PRAGUE SECURITY STUDIES INSTITUTE (PSSI) / ČERVEN 2020

NEJEN HUAWEI: ČÍNSKÉ FIRMY A NAŠE BEZPEČNOST

Autoři:
Petr Lang, Tomáš Koutský, Ondřej Černý

Prague Security Studies Institute

OBSAH

Autoři by tímto rádi poděkovali
konzultovaným českým a zahraničním expertům
za cenné rady, podněty a doporučení.

ÚVOD

Informační a komunikační technologie (ICT) hrají v našich životech stále důležitější a komplexnější roli, která se bude v budoucnu nadále prohlubovat a rozšiřovat. Větší využívání nových technologických řešení slibuje obrovské přínosy pro rozvoj ekonomiky, lékařství, energetiky, dopravy, zemědělství, urbanismu, státní správy a jiných oborů. Ve vládní Inovační strategii 2019-2030, která plánuje modernizovat naši ekonomiku pro potřeby 21. století, se slovo digitální vyskytuje 21x.[1] V této souvislosti je zapotřebí zmínit hlavně očekávané možnosti využití sítí páté generace a tzv. internetu věcí. S rostoucím počtem navzájem propojených přístrojů, které budou sbírat velká množství dat, analyzovat je a navzájem si je předávat, však roste i nutnost dbát o trvanlivé a spolehlivé zabezpečení těchto systémů. Nejedná se o lehký úkol, neboť živelný vývoj digitálních technologií a jejich nová a leckdy nečekaná praktická využití znamenají, že jejich bezpečnost nelze zajistit jednou provždy, ale je nutné se o ni neustále starat, analyzovat možné hrozby a rizika a odpovědně na ně reagovat. Bohužel, počet a závažnost kybernetických útoků rostou, jak dokazují nedávné útoky na české nemocnice, Povodí Vltavy, ministerstvo zahraničí a jiné instituce.[2]

Zatímco stát disponuje poměrně širokým a účinným množstvím nástrojů k ochraně kybernetické bezpečnosti strategických institucí a důležitých systémů určených § 3 zákona o kybernetické bezpečnosti, je nutné poznamenat, že ve všech ostatních případech (tedy ve všech firmách a institucích, které pod zákon o kybernetické bezpečnosti nespadají) je odpovědný přístup k zajištění bezpečnosti pouze na jejich vlastní úvaze."[3] Role soukromého sektoru je pro další rozvoj naší ekonomiky naprosto zásadní a je proto nutné, aby byla zajištěna integrita, dostupnost a správné fungování technologií, které ve své činnosti využívá.

Kybernetická zranitelnost nemusí být zneužita pouze k narušení dostupnosti a funkčnosti systémů, ale také ke krádeži know-how, patentů a intelektuálního vlastnictví. Útoky na soukromé společnosti, které vyrábějí produkty či dodávají služby pro kritickou infrastrukturu také mohou znamenat závažné ohrožení národní bezpečnosti jako celku. Rizikem je pochopitelně i lidský faktor, kterého mohou útočníci pomocí vydírání na základě osobních informací získaných ze špatně zabezpečených mobilních telefonů, laptopů či bezpečnostních kamer využít k tomu, aby jim kýžené informace předal či ovlivnil rozhodování daného subjektu v jejich prospěch.

Dalším trendem, který můžeme v současné době v oblasti kybernetické bezpečnosti pozorovat, je vyhodnocování rizik spojených s dodavateli technologií a produktů, kteří mohou působit v zájmu cizího státu, byť se může jednat o formálně soukromé subjekty. Bohužel, ne všechny firmy se chovají ekonomicky standardně, tedy tak, že sledují pouze čistě ekonomické cíle: vyšší zisk založený na dlouhodobém vztahu se svými zákazníky. Toto tvrzení by mohlo být obecněji platné pouze v případě, kdyby všechny firmy pocházely z demokratických států s dobře fungující dělbou moci a efektivním právním státem, což bohužel neodpovídá současné geopolitické a geoekonomické realitě.

Historickou paralelu lze najít v debatě o evropské energetické bezpečnosti v souvislosti s dodávkami ruské ropy a zemního plynu. Standardní ekonomické chování by v tomto případě znamenalo, že by ruští dodavatelé měli svým evropským zákazníkům dodávat nasmlouvané produkty bez přerušení a za oboustranně výhodné ceny a hrozba politicky motivovaných přerušení dodávek by měla být mizivá. Tento koncept tzv. vzájemné závislosti (Evropa potřebuje ruské suroviny, Rusko pak peníze na většinu státních výdajů) vzala za své během plynových krizí v letech 2006 či 2009 či během přerušení dodávek ropy do České republiky po podepsání memoranda o výstavbě systému protiraketové obrany v roce 2008. Stejně tak i ceny zemního plynu byly určovány Ruskem tak, aby danou zemi buď pochválily, či potrestaly. Neblahá zkušenost s tímto vysoce rizikovým dodavatelem tak evropské státy donutila k radikálním a ve výsledku úspěšným krokům jako je diverzifikace dodavatelů, dopravních tras a dodávaného skupenství produktů (LNG), propojení vnitroevropských přepravních tras, liberalizace trhu a nastavení nového mechanismu určování ceny (spot vs. dlouhodobé kontrakty), které tuto formu politického nátlaku značně omezily.

Fyzická síť mezinárodních plynovodů a ropovodů je ve srovnání s moderními informačními a komunikačními systémy mnohem jednoduší, ale spojuje je obecně uplatnitelný princip důvěry/nedůvěry v druhou stranu. Důvěra hraje v bezpečnosti zcela zásadní roli, je základním prvkem spojeneckých vazeb či mezistátní zpravodajské spolupráce. Důvěra vzniká na základě sdílených zájmů a hodnot a dlouhodobého vztahu. Důvěra je zapotřebí tam, kde jedna strana nemá dostatek informací a možností vlastními silami zajistit/zjistit, že druhá strana nikdy nezneužije svých informací a možností k tomu, aby ji poškodila či jednala proti jejím zájmům. Důvěra je obsažena i v široce uplatnitelné definici národní bezpečnosti Davida Omanda: „Národní bezpečnost má být v současné době definovaná jako stav důvěry ze strany občana, že rizika každodenního života, ať už původu lidského či přírodního, jsou dostatečně zvládána/řízena tak, že posilují víru v to, že normální život nebude ohrožen. [4]

Národní bezpečnost v tomto smyslu už není záležitostí pouze státních orgánů, ale ve věku hybridních hrozeb i zásadním tématem pro soukromý sektor. Ne každý podnik či instituce, které jsou důležité pro normální chod života, musí respektovat státní nařízení, která se týkají kybernetické bezpečnosti. Bohužel, soukromá sféra často považuje nutnost zkoumat bezpečnostní rizika (především ta geopolitická) a odpovědně na ně reagovat za nepříjemnou komplikaci, která jí znesnadňuje život a ohrožuje její ekonomické výsledky. Zavádění bezpečnostních opatření je náročné a v období neustálého tlaku na optimalizaci nákladů se může zdát jako těžko obhajitelné. Toto je však velmi nebezpečný a krátkozraký postoj. Bezpečnost by měla soukromý sektor zajímat více než kdykoli v minulosti. S rostoucí komplexitou technologických systémů a jejich propojeností bude útoků, ať už budou jejich cíl a motivace jakékoli, přibývat a budou ohrožovat jak samotné fungování firem, poptávku po jejich výrobcích a v konečném důsledku i stabilitu státu, ve kterém podnikají.

Cílem této studie je poukázat na koncept tzv. netechnických rizik spojených s dodavateli ICT produktů, popsat konkrétní kroky, které ke snížení těchto rizik podnikly státní instituce v ČR a ve spojeneckých zemích, uvést příklady využívání technologií čínských firem, které byly v ČR nebo ve spojeneckých zemí označeny za hrozbu pro národní bezpečnost a navrhnout doporučení, jak zvýšit povědomí o těchto rizicích obecně, tedy i u uživatelů, kteří nejsou součásti KII.

