního centra pro kybernetickou bezpečnost (dále NKSC) měly k roku 2020 vybrané kamerové systémy od Hikvision a Dahua povoleno servisní prostředí, které umožňuje je ovládat na dálku.[7] **Hlavní hrozbou je v daném případě systematický sběr dat za účelem dalšího zneužití.** Riziková je pak také správa kamer třetí stranou, u níž mohou panovat pochybnosti, jak nakládá se svým přístupem a získanými daty. NKSC poukázalo i na další slabiny vybraných kamer společností Hikvision a Dahua:

- umístění aktualizační infrastruktury na čínských nebo ruských serverech;
- nestandardní chování mobilních aplikací ovládajících kamery (např. vytváření spojení do ČLR či jejich selektivní chování v závislosti na umístění v konkrétní zemi);
- využití méně zabezpečeného autentifikačního schématu HTTP Digest;
- nasazení uzavřených a netransparentních protokolů v infrastruktuře (např. nešifrovaný SADP pro detekci produktů Hikvision v síťové infrastruktuře).[8]

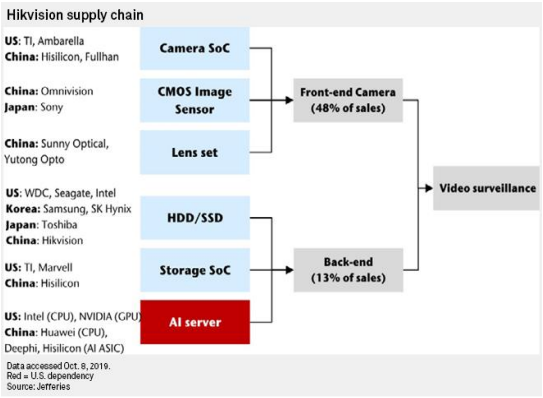
KVŮLI STRIKTNÍ ČÍNSKÉ LEGISLATIVĚ A ÚZKÝM VAZBÁM NA STÁT MOHOU VÝROBCI KAMER JEDNAT I PROTI ZÁJMŮM ZÁKAZNÍKŮ

Přestože čínské podnikatelské prostředí funguje na formálně kompetitivní bázi, tak stát si ve vztahu ke společnostem udržuje široce nastavené pravomoci. Zásadní je v tomto ohledu legislativa ČLR, zejména zákon o státní bezpečnosti, kontrašpionážní zákon, zákon o společnostech či zákon o státní zpravodajské činnosti (viz Příloha 1). **Je téměř jisté (90–100 %), že bezpečnostní a stranické orgány danou legislativu využívají ve svůj prospěch prostřednictvím čínských společností, a to včetně systematického sběru dat využitelných pro zpravodajskou činnost.** Mezi tento typ dat patří i záznamy z kamerových systémů či jiná s nimi spojená data.

ČLR navíc často drží vlastnický podíl v soukromých společnostech. Hikvision je téměř ze 40 % vlastněn státem skrze China Electronics Technology Group Corporation (dále CETC), která spadá pod komisi Státní rady ČLR (viz Příloha 2).[9] Stejně tak drží stát podíl ve společnosti Dahua skrze China Mobile.[10] **Vlastnická role státu je kritická s ohledem na to, že pokud společnost hypoteticky chce fungovat více autonomně, a nikoliv plně v souladu se státními zájmy, tak stát tomu může zamezit skrze různá opatření (např. výměna managementu).**

Čínské společnosti však cílí primárně na zisk, tudíž v zájmu profitu ze státních zakázek nemají důvod spolupráci odmítat. **Stejně tak množství firem čerpá podporu ze státních subvencí, což pak v kombinaci s výhodnými zakázkami ze strany státu, nízkými výrobními náklady a nízkými maržemi představuje jeden z důvodů jejich ekonomického úspěchu.**[11]

Obr. 3: Dodavatelský řetězec Hikvision



Zdroj: S&P Global

Dle zákona o společnostech musí být ustanovena stranická buňka i ve formálně soukromých firmách.[12] **Stát tak posiluje kontrolu nad interním děním.** Vrcholné vedení technologických firem (např. Hikvision, Huawei nebo Baidu) má navíc často vazby na čínskou armádu, s níž společnosti spolupracují na různých projektech.[13] Jedná se o ukázku vojensko-civilní fúze, která využívá civilní technologie pro armádní účely.[14] **V kontextu ČLR pak tato symbióza mezi firmami, stranou a bezpečnostními složkami znamená významné riziko pro zahraniční uživatele čínských technologií.**

SPOLUPRÁCE VÝROBCŮ KAMER S DALŠÍMI ČÍNSKÝMI TECHNOLOGICKÝMI SPOLEČNOSTMI PŘINÁŠÍ NOVÉ VÝZVY V RÁMCI BEZPEČNOSTI DODAVATELSKÉHO ŘETĚZCE

Dodavatelský řetězec kamerových systémů je velmi komplexní, přičemž vedle samotných výrobců v něm hrají roli též společnosti zaměřující se na umělou inteligenci (např. Megvii nebo SenseTime) a čínské technologické společnosti (např. Huawei či Alibaba). Jednotlivé společnosti prokazatelně spolupracují na různých projektech, což je dáno i jejich unikátním know-how. [15] **Avšak nelze vyloučit (25–50 %), že spolupráci prosazuje přímo režim, zejména kvůli vytvoření efektivního produktu, jenž by obsahoval nejpokročilejší technologie jednotlivých firem a byl zároveň schopný sloužit pro špionáž.**

Problematický faktor představuje primárně fakt, že kamerové systémy mohou obsahovat software či hardware výrobců, s nimiž jsou spojena obdobná rizika (např. čínská legislativa či úzké vazby na stát) jako s producenty koncových produktů. **Právě daná rizika jsou významná pro maximální zabezpečení dodavatelského řetězce, včetně subdodavatelů.** Nasazení produktů rizikových subdodavatelů může výrazně zvýšit rizika i jinak nerizikového dodavatele koncového produktu.

