Institut
pro křesťansko-demokratickou
politiku

Rizika expanze čínských technologických společností do zahraničí

Martin Hála

Ředitel projektu Sinopsis.cz

Obsah

Institut pro křesťansko-demokratickou politiku, z.ú.

2019

1 Úvodem

Současná intenzivní debata, domácí i mezinárodní, o bezpečnostních rizicích spojených s čínskými technologickými firmami Huawei a ZTE (případně dalšími) razantně nastolila otázku o politických a bezpečnostních rozměrech spolupráce s Čínskou lidovou republikou (ČLR) v oblasti informačních a komunikačních technologií (ICT).

2 "Inteligizace" kontroly v "Nové epoše"

ČLR se snaží v posledních letech stále více prosazovat jako dodavatel ICT komponentů i celých systémů, a současně usiluje o vliv na formulování globální politiky a správy (global policy-making and governance) v této oblasti, především prostřednictvím každoročních "internetových summitů" v jihočínském městě Wu-čen, ale také systematickým působením v nejrůznějších regulačních orgánech, agenturách OSN apod.

Důležitým referenčním bodem při posuzování snah ČLR – včetně působení nominálně soukromých čínských firem – v zahraničí je přitom domácí čínská politika v oblasti ICT. ČLR zaznamenává od poloviny 90. let prudký rozvoj ICT, který z ní učinil po dvou desetiletích jednoho z globálních leaderů v celé řadě oborů včetně budování informační infrastruktury, zpracování velkých dat a umělé inteligence.

Ve sféře domácí politiky využívá ČLR, resp. stranické a vládní orgány, informační technologie k systematické "inteligizaci" (智能化) státní správy. Ta zahrnuje mj. snahu o automatizovanou centrální kontrolu nad ekonomikou a společností. Automatizovaný sběr "velkých" dat z nejrůznějších zdrojů a jejich zpracování s pomocí umělé inteligence má čínským orgánům umožnit opětovnou re-centralizaci hospodářského řízení, jakož i politické a ideologické kontroly nad početným čínským obyvatelstvem.

"Inteligizace" jako technologický nástroj umožňující obnovu centrální kontroly nad ekonomikou i společností se stala jedním z ústředních bodů teoretického zdůvodnění tzv. "Nové epochy" (新时代) generálního tajemníka ÚV KS Číny a prezidenta Si Ťin-pchinga. Tato teorie (zanesená na 19. sjezdu KS Číny do stanov strany, a posléze na březnovém zasedání Všečínského shromáždění lidových zástupců i do státní ústavy jako "Si Ťin-pchingovo myšlení o socialismu s čínskými rysy v Nové epoše") rozděluje dosavadní historii ČLR na tři fáze.

V první fázi (1949-1976) ustavil Mao Ce-tung centralizovanou a disciplinovanou komunistickou společnost, avšak materiální základ a dostupné technologie nestačily na její udržení. Výsledkem byl hospodářský a politicky chaos po Maově smrti na konci Kulturní revoluce. Ve druhé fázi (1978-2012) musel Teng Siao-pching (a jeho nástupci) dočasně ustoupit v zájmu odvrácení hospodářské a politické katastrofy od Maova centralismu a disciplíny zavedením hospodářských a společenských reforem, známých jako "politika reforem a otevřenosti" (改革开放). Výsledkem byl prudký hospodářský růst, ale také všeobecná korupce a ústup od komunistických ideálů.

S nástupem Si Ťin-pchinga na post generálního tajemníka v roce 2012 nastává třetí, "Nová epocha", která má představovat jakousi syntézu dvou předchozích. Hospodářská základna a digitální technologie

dnes umožňují, aby se Strana vrátila k “původnímu záměru/ideálům” (初心) a na kvalitativně nové úrovni realizovala Maův komunistický ideál. Prostředkem k efektivní centrální kontrole hospodářství i společnosti, která dříve selhávala ve všech komunistických státech, mají být nyní v Nové epoše právě pokročilé ICT, zejména velká data a umělá inteligence.