Z metodologického hlediska se tato studie bude zabývat především čínskými technologickými firmami, které české či spojenecké instituce vyhodnotily jako potenciálně rizikové na základě národně-bezpečnostní argumentace. Konkrétně se jedná o firmy Huawei, ZTE, DJI, Dahua, CGN a Hytera. Za potenciálně rizikové bývají označovány firmy, které jsou přímo většinově vlastněny státem (State-Owned Enterprises - SOEs) nebo ty s nejasnou vlastnickou strukturou. V nedávné době se však tato definice rozšířila kvůli přijetí zákona o státní zpravodajské činnosti v roce 2017, který nakazuje každé čínská firmě a občanovi spolupracovat s čínskými zpravodajskými službami. Provázanost čínského soukromého sektoru s vládnoucí komunistickou stranou nadále posiluje i nařízení, které ukládá všem firmám, kde pracují více jak tři členové komunistické strany, zřídit stranické buňky, které budou mít vliv na chod podniku. Dalším možným rizikovým faktorem je i napojení firem na státní bezpečnostní aparát, který se projevuje např. při stavbě internačních táborů pro Ujgury.

BEZPEČNOST ICT TECHNOLOGIÍ A TZV. NETECHNICKÁ RIZIKA

Se zvyšující se složitostí ICT řešení, která ovlivňují stále širší oblasti našeho života, dochází k zásadnímu vývoji při určování a měření rizik u jednotlivých technologií, respektive jejich dodavatelů. Kódy ve kterých je napsán dodávaný software, obsahují tisíce řádků a najít v nich úmyslné či neúmyslné chyby trvá dlouho dobu, navíc se kód může zásadně změnit s každou novou aktualizací. Plánovaný rozvoj sítí páté generace a internetu věcí zvýší exponenciálně počet přístrojů, které budou sbírat data, analyzovat je a navzájem si je mezi sebou vyměňovat např. v cloudovém uložišti. Očekávané přínosy v podobě

[1] "Inovační strategie České republiky 2019–2030". Vláda ČR, https://www.vlada.cz/assets/urad-vlady/poskytovani-informaci/poskytnute-informace-na-zadost/Priloha_1_Inovacni-strategie.pdf

[2] "Ostravská nemocnice odrazila kybernetický útok, vyřazení sítě v době epidemie zůstává velkou hrozbou". iROZHLAS, https://www.irozhlas.cz/zpravy-domov/nemocnice-ostrava-kyberneticky-utok_2004171249_jak a "Systém Povodí Vltavy napadli hackeři. Přehrady ani dodávky vody v ohrožení nejsou. Aktuálně.cz, https://zpravy.aktualne.cz/domaci/informacni-system-povodi-vltavy-napadli-hackeri/r~fe9196b478d811eab115ac1f6b220ee8/.
a "Hackeři se znovu nabourali do počítačů ministerstva zahraničí, policie útok prověřuje". iROZHLAS, https://www.irozhlas.cz/zpravy-domov/ncoz-nku-narodni-kyberneticky-urad-hackerske-utoky-ministerstvo-zahranici-rusko_1907311925_cha.

[3] Užitečný materiál k určení prvku KKI je zde: "Kritická kybernetická infrastruktura", GovCert, https://www.govcert.cz/download/kii-vis/Schema_KII.pdf

[4] Omand, David. Securing the State. Hurst, 2012. p.9

vyšší produktivity, autonomních aut či efektivnějšího využívání obnovitelných zdrojů energie, však povedou ke zvýšení počtu rizikových bodů (attack surface), které může možný útočník využít a narušit tak dostupnost, důvěrnost či integritu informací a bezpečné fungovaní celých systémů.

Odpovědná a zevrubná analýza rizik je o to obtížnější, pokud se týká právě potenciálně revolučních (či disruptivních) technologií, jako je 5G a internet věcí, které jsou téměř na začátku svého vývoje a nikdo neví, jak budou ve své pokročilé a rozšířené fázi vypadat. Aby byla analýza rizik u stávajících a budoucích systémů, které hrají a budou hrát zásadní roli pro naši společnost, co nejúplnější, je nutné brát v úvahu i netechnická rizika, která se týkají dodavatelů technologií a zemí jejich původu. Nejedná se pouze o výrobce součástí telekomunikačních a počítačových sítí, ale i dodavatele periférií (kamer, dronů), které budou představovat důležitou součást internetu věcí a jejichž plnohodnotné využití bude vyžadovat připojení k síti.

Posuzování rizikovosti zahraničního ekonomického aktéra v širším geopolitickém, hodnotovém a právním kontextu se netýká pouze oblasti kybernetické bezpečnosti, ale je využíváno např. také v mechanismech pro prověřování zahraničních investic do strategických firem, které v nedávné době zavedlo či významně posílilo mnoho členských států EU/NATO.

Jedním z často používaných hledisek, je země původu zahraničního investora. Více jak polovina států EU tak prověřuje investice ze třetích zemí. USA mohou prověřit jakoukoli zahraniční investici, pokud může mít dopad na národní bezpečnost s tím, že blízcí spojenci jako je Austrálie, Kanada a Velká Británie mají výhodnější pozici a některé kontroly se jich nemusejí týkat. Indie prověřuje investice ze všech zemí, se kterými sousedí.[5]

Dalším používaným indikátorem možné rizikovosti investice je vztah dané firmy a jejího domovského státu. Jako potenciálně rizikoví investoři tak bývají označovány především firmy, jejímž hlavním vlastníkem je stát (SOEs – State-Owned Enterprises) či státní suverénní fondy (SWFs-Sovereign Wealth Funds), neboť pokud má stát nad nějakou institucí kontrolu, může ji využít k prosazování svých zájmů. Pokud se jedná o stát, který nepatří mezi naše spojence, může se jednat o aktivity rizikové. Pokud je dodavatel/investor ovládán cizím státem, může být donucen k nestandardnímu ekonomickému chování, kdy při sledování politických cílů své země nemusí respektovat standardní podnikatelské hodnoty jako jsou tržně naceněné produkty/služby, spolehlivost či dlouhodobý vztah se zákazníkem založený na důvěře. Aby byli podchyceni všichni možní rizikoví aktéři, je zapotřebí neopomínat i firmy, které jsou formálně na státu nezávislé (stát v nich nemá rozhodující či žádný majetkový podíl), ale může nad nimi vykonávat kontrolu jinými prostředky. A nemusí se jednat jen o instituce, ale i jednotlivé občany dané země. Některé screeningové mechanismy nezachycují jen odprodeje určitého počtu akcií, ale prověřují i jiné formy získaní kontroly či přístupu k zásadním informacím, např. složení výkonných orgánů dané firmy.

V oblasti ICT technologií a kybernetické bezpečnosti se tento vývoj hodnocení rizikových aktérů projevil v několika důležitých dokumentech, které mají bezprostřední dopad i na Českou republiku.

Varování Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) (17. 12. 2018)[6]

První varování, které NÚKIB za dobu své existence vydal, označilo za hrozbu v oblasti kybernetické bezpečnosti výrobky a software čínských společností Huawei a ZTE. Jako odůvodnění tohoto varování uvádí NÚKIB argumenty především netechnického rázu: 1) právní prostředí v Čínské lidové republice (ČLR), které nutí čínské společnosti a občany ke spolupráci (včetně zpravodajské) s čínskými státními orgány, a vzbuzuje obavu že, „zájmy ČLR mohou být stavěny nad zájmy uživatelů technologií uvedených společností."[7] 2) zpravodajské operace ČLR na území ČR, na které dlouhodobě upozorňují poznatky Bezpečnostní informační služby. 3) zpravodajské poznatky o fungování výše zmíněných společností na území ČR, které vyvolávají obavy z využívání technologií a produktů těchto firem k prosazování zájmu ČLR. Samotné varování neznamenalo zákaz používání produktů a softwaru ZTE a Huawei, ale všichni správci systémů kritické kybernetické infrastruktury, které pod pravomoc NÚKIBu spadají, museli provést novou analýzu rizik.[8] Následně provedené hodnocení, který NÚKIB zpracoval ukázal o, že ze 126 institucí spadajících pod zákon o kybernetické bezpečnosti výrobky těchto firem většina (75/126) nepoužívá.[9]

The Prague Proposals (3. 5. 2019)[10]

Důležitost posuzování netechnických rizik se projevila i v závěrečném dokumentu mezinárodní konference o bezpečnosti sítí páté generace, která se uskutečnila v květnu 2019 v Praze. The Prague Proposals rozšiřují samotný rozměr kybernetické bezpečnosti o netechnické aspekty, jako jsou národní strategie, právní rámec či lidské zdroje, při analýze rizik pak doporučují zaměřit se na politické a ekonomické chování rizikových aktérů. Dokument také detailně popisuje metodu určení rizika vyplývajícího z možného ovlivňovaní dodavatele ze strany státu: jedná se o strukturu vnitřního řízení firmy či o zapojení do mezinárodních úmluv zaměřených na ochranu dat a kybernetickou bezpečnost.