Čínské kamery používají západní i domácí produkty, přičemž rizikové jsou zejména ty pocházející z ČLR. Například kamery od společnosti Hikvision v rámci back-endu („neviditelná“ část produktu) nasadily AI servery (servery vytvořené pro podporu AI), které dodává Huawei (viz Obr. 3). Hikvision pak měla dle bývalého zaměstnance SenseTime, významné čínské společnosti na poli AI, být i jejím zákazníkem. [16] **Jde pouze o výčet případů podobných spoluprací pro ilustraci komplexity a rizikovosti dodavatelského řetězce kamer.**

Box 2: Koncept bezpečných měst

Napříč celou ČLR jsou instalovány systémy, jež monitorují či predikují zločin a protesty. Jedná se o příklad tzv. safe city (bezpečné město), který propaguje zejména společnost Huawei. Fakticky je cílem disponovat „kamerami všude a AI nad nimi“. Společnost koncept vyváží též mimo ČLR, zejména pak do zemí tzv. Globálního jihu.

NASAZENÍ ČÍNSKÝCH KAMER PROTI UJGURŮM SPOJENÉ S REPRESEMI UKAZUJE NA ETICKOU NEDŮVĚRYHODNOST VÝROBCŮ

Čínské soukromé společnosti dodávají svá řešení pro stát, který je prokazatelně využívá při represivní činnosti, zejména pak v oblasti čínské východní provincie Sin-ťiang, jíž obývá muslimské etnikum Ujgurů. [17] **Výrobci kamer jako Hikvision, Dahua či Uniview nabízejí tzv. ujgurskou analytiku, v rámci které systémy umí rasově/etnicky odlišit Ujgury od dalších etnik.**[18] Analytiku na základě etnicity rozvíjejí též čínské společnosti Megvii, SenseTime, Huawei, Alibaba nebo Baidu.[19]

Obr. 4: Kamera v ujgurském městě Kašgar

Zdroj: BuzzFeed News

Podobné systémy jsou mimořádně rizikové, neboť jejich nasazení v západních státech může Pekingu poskytnout biometrická data, na nichž lze AI dále trénovat. Je téměř jisté (90–100 %), že Peking usiluje nejenom o analytiku Ujgurů a etnik v ČLR, ale také jiných etnických skupin a ras.

Hikvision i Dahua v regionu Sin-ťiang získaly mnoho vládních kontraktů, jež jenom v letech 2016-2018 přesáhly hodnotu jedné miliardy dolarů (cca 22 miliard korun). [20] Hikvision například vyhrál v tendru na systémy rozpoznávání tváří před stovkami mešit nebo kamery v tzv. převýchovných táborech.[21] Dále jsou napříč provincií nasazeny také další sledovací nástroje, přičemž je velmi pravděpodobné (75–85 %), že jejich dodavateli mohou být i některé společnosti zmíněné v předložené analýze.[22]

IMPLIKACE: KOMBINACE TECHNICKÝCH SLABIN SPOLU S ČÍNSKÝM POLITICKÝM A PRÁVNÍM PROSTŘEDÍM ZNAMENÁ VYSOKÉ RIZIKO

TECHNICKÁ DOPORUČENÍ: ZÁKLADEM JE IZOLACE KAMER OD INTERNETU

Vzhledem k množství zranitelností, jimž čínské kamery čelí a možnostem jejich zneužití, se na technické rovině doporučuje především jejich izolace a nevystavení do internetu. Tím bude výrazně mitigována možnost jejich komunikace směrem k aktérům se škodlivými úmysly.

V případě, že jsou kamery z nějakého důvodu připojeny k internetu, tak by mělo probíhat pravidelné auditování aktivity na portech za účelem detekce nezvyklé komunikace. Zejména čínští aktéři jsou typičtí využíváním často méně známých portů jako svých C2 serverů, jež jsou používány pro škodlivou komunikaci.

Celkově mnoho výrobků, včetně kamer, trpí problémem slabých přednastavených hesel. **Je klíčové, aby tato hesla byla ihned po nastavení změněna a následně periodicky aktualizována, přičemž by měla být silná a unikátní.** Tím se snižuje pravděpodobnost úspěchu útoku hrubou silou (brute-force) či slovníkového útoku.

V případě nasazení kamer čínského původu je zásadní permanentně sledovat informace stran zranitelností. S ohledem na fakt, že výrobci jsou povinni je nejprve hlásit orgánům ČLR, existuje reálná možnost (25–50 %), že se o nich uživatelé včas nedozví.

