Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.j. 1852/2022-NÚKIB-E/310 • BRNO • 12. DUBNA 2022
[ANALÝZA HROZBY]

BEZPEČNOST MOBILNÍCH SÍTÍ PÁTÉ GENERACE (5G): VÝZNAMNÁ RIZIKA A KOMPLEXITA TECHNOLOGIE VYŽADUJE PROVĚŘENÍ VÝROBCŮ NAD MOŽNOSTI MOBILNÍCH OPERÁTORŮ

SHRNUTÍ

- **Sítě 5G v plně rozvinuté podobě mají, kromě benefitů pro mobilní telefony, potenciál stát se klíčovou součástí průmyslu, autonomní dopravy, internetu věcí, a přinést rozvoj odvětví jako telemedicína a virtuální realita.**
- **Síť 5G by v případě kompromitace mohla sloužit jako nástroj k velmi obtížně zjistitelným a prokazatelným sabotážím a špionáži. V případě, že by ji útočník dokázal vyřadit z provozu, paralyzoval by na ni navázané služby.**
- **Kompromitace sítě 5G v ČR by pro stát mohla představovat riziko ohrožení životů a zdraví obyvatel, velkých finančních škod, včetně škod na duševním vlastnictví.**
- **Zajištění bezpečnosti sítí 5G není otázka čistě technického charakteru. Hledání slabin v jednotlivých zařízeních je kvůli jejich komplexitě a novým aktualizacím softwaru nedostatečné. Je proto třeba brát v potaz i netechnické faktory jako důvěru ve výrobce a právní nebo politické prostředí, ve kterém se výrobce pohybuje. Mobilní operátoři však nemají kapacity na vyhodnocování těchto faktorů a jakožto subjekty maximalizující zisk mohou navíc preferovat ekonomické faktory nad bezpečností.**
- **Případová studie: Čínská společnost Huawei je v současnosti nejvíce kontroverzním výrobcem 5G komponent. Kromě vazeb společnosti na Čínskou komunistickou stranu a Čínskou lidově osvobozeneckou armádu existuje i řada konkrétních případů, kdy Huawei zneužila svou pozici ve prospěch Číny. Zdrojem problému je čínské právní a politické prostředí a potenciální riziko tak představují všichni čínští výrobci.**
- **Do budoucna se ovšem nemusí jednat jen o Čínu, jelikož geopolitická a ekonomická situace s výrobci a dodavateli 5G sítí se může během dlouhého životního cyklu těchto technologií proměnit. Je proto třeba univerzální systémové řešení.**

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

S MOŽNOSTMI 5G SÍTÍ ROSTOU POTENCIÁLNÍ DOPADY JEJICH KOMPROMITACE

Mobilní sítě páté generace (5G) představují nástupce současných mobilních telekomunikačních sítí.[1] Oproti sítím čtvrté generace mají přinést kvalitativní posun především v rychlosti přenosu dat, nízké latenci a množství současně připojených zařízení.

Sítě 5G necílí pouze na uživatele mobilních telefonů, ale mají ambici stát se univerzální telekomunikační sítí pro širokou škálu současných a budoucích aplikací, jako je internet věcí (IoT), samořídící vozidla, telemedicína, nebo nová generace automatické průmyslové výroby a streamování virtuálních realit.[2]

Obrázek 1: Možné přínosy 5G sítí

Zdroj: T-Mobile.cz

S rostoucím významem a množstvím připojených zařízení a služeb ovšem narůstají potenciální rizika v případě, že se taková univerzální síť stane terčem kybernetického útoku. Rizika kompromitace budou vyhodnocena v následujících třech kapitolách, a to na bázi CIA triády (viz obrázek 2).[3]

Obrázek 2: Triáda kybernetické bezpečnosti CIA

Zdroj: NÚKIB

DOSTUPNOST: MOŽNOST VYŘAZENÍ KLÍČOVÝCH SLUŽEB ZÁVISLÝCH NA 5G KONEKTIVITĚ

Dostupnost (Availability) dat je primární zranitelností telekomunikační sítě. Pokud útočník vyřadí z provozu klíčové části sítě, data přenášena skrze síť se stanou nedostupná. [4] **Útok na dostupnost může vyřadit z provozu každou službu a technologii, jež bude na 5G sítích závislá. Vzhledem k množství technologií, a služeb, které na 5G mohou být v budoucnu závislé (autonomní doprava, telemedicína, průmysl atd.), se tak jedná o velice účinný nástroj sabotáže, který může výrazně narušit chod státu, ekonomiky a v krajním případě ohrozit lidské životy.** Takový útok by na rozdíl od narušení integrity dat byl méně nenápadný, ale za cenu mnohem efektivnějších plošných výsledků a okamžitých dopadů. Jedná se tak o scénář nízké pravděpodobnosti, ale vysokého dopadu. Riziko takového útoku následně stoupá v případě otevřeného ozbrojeného konfliktu, kdy útočník nemá potřebu skrývat svou agresi. Ačkoliv taková situace nemusí být v současnosti aktuální, komponenty 5G sítě mají plánovanou životnost na dobu až deseti let a geopolitická situace se může v tomto horizontu změnit.