EU-coordinated risk assessment of the cybersecurity of 5G networks (9. 10. 2019)[11]

Velmi podrobně jsou tyto netechnická aspekty rozpracovány v celoevropském hodnocení rizik spojených s budováním 5G sítí z října 2019. Za důležitý faktor je určena podniková řídící struktura, která je důležitá pro transparentnost a výkon řízení, který se mezi jednotlivými dodavateli významně liší. Při určování rizikovosti dodavatele, resp. možného uplatňování vlivu ze strany vlády třetí země dokument dále doporučuje posuzovat následující faktory.

1. sílu vazby mezi dodavatelem a jeho vládou
2. zákony dané země, především tam, kde není nastaven systém institucionálních brzd a protiváh a neexistují zákony na ochranu bezpečnosti dat
3. schopnost vlády vykonávat tlak na výrobce
4. schopnost zaručit dostupnost dodávek
5. celkovou kvalitu dodavatelových produktů a nařízení k ochraně kybernetické bezpečnosti včetně kontroly dodavatelského řetězce

Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures (29. 01. 2020)[12]

Na výše uvedené celoevropské hodnocení rizik z října 2019 navázalo v lednu 2020 sdělení Evropské komise pod názvem Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures. Tento dokument je souborem doporučení pro členské státy k zajištění bezpečné výstavby a fungování sítí páté generace. Kromě upozornění na důležitost posuzování netechnických rizik, doporučení zahrnují i varování před přílišnou závislostí na jednom dodavateli (vendor lock-in). Na dodavatele, kterého členský stát vyhodnotí jako vysoce rizikového, by měla být uvalena účinná omezení včetně jeho vyloučení z kritických/strategických součástí komunikační architektury (např. jádro sítě). K ochraně 5G sítí před riziky ze strany investorů ze třetích zemí by měl být také využíván vznikající evropský rámec pro prověřování investic.

Společná deklarace v oblasti bezpečnosti sítí 5. generace (06. 05. 2020)[13]

Dalším dokumentem, který se věnuje netechnickým rizikům dodavatelů 5G sítí je společná deklarace České republiky a Spojených států, kterou český premiér Andrej Babiš a americký ministr zahraniční Mike Pompeo podepsali v květnu 2020. Při posuzování rizikového profilu dodavatelů se kromě již standardně uváděných faktorů (nepatřičný vliv státu, transparentnost vlastnické a kontrolní struktury) uvádí i respekt k ochraně k duševnímu vlastnictví a zda je jednání dodavatelů dlouhodobě etické a zda jsou povinni zákonem dodržovat principy korporátní transparence. Důraz na etické chování je velmi důležitý, neboť právě z jeho porušování je mnoho čínských dodavatelských firem obviňováno

5 "Exclusive: India plans to fast track Chinese investments after policy change - Sources". Reuters, https://www.reuters.com/article/us-india-china-investments-exclusive-idUSKCN2270L9.

6 "Varování NÚKIB před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation". Národní úřad pro kybernetickou a informační bezpečnost, https://www.nukib.cz/download/uredni-deska/Varován%C3%AD%20NÚKIB%202018-122-17.pdf

7 Ibid.

8 "Metodika k varování ze dne 17. prosince 2018". Národní úřad pro kybernetickou a informační bezpečnost, https://www.govcert.cz/download/kii-vis/2019_01_04_metodika_k_varov%C3%A1n%C3%AD_z_17-12-2018_v1.0.pdf

9 "Ministerstva, úřady i firmy vzaly varování NÚKIB vážně." Národní úřad pro kybernetickou a informační bezpečnost, https://www.nukib.cz/cs/informacni-servis/aktuality/1349-ministerstva-urady-i-firmy-provedly-predepsane-analyzy-prijimaji-opatreni-ke-snizeni-rizika/.

10 "Prague 5G Security Conference announced series of recommendations: The Prague Proposals." Vláda ČR, https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

11 "EU-coordinated risk assessment of the cybersecurity of 5G networks". European Commission, https://ec.europa.eu/newsroom/dae/document.cfm?-doc_id=62132

12 "Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures". European Commission, https://ec.europa.eu/newsroom/dae/document.cfm?-doc_id=64468

13 "Společná deklarace v oblasti bezpečnostní sítí 5. generace". Vláda ČR, https://www.vlada.cz/assets/media-centrum/aktualne/deklarace-G5.pdf

především kvůli svému zapojení do budování internačních táborů pro Ujgury.

Další debata o netechnických rizicích a důvěryhodných dodavatelích

Definice důvěryhodného dodavatele se stala i součástí politické debaty ve Velké Británii a v Německu. Poslanci britské vládnoucí Konzervativní strany nesouhlasící s vládním rozhodnutím umožnit firmě Huawei budovat sítě páté generace požadují, aby se do jejich výstavby mohly zapojit pouze společnosti ze států, které mají společenský systém nastavený na spravedlivé hospodářské soutěži, vládě práva, respektu k lidským právům a ochraně soukromých dat.[14]

Německá vláda zatím o případné účasti či neúčasti čínských firem na budování 5G sítí ještě nerozhodla. Koaliční SPD je proti zapojení Huawei,[15] CDU/CSU po explicitním zákazu nevolá.[16] Ve vnitrostranickém strategickém dokumentu o výstavbě 5G však požaduje, aby se na výstavbě (a to bez rozlišení, zda se jedná o jádro či okraj sítě) podíleli pouze důvěryhodní partneři, kteří budou muset splnit řadu bezpečnostních podmínek (více neupřesněných, pozn. aut.) Takto vybudované sítě by měly být chráněny před zásahy cizích států.[17] Pokud dodavatel uvedené podmínky nesplní, měly by být jeho výrobky zakázány.[18]

Vyloučení nedůvěryhodných dodavatelů může být také navázáno na snahu posílit domácí výrobní kapacitu, jak dokazuje iniciativa amerického ministerstva obrany "Trusted Capital Market Place", která by měl propojit "prověřené" kapitálové investory s malými a středními výrobci technologií důležitých pro národní bezpečnost např. dronů. [19]

ČÍNSKÉ FIRMY A NETECHNICKÁ RIZIKA

Z výše uvedeného přehledu faktorů, které české úřady a spojenecké země považují u možných dodavatelů za rizikové, se nejčastěji objevuje státní vliv na daného výrobce. V případě čínských firem však nesmíme zapomenout na to, že moc v této zemi nevykonává formálně jen vláda a státní orgány, ale především Komunistická strana Číny. Při určování míry vztahu mezi danou firmou a státem lze tedy hovořit o třech faktorech: (1) míra majetkové státní účasti v dané firmě; 2) vliv Komunistické strany Číny uvnitř firmy a 3) obecný legislativní rámec, ve kterém se firmy a jejich zaměstnanci pohybují.