Nasazení kamer čínského původu znamená vysoké riziko s ohledem na kombinaci těchto faktorů:

- **technické slabiny (např. zranitelnosti);**
- **nestandardní požadavky legislativy ČLR;**
- **vlastnický podíl státu v soukromých firmách;**
- **spolupráce výrobců se silovými složkami ČLR;**
- **podíl společností na potlačování lidských práv;**
- **škodlivé aktivity ČLR v zahraničí.**

Samotné technické aspekty jsou sice samy o sobě problematické, avšak zároveň se jedná o problém, jímž trpí i systémy nečínského původu. **Klíčová je tak kombinace se strategickým aspektem, kdy má ČLR zájem kamerové systémy spolu s AI zneužívat za účelem sběru zpravodajsky využitelných informací nebo potlačování lidských práv. Je pravděpodobné (55–70 %), že část kamer je čínskými orgány do jisté míry kompromitována.**

ČLR disponuje prostředky, jimiž si může efektivně vynutit nebo motivovat spolupráci soukromých firem na špionáži. Těmi jsou zejména legislativa ČLR, která mimo jiné po organizacích žádá podílet se na zpravodajské činnosti, vlastnický podíl státu ve společnostech nebo blízké vztahy části z nich se silovými orgány či aparátem komunistické strany. **Navzdory tomu, že výrobci kamer cílí primárně na finanční zisk, jsou se státem propojeni do míry, že v zájmu zachování profitů a své obchodní činnosti velmi pravděpodobně (75–85 %) participují na jeho škodlivých aktivitách.**

Data zpracovávaná v souvislosti s provozem kamer čínských značek mohou být zneužita nejenom pro zpravodajské účely či kompromitaci určitých osob, nýbrž i pro další trénink AI a její zefektivnění za účelem špionážních aktivit.

STRATEGICKÁ DOPORUČENÍ: DŮKLADNÁ ANALÝZA RIZIK A ZOHLEDNĚNÍ VAROVÁNÍ NÚKIB

Již při samotné úvaze nad akvizicí kamerového systému by si měli uživatelé uvědomit, co vše podobný systém dokáže zpracovávat za data. **Proto je klíčové provést před nákupem a poté nasazením důkladnou analýzu rizik.** Ta by měla zahrnovat taktéž screening prodejce, tedy zda nedistribuuje kamery formou OEM.

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: ČÍNSKÁ LEGISLATIVA RELEVANTNÍ PRO OBLAST KAMEROVÝCH SYSTÉMŮ

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[23] (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[24] (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.[25]

Rozšířená formulace dává čínským orgánům volnost při definování toho, jaké informace se týkají bezpečnosti nebo zájmů státu. Například 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.[26]

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[27] (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.[28]

ZÁKON O STÁTNÍ ZPRAVODAJSKÉ ČINNOSTI (2017)

Zákon o státní zpravodajské činnosti[29] (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.[30]

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.

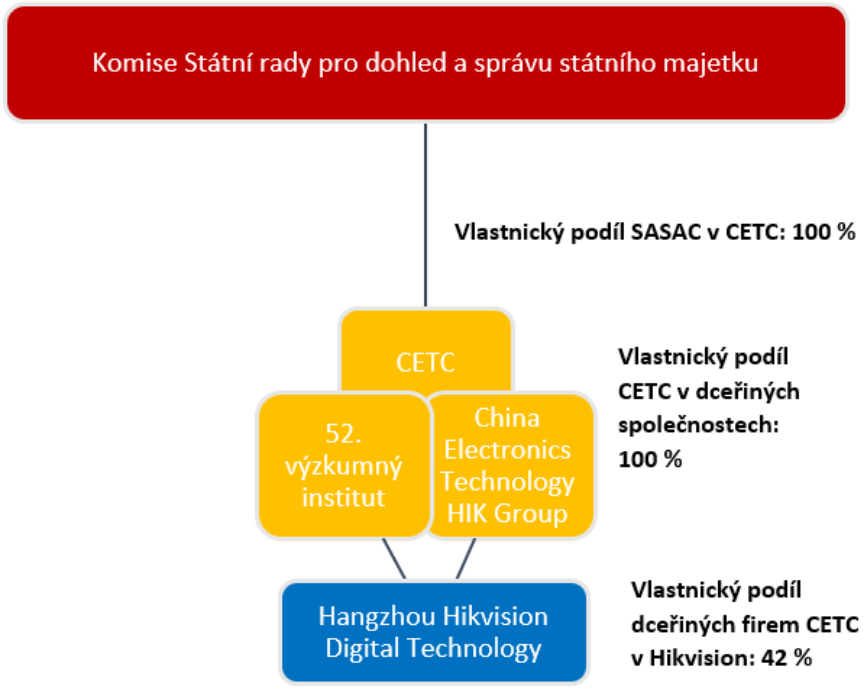
Zákon o bezpečnosti dat (Data Security Law, 中华人民共和国数据安全法)	01.09.2021	zákon	Upravuje podmínky zajištění bezpečnosti dat a zamezení jejich úniku mimo území ČLR. Zákon dává státním autoritám možnost zastavit fungování společnosti, která dle nich bude v rozporu s požadavky zákona.
Zákon o ochraně osobních 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 (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.[31] Nařízení má doplňovat nařízení o internetových algoritmech.
Ustanovení o správě informací v internetových uživatelských účtech	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.