DŮVĚRNOST: 5G SÍTĚ ZDROJEM CITLIVÝCH DAT STÁTU, PRŮMYSLU, ZDRAVOTNICTVÍ I KONCOVÝCH UŽIVATELŮ

Důvěrnost (Confidentiality), v tomto ohledu zajištění, aby k datům neměl neautorizovaný přístup cizí aktér, představuje problematický aspekt telekomunikačních sítí všech generací. Telekomunikační sítě ze své podstaty představují řečiště dat, jejichž obsah se odvíjí od jejich uživatelů. V případě 5G sítí tak pravděpodobně (55–70 %) budou na sítích kolovat citlivá zdravotní data (telemedicína), polohová data (autonomní doprava, polohové služby mobilních telefonů), citlivé osobní údaje (IoT zařízení v domácnosti), obchodní know-how (Průmysl 4.0) a mnoho dalších. **Sítě 5G jsou zdrojem vysoce citlivých a cenných dat relevantních pro stát, společnosti i koncové uživatele a v případě kompromitace mohou tato data získat i útočníci.** V případě použití šifrované komunikace stále dochází k produkci velkého množství metadat,[5] která mohou být pro útočníka také užitečná. K prolomení šifrování nemusí dojít okamžitě, ale může být prolomeno v budoucnosti, až budou vyvinuty dostatečné technické prostředky (např. kvantové počítače).[6] **Pokud si útočník data uloží, může je tak prolomit dodatečně. Takto získané informace mohou mít pro útočníka velkou cenu, jelikož některé informace jsou hodnotné i s dlouhým časovým odstupem.** Telekomunikační síť tak ze své podstaty představuje vhodný nástroj pro získávání dat.[7]

INTEGRITA: NARUŠENÍ DAT V 5G SÍTÍCH MŮŽE VÉST K ŠIROKÉ ŠKÁLE ÚTOKŮ OHROŽUJÍCÍCH ZDRAVÍ, ŽIVOTY I MAJETEK

Integrita (Integrity) dat představuje jistotu, že data nebyla pozměněna cizím aktérem. Její narušení přináší rizika navázaná na provoz jednotlivých služeb, procesů a technologií stojících na fungování 5G. Narušení integrity dat může:

- v autonomní dopravě způsobit dopravní nehody a následné dopravní a logistické kolapsy,[8]
- v průmyslu vést k průmyslovým nehodám a zastavení výroby (které by v četnějších případech mohlo vést k významným ekonomickým ztrátám).[9]
- v telemedicíně dopadnout na přímé ohrožení zdraví a života pacienta.

Útok na integritu dat v 5G sítích proto představuje potenciálně silný nástroj pro různé formy sabotáže. Ačkoliv provedení takovýchto činů by bylo velmi pravděpodobně (75–85 %) náročné i pro pokročilého aktéra, nelze tato rizika podceňovat. **Přestože je taková forma útoku méně pravděpodobná, nese s sebou velkou míru závažného dopadu. Tento aspekt v kombinaci s obtížným odhalením a následně ztíženou atribucí je pro sofistikovaného útočníka zajímavou příležitostí.**

UNIKÁTNÍ POZICE VÝROBCŮ: MOŽNOST ZNEUŽÍT 5G SÍŤ JAKO VEKTOR ÚTOKU

Telekomunikační sítě jsou zpravidla poměrně robustně zabezpečené proti kybernetickým útokům a 5G přináší řadu nových bezpečnostních prvků pro zvýšení obecné kybernetické bezpečnosti. Výše zmíněné hrozby proto představují velmi náročně proveditelné scénáře, vyžadující velké množství expertízy a prostředků. Problematická je ale v této situaci pozice dodavatele klíčových komponent 5G sítě jako jsou například vysokovýkonné MIMO antény. Ta spočívá především ve zvýšené komplexitě výpočetních zařízení, která jsou nezbytná k fungování 5G sítě. **Komponenty 5G sítí (jak hardware, tak software) jsou natolik komplexní, že je prakticky nemožné je efektivně kontrolovat. Ve výpočetních zařízeních, jež budou součástí 5G infrastruktury, se tak mohou ukrývat úmyslné zranitelnosti ze strany dodavatele, které není možné efektivně vyhledat a eliminovat.** Bez těchto výpočetních kapacit se ovšem chod 5G sítí neobejde. Vysoký výpočetní výkon potřebují například antény aplikující formování paprsků signálu, které představují jeden z klíčových prvků 5G sítí.[10]

BOX 1: Huawei Cyber Security Evaluation Centre (HCSEC) ve Spojeném království

Huawei Cyber Security Evaluation Centre (HCSEC), bylo zřízeno vládou Spojeného království a společností Huawei k ověřování a vyhodnocování Huawei produktů mířících do britských telekomunikačních sítí. Ačkoliv se Huawei finančně podílí na provozu HCSEC, provoz centra spadá výlučně pod britské autority. Centrum bylo spuštěno v roce 2010 a od té doby jeho dozorčí komise vydává každoroční zprávy shnující činnost centra a analyzující kyberbezpečnostní aspekty produktů Huawei a přístup společnosti k jejich řešení a mitigaci

Druhým problematickým aspektem bezpečnosti je u plně rozvinutých (tzv. standalone) 5G sítí absence efektivního dělení na periferii a jádro ve snaze o snížení latence.[11] **Kvůli této nové decentralizované struktuře odpadá možnost rozdělit sítě na jádro a periferii, čímž bylo u předchozích generací sítí možné zamezit vstupu rizikových dodavatelů do citlivých částí sítě (jádro) a umožnit jim participaci pouze na okraji (periferie), kde je riziko výrazně menší.**[12] Potenciálně citlivá data mohou procházet jakoukoliv částí 5G sítí a být oddělena pouze virtuálně. Takovéto oddělení jednotlivých funkcí sítě je garantováno technologií výrobce, a ten je tak ve výhodné pozici v případech, kdy se chce dostat k citlivým datům.