3 Využívání kybernetických nástrojů doma a v zahraničí

ICT a “inteligizace” tak hrají ústřední roli v Si Ťin-pchingově snaze o opětovné nastolení (částečně) ztracené kontroly stranického “jádra” (党核心) nad společností a ekonomikou. Konkrétním výrazem “inteligizace” společenské kontroly jsou potom projekty jako “systém společenského kreditu/věrohodnosti” (社会信用系统) (zatím ve stadiu pilotních iniciativ) nebo Projekt sněhová záře (雪亮工程), tedy propojená síť milionů bezpečnostních kamer s rozpoznáváním obličejů, schopná sledovat konkrétního jedince po celé Číně v reálném čase (rovněž v testovací fázi).

Zatím nejkřiklavějším příkladem “inteligizace” společenské kontroly, je použití ICT v probíhající represivní kampani v Ujgurské autonomní oblasti Sin-ťiang. Čínské úřady zde experimentují s různými formami automatizovaného digitálního dohledu nad obyvatelstvem za pomoci technologických společností jako jsou právě Huawei a ZTE, ale např. také výrobci bezpečnostních kamer Hikvision a Dahua (které jsou dominantními dodavateli i na českém trhu s bezpečnostní technikou).

Čínské společnosti tyto systémy vyvážejí do okolního světa, mj. i prostřednictvím systému “Safe Cities”, který inzerují jako součást širšího konceptu “Smart Cities”. Příjemci jsou země jako Pákistán, ale také různé autoritářské státy v Africe, např. Zimbabwe. Některé bezpečnostní systémy vyvíjejí čínské firmy pro zahraniční zákazníky na míru, např. digitalizovaný systém osobní identifikace ve Venezuele, nebo národní bezpečnostní systém v Ekvádoru (Ecu911).

Samostatnou kapitolou je potom systematické využívání ICT pro zpravodajskou činnost v zahraničí, včetně ekonomické špionáže. Masové zcizování komerčních i vojenských technologií od privátních subjektů i státních institucí prostřednictvím státem sponzorovaných hackerských skupin bývá označováno za “největší transfer bohatství v dějinách lidstva”. Alarmující rozsah čínských hackerských operací proti americkým společnostem vedl Obamovu administrativu v roce 2015 k uzavření dohody přímo s generálním tajemníkem Si Ťin-pchingem o neútočení na počítačové sítě komerčních subjektů.

Tato dohoda skutečně dočasně snížila kvantitu kybernetických útoků z Číny. Vzhledem k tomu, že transfer cizích technologií je nezbytný pro plány čínského vedení na modernizaci země, nahradily ale brzy kvantitu dřívějších útoků koncentrovanější a sofistikovanější průniky. ČLR také začala experimentovat s novými metodami, které technicky nepokrývá dohoda z roku 2015, jako je tzv. “Border Gateway Protocol (BGP) hijack”, čili dočasné odklánění datových toků z páteřních sítí v USA a jinde do Číny prostřednictvím komerčních přístupových bodů (PoP) čínského státního telekomu v cizích páteřních sítích.

Kybernetická špionáž, ať už vojenská, politická nebo komerční, je jednou ze základních metod čínské rozvědné činnosti, a také nezbytným předpokladem rychlého hospodářského růstu Číny. Vzhledem

k nízkým nákladům, snadné popiratelnosti a obrovské výtěžnosti takové činnosti je nepravděpodobné, že by se jí ČLR v dohledné době bez vnějšího tlaku sama vzdala.

4 Případ Huawei

Na současnou kontroverzi kolem společnosti Huawei je možno nahlížet ze tří základních rovin: technické, politické a geopolitické.

Z hlediska technického jde v zásadě o to, zda existují "hmatatelné" důkazy zneužívání technologií a komponentů firmy Huawei pro špionážní cíle ČLR. Ve veřejném diskurzu se tato rovina obvykle dále zužuje na otázku "zadních vrátek" (back door access) a škodlivých skriptů (malware). To jsou velmi technické záležitosti pro kvalifikované odborníky, působící obvykle v neveřejných institucích. Detaily případných poznatků v této oblasti si tyto instituce vesměs nechávají pro sebe, a spokojí se maximálně s obecně formulovanými varováními.