(Provisions on the Management of Internet User Account Information, 互联网用户账号信息管理规定)			
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.

PŘÍLOHA 2: VLASTNICKÁ STRUKTURA SPOLEČNOSTI HIKVISION

Vlastnická struktura společnosti Hikvision je jedním z příkladů komplexity čínského podnikatelského prostředí, propojení státu a byznysu a určité míry státního kapitalismu. Čtyřicetiprocentní vlastnický podíl drží společnost China Electronics Technology HIK Group, která je ze 100 % dceřinou společností China Electronics Technology Group (CETC). Stejně tak je dceřinou společností CETC také 52. výzkumný institut, který drží v Hikvision minoritní dvouprocentní podíl.[32] CETC je ve vlastnictví státu a zaměřuje se primárně na obranný sektor, elektroniku, telekomunikace nebo IT, přičemž je historicky úzce spojen s armádou.[33] CETC a její dceřiné firmy figurují v několika sankčních seznamech USA. CETC je kompletně pod kontrolou Komise Státní rady pro dohled a správu státního majetku (dále SASAC), jež je speciální komisí Státní rady ČLR. Ta je nejvyšším orgánem výkonné moci, přičemž v jejím čele stojí premiér. Mezi zákazníky společnosti patří provinční i lokální instituce veřejné bezpečnosti (včetně Úřadu veřejné bezpečnosti Lidové vlády Ujgurské autonomní oblasti Sin-ťiang) a univerzity velmi těsně navázané na čínské ozbrojené síly (Huazhong University of Science and Technology, Wuhan University)

Obr. 5: Zapojení čínského státu do vlastnické struktury společnosti Hikvision



Zdroj: WSJ

PŘÍLOHA 3: VLASTNICKÁ STRUKTURA SPOLEČNOSTI DAHUA

Ve společnosti Dahua má stát skrze prostředníky nižší vlastnický podíl ve srovnání se společností Hikvision. Na základě otevřených zdrojů by mělo jít přibližně o 12 %. Podíl ve výši 10,42 % drží společnost China Mobile, za níž stojí státem vlastněná China Mobile Communications Group (CMCG), jež je pod přímou kontrolou čínské vlády. Podle amerického resortu obrany má CMCG úzké vazby na lidovou osvobozeneckou armádu.[34] Podíl ve výši 1 % v Dahua kontroluje také suverénní investiční fond Central Huijin Investment (CHI). Ten vlastní China Investment Corporation (CIC), která představuje po norském Vládním penzijním fondu Global druhý největší suverénní investiční fond světa, přičemž je kompletně vlastněna čínským státem. Společnost Dahua se nachází na sankčních seznamech USA. Mezi zákazníky společnosti patří provinční i lokální instituce veřejné bezpečnosti a subjekty navázané na ruské ozbrojené síly (National Industrial Information Security Development Research Center, Zhejiang University, Wuhan University of Technology)

Obr. 6: Zapojení čínského státu do vlastnické struktury společnosti Dahua

Zdroj: NÚKIB

PŘÍLOHA 4: OMEZENÍ UVALENÁ NA ČÍNSKÉ SPOLEČNOSTI ČINNÉ V OBLASTI AI A KAMEROVÝCH SYSTÉMŮ

Přestože čínské kamerové systémy jsou dlouhodobě rizikové, tak ke komplexnějšímu řešení problematiky skrze zákazy a různá omezení dochází přibližně až od roku 2019. **Důvodem dosud byly takřka výlučně podíl společností na potlačování lidských práv, zejména Ujgurů v oblasti Sin-ťiang, případně riziko špionáže ze strany čínských zpravodajských služeb skrze produkty daných firem.** Nejde o vyčerpávající výčet.