NELZE SE SPOLÉHAT JEN NA TECHNICKOU BEZPEČNOST

Vzhledem ke komplexitě prvků sítí 5G jsou řešení čistě technického rázu, tedy aktivní kontrola jednotlivých prvků (jak softwaru, tak hardwaru) na přítomnost zranitelností, nedostačující. O takovýto přístup vůči produktům mířícím do telekomunikačních sítí od společnosti Huawei usiluje britský Huawei Cyber Security Evaluation Centre (HCSEC), ale vzhledem ke kvantitě těchto zařízení a jejich častým aktualizacím je jejich postup ve velkém měřítku neefektivní. Navíc je zde ještě problematika bezpečnostních záplat – v případě odhalení (i zcela neúmyslných) slabin, je potřeba co nejrychleji vydat softwarové aktualizace, než jich využijí útočníci. Takové aktualizace proto nemohou být podrobeny důkladné analýze, a nelze tak vyloučit riziko, že budou obsahovat například backdoor, nebo jiný škodlivý kód.

Řada kyberbezpečnostních autorit v různých státech se shoduje, že výběr dodavatele nemůže být podmíněn pouze technickými aspekty. [13] **Klíčovým faktorem zabezpečení 5G sítě je proto důvěra v dodavatele, že nezneužije své unikátní postavení ve prospěch svůj, svého domovského státu či jiného aktéra.** Ačkoliv výrobci 5G komponentů mají s ohledem na generování zisku zájem o prodej kvalitních a bezpečných produktů, s nimiž budou zákazníci spokojeni, ne vždy se musí jednat o jejich jediný zájem. Výrobci se nepohybují ve vakuu, ale mají svá sídla v různých zemích a podléhají rozličným právním rámcům, mocenským strukturám a jiným neobchodním vlivům. **Problém představují primárně výrobci a dodavatelé z autoritářských států, které mají silný vliv na své domácí společnosti a nebojí se jej zneužít pro svoje geopolitické cíle, jež mohou být v rozporu se zájmy ČR či jejich spojenců.** Výrobce může být natolik propojený se státním a politickým aparátem své domovské země, že bude nezřídka činit i ekonomicky kontraproduktivní rozhodnutí v zájmu vyšších zájmů režimu, který mu potenciální škodu může případně kompenzovat. V řadě států mohou být společnosti také nuceny ke spolupráci se zpravodajskými službami státu prostřednictvím legislativy, jež na ně dopadá. [14] Navíc, vzhledem k obtížnému odhalení, a ještě obtížnější atribuci útoku, mohou tyto aktivity představovat pro výrobce přijatelné riziko, které mu zajistí výhodné postavení v domovském státě a výrazněji neohrozí jeho zisk.

5G SÍTĚ JAKOŽTO KRITICKÁ INFORMAČNÍ INFRASTRUKTURA: STÁT MÁ ZÁKONNOU POVINNOST ZAJISTIT JEJICH BEZPEČNOST

Dopady možných kybernetických útoků vedených dodavateli (nebo s jejich asistencí) proti 5G sítím mohou výrazně narušit fungování státu, ekonomiky, společnosti a v krajním případě ohrozit zdraví a životy obyvatel. Stát tak ze své podstaty musí na takové riziko reagovat a mitigovat ho. Ústavní zákon o bezpečnosti České republiky říká: „**Zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot je základní povinností státu.“**[15] **Stát by neměl rezignovat na svou povinnost tím, že ji přenese na soukromou osobu (tedy operátory).** Stát proto nemůže ponechat výhradní výběr potenciálně rizikového dodavatele tak kritického vybavení jako je 5G síť zcela v rukou soukromých firem, které nemusí být dostatečně vybaveny nebo motivovány k ochraně bezpečnosti ČR. Pro tento přístup již existují precedenty z jiných otázek spadajících do oblasti národní bezpečnosti jako je například výstavba jaderných elektráren, [16] prověřování přímých zahraničních investic [17] či prověřování poskytovatelů služeb cloud computingu. Hlavní role státu v zajištění bezpečnosti 5G sítí je rovněž v souladu s Bezpečnostní strategií České republiky.[18]

Ačkoliv operátoři mohou do jisté míry reflektovat a kontrolovat technickou bezpečnost 5G produktů (a jsou k ní nejlépe vybaveni), nemají nástroje na plnohodnotné ohodnocení netechnických aspektů bezpečnosti dodavatelů/výrobců. Stát je v tomto ohledu vybaven zpravodajskými službami s pravomocemi a nástroji danými zákonem, diplomatickým aparátem vybaveným na vyhodnocovaní geopolitických rizik a politicko-právních kritérií a dalšími institucemi k provedení komplexního prověření netechnických aspektů bezpečnostní spolehlivosti zahraničních dodavatelů. Neméně významným faktorem je fakt, že operátoři jsou ziskovými subjekty, primárně motivovanými ekonomickými faktory. Pokud potenciálně rizikový výrobce nabízí své produkty za dostatečně výhodné ceny, může pro operátory ekonomický faktor vyvážit možná rizika. Tohoto mohou státní aktéři zneužít, a úmyslně dotovat své domácí výrobce 5G komponentů, aby si skrze výhodné podmínky získali přístup do 5G sítí svých potenciálních oponentů. Operátoři se rovněž zpravidla zodpovídají mateřským zahraničním společnostem, investorům a dalším subjektům, jejichž cíle a záměry nemusí být vždy v souladu s tím, co je nejlepší pro bezpečnost občanů ČR.