První faktor je jasný a mezi níže uvedenými firmami najdeme ty, kde je hlavním vlastníkem stát (CGN), ty, kde je stát sice menšinovým majitelem, ale přesto vykonává kontrolní funkci (Hikvision) a také firmy, ve kterých stát majetkový podíl nemá (DJI, Huawei). I když posledně uvedené firmy mohou být na státní kontrole z hlediska výkonu majetkových práv formálně nezávislé, některé z nich dostávají od státu velmi vysoké finanční pobídky a podporu, což je často velmi zvýhodňuje oproti jejich západním konkurentům.[20]

Státní podniky musely nedávno také změnit své stanovy tak, aby explicitně uznávaly vůdčí roli komunistické strany.[21]

Další dva faktory jsou však mnohem důležitější, neboť se týkají všech firem bez ohledu na to, kdo je vlastní. Z hlediska vlivu komunistické strany na fungování podniku je důležité posilování moci podnikových stranických buněk, které musí zřídit každá organizace ve které pracují více jak tři členové komunistické strany a tyto podnikové organizace mají kontrolovat naplňování stranických cílů.[22] K tomu, aby zřídily stranické buňky, jsou nuceny i pobočky nečínských firem[23] a některé tak i učinily.[24] Dalším kontrolním mechanismem, který může čínská komunistická strana a státní orgány využít pro prosazování svých zájmů u soukromých firem je zákon o státní zpravodajské činnosti z roku 2017 vyzývající v článku 7 všechny čínské organizace a občany k tomu, aby se v zájmu národní bezpečnosti podíleli na státních zpravodajských aktivitách: „Každá organizace i občan musí v souladu se zákonem podporovat, napomáhat a podílet se na státní zpravodajské činnosti a zachovávat v tajnosti vše, co je jim známo o státní zpravodajské činnosti. Stát poskytuje ochranu jednotlivcům a organizacím, které podpoří státní zpravodajskou činnost, napomohou jí a podílejí se na ní."[25]

Profil čínských společností označených ČR nebo spojenci za bezpečnostní riziko

Dahua Technology

Společnost Dahua je významným výrobcem kamer, sledovacích a nahrávacích zařízení. Největším podílníkem firmy je její předseda představenstva Fu Liquan (36,1% akcií).[26] Dle jejích vlastních informací dodává Dahua své výrobky do více než 180 zemí a jedná se o "druhou největší společnost dodávající sledovací vybavení."[27] Mezi hodnoty, na nichž je fungování společnosti založeno, patří společensky odpovědné chování spočívající v budování lépe zabezpečeného světa („a better secured world").[28] V roce 2017 byla většina kamer této firmy ohrožena softwareovou chybou (backdoor)[29], která se však po následující opravě podezřele objevila v jiném místě kódu.[30] Podílela se také na výstavbě internačních táborů pro Ujgury v provincii Sin-ťiang.[31] V roce 2019 byla u kamer Dahua objevena zvláště nebezpečná bezpečnostní chyba, která umožnila využít připojené zařízení k odposlouchávání, i když uživatel vypnul zvukový vstup.[32] Dalším incidentem byla chyba objevená v roce 2017, která umožnila obejít zabezpečení kamery heslem a získat tak přístup k celkovému nastavení a citlivým informacím.[33]

Hytera

Hytera je výrobcem komunikačních zařízení typu vysílaček a radiostanic. Jedná se o soukromou společnost založenou v roce 1993, která své výrobky dodává do více než 120 zemí na světě.[34] V její expanzi významně napomohla akvizice britské společnosti Sepura Group v roce 2017, která však vyvolala obavy britského ministerstva vnitra z možných negativních dopadů na národní bezpečnost.[35] Využívání svých výrobků čínskými bezpečnostními složkami v internačních táborech pro Ujgury uvádí Hytera jako úspěšný příklad nasazení své technologie v oblasti veřejného pořádku.[36] Národně bezpečnostní rizika zmiňovaná v souvislosti se společností Hytera jsou zaměřena především na možnost odposlouchávání bezpečnostních složek, které její vybavení používají[37]. Spojené státy také v roce 2017 protestovaly proti rozhodnutí kanadské vlády povolit společnosti Hytera akvizici kanadského výrobce satelitní a komunikační techniky Norsat, mezi jejíž odběratele patří i americké ozbrojené síly.[38] Hytera v roce 2020 také prohrála

14 "Chinese diplomat accuses Tory MPs of Huawei 'witch hunt'".Financial Times. https://www.ft.com/content/8858c230-4b3b-11ea-95a0-43d18ec715f5.

15 "German Parliament to decide on Huawei 5G livolvement, Merkel's CDU Party agrees". DW.COM, https://www.dw.com/en/german-parliament-to-decide-on-huawei-5g-involvement-merkels-cdu-party-agrees/a-51379848.

16 "German Conservatives vote ‚in unison' against excluding Huawei from 5G Network". Www.Euractiv.Com, https://www.euractiv.com/section/5g/news/german-conservatives-vote-in-unison-against-excluding-huawei-from-5g-network/.

17 "Deutschlands digitale Souveränität sichern – Maßstäbe für sichere 5G-Netze setzen". CDU/CSU, https://www.cducsu.de/sites/default/files/2020-02/Positionspapier%205G-Netzaufbau-100220.pdf

18 Ibid.

19 "Pentagon about to kick off first Trusted Capital Marketplace event". National Defense Magazine, https://www.nationaldefensemagazine.org/articles/2019/10/18/pentagon-about-to-kick-off-first-trusted-capital-marketplace-event.

20 "State support helped fuel Huawei's global rise". Wall Street Journal, https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

21 "China's Communist party writes itself into company law". Financial Times, https://www.ft.com/content/a4b28218-80db-11e7-94e2-c5b903247afd#myft:saved-articles:page.

22 "The Party leads on everything". Mercator Institute for China Studies. https://www.merics.org/en/china-monitor/the-party-leads-on-everything

23 "German trade body warns firms may pull out of China". South China Morning Post, https://www.scmp.com/news/china/economy/article/2122104/german-trade-body-warns-firms-may-pull-out-china-over-communist.

24 "Wal-Mart bends to party rules in China, allowing store cells".Wall Street Journal, https://www.wsj.com/articles/SB116643170055253261.

25 "Čínský zákon o celonárodní špionáži". Sinopsis, https://sinopsis.cz/cinsky-zakon-o-celonarodni-spionazi/.

26 "2019 Q1 Report". Dahua. https://www.dahuatech.com/upload/2019/04/30/1556590642554i8zji.pdf

27 "Overview". Dahua, https://www.dahuasecurity.com/ceen/aboutUs/introduction/0

28 "Core values". Dahua, https://www.dahuasecurity.com/ceen/aboutUs/introduction/1172

29 "Dahua backdoor". Krebs on Security. https://krebsonsecurity.com/tag/dahua-backdoor/.

30 "Hacker heaven: Huawei's hidden back doors found". Breaking Defense, https://breakingdefense.com/2019/07/hunting-huaweis-hidden-back-doors/.

31 "Mapping China's tech giants". Australian Strategic Policy Institute, https://chinatechmap.aspi.org.au/

32 "Warning as millions of Chinese-made cameras can be hacked to spy on users: Report". Forbes, https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/.

33 "ICS Advisory (ICSA-17-124-02) Dahua Technology Co., Ltd Digital Video Recorders and IP Cameras". CISA. https://www.us-cert.gov/ics/advisories/ICSA-17-124-02.

34 "Why Hytera". Hytera. https://www.hytera.com/en/#/index/category/196/196

35 "Hytera-Sepura". Competition & Martkets Authority https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/613459/sepura-hytera-cma-report-redacted.pdf

36 "Solution in public security". Hytera, https://www.hytera.com/en/category/907

37 "Chinese Maker of Radios for Police, Firefighters Struggles to Outlast Trump Trade Fight". Washington Post, https://www.washingtonpost.com/business/economy/chinese-maker-of-radios-for-police-firefighters-promises-to-outlast-trump-trade-fight/2019/01/30/42a118a8-1f33-11e9-8b59-0a28f2191131_story.html

38 Ibid.

soudní spor se svým hlavním rivalem Motorola, který ji obvinil z krádeže obchodních tajemství.[39]

Hikvision

Firma Hikvision je největším výrobcem bezpečnostních kamer na světě se zhruba čtvrtinovým tržním podílem.[40] Zaměřuje se také na výzkum a vývoj v oblasti „internetu věcí", strojového učení a umělé inteligence [41] a vývoj vlastního cloudového řešení, které by propojilo data zachycená periferními zařízeními (kamery) s širším informačním prostorem. [42] Společnost také navrhuje různá řešení téměř ve všech sférách společenského a ekonomického chování, od chytrých domácností po komunální rozhodování.[43] Největším akcionářem (39,6%) Hikvision je státní společnost China Electronics Technology HIK Group (CETHIK), která v Hikvision má i další menšinový podíl (1,96%) skrze svůj The 52nd Research Institute.[44] Podobně jako Dahua má i Hikvision problémy se zabezpečením svých kamer, které tak mohou být zneužity k získání citlivých informací.[45]