Státy a entity	Typ opatření
Austrálie	Australská vláda v roce 2023 oznámila, že dojde k odstranění kamer čínských výrobců instalovaných na místech významných pro obranu země (defence sites). Oznámení přišlo poté, co audit odhalil, že na vládních budovách či pozemcích je nainstalováno až 900 kamer společností Hikvision a Dahua. Minimálně jedna kamera byla detekována i na ministerstvu obrany, nicméně celkový počet v dalších institucích, jež jsou spojeny s resortem je neznámý. Stínový ministr pro kybernetickou bezpečnost, James Patterson, který si audit vyžádal, přiznal, že Canberra nemá informace o předávání dat z kamer čínským zpravodajským službám.[35] Kamery od společnosti Hikvision byly již v roce 2018 odstraněny z leteckých základen.[36] Kamery čínských výrobců se rozhodly nahradit i další australská města a státy, mj. stát Victorie nebo město Geelong.[37]
Dánsko	Dánské námořnictvo a národní policejní síly odstranily v červnu 2023 z bezpečnostních důvodů 152 kamer čínských výrobců. Rok dříve region Hovedstaden rozhodl zastavit nákup kamer Hikvision. Rozhodnutí v regionu hlavního města přichází na pozadí dlouhodobé veřejné debaty o kamerách tohoto výrobce.[38]
Evropská unie	Evropský parlament v roce 2021 odhlasoval odstranění termokamer Hikvision ve svých prostorách. Ty v nich byly instalovány od vypuknutí pandemie covid-19.[39]
Indie	Indické námořní velitelství v roce 2021 požádalo všechny své jednotky, aby přerušily nákup kamer a sledovacích systémů od společnosti Hikvision. Současně nařídilo jejich postupnou výměnu. Důvodem bylo varováním nejvyšších bezpečnostních a zpravodajských agentur, které upozornilo na vážné obavy z možné hrozby úniku dat jejich prostřednictvím.[40] Dále v roce 2025 došlo k přijetí opatření nakazující výrobcům kamer předložit hardware, software a zdrojový kód k posouzení do státních laboratoří. Toto nařízení se dotýká včech výrobců kamer.[41]
Kanada	Kanadská vláda v roce 2025 nařídila společnosti Hikvision, aby z důvodu obav o národní bezpečnost ukončila své aktivity v Kanadě.[42] Na konci prosince 2023 vydal ministr pro kybernetickou bezpečnost provincie Quebec Éric Caire ministerskou vyhlášku zakazující veřejným institucím v Quebecu instalovat nové telekomunikační a sledovací technologie Hikvision a Dahua.
Litva	V roce 2022 litevská vláda zakázala používání technologií z nepřátelských zemí, tedy včetně kamer společností Dahua a Hikvision, pro přibližně 400 institucí, přičemž dala čas na výměnu stávajících zařízení do roku 2025. Dotčené instituce zahrnovaly správce kritické informační infrastruktury, ty, které se podílí na mobilizačních úkolech, působí v oblasti obrany nebo v odvětví významných pro národní bezpečnost.[43]

Nizozemsko	Zástupce starosty Amsterdamu v roce 2024 uvedl v oficiálním dopise, že město zakazuje nákup čínských kamer, včetně značek Hikvision a Dahua. Zároveň plánuje v příštích pěti letech jejich používání postupně ukončit. Jako důvody uvedl lidská práva a kyberberpečnost.[44]
Norsko	V roce 2020 Etická rada doporučila, aby Vládní penzijní fond Global (dále GPF-G či tzv. Ropný fond), jenž je součástí Vládního penzijního fondu Norska, neinvestoval do společnosti Hikvision. GPF-G je jedním z největších suverénních investičních fondů na světě a kontroluje 1,4 % všech světových společností kótovaných na burze. Fond neinvestuje do firem, jež se podílejí na porušování lidských práv, znečišťují přírodu či vyrábí tabákové výrobky.[45] Norské hlavní město Oslo zakázalo kamery od čínského výrobce Hikvision v zařízeních, včetně těch, která slouží k přenosům sportovních utkání v městských sportovních halách.[46]
Nový Zéland	Ačkoliv Nový Zéland zákaz používání kamer od čínských výrobců dosud nevydal, v roce 2022 se tamní Ministerstvo obchodu, inovací a zaměstnanosti (Ministry of Business, Innovation and Employment, MBIE) rozhodlo vyloučit společnost Hikvision ze svých dodavatelů.[47]
Spojené státy americké	V roce 2019 bylo celkem 28 čínských subjektů, včetně společností Hikvision, Dahua, Megvii a SenseTime, zařazeno na tzv. Seznam entit (Entity List). Toto zařazení fakticky brání americkým subjektům či těm využívajícím americké technologie prodávat sankcionovaným entitám.[48] V roce 2022 Federální komise pro komunikace (dále FCC) rozšířila původní zákaz na dovoz čínských technologií, jež představují neakceptovatelné riziko pro národní bezpečnost. Ten se v případě kamer týká společností Hikvision, Dahua a Huawei. Ty nesmí do země dovážet své produkty, pokud nezajistí, že nedojde k jejich využití v oblastech veřejné bezpečnosti, ochrany vládních objektů a národní bezpečnosti.[49] Omezení na prodej či použití vydaly taktéž americké státy Georgia, Indiana, Florida, Jižní Dakota , Louisiana, Maine, Nebraska, Nevada, New Hampshire, New Jersey a Wisconsin.[50]
Spojené království	Vládní úřady dostaly v roce 2022 pokyn neinstalovat nové kamery čínské provenience na citlivých místech (sensitive sites). Omezení se vztahuje na produkty firem podléhajících zákonu o státní zpravodajské činnosti. Představitelé dotčených organizací mají zvážit také odstranění již instalovaných zařízení, přičemž ta by neměla být připojena do interních sítí. Zajímavostí je, že po daném pokynu se začala diskutovat aféra poslance Matta Hancocka s jeho poradkyní, kterou v roce 2021 zachytil právě čínský kamerový systém. Přestože neexistují informace, že by daná data byla Pekingem zneužita, tak tento případ ilustruje široké spektrum možností, jak například kompromitovat skrze eventuálně zneužitý systém zájmové osoby či je vydírat pomocí podobně citlivých záznamů. [51] V roce 2022 se k nahrazení kamer Hikvision ve vládních institucích odhodlalo i Skotsko a o rok později Wales, který se rozhodl nahradit kamery Hikvision i v rámci policie.[52]
Tchaj-wan	Tchaj-wan v roce 2021 vydal zákaz používání čínských technologií, včetně produktů výrobců Hikvision a Dahua, ve všech vládních institucích.[53]
Korporátní entity	Výrobky společností Hikvision a Dahua omezily či zakázaly taktéž korporátní entity. Spolupráci s oběma výrobci ukončilo např Tesco (2023) Spolupráci se společností Hikvision ukončil skandinávský poskytovatel bezpečnostních služeb Avarn (2021). Spolupráci se společností Dahua ukončily Bosch (2020), Honeywell (2022).