DODAVATEL TECHNOLOGIE JAKO PROBLEMATICKÝ PARTNER, KTERÝ JIŽ V MINULOSTI ZNEUŽIL DŮVĚRU

Čínská společnost Huawei, která je jedním z dominantních výrobců 5G produktů na světě, je příkladem dodavatele, jenž je dlouhodobě spojován s problematickými incidenty, při kterých došlo ke zneužití důvěry. Jako klíčový incident bývá často uváděn případ odposlechu nespecifikované „velké australské telekomunikační společnosti“. Čínští zpravodajští důstojníci, či jejich spolupracovníci měli podle dostupných informací kompromitovat zařízení Huawei a využít je k následnému odposlechu společnosti. [19] K tomuto incidentu mělo dojít v roce 2012, nicméně informace o jeho existenci vyšly na povrch teprve v nedávné době. **Čínští agenti údajně pronikli do řad techniků společnosti Huawei, kteří pomáhali udržovat telekomunikační síť společnosti, a prostřednictvím aktualizace softwaru zavedli do zařízení škodlivý kód.** Ten přeprogramoval zařízení tak, aby zaznamenávalo veškerou komunikaci, která jím prochází, a poté data odesílalo na servery do Číny. Po několika dnech se daný kód měl sám smazat. Australské orgány odmítly tento incident komentovat. Michèle Flournoyová, bývalá náměstkyně ministra obrany USA, však pravdivost informací potvrdila. **Je velmi pravděpodobné (75–85 %), že tento doposud nezveřejněný incident byl jedním z klíčových faktorů pro kurz současné americké a australské politiky vůči Huawei a čínským dodavatelům všeobecně**.

Obrázek 3: Sídlo Africké unie

Zdroj: Theguardian.com

Dalším incidentem byla průmyslová špionáž proti americkému T-Mobile v letech 2012 až 2014, kdy Huawei zneužil svého partnerského postavení k odcizení dat o pokročilém robotickém výzkumu. [20]

Ochotu zneužít svého postavení ve prospěch Číny a možnosti, které poskytuje insiderská znalost vlastního vybavení, pak dále demonstrují incidenty spojené se sídlem Africké unie (AU) v Addis Abebě, Etiopii. Čína zaplatila, vyprojektovala a pomáhala postavit v roce 2012 nové sídlo AU a Huawei se stal hlavním dodavatelem IT vybavení. V roce 2018 vyšlo najevo, že ve večerních hodinách pravidelně dochází k nelegitimnímu kopírování dat na servery v Šanghaji.[21] Druhý incident byl odhalen v roce 2020, kdy bylo zjištěno, že čínští hackeři měli přístup k záznamům bezpečnostních kamer v budově.[22] V obou případech je velmi pravděpodobné (75–85 %), že k útoku byly využity zranitelnosti, které v infrastruktuře Huawei úmyslně zanechal. Další významně znepokojivý incident lze najít ve výroční zprávě dozorčí komise HCSEC z roku 2020. **V zařízeních, které byly v centru testovány, byla nalezena „zranitelnost národního významu“.** [23] Kromě toho HCSEC opakovaně poukazuje na množství méně významných slabin v posuzovaných zařízeních a neochotu Huawei je promptně opravovat. **Ačkoliv není průkazné, že tyto slabiny byly v produktech úmyslně, zpráva konstatuje, že „pokud by útočník měl znalost těchto slabin a dostatečný přístup k jejich zneužití, mohl by ovlivnit fungování telekomunikačních sítí Spojeného Království a v některých případech jejich fungování narušit“.** [24]

PROBLÉMEM JE ČÍNSKÉ STRANICKÉ A PRÁVNÍ PROSTŘEDÍ, NIKOLIV POUZE HUAWEI

Huawei je v souvislosti s hrozbami pro 5G sítě ze strany dodavatele nejčastěji skloňovaným aktérem. **Je to dáno především faktem, že se jedná o jednoho z mála výrobců těchto technologií, v kombinaci s historií výše zmíněných incidentů a známými vazbami Huawei a jejího zakladatele (Ren Zhengfeie) na Čínskou lidově osvobozeneckou armádu (ČLOA) a Komunistickou stranu Číny.[25]**

To ovšem neznamená, že Huawei je v této pozici unikátní. NÚKIB, ale i další aktéři varovali v souvislosti s riziky pro 5G sítě také například před společností ZTE.[26] **Klíčovým problémem je však fakt, že problémy spjaté s těmito společnostmi jsou systémové. Čínský politický a právní systém vyžaduje, aby každá čínská společnost měla buňku komunistické strany a 92 % z 500 největších čínských firem jimi disponuje.[27]** Vazby na ČLOA jsou následně velmi obvyklé a často jsou předpokladem k tomu, aby společnost mohla podnikat ve velkém měřítku a získávat lukrativní státní zakázky. **V neposlední řadě pak Čína disponuje striktní legislativou, která čínským společnostem nakazuje spolupracovat se zpravodajskými službami [28] (viz příloha 1). V současnosti je tak velmi nepravděpodobné (0–10 %), aby čínská firma dokázala zcela odolat požadavkům čínské vlády a komunistické strany.[29]**