Britská sigintová agentura GCHQ identifikovala již v roce 2011 blíže neurčené problémy se síťovými komponenty Huawei, jinak hojně využívanými britským telekomem. S těmito zjištěními seznámila podle zpráv z veřejných zdrojů své partnery v anglofonní zpravodajské alianci "Pět očí" (Five Eyes). V Británii poté vznikla speciální laboratoř k prověřování komponentů a technologií Huawei. Loni vydala veřejné prohlášení, že "nemůže zaručit" bezpečnost výrobků Huawei. Podobná laboratoř existuje i v Německu. Na její výsledky se teprve čeká.

V loňském roce proběhlo v Kanadě setkání ředitelů zpravodajských služeb zemí aliance "Pěti očí" (USA, Kanada, Velká Británie, Austrálie a Nový Zéland) speciálně k tématu Huawei a obecněji bezprecedentních hrozeb, které představuje pro demokratické země politika KS Číny pod vedením Si Ťin-pchinga. Toto setkání a některé jeho závěry bylo – zjevně úmyslně - medializováno v anglofonním tisku. Představitelé zpravodajských služeb Pěti očí se dohodli na veřejném vystupování v této věci, aby upozornili na vážnost situace. Od té doby bylo v těchto zemích vydáno několik varování a zákazů pro přístup společnosti Huawei k veřejným zakázkám, a zejména k budování sítí 5G, jež se mají v brzké budoucnosti stát základem "Internetu věcí" (IoT) a tedy páteří informatizovaných společností.

Bezprecedentní koordinovaný postup klíčových západních zemí proti společnosti Huawei současně zakládá geopolitický rozměr celé kontroverze. Na případu Huawei se do značné míry lomí narůstající konflikt mezi ČLR a západním světem. Tzv. obchodní válka mezi Spojenými státy a Čínou je do velké míry válkou technologickou. Vposledku se nejedná o nic menšího než střet dvou odlišných koncepcí organizace společnosti a mezinárodních vztahů. Vzhledem k roli, jež se v budoucí informatizované společnosti přisuzuje sítím 5G, je celkem přirozené, že se tento základní střet promítá výrazně právě do otázky budování těchto sítí.

Veřejnost patrně nikde nebude mít k dispozici "technické" důkazy o rizicích spojených se společností Huawei v podobě jasně identifikovaných backdoors či malware. Tato oblast zůstane v kompetenci specializovaných institucí, jako je NÚKIB a jejich zahraniční partneři z řad spojeneckých zpravodajských služeb. Na veřejnost nejspíš prosáknou jen některé zvlášť nápadné incidenty, jako bylo odposlouchávání a přenos dat z budovy Africké unie v Addis Abebě.

Výrazným vodítkem pro veřejnou diskuzi tak budou politické (ve smyslu policy) aspekty celé věci. Čínské úřady kladou jasný důraz na využívání ICT pro kontrolu svých obyvatel, a pro transfer (zcizovaní) technologií a dalších informací ze zahraničí. Podle platných čínských zákonů nemůže žádná firma ani jednotlivec odmítnout spolupráci při výzvědné činnosti.

Společnost Huawei má navíc zřetelné vazby, včetně personálních, na čínskou armádu a zpravodajské organizace. Zakladatel společnosti Žen Čeng-fej 任正非 je bývalý (1974 - 1983) důstojník Čínské lidové osvobozenecké armády. Dlouholetá (1992 - 2018) předsedkyně společnosti Sun Ja-fang pracovala před nástupem k Huawei na Ministerstvu státní bezpečnosti (国安部, MSS), jakési čínské obdoby někdejšího KGB na úrovni celého ministerstva.

29. ledna 2019 byly v USA oficiálně zveřejněny hned dvě ožaloby proti společnosti Huawei a jejím představitelům: u soudu v New Yorku kvůli porušování sankcí proti Íránu a klamání amerických bank finanční ředitelkou společnosti Meng Wan-čou a v Seattlu kvůli průmyslové špionáži, konkrétně snaze ukrást technologii testovacího robota společnosti T-Mobile. Součástí obžaloby v Seattlu je také obvinění, že firma Huawei zavedla v roce 2013 systém odměňování svých pracovníků za informace zcizené od jiných společností po celém světě. Obě obžaloby mají celkem 23 bodů, jež mají dokládat systematické porušování zákonů v cizích zemích, kde společnost Huawei působí.

Hrozba se zpravidla definuje jako úmysl a schopnost akce v dané oblasti. Dostupné indicie naznačují, že ani jedno v případě Huawei nechybí.