ZDROJE

[1] IPVM. 2022. Dahua OEM Directory. Dostupné z: https://ipvm.com/reports/dahua-oem

[2] IPVM. 2023. Bosch Stopped Selling Made in PRC Cameras to the United States. Dostupné z: https://ipvm.com/reports/bosch-prc-usa ; Chris Burt. 2019. U.S. drops Entity List hammer on Chinese facial recognition unicorns and biometrics providers. Dostupné z: https://www.biometricupdate.com/201910/u-s-drops-entity-list-hammer-on-chinese-facial-recognition-unicorns-and-biometrics-providers

[3] IPVM. 2023. Hikvision OEM Directory 2023. Dostupné z: https://ipvm.com/reports/hik-oems-dir

[4] Catalin Cimpanu. 2021. Chinese government lays out new vulnerability disclosure rules. Dostupné z: https://therecord.media/chinese-government-lays-out-new-vulnerability-disclosure-rules

[5] Bill Toulas. 2022. Over 80,000 exploitable Hikvision cameras exposed online. Dostupné z: https://www.bleepingcomputer.com/news/security/over-80-000-exploitable-hikvision-cameras-exposed-online/ ; Bill Toulas. 2022. Moobot botnet spreading via Hikvision camera vulnerability. Dostupné z: https://www.bleepingcomputer.com/news/security/moobot-botnet-spreading-via-hikvision-camera-vulnerability/

[6] Jordan Robertson a Jamie Tarabay. 2021. Chinese Spies Accused of Using Huawei in Secret Australia Telecom Hack. Dostupné z: https://www.bloomberg.com/news/articles/2021-12-16/chinese-spies-accused-of-using-huawei-in-secret-australian-telecom-hack#xj4y7vzkg ; Jordan Robertson a Michael Riley. 2018. The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. Dostupné z: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies#xj4y7vzkg

[7] National Cyber Security Centre. 2020. Assessment of cyber security of video surveillance cameras supplied in Lithuania: analysis of Hikvision and Dahua product samples. Dostupné z: https://www.nksc.lt/doc/en/analysis/2020_06_09_Hikvision-Dahua.pdf ; Zak Doffman. 2019. Warning As Millions Of Chinese-Made Cameras Can Be Hacked To Spy On Users: Report. Dostupné z: https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras ; John Honovich a John Scanlan. 2019. Dahua Wiretapping Vulnerability. Dostupné z: https://ipvm.com/reports/dahua-audio

[8] National Cyber Security Centre. 2020. Assessment of cyber security of video surveillance cameras supplied in Lithuania: analysis of Hikvision and Dahua product samples. Dostupné z: https://www.nksc.lt/doc/en/analysis/2020_06_09_Hikvision-Dahua.pdf

[9] John Honovich. 2015. Hikvision And The PRC China Government. Dostupné z: https://ipvm.com/reports/hikvision-prc-gov ; John Honovich. 2016. Hikvision PRC China Government Origin And Control. https://ipvm.com/reports/hikvision-origin

[10] Charles Rollet. 2021. State-Owned China Mobile Acquiring 10% of Dahua. Dostupné z: https://ipvm.com/reports/china-mobile-dahua

[11] Ryan Mcmorrow. 2019. Huawei a key beneficiary of China subsidies that US wants ended. Dostupné z: https://phys.org/news/2019-05-huawei-key-beneficiary-china-subsidies.html ; Ann Cao. 2023. China gave 190 chip firms US$1.75 billion in subsidies in 2022 as it seeks semiconductor self-sufficiency. Dostupné z: https://www.scmp.com/tech/tech-war/article/3219697/china-gave-190-chip-firms-us175-billion-subsidies-2022-it-seeks-semiconductor-self-sufficiency ;

[12] Richard McGregor. 2019. How the state runs business in China. Dostupné z: https://www.theguardian.com/world/2019/jul/25/china-business-xi-jinping-communist-party-state-private-enterprise-huawei

[13] IPVM. 2021. Hikvision And China's Military. Dostupné z: https://ipvm.com/reports/hikvision-prc-military ; Dan Strumpf. 2021. Chinese Surveillance-Gear Maker Hikvision Has Ties to Country's Military, Report Says. Dostupné z: https://www.wsj.com/articles/chinese-surveillance-gear-maker-hikvision-has-ties-to-countrys-military-report-says-11621941983

[14] Elsa B. Kania a Lorand Laskai. 2021. Myths and Realities of China's Military-Civil Fusion Strategy. Dostupné z: https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy ; Audrey Fritz. 2021. At the Nexus of Military-Civil Fusion and Technological Innovation in China. Dostupné z: https://thediplomat.com/2021/07/at-the-nexus-of-military-civil-fusion-and-technological-innovation-in-china/