Obrázek 4: Zakladatel Huawei Ren Zhengfei s čínským prezidentem Xi Jinpingem

Zdroj: Theconversation.com

ČÍNA AKTIVNĚ ZNEUŽÍVÁ SVŮJ VLIV, OHROŽENA JE I ČR

Čína dlouhodobě vykazuje velkou ochotu pouštět se do (často disproporčních) diplomatických a ekonomických konfrontací a zároveň se nebojí obcházet mezinárodní pravidla a úmluvy. Na tuto skutečnost ukazuje například roztržka s Litvou ohledně otevření tchajwanského zastupitelského úřadu ve Vilniusu.[30] Čína v odvetě zablokovala vstup litevským produktům na svůj trh, v rozporu s pravidly světové obchodní organizace. **Existuje proto reálná možnost (25–50 %), že by Čína mohla v budoucnu využít svůj vliv na výrobce 5G technologií a 5G infrastrukturu k odvetným opatřením za domnělé prohřešky vůči svým zájmům apod.** Česká republika má s odvetnými kroky Číny zkušenost například v rámci cesty předsedy senátu Miloše Vystrčila na Tchaj-wan [31] a je velmi pravděpodobné (75–85 %), že se Česká republika v rámci své pozice v EU a NATO a svého hodnotového ukotvení v budoucnu stane cílem represí Pekingu. **Nelze vyloučit (25–50 %), že by v případě významného vlivu na české 5G sítě mohla Čína tuto pozici zneužít.**

Kromě odvetných opatření a sabotáží má Čína rovněž dlouhou historii průmyslové i politické špionáže. Vzhledem k propojení sítí 5G a koncepce Průmyslu 4.0 se 5G sítě mohou stát nástrojem pro průmyslovou špionáž Pekingu. **Existují důkazy, že Čína v ČR v minulosti průmyslovou špionáž prováděla, [32] a je reálná možnost (25–50 %), že v případě vlivu na 5G sítě**

by mohla své postavení zneužít pro krádež duševního vlastnictví českých firem. Stejně tak je Čína (opět skrze Huawei) podezřelá ze shromažďování dat o českých občanech.[33]

Dalším významným rizikem je následně potenciální válečný konflikt. V současnosti stoupá napětí mezi Čínou a USA, převážně v oblasti Jihočínského moře, a ozbrojený konflikt nelze vyloučit (25–50 %). Čína nadále posiluje svou pozici a militarizuje uměle vybudované ostrovy a stupňuje vojenské provokace vůči Tchaj-wanu. Skrze potenciální konflikt USA s Čínou by se Česká republika teoreticky v rámci členství v NATO mohla ocitnout s Pekingem v otevřeném ozbrojeném konfliktu. **Ačkoliv by se Česká republika nacházela téměř jistě (90–100 %) daleko od oblastí ozbrojených střetů, velké kybernetické útoky vůči ČR by v takovém scénáři byly velmi pravděpodobné (75–85 %). Skrze infrastrukturu 5G sítí by Čína mohla mít nástroj, jak tyto útoky provádět, a páchat významné škody jak materiální, tak na zdraví a životech občanů ČR.**

Obrázek 5: Zastupitelský úřad Tchaj-wanu ve Vilniusu

Zdroj: BNN.com

ČÍNA PŘEDSTAVUJE RIZIKO V SOUČASNOSTI, DO BUDOUCNA JE TŘEBA UNIVERZÁLNÍ ŘEŠENÍ

Z výše uvedených důvodů, společně se současnou geopolitickou situací, kdy se Peking stále více vzdaluje hodnotově i politicky západním demokraciím, Čína a její výrobci představují v současnosti největší bezpečnostní hrozbu pro české sítě. **Sítě 5G ovšem představují infrastrukturu, která může sloužit i několik budoucích dekád** (pro srovnání, technologie 2G sítí, spuštěných poprvé v 90. letech 20. století se používají v ČR dodnes a budou se zřejmě používat až do roku 2028).[34] **V dlouhodobém časovém horizontu se tak může situace změnit. Výrobce, který je dnes bez identifikovaného bezpečnostního rizika, může být odkoupen společností spadající pod právní řád nedemokratické země, v jeho domovské zemi může dojít ke zhoršení poměrů anebo se mohou objevit noví rizikoví výrobci z dalších zemí, jejichž zájmy mohou jít proti zájmům České republiky a jejích občanů. V tomto ohledu je žádoucí vytvořit univerzální mechanismus pro posuzování rizik spojených s dodavateli 5G technologií.** NÚKIB proto s Ministerstvem vnitra, Ministerstvem průmyslu a obchodu, Ministerstvem zahraničních věcí, Českým telekomunikační úřadem, Bezpečnostní informační službou, Úřadem pro zahraniční styky a informace a Vojenským zpravodajstvím do konce roku 2022 předloží návrh věcného záměru zákona posuzování a omezování rizik spojených s dodavateli, tak jak mu bylo uloženo Bezpečnostní radou státu.

Smyslem navrhovaného mechanismu je účinné prověřování dodavatele a určení jeho bezpečnostní spolehlivosti. Mechanismus umožní omezit či vyloučit dodavatele z dodávek do kritické informační infrastruktury na základě míry identifikovaného rizika, aby 5G sítě v ČR regulované dle zákona o kybernetické bezpečnosti byly budovány zejména na technologiích důvěryhodných dodavatelů. Mechanismus je žádoucí a potřebný, jelikož v současné době neexistuje právní úprava pro hodnocení dodavatelů a případné omezení jejich přístupu k této důležité infrastruktuře státu, a to jak v otázce 5G, tak i dalších sektorech (například v energetice).

PŘÍLOHA 1: ČÍNSKÉ ZÁKONY VZTAHUJÍCÍ SE NA VÝROBCE 5G KOMPONENT

Působení čínských technologických firem, mezi které výrobci 5G spadají, je definováno řadou formálních i neformálních pravidel, **jejichž dodržování je nutným předpokladem jejich pokračující existence**. Formální požadavky jsou dány rámcem zákonů týkajících se státní bezpečnosti a kybernetické bezpečnosti, a to konkrétně:

- Zákonem o státní bezpečnosti (2015)[37]
- Zákonem o státní kontrašpionážní činnosti (2014)[38]
- Zákonem o kybernetické bezpečnosti (2017)[39]
- Zákonem o státní zpravodajské činnosti (2017)[40]

Soubor výše uvedených zákonů ukládá široce definovanou povinnost spolupracovat se státními orgány na zpravodajské a kontrašpionážní činnosti (včetně sledování zájmových osob v zahraničí) a poskytovat orgánům státní bezpečnosti veškerá data.

Zákon o společnostech (2013) ukládá všem společnostem ustanovit uvnitř svých struktur buňku Komunistické strany Číny (dále KS Číny či Strana), pokud ve společnosti pracují nejméně tři členové Strany. V praxi to znamená přímý dosah strany na dění v jakékoli významné společnosti. Stranické buňky nejsou jen čistě formální strukturou, naopak mají významný vliv na fungování společností, a šéfové stranických buněk patří mezi nejvyšší představitele vedení společnosti. **KS Číny vykonává skrze stranické buňky přímou kontrolu a zajišťuje, že společnosti beze zbytku plní, co se od nich očekává, včetně požadavků v oblasti státní bezpečnosti.**

Poslušnost KS Číny je centrálním prvkem neformálních požadavků na nominálně soukromé či státní společnosti. I bez existence výše uvedených zákonů a kontrolních mechanismů by pro jakoukoli společnost bylo obtížné odporovat požadavkům státních či stranických orgánů. KS Číny nemá k případnému donucení či potrestání neposlušnosti k dispozici jen policii, tajné služby a Straně podřízený justiční systém. **Mimosoudní systém výslechů a časově neomezených detencí, vykonávaný stranickou Ústřední komisí pro disciplinární vyšetřování (CCDI) je významným prostředkem vymáhání vůle Strany mezi jejími členy**.[41]

ČLR: Vztah státu vůči soukromým entitám
▪ Klíčovým zákonem je Zákon o kybernetické bezpečnosti z roku 2017, který do sebe zahrnul několik dřívějších regulací. ▪ Dopady na KB mají i zákony o státní bezpečnosti (2015)[35], státní zpravodajské činnosti (2017)[36] a státní kontrašpionážní činnosti (2014). ▪ **Zákonem definovaná povinnost poskytnout backdoory do digitální infrastruktury.** ▪ **Zákon o KB ustanovil povinnost poskytnout technickou podporu a spolupráci orgánům veřejné bezpečnosti a státní bezpečnosti.**
Kontrola a licencování ICT produktů
▪ Za licencování produktů pro fungování v ČLR je zodpovědná agentura China Information Technology Security Evaluation Center (CNITSEC). ▪ **CNITSEC je přímo kontrolována civilní rozvědkou MSS.** ▪ **Možnost státních orgánů zneužívat zranitelnosti v čínských a zahraničních produktech.**
Kontrola dat
▪ Zákon o KB a Správa kyberprostoru Číny jsou i nástroji kontroly dat a cenzury. ▪ Zodpovědnými institucemi za kontrolu internetu byly a jsou zejména oddělení propagandy KS Číny a Státní rada ČLR (obdoba úřadu vlády). ▪ Celkově se na regulaci internetu a jeho cenzuře jen na ústřední úrovni podílí až 15 institucí na státní a stranické úrovni.
Izolace od vnější sítě
▪ Velký čínský firewall je souhrnný název pro sérii technických a administrativních opatření, které tvoří komplexní systém cenzury, kontroly obsahu a masového sledování.

Tlak na technologický sektor se v posledních letech stupňuje na ideologické i regulatorní úrovni. V roce 2017 vydala Strana nařízení, jehož cílem je posílit loajalitu a stranickou kontrolu mezi podnikateli. Další nařízení z roku 2020 předpokládají posílení ideologického vedení s cílem vytvořit ústřední skupinu vedoucích představitelů soukromého sektoru, na které se strana může spolehnout v krizových situacích.[42]

Nové regulace, které vstoupily v platnost 1. září 2021, je nutné vidět v kontextu stranického pojetí státní bezpečnosti a snahy o silnější ideologickou kontrolu.

První regulací je vydání nových pravidel pro nahlašování zranitelností v síťových zařízeních.[43] Nově bude organizacím a jednotlivcům zakázáno zveřejňovat bezpečnostní zranitelnosti. Výrobci technologií mají nyní povinnost nahlašovat zranitelnosti nejprve Ministerstvu průmyslu a IT (MIIT), a to nejpozději dva dny od zjištění. Zároveň je zakázáno nahlašovat zranitelnosti zahraničním organizacím nebo jednotlivcům. **V praxi to bude znamenat, že MIIT bude mít znalost o zranitelnostech, které ještě nemají opravu, a zároveň nebude legálně možné pro bezpečnostní experty sdílet informace o zranitelnosti s kyberbezpečnostní komunitou v zahraničí.** Čínský stát tak získá přímou kontrolu nad procesem tzv. zodpovědného nahlášení (responsible disclosure), který je mimo Čínu standardně decentralizovaný a nezávislý na státní autoritě. Již před touto regulací platilo, že bezpečnostní složky mají včasný přístup k neopraveným zranitelnostem, vzhledem ke skutečnosti, že je čínská národní databáze zranitelností (CNNVD) pod kontrolou civilní rozvědky MSS.[44] **Získané informace budou téměř jistě (90–100 %) zneužité ke kybernetickým útokům.**

Druhým opatřením je Zákon o bezpečnosti dat, který upravuje podmínky zajištění bezpečnosti dat a zamezení jejich úniku mimo území ČLR.[45] Zákon dává státním autoritám možnost zastavit fungování společnosti, která dle nich bude v rozporu s požadavky zákona. **Je velmi pravděpodobné (75–85 %), že opatření bude použito k nátlaku na technologické společnosti, pokud bude shledáno, že dostatečně nespolupracují se státními a stranickými autoritami.**