ZTE Corporation

ZTE je významným výrobcem prvků telekomunikačních sítí (včetně 5G), a koncových zařízení, které dodává do více sto světových zemí.[46] Největším (a kontrolujícím) akcionářem je s 27,18% společnost Zhongxingxin Telecom Company Limited [47,] ve kterém mají významný podíl přes své dceřiné firmy jedny z nejvýznamnějších státních společnosti China Aerospace Science and Technology Corporation (CASC, 34%) a China Aerospace and Industry Corporation (CASIC, 14,5%).[48] Používání produktů firmy ZTE označilo za bezpečnostní riziko v roce 2018 britské National Cyber Security Centre[49], ve stejném roce i český Národní úřad pro kybernetickou a informační bezpečnost a jejich používání výslovně zakázala i americká Federal Communications Commission v listopadu 2019.[50]

SZ DJI Technology Co., Ltd

Společnost DJI je jedním z největších výrobců civilních bezpilotních leteckých prostředků (dronů) a např. v USA její tržní podíl dosahuje více než 70%.[51] Jedná se o soukromou společnost, zcela vlastněnou hongkongskou společností iFlight Technology Com.[52] Drony této společnosti jsou také využívány k zajišťování internačních táborů v provincii Sin-ťiang. Bezpečnostní obavy spojené s využíváním dronů DJI vzbuzuje především nakládání se získanými daty a možnost jejich odeslání do zahraničí[53] a obecnou nízkou úrovní bezpečnosti.[54]

China General Nuclear Power Corporation (CGN)

CGN je vlastněna čínským státem skrze The State-owned Assets Supervision and Administration Commission (SASAC).[55] Zabývá se především výstavbou a provozem jaderných elektráren včetně výroby jaderného paliva. Vlajkovou lodí jejího jaderného programu je vlastní reaktor HPR 1000.[56] V samotné Číně CGN provozuje pět jaderných elektráren[57] a dlouhodobě se snaží o expanzi do zahraničí, především pak do Velké Británie (projekt Hinkley Point C, Bradwell B, viz dále). Zájem o výstavbu nových jaderných bloků projevila také v České republice[58], Keni[59] a Rumunsku, kde měla podle dohody podepsané v květnu 2019 postavit dva nové reaktory v jaderné elektrárně Cernavoda. Na začátku roku 2020 však rumunský premiér Ludovic Orbán, oznámil, že Rumunsko od dohody odstupuje s tím, že „dohoda nemůže fungovat".[60] V roce 2016 byla CGN obviněna z provádění špionáže s cílem získat informace o americkém jaderném sektoru[61], což vedlo k zavedení zákazu na dodávky amerických jaderných technologií do Číny.[62]

Huawei Technologies Co.

Společnost Huawei byla založena v roce 1987 a dnes patří mezi největší světové výrobce a dodavatele informačních a komunikačních technologií, včetně infrastruktury pro sítě 5. generace. Společnost opakovaně zdůrazňuje to, že mezi jejími podílníky není žádná státní instituce[63] a že nespolupracuje se státními orgány.[64] V dodávkách vybavení pro mobilní sítě je její tržní podíl zhruba dvojnásobný oproti společnému podílu společností Ericsson a Nokia.[65] V prodeji mobilních telefonů je pak Huawei druhá na světě.[66] Mezi bezpečnostní rizika spojovaná s firmou Huawei patří existence „zadních vrátek" (backdoors) v jejich produktech[67], provádění špionáže v sídle Africké unie[68] či v Polsku.[69]

Další rizika představují různé aplikace, které mohou narušit soukromí uživatelů či o nich sbírat osobní data, která pak mohou být využita ke spearphishingovým útokům nebo klasickému vydírání. V nedávné době byla v této souvislosti prověřována populární aplikace na sdílení krátkých videí TikTok, jejíž používání zakázalo svým zaměstnancům několik federálních institucí v USA[70]. Z důvodu možného zneužití citlivých dat pro vydírání a např. i donucení ke zpravodajské spolupráci nařídila americká Committee on Foreign Investment in the United States (CFIUS) čínské společnosti Kunlun prodat nedávno koupenou seznamovací aplikaci Grindr.[71] Dalším relevantním rozhodnutím CFIUS bylo zablokování akvizice společnosti MoneyGram, zabývající se převody peněz, čínskou firmou Ant Financial patřící do konsorcia Alibaba.[72] V nedávně době také vyšlo najevo, že data o svých uživatelích sbírají a bez jejich vědomí odesílají servery v Číně, Rusku a Singapuru i mobily čínského výrobce Xiaomi.[73]

39 "Motorola wins $765 million over theft by Chinese radio rival". Bloomberg.Com, https://www.bloomberg.com/news/articles/2020-02-14/motorola-solutions-wins-764-6-million-in-trial-against-hytera.

40 "2018 Annual Report". Hikvision, https://www.hikvision.com/content/dam/hikvision/en/brochures/hikvision-financial-report/Hikvision%202018%20Annual%20Report.pdf

41 Ibid.

42 Ibid.

43 Ibid.

44 Ibid.

45 "ICS Advisory (ICSA-17-124-01) Hikvision Cameras". CISA, https://www.us-cert.gov/ics/advisories/ICSA-17-124-0 a "5G and the Internet of Things: Chinese Companies' Inroads into 'Digital Poland'". Sinopsis, https://sinopsis.cz/en/sarek-5g-iot/

46 "Annual Report 2019". ZTE, https://res-www.zte.com.cn/mediares/zte/Investor/20200417/E1.pdf

47 Ibid.

48 "ZTE's less-known roots: Chinese tech company falls from grace". Nikkei Asian Review, https://asia.nikkei.com/Business/Company-in-focus/ZTE-s-less-known-roots-Chinese-tech-company-falls-from-grace.

49 "China's ZTE deemed a ‚national security risk' to UK". The Guardian, https://www.theguardian.com/technology/2018/apr/17/chinas-zte-a-national-security-risk-to-uk-warns-watchdog

50 "Huawei, ZTE urge U.S. not to impose national security risk labels". Reuters, https://www.reuters.com/article/us-usa-china-huawei-tech-idUSKBN1ZX2V1.

51 "Drone manufacturer market shares: DJI leads the way". Drone Industry Insights, https://www.droneii.com/drone-manufacturer-market-shares-dji-leads-the-way-in-the-us

52 "Mapping China's tech giants". | Australian Strategic Policy Institute". Australian Strategic Policy Institute, https://chinatechmap.aspi.org.au/

53 "Chinese drone maker tries to quell talk of data siphoning -". FCW, https://fcw.com/articles/2019/06/24/drones-dji-pushback-senate-hearing.aspx

54 "Why is DJI getting the Huawei treatment?" CyberScoop, https://www.cyberscoop.com/dji-cybersecurity-huawei-data-breach-china/.

55 "CGN nails down its first A-share platform". CGN, http://en.cgnpc.com.cn/encgn/c100035/2017-10/20/content_3b679c150e4f453f90332e245ed0cb0f.shtml.

56 "HPR100". CGN, http://en.cgnpc.com.cn/encgn/c100048/business_tt.shtml

57 "Nuclear power". CGN, http://en.cgnpc.com.cn/encgn/c100044/nuclearpower.shtml

58 "Communications"., CGN, http://en.cgnpc.com.cn/encgn/c100101/2016-03/31/content_4f5e26ac4a92404ba5ef27c3b6a156d3.shtml

59 "China's CGN extends its cooperation with Kenya"., World Nuclear News, https://www.world-nuclear-news.org/C-Chinas-CGN-extends-its-cooperation-with-Kenya-2303174.html

60 "Nuclear power". CGN, http://en.cgnpc.com.cn/encgn/c100044/nuclearpower.shtml

61 "U.S. nuclear engineer, China General Nuclear Power Company and Energy Technology International indicted in nuclear power conspiracy against the United States". US Department of Justice, https://www.justice.gov/opa/pr/us-nuclear-engineer-china-general-nuclear-power-company-and-energy-technology-international.

62 "US adds China's biggest nuclear company to ‚entity list'". Nikkei Asian Review, https://asia.nikkei.com/Economy/Trade-war/US-adds-China-s-biggest-nuclear-company-to-entity-list.

63 "Corporate Information". Huawei, https://www.huawei.com/en/corporate-information.

64 "Huawei Founder Denies Spy Risk Claims". BBC News, https://www.bbc.com/news/technology-46875747.

65 Nokia calls up former star to lead 5G turnaround". Financial Times, https://www.ft.com/content/61cde5a2-5c96-11ea-8033-fa40a0d65a98

66 "Apple, Huawei boost market share, as first-quarter China smartphone shipments fall". Reuters, https://www.reuters.com/article/us-smartphone-sales-china-idUSKBN22D44U.

67 "Researcher: Backdoor mechanism still active in many IoT products". ZDNet, https://www.zdnet.com/article/researcher-backdoor-mechanism-still-active-in-many-iot-products/ a či "U.S. officials say Huawei can covertly access telecom networks". Wall Street Journal, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

68 "The African Union headquarters hack and Australia's 5G network". The Strategist, https://www.aspistrategist.org.au/the-african-union-headquarters-hack-and-australias-5g-network/.

69 "Poland arrests huawei worker on allegations of spying for China". The Guardian, https://www.theguardian.com/technology/2019/jan/11/huawei-employee-arrested-in-poland-over-chinese-spy-allegations.

70 "US government agencies are banning TikTok, the social media app teens are obsessed with, over cybersecurity fears — here's the full list". Business Insider, https://www.businessinsider.com/us-government-agencies-have-banned-tiktok-app-2020-2.

71 "Grindr is being sold by Chinese owner after U.S. raises national security concerns". Los Angeles Times, https://www.latimes.com/business/technology/story/2020-03-06/grindr-sold-by-chinese-owner-after-us-national-security-concerns.

72 "U.S. blocks MoneyGram sale to China's Ant Financial on national security concerns". Reuters, https://www.reuters.com/article/us-moneygram-intl-m-a-ant-financial-idUSKBN1ER1R7.

73 "Mobily firmy Xiaomi posílají data do Číny. Mají je stovky českých úředníků". Seznam Zprávy. https://www.seznamzpravy.cz/clanek/mobil-od-cinskeho-xiaomi-maji-stovky-ceskych-uredniku-kdo-ma-jejich-data-105028.

REAKCE NA RIZIKA SPOJENÁ S ČÍNSKÝMI TECHNOLOGIEMI

Zákaz nákupu a využívání výrobků firem Huawei, ZTE, Hytera, Hikvison a Dahua je v americkém právu obsažen v John McCain National Defense Act pro rozpočtový rok 2019, který vstoupil v platnost 13. srpna 2018[74] Kromě výše vyjmenovaných firem se může týkat jakýchkoli dalších telekomunikačních či sledovacích zařízení vyrobených čínskými firmami, pokud tak rozhodne americký ministr obrany. Americké federální agentury nesmí výše uvedené výrobky nakupovat, prodlužovat stávající smlouvy (s platností od 13. 8. 2019) a nesmí je využívat ani jejich subdodavatelé (s platností od 13. 8. 2020). Instituce a firmy, které zakázané technologie používají, se mohou obrátit na federální úřady, které jim mají pomoci finančně a technicky dané systémy nahradit. Dotčené instituce mohou žádat o odložení povinnosti splnit ustanovení zákona, ale jen po dva roky.[75]

Dalším produktem čínských firem, jejichž používání bylo omezeno z národně-bezpečnostních důvodů, jsou drony, které americké federální instituce široce využívají.[76] V květnu 2019 vydalo americké ministerstvo vnitra varování s upozorněním na riziko, že data z dronů mohou být zneužita čínskými zpravodajskými službami.[77] V září 2019 pak americký senátor Rick Scott předložil návrh zákona, který by zakázal nákup a používání dronů vyrobených v Číně, což by se pochopitelně týkalo i společnosti DJI.[78] O měsíc později pak americké ministerstvo vnitra dočasně pozastavilo využívání všech dronů vyrobených v Číně nebo obsahujícím čínské komponenty. [79]

Dalším důležitým zákonem, resp. jeho novelou, která v nedávné době vstoupila v platnost, je Foreign Investment Risk Review Modernization Act z roku 2018, posilující a zpřísňující systém na prověřování možných rizik spojených s ekonomickou činností cizích osob a firem v USA. Tento zákon umožňuje americké vládě poskytnout státům, které jsou důležitými americkými spojenci, výjimku z nutnosti podstoupit v některých případech prověření svých ekonomických aktivit v USA.[80] Podmínkou pro zařazení na tento „whitelist" je existence silných a účinných zákonů na ochranu před nestandardním ekonomickým chováním cizích mocností v dané zemi (např. existence zákona na prověřování zahraničních investic, dobře definované moderní technologie, které mají být chráněny) nebo velmi úzká zpravodajská spolupráce mezi daným státem a USA.[81] V současné chvíli byla tato výjimka udělena Austrálii, Kanadě a Velké Británii, se kterými USA sdílí nejcitlivější zpravodajské informace. Když britský premiér Johnson začátkem roku 2020 nezakázal účast Huawei na výstavbě 5G sítí ve Velké Británii, navrhl americký senátor Rubio, aby byla Velká Británie z výše uvedeného seznamu vyškrtnuta a výše uvedená FIRRMA byla novelizována tak, aby zohledňovala přítomnost čínských technologií v 5G sítích u států, které by se chtěly dostat na preferenční seznam. [82]

Rizik spojených s používáním čínských technologií se týkají i vývozní kontroly, které americká administrativa v několika posledních letech vůči čínským firmám (ZTE, Huawei) zavádí. Čínští výrobci tak často nemají přístup k nejnovějším a nejbezpečnějším komponentům či softwaru (např. nemohou na vyráběné telefony instalovat operační systém Android).[83] Tyto vývozní kontroly se netýkají pouze čínských ICT firem, ale i CGN, která byla na tzv. entity list zahrnuta kvůli obvinění z krádeže technologií a využívání pro vojenský jaderný výzkum.[84]

[74] "John S. McCain National Defense Authorization Act for Fiscal Year 2019"., U.S. Congress, https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf

[75] Ibid.

[76] "Public safety drones: An update". Center for the Study of the Drone, https://dronecenter.bard.edu/files/2018/05/CSD-Public-Safety-Drones-Update-1.pdf

[77] "DHS warns of data threat from Chinese-made drones". Reuters, https://www.reuters.com/article/us-usa-drones-china-idUSKCN1SQ1ZY.

[78] "American Security Drone Act of 2019". U.S. Congress, https://www.congress.gov/bill/116th-congress/senate-bill/2502/text.

[79] US agency grounds Chinese drones on security fears". Financial Times, https://www.ft.com/content/ada688c8-fbeb-11e9-a354-36acbbb0d9b6

[80] "US exempts allies from some national security deal reviews". Financial Times, https://www.ft.com/content/41d71314-364d-11ea-a6d3-9a26f8c3cba4

[81] "Excepted foreign state – factors for determination". U.S. Department of Treasury, https://home.treasury.gov/system/files/206/Excepted-Foreign-State-Factors-for-Determinations.pdf

[82] "Rubio joins Cotton, Cruz, Hawley to introduce bill requiring CFIUS to reexamine U.K. status after 5G decision". Marco Rubio, https://www.rubio.senate.gov/public/index.cfm/2020/3/rubio-joins-cotton-cruz-hawley-to-introduce-bill-requiring-cfius-to-reexamine-u-k-status-after-5g-decision

[83] "Huawei shown to have switched to Chinese parts after US blacklisting". Financial Times, https://www.ft.com/content/449f6962-a705-437e-8679-f6a7057594c4

[84] "US warns Britain against Chinese alliances on nuclear plants". Financial Times, https://www.ft.com/content/84ab26f6-d7a5-11e8-a854-33d6f82e-62f8#myft:saved-articles:page

Stejně jako Spojené státy má velice obezřetný postoj k čínským ICT dodavatelům například třistakrát menší Estonsko, jehož ekonomika je postavena na využívání moderních technologií. Ve své poslední výroční zprávě uvádí estonská rozvědka, že „možný vznik technologické závislosti představuje ohrožení estonské bezpečnosti" a „protože pro digitalizovaný národ, jako je Estonsko, komunikační technologie představují životně důležitou část infrastruktury, je nutné zvážit všechna rizika spojená s používanými technologiemi. Menší státy představují pro Čínu snadnější cíl k vybudování závislosti a pozdějšího vyvíjení tlaku.[85]" A právě obavy z možného zneužití čínských technologií k politickým cílům vedly estonské úřady k vyloučení Huawei z výstavby sítí 5G v této zemi.[86] Estonský premiér Jüri Ratas také podepsal i memorandum s americkým viceprezidentem Mikem Pencem, ve kterém odkazují na Prague Proposals.[87] Podobné memorandum podepsalo i Polsko a Rumunsko[88], Lotyšsko[89] a v květnu 2020 i Česká republika.

Zajímavým vývojem ve vztahu k čínským technologiím prošla Velká Británie. Pro mnoho čínských firem se Velká Británie stala důležitým odrazovým můstkem pro vstup na „západní" trh, který byl podporován tehdejší vládou premiéra Camerona, který v roce 2015 mluvil o „zlaté éře" britsko-čínských vztahů.[90] Jedním z příkladů užších vztahů měla být účast čínské státní firmy China General Nuclear Power Group (CGN) na budování britských jaderných elektráren. Výstavba nových britských jaderných elektráren se dlouhodobě potýká s nedostatkem finančních prostředků a CGN tak investičně vstoupila do projektu jaderné elektrárny Hinkley Point C, který staví francouzská firma EDF (CGN získala 1/3 podíl)[91], má spolufinancovat výstavbu další elektrárny (Sizewell C)[92] a ve třetím jaderném projektu (Bradwell) by měla postavit vlastní reaktor Hualong HPR 1000.[93] Tento „progresivní vstup" CGN do britského civilního jaderného sektoru byl založen na britsko-čínské dohodě z roku 2014.[94]

V létě roku 2016 se však nová britská premiérka Theresa May rozhodla celý projekt Hinkley Point C pozastavit a nechat ho prověřit z národně bezpečnostních důvodů.[95] Na toto rozhodnutí okamžitě reagoval čínský velvyslanec, který naznačil, že britské rozhodnutí se může stát klíčovým zlomem v britsko-čínských vztazích a ohrozit i další spolupráci.[96] Britská vláda se nakonec v září 2016 rozhodla projekt schválit, ale za zpřísněných podmínek. Bez jejího souhlasu se nebude moci měnit vlastnická struktura konsorcia a všechny další jaderné projekty budou probíhat za zpřísněných kontrol hlavních dodavatelů a subdodavatelů tak, aby případná účast cizích firem neohrozila britskou národní bezpečnost.[97]

Ještě radikálněji změnila britská vláda svůj názor na společnost Huawei, která je ve Velké Británii dlouhodobě aktivní[98] a v roce 2010 zde ve spolupráci s britskou vládní agenturou Government Communications Headquaters (GCHQ) zřídila Huawei Cyber Security Evaluation Centre, ve kterém měla mít britská vláda možnost zhodnotit všechna možná rizika spojená s použitím této technologie.[99] Výroční zprávy tohoto centra rozhodně

[85] "International Security and Estonia", Estonian Foreign Intelligence Service, https://www.valisluureamet.ee/pdf/raport-2020-en.pdf

[86] "Estonia plans to restrict govt use of Huawei 5G technology". AP NEWS, https://apnews.com/5252717083c64dc48aa92004cad5294b.

[87] "Estonia and the US Sign a memo on 5G Security, exclude Chinese Huawei". Estonian World, https://estonianworld.com/security/estonia-and-the-us--sign-a-memo-on-5g-security-exclude-chinese-huawei/.

[88] "Poland wants to go beyond EU on 5G security, says minister". POLITICO, https://www.politico.eu/article/poland-wants-to-go-beyond-5g-security-toolbox-restrictions/.

[89] "Latvia-US declaration on 5G network security underscores necessity to evaluate suppliers". Baltic Times, https://www.baltictimes.com/latvia-us_declaration_on_5g_network_security_underscores_necessity_to_evaluate_suppliers/.

[90] "China, Britain to benefit from ‚golden Era' in ties - Cameron". Reuters, https://www.reuters.com/article/us-china-britain-idUSKCN0SB10M20151017.

[91] "Final contracts signed for Hinkley Point C project". World Nuclear News, https://world-nuclear-news.org/Articles/Final-contracts-signed-for-Hinkley-Point-C-project

[92] "EDF Energy submits plans for Sizewell C : New Nuclear", World Nuclear News, https://world-nuclear-news.org/Articles/EDF-Energy-submits-plans-for-Sizewell-C

[93] "UK's reliance on China's nuclear tech poses test for policymakers", Financial Times, https://www.ft.com/content/7734e3be-2f6f-11e9-8744-e7016697f225

[94] Ibid

[95] "Hinkley Point review signals UK rethink on Chinese investment". Financial Times, https://www.ft.com/content/2af4e1c8-5562-11e6-befd-2fc0c26b3c60

[96] "China warns UK over £18bn nuclear power deal". Financial Times, https://www.ft.com/content/b28e83a6-5d86-11e6-a72a-bd4bf1198c63

[97] https://www.gov.uk/government/news/government-confirms-hinkley-point-c-project-following-new-agreement-in-principle-with-edf

[98] "Government confirms Hinkley Point C Project following new agreement in principle with EDF". GOV.UK, https://www.gov.uk/government/news/government-confirms-hinkley-point-c-project-following-new-agreement-in-principle-with-edf.

[99] "Huawei Opens Cyber Security Evaluation Centre in the UK". Huawei, https://www.huawei.com/au/news/au/2010/hw-u_151000

neoznačují technologie společnosti Huawei za bezproblémové.[100] Ba naopak. A to i pro závažné chyby ve zdrojovém kódu a další bezpečnostní zanedbání.[101] Společnost Huawei oznámila, že náprava těchto chyb jí bude trvat nejméně tři roky.[102]

Za rizikové byly v květnu 2018 britským National Cyber Security Centre označeny i technologie společnosti ZTE s tím, že tato rizika nelze eliminovat přijetím žádných nápravných opatření (mitigation measures).[103] Přesto se v lednu 2020 britská vláda rozhodla, že se společnost Huawei bude moci na výstavbě sítí páté generace podílet pod podmínkou, že výrobky této společnosti mohou dosahovat nejvýše 35% tržního podílu v okrajových částech 5G sítě (edge), nebudou moci být využity v jádru sítě (core) a také nesmí být používány v jakýchkoli částech britské kritické infrastruktury jakou jsou vojenská zařízení či jaderné elektrárny.[104] Proti britskému rozhodnutí protestovaly nejen Spojené státy (i kvůli britskému zapojení do zpravodajské skupiny Five Eyes), ale také vlivná část vládnoucí konzervativní strany.[105] Obavy z rostoucích rizik spojených s čínskými technologiemi vyjádřily i britské zpravodajské služby.[106] Britský premiér nakonec své stanovisko v květnu 2020 přehodnotil a britská vláda nyní připravuje plán na úplné odstranění prvků Huawei z 5G sítí do roku 2023.[107]

VÝVOJ V ČR PO VAROVÁNÍ NÚKIB

Varování NÚKIB, které stran Huawei a ZTE v prosinci 2018 vydal, nevedlo pouze k přijetí nápravných opatření v již existujících systémech, ale mělo dopad i na veřejné zakázky na dodání výrobků a technologií této společnosti, které se teprve rozbíhaly. Jednalo se například o vyloučení společnosti Huawei z veřejné zakázky na systém Moje daně[108], úplnému zákazu využívat technologie Huawei a ZTE v sítích ministerstva zdravotnictví či rozhodnutí Nejvyššího soudu nenaistalovat již zakoupené servery této společnosti. Po varování vyloučilo firmu Huawei z ještě běžícího tenderu na dodávku serverů a dalších komponentů i Letiště Praha. [109]

Zajímavě se k analýze rizik spojených s využíváním těchto technologií postavilo ministerstvo vnitra, které výrobky od společnosti Huawei hodlá využívat i nadále[110], protože dané produkty nepůjdou do systémů, kterých se týká varování NÚKIB, a veřejné zakázky (kvůli nejnižší nabídnuté ceně) tak ministerstvo čínské společnosti uděluje i nadále.[111] To, že nejnižší nabídková cena při veřejných tendrech by již neměla být jediným důvodem pro udělení, zdůrazňuje jak EU 5G Toolbox[112], tak metodika NÚKIB, která poskytuje přehled toho, jaké možnosti mají zadavatelé při hodnocení bezpečnostních rizik v různých fázích zadávání veřejných zakázek tak, aby dostály všem českým zákonům a zároveň neohrozily národní bezpečnost.[113]

S blížícím se rozhodnutím, kdo a za jakých podmínek se bude na výstavbě českých sítí páté generace podílet, začala být společnost Huawei v ČR velmi aktivní. Pro své místní zastoupení plánuje zřídit funkci vedoucího kybernetické bezpečnosti, který by měl komunikovat s českými úřady.[114] Zároveň společnost spustila webovou stránku 5gvcesku.cz, která kromě představení očekávaných možných využití sítí 5G a internetu věcí obsahuje i dva dokumenty, které se jednak snaží napadnout široce přijímanou definici netechnických rizik dodavatelů a za druhé varují před vyššími náklady při budování sítí 5G, pokud by z něho byl vyřazen jeden z velkých dodavatelů. První dokument[115] zpracovala advokátní kancelář Toman, Devátý a partneři, která Huawei v České republice zastupuje[116] a jedná se o komentář k implementaci EU Toolbox v českém prostředí. Autoři komentáře tvrdí, že rizikovost by měla být posuzována u každého výrobku zvlášť a rozhodnutí o vyloučení dodavatele na základě jeho vztahu s vlastní vládou či povahy právního rámce jeho domovské země, které jsou v EU Toolbox uváděny jako rizikové faktory, nemusejí být dostatečně konkrétní a objektivní. Dodavatel nemá podle autorů „možnost legislativu určité země ovlivnit" a neměl by být vyloučen bez toho, aby byla předem vyhodnocena jeho rizikovost.[117]

Druhým dokumentem je studie vypracovaná na objednávku společnosti Huawei ekonomickým think-tankem CETA (Centre for Economic and Market Analyses).[118] Autoři studie se pokoušejí odhadnout finanční vícenáklady, které by České republice přineslo vyloučení jednoho z významných dodavatelů při výstavbě sítí páté generace v České republice.[119] Tato studie je založena na modelech vypracovaných pro Huawei britským výzkumným centrem Oxford Economics (OE), které publikovalo obdobně zaměřené případové studie pro Spojené státy, Velkou Británii a jiné země. CETA převzala blíže nevysvětlené a žádnými konkrétními výpočty nepodložené modely od OE a pro určení možné ztráty v ČR navíc použila několik let starou analýzu Hospodářské komory, ve které se o nákladech na vybudování sítí 5G vůbec nepíše.[120]

Bez reakce z čínské strany se neobešel ani podpis společné česko-americké deklarace o bezpečnosti sítí páté generace z května 2020, byť v ní není Čína vůbec zmíněna. Zástupce čínského velvyslanectví si na českém ministerstvu zahraničních věcí stěžoval, že ČR pojímá svoji kybernetickou bezpečnost v „silně protičínském duchu" a že podepsaná deklarace je „jasně formulovaná proti čínským zájmům, i když nikoho explicitně nejmenuje."[121]

To, že národně-bezpečnostní ohledy budou hrát roli při budování sítí páté generace v ČR dokazují i připomínky českého ministerstva vnitra k podmínkám aukce kmitočtů, které budou tyto sítě využívat. Konkrétně se jedná o část pásma, která bude zajišťovat komunikaci bezpečnostních a záchranářských složek (Broadband Public Protection & Disaster Relief - BB-PPDR). Ministerstvo požaduje, aby z této části sítě byly vyloučeny technologie firem, proti kterým NÚKIB vydal, či vydá varování.[122] Obecně se návrh podmínek dražby bezpečnostními aspekty konkrétně příliš nezabývá, ČTÚ pouze zmiňuje, že očekává,

100 "GCHQ Director says ‚Shoddy' Huawei security engineering belongs in the year 2000". Forbes, https://www.forbes.com/sites/daveywinder/2019/04/08/gchq-director-says-shoddy-huawei-security-engineering-belongs-in-the-year-2000/

101 "Huawei cyber security evaluation centre oversight board: Annual report 2019". GOV.UK, https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019

102 "UK intelligence panel warns on Huawei security flaws". Financial Times, https://www.ft.com/content/8d701096-50ac-11e9-b401-8d9ef1626294

103 "ZTE: NCSC advice to select telecommunications operators with national security concerns", NSCC. https://www.ncsc.gov.uk/news/zte-ncsc-advice-select-telecommunications-operators-national-security-concerns-0.

104 "UK Huawei decision appears to avert row with US". The Guardian, https://www.theguardian.com/technology/2020/jan/28/boris-johnson-gives-green-light-for-huawei-5g-infrastructure-role

105 "Chinese diplomat accuses Tory MPs of Huawei 'witch hunt'". Financial Times, https://www.ft.com/content/8858c230-4b3b-11ea-95a0-43d18ec715f5

106 UK spy agencies urge China rethink once Covid-19 crisis is over". The Guardian, https://www.theguardian.com/world/2020/apr/12/uk-spy-agencies-urge-china-rethink-once-covid-19-crisis-is-over.

107 "UK draws up 3-year plan to remove Huawei from 5G networks. Financial Times, https://www.ft.com/content/1c226144-a3a9-4533-ab14-88d65142ba05

108 "Konkrétní důsledky kauzy Huawei. Projděte si, které projekty kvůli hrozbě skončily". Aktuálně.cz, https://zpravy.aktualne.cz/domaci/konkretni-dusledky-kauzy-huawei-projdete-si-ktere-projekty k/r~5042cc76337a11e9b869ac1f6b220ee8/v~sl:224d7517ebe1d0a36cdb641f82e60d94/.

109 "Pražské letiště vyřadilo Huawei z dalších zakázek za sedm milionů". Deník N, https://denikn.cz/208602/ruzynske-letiste-vyradilo-huawei-z-dalsich-zakazek-za-sedm-milionu/.

110 "Konkrétní důsledky kauzy Huawei. Projděte si, které projekty kvůli hrozbě skončily | Aktuálně.cz, https://zpravy.aktualne.cz/domaci/konkretni-dusledky-kauzy-huawei-projdete-si-ktere-projekty-k/r~5042cc76337a11e9b869ac1f6b220ee8/v~sl:c8627b43b3bd09e7191910c2dc84cf9e/.

111 "Huawei dodá datová úložiště pro vnitro a NAKIT, firma nabídla nejnižší cenu". Lupa.cz, https://www.lupa.cz/aktuality/huawei-doda-datova-uloziste-pro-ministerstvo-vnitra-a-nakit-nabidlo-nejnizsi-cenu/?utm_source=rss & utm_medium=text & utm_campaign=rss.

112 " Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures". European Commission, https://ec.europa.eu/newsroom/dae/document.cfm?-doc_id=64468

113 "Metodika k varování ze dne 17. prosince 2018". Národní úřad pro kybernetickou a informační bezpečnost, https://www.govcert.cz/download/kii-vis/2019_01_04_metodika_k_varov%C3%A1n%C3%AD_z_17-12-2018_v1. 0. pdf

114 "Huawei v Česku hledá šéfa kyberbezpečnosti. Má mluvit se státem a řešit krize". Lupa.cz, https://www.lupa.cz/clanky/huawei-v-cesku-hleda-sefa-kyberbezpecnosti-ma-mluvit-se-statem-a-resit-krize/

115 "Stanovisko k implementaci 5G Toolbox", AK Toman, Devátý a partneři, https://www.5gvcesku.cz/DATA/dokumenty/A_Toman_Pravni_stanovisko_Implementace_EU_Toolbox.pdf

116 "Huawei Technologies (Czech) s.r.o." Advokátní kancelář Toman, Devátý & partneři, https://iustitia.cz/blog/kauzy/kauzy-it