[15] FT. 2021. Can SenseTime become a Chinese AI champion?. Dostupné z: https://www.ft.com/content/c735e0f3-5704-47b5-a76f-7a02d53a1525 ; Xiuxi Zhu a Priyanka Boghani. 2019. US ban to impact Megvii IPO, force Hikvision to swap suppliers. Dostupné z: https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/us-ban-to-impact-megvii-ipo-force-hikvision-to-swap-suppliers-54647205 ; Jon Russell. 2018. Alibaba's

newest initiative aims to make Hong Kong a global AI hub. Dostupné z: https://techcrunch.com/2018/05/21/alibaba-senstime-hong-kong-ai-lab/ ; Rita Liao. 2019. Alibaba-backed facial recognition startup Megvii raises $750 million. Dostupné z: https://techcrunch.com/2019/05/08/megvii-750-million/

[16] FT. 2021. Can SenseTime become a Chinese AI champion?. Dostupné z: https://www.ft.com/content/c735e0f3-5704-47b5-a76f-7a02d53a1525

[17] Paul Mozur. 2019. One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority. Dostupné z: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html ; Megha Rajagopalan. 2017. This Is What A 21st-Century Police State Really Looks Like. Dostupné z: https://www.buzzfeednews.com/article/meghara/the-police-state-of-the-future-is-already-here ; Darren Byler. 2019. China's hi-tech war on its Muslim minority. Dostupné z: https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition

[18] Charles Rollet. 2019. Hikvision Markets Uyghur Ethnicity Analytics, Now Covers Up. Dostupné z: https://ipvm.com/reports/hikvision-uyghur ; IPVM Team. 2020. Dahua Racist Uyghur Tracking Revealed. Dostupné z: https://ipvm.com/reports/dahua-uyghur ; Charles Rollet. 2020. Uniview Racist Uyghur Recognition Revealed. Dostupné z: https://ipvm.com/reports/uniview-uyghur

[19] IPVM Team. 2021. Patenting Uyghur Tracking - Huawei, Megvii, More. Dostupné z: https://ipvm.com/reports/patents-uyghur ; Mitchell Clark. 2021. Leaked documents link Huawei to China's domestic spying in Xinjiang. Dostupné z: https://www.theverge.com/2021/12/14/22834860/huawei-leaked-documents-xinjiang-region-uyghur-facial-recognition-prisons-surveillance

[20] Charles Rollet. 2018. Dahua and Hikvision Win Over $1 Billion In Government-Backed Projects In Xinjiang. Dostupné z: https://ipvm.com/reports/xinjiang-dahua-hikvision

[21] Charles Rollet. 2018. Hikvision Wins PRC Government Forced Facial Recognition Project Across 967 Mosques. Dostupné z: https://ipvm.com/reports/hik-mosques

[22] Josh Chin a Clément Bürge. 2017. Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life. Dostupné z: https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355

[23] Ministry of National Defense of the People's Republic of China. 2015. National Security Law of the People's Republic of China. Dostupné z: http://eng.mod.gov.cn/publications/2017-03/03/content_4774229.htm

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

[25] Nikkei Asia. 2023. China's planned changes to espionage law alarm foreign businesses. Dostupné z: https://asia.nikkei.com/Politics/China-s-planned-changes-to-espionage-law-alarm-foreign-businesses

[26] Informace od partnerů.

[27] Cyberspace Administration of China. 2017. 中华人民共和国网络安全法. Dostupné z: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

[28] Informace od partnerů.

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

[30] Law Bridge. 2013. Company Law of the People's Republic of China (Revised in 2013). Dostupné z: http://www.lawbridge.org/zhong-hua-ren-min-gong-he-guo-gong-si-fa-2013-nian-xiu-ding/

[31] Global Times. 2022. China's draft regulation bans app providers from endangering national security. Dostupné z: https://www.globaltimes.cn/page/202201/1245154.shtml

[32] Dan Strumpf. 2017. Surveillance Cameras Made by China Are Hanging All Over the U.S. Dostupné z: https://www.wsj.com/articles/surveillance-cameras-made-by-china-are-hanging-all-over-the-u-s-1510513949

[33] Matthew Luce. 2012. A Model Company: CETC Celebrates 10 Years of Civil-Military Integration. Dostupné z: https://jamestown.org/program/a-model-company-cetc-celebrates-10-years-of-civil-military-integration/

[34] Bethany Allen-Ebrahimian a Zach Dorfman. 2020. Defense Department produces list of Chinese military-linked companies. Dostupné z: https://www.axios.com/2020/06/24/defense-department-chinese-military-linked-companies

[35] Tiffanie Turnbull. 2023. Australia to remove Chinese surveillance cameras amid security fears. Dostupné z: https://www.bbc.com/news/world-australia-64577641

[36] Charles Rollet. 2018. Australia and French National TV Investigate Hikvision, Australia Military To Remove Hikvision Cameras. Dostupné z: https://ipvm.com/reports/aus-fra-hik