ZDROJE

[1] Qualcomm. 2021. Everything you need to know about 5G. What is 5G | Everything You Need to Know About 5G | 5G FAQ | Qualcomm

[2] O2. 2021. Stavíme pro vás nejrychlejší síť. O2 | O2 pro vás staví nejrychlejší síť 5G, T-Mobile. 2021. 5G síť: Zítřek začíná již dnes. 5G - T-Mobile.cz, Vodafone, 2021. Co je to 5G? 5G síť - Vodafone.cz

[3] Doucette, Chris. 2018. What is the CIA Triad and Why You Should Care. Medium. https://medium.com/ediblesec/what-is-the-cia-triad-and-why-you-should-care-b7592cc2d89a

[4] HCSEC Oversight Board. 2020. Annual Report. Huawei Cyber Security Evaluation Centre HCSEC Oversight Board- annual report 2020.pdf (publishing.service.gov.uk)

[5] Metadaty se rozumí informace, které nejsou součástí odesílaných dat, ale které vznikají při jejich odeslání, jako například velikost souboru, adresát, atd.

[6] Foremski, Tom. 2018. IBM warns of instant breaking of encryption by quantum computers: 'Move your data today'. ZDNet. https://www.zdnet.com/article/ibm-warns-of-instant-breaking-of-encryption-by-quantum-computers-move-your-data-today/

[7] Interní informace od partnerů NÚKIB

[8] Huq, N, Gibson C, Kropotov, V, Vosseler R. 2021. Trend Micro. Cybersecurity for Connected Cars: Exploring Risks in 5G, Cloud, and Other Connected Technologies. Cybersecurity for Connected Cars: Exploring Risks in 5G, Cloud, and Other Connected Technologies (trendmicro.com)

[9] CGI. 2020. Industry 4.0 and cybersecurity: How to protect your business against cyber risks. Industry 4.0 and cybersecurity white paper (cgi.com)

[10] Electronics notes. 2019. MIMO Antenna Beamforming. Electronics notes. https://www.electronics-notes.com/articles/antennas-propagation/mimo/antenna-beamforming.php

[11] CISA. 2020. Edge vs. Core - An increasingly less Pronounced distinction In 5G networks. Edge vs. Core - An Increasingly Less Pronounced Distinction in 5G Networks (cisa.gov)

[12] ibidem

[13] NIS Cooperation Group. 2020. Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures.pdf (ccdcoe.org), Evropská rada. 2019. Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G - Council Conclusions (3 December 2019). st14517-en19.pdf (europa.eu), Vláda. 2019. Prague 5G Security Conference announced series of recommendations: The Prague Proposals. Prague 5G Security Conference announced series of recommendations: The Prague Proposals | Government of the Czech Republic (vlada.cz), Australian Goverment. 2021. Critical Technology Suppy Chain Principles. Critical Technology Suppy Chain Principles (homeaffairs.gov.au), NCSC. 2020. NCSC advice on the use of equipment from high risk vendors in UK telecoms networks. NCSC advice on high risk vendors in UK telecoms - NCSC.GOV.UK, Stockwell, J. 2021. Australian Goverment. Jennifer Stockwell | Australian Government Department of Foreign Affairs and Trade (dfat.gov.au), R, Spearman.

[14] Kharpal, A. 2019. Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice. CNBC. Huawei would have to give data to China government if asked: experts (cnbc.com)

[15] Předpis č. 110/1998 Sb., zdroj: SBÍRKA ZÁKONŮ ročník 1998, částka 39, ze dne 29. 5. 1998 - Sbírka zákonů - Nakladatelství Sagit, a.s.

[16] Zákon č. 367/2021 Sb. Zákon o opatřeních k přechodu České republiky k nízkouhlíkové energetice a o změně zákona č. 165/2012 Sb., o podporovaných zdrojích energie, ve znění pozdějších předpisů. 367/2021 Sb. Zákon o opatřeních k přechodu České republiky k nízkouhlíkové energetice a o změně zákona č. 165/201... (zakonyprolidi.cz)

[17] Saxlová, J. 2021. Prověřování zahraničních investic v České republice. Právní Prostor. Prověřování zahraničních investic v České republice | Právní prostor (pravniprostor.cz)

[18] Vláda. 2015. Bezpečnostní strategie České republiky. bezpecnostni-strategie-2015.pdf (vlada.cz)

[19] Tarabay, J, Robertson, J. 2021. Chinese Spies Accused of Using Huawei in Secret Australia Telecom Hack. Bloomberg. Chinese Spies Accused of Using Huawei in Secret Australian Telecom Hack - Bloomberg

[20] Orlowski, A. 2017. Huawei spied, US federal jury finds. The Register. Huawei spied, US federal jury finds • The Register

[21] Kadiri, G, Tiloune, J. 2018. A Addis-Abeba, le siège de l'Union africaine espionné par Pékin. Le Monde. A Addis-Abeba, le siège de l'Union africaine espionné par Pékin (lemonde.fr)

[22] Chaudhury, D, R. 2020. China uses Huawei cameras to spy on African Union headquarters. The Economic Times.

China uses Huawei cameras to spy on African Union headquarters - The Economic Times (indiatimes.com)

[23] Ranger, S. 2020. UK found flaw of 'national significance' in Huawei tech, says report UK found flaw of 'national significance' in Huawei tech, says report | ZDNet, HCSEC Oversight Board. 2020. Annual Report. Huawei_Cyber_Security_Evaluation_Centre__HCSEC__Oversight_Board-_annual_report_2020.pdf (publishing.service.gov.uk) Huawei Cyber Security Evaluation Centre HCSEC Oversight Board-annual report 2020.pdf (publishing.service.gov.uk)

[24] HCSEC Oversight Board. 2020. Annual Report. Huawei Cyber Security Evaluation Centre HCSEC Oversight Board- annual report 2020.pdf (publishing.service.gov.uk).

[25] Davies, R. 2018. The giant that no one trusts: why Huawei's history haunts it. The Guardian. The giant that no one trusts: why Huawei's history haunts it | Huawei | The Guardian

[26] NÚKIB. 2018. Software i hardware společností Huawei a ZTE je bezpečnostní hrozbou. Národní úřad pro kybernetickou a informační bezpečnost - Software i hardware společností Huawei a ZTE je bezpečnostní hrozbou (nukib.cz)

[27] Institut Montaigne. 2021. Influence without Ownership: the Chinese Communist Party Targets the Private Sector. Influence without Ownership: the Chinese Communist Party Targets the Private Sector | Institut Montaigne

[28] Kaska, K, Beckvard, H, Minárik, T. 2019. Huawei, 5G and China as a Security Threat. CCDCOE. CCDCOE-Huawei-2019-03-28-FINAL.pdf

[29] Wei, L. 2020. China's Xi Ramps Up Control of Private Sector. 'We Have No Choice but to Follow the Party. Wall Street journal. China's Xi Ramps Up Control of Private Sector. 'We Have No Choice but to Follow the Party.' - WSJ, Kharpal, A. 2019. Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice. CNBC. Huawei would have to give data to China government if asked: experts (cnbc.com)

[30] LRT English. 2021. China's blockade of Lithuania hits other EU exports, says trade commissioner. China's blockade of Lithuania hits other EU exports, says trade commissioner - LRT

[31] Birdmanová, M. 2020. Čínská odveta za Vystrčila. Po Petrofu je v hledáčku Brano. Seznam Zprávy. Čínská odveta za Vystrčila. Po Petrofu je v hledáčku Brano - Seznam Zprávy (seznamzpravy.cz)

[32] Břešťan, R. 2017. Čínská špionáž u českých vynálezců. Sinopsis. Čínská špionáž u českých vynálezců - Sinopsis

[33] iDnes. 2019. Huawei sbírá v Česku data o dětech, zájmech i majetku, tvrdí exmanažeři. Huawei sbírá v Česku data o dětech, zájmech i majetku, tvrdí exmanažeři - iDNES.cz

[34]Root. 2021. Mobilní sítě 2G tu s námi budou minimálně do roku 2028. Mobilní sítě 2G tu s námi budou minimálně do roku 2028 - Root.cz

[35] 国家安全法, 2015. China Law Translate. 中华人民共和国国家安全法（主席令第二十九号）_法律_法律法规_政策_中国政府网 (www.gov.cn) a National security law (chinalawtranslate.com)

[36] Původní text v čínském jazyce: 中华人民共和国国家情报法_中国人大网 (npc.gov.cn); neoficiální překlad do angličtiny: https://chinacopyrightandmedia.wordpress.com/2017/05/16/national-intelligence-law-of-the-peoples-republic-of-china-draft/; commentary: Beijing's New National Intelligence Law: From Defense to Offense, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

[37] 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

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

[39] 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

[40] 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

[41] HRW. 2016. "Special Measures" Detention and Torture in the Chinese Communist Party's Shuanggui Systém. https://www.hrw.org/report/2016/12/06/special-measures/detention-and-torture-chinese-communist-partys-shuanggui-system

[42] Fergus Ryan. 2021. China takes on its tech leaders. https://warontherocks.com/2021/08/china-takes-on-its-tech-leaders/

[43] The Record. 2021. Chinese government lays out new vulnerability disclosure rules. https://therecord.media/chinese-government-lays-out-new-vulnerability-disclosure-rules/, původní text v čínštíně viz CAC. 2021. 工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知. http://www.cac.gov.cn/2021-07/13/c_1627761607640342.htm

[44] Recorded Future. 2017. Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3. https://www.recordedfuture.com/chinese-mss-behind-apt3/

[45] Bloomberg. 2021. China's New Data Law Gives Xi the Power to Shut Down Tech Firmshttps://www.bloomberg.com/news/articles/2021-06-10/china-passes-law-to-strengthen-control-over-tech-firms-data

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách www.us-cert.gov/tlp). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená **TLP: RED**	Informace nemůže být použita jinou osobou než konkrétní osobou na straně příjemce, které byla informace poskytnuta, nebudou-li výslovně stanoveny další osoby, kterým lze tuto informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit po dohodě s původcem informace.
Oranžová **TLP: AMBER**	Informace může být sdílena pouze mezi pracovníky příjemce, kteří mají 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, nebudou-li výslovně stanoveny další osoby, kterým ji lze poskytnout.
Zelená **TLP: GREEN**	Informace může být sdílená v rámci příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály. Příjemce při předání musí zajistit důvěrnost komunikace informace. Příjemce nesmí informaci poskytnout veřejně, může ji však při splnění a zajištění stejných podmínek ochrany předat dalším partnerským subjektům příjemce.
Bílá **TLP: (WHITE)**	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 VE VÝSTUPECH NÚKIB

Pravděpodobnostní výrazy a vyjádření jejich procentuálních hodnot:

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 %

Digitálně podepsal:
Mgr. Petr Novotný
Národní úřad pro kybernetickou a informační bezpečnost
Dne: 22.04.2022 09:27

NÚKIB