[37] IPVM Team. 2024. Where Dahua and Hikvision Are Banned. Dostupné z: https://ipvm.com/reports/hikua-bans
[38] Signe Julie Andersen. 2022. Farvel og tak: Region dropper kinesiske overvågningskameraer . Dostupné z: https://www.tv2kosmopol.dk/region-hovedstaden/farvel-og-tak-region-dropper-kinesiske-overvaagningskameraer
[39] Charles Rollet. 2021. EU Parliament Removes Hikvision, Citing Human Rights Abuses. Dostupné z: https://ipvm.com/reports/hik-eu
[40] Pradip R Sagar. 2021. EXCLUSIVE: Indian military under target by Chinese origin surveillance systems . Dostupné z: https://www.theweek.in/news/india/2021/09/03/indian-military-under-target-by-chinese-origin-surveillance-systems.html
[41] Aditya Kalra. 2025. India's alarm over Chinese spying rocks the surveillance industry. Dostupné z: https://www.reuters.com/world/china/indias-alarm-over-chinese-spying-rocks-surveillance-industry-2025-05-28/
[42] Kanishka Singh a Ismail Shakil. 2025. Canada orders China's Hikvision to close Canadian operations. Dostupné z: https://www.reuters.com/markets/emerging/ottawa-orders-chinese-manufacturer-hikvision-shutter-canadian-operations-2025-06-28/, Martin Patriquin. 2024. Quebec has banned Chinese-made surveillance gear. Why won't the feds? Dostupné z: https://thelogic.co/news/quebec-ink/quebec-has-banned-chinese-made-surveillance-gear-why-wont-the-feds/
[43] Kristina Karloné. 2023. Kaunas reluctant to scrap brand new cameras after Lithuania bans Chinese tech. 2021. Dostupné z: https://www.lrt.lt/en/news-in-english/19/1960334/kaunas-reluctant-to-scrap-brand-new-cameras-after-lithuania-bans-chinese-tech, BNS. 2021. Lithuanian MoD moves to ban Chinese, Russian tech. Dostupné z: https://www.lrt.lt/en/news-in-english/19/1542279/lithuanian-mod-moves-to-ban-chinese-russian-tech
[44] IPVM Team. 2024. Where Dahua and Hikvision Are Banned. Dostupné z: https://ipvm.com/reports/hikua-bans, Dopis radního pro ICT města Amsterdam Alexandera Scholtese. Dostupné z: https://s.ipvm.com/uploads/embedded_file/b05c034fd409063b8d9fc950cc0a8173a6af3ea30345dc22a8a2b25f3f2ee09e/3edda1bc-54aa-492b-a128-6081deedb85e.pdf
[45] Council on Ethics – the Government Pension Fund Global. 2020. Recommendation to exclude Hangzhou Hikvision Digital Technology Co Ltd from investment by the Government Pension Fund Global. Dostupné z: https://d1tzzns6d79su2.cloudfront.net/uploads/embedded_file/4e20e1c7e36f45b1bc4d4ff8e9c64acfcf89f5c4f779b353035ee03e9642175c/bac9cd2a-4b1c-4193-add4-7202d6540b5a.pdf
[46] IPVM Team. 2024. Where Dahua and Hikvision Are Banned. Dostupné z: https://ipvm.com/reports/hikua-bans,
[47] Radio New Zealand. 2022. Ministry will no longer accept equipment from Chinese firm Hikvision. Dostupné z: https://www.rnz.co.nz/news/national/472545/ministry-will-no-longer-accept-equipment-from-chinese-firm-hikvision
[48] John Honovich. 2019. Hikvision and Dahua Sanctioned for Human Rights Abuses. Dostupné z: https://ipvm.com/reports/sanction-hikua ; Department of Commerce. 2019. Addition of Certain Entities to the Entity List. Dostupné z: https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list
[49] Carly Page. 2022. US government bans Huawei, ZTE and Hikvision tech over 'unacceptable' spying fears. Dostupné z: https://techcrunch.com/2022/11/28/fcc-huawei-zte-hikvision-hytera-dahua-ban/ ; Bill Toulas. 2022. US bans sales of Huawei, Hikvision, ZTE, and Dahua equipment. Dostupné z: https://www.bleepingcomputer.com/news/security/us-bans-sales-of-huawei-hikvision-zte-and-dahua-equipment/
[50] IPVM Team. 2024. Where Dahua and Hikvision Are Banned. Dostupné z: https://ipvm.com/reports/hikua-bans
[51] BBC. 2022. UK government bans new Chinese security cameras. Dostupné z: https://www.bbc.com/news/uk-politics-63749696 ; Gareth Corfield. 2023. Chinese CCTV cameras that caught Matt Hancock affair kiss to be banned. Dostupné z: https://www.telegraph.co.uk/business/2023/06/06/chinese-cctv-cameras-that-caught-matt-hancock-affair/
[52] Peter Gillibrand. 2023. CCTV: Welsh police and government turn off Chinese Hikvision cameras. Dostupné z: https://www.bbc.com/news/uk-wales-64629861
[53] Yu-fu Chen. 2022. Report details why Chinese products banned at agencies. Dostupné z: https://www.taipeitimes.com/News/taiwan/archives/2022/10/25/2003787690

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
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.
TLP: AMBER	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám než výše uvedeným, nesmí být informace poskytnuta.
TLP: AMBER+STRICT	Informace může být sdílena pouze v rámci organizace, které byla informace poskytnuta.
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.
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	*25–50 %*
Nepravděpodobně	*15–20 %*
Velmi nepravděpodobně	*0–10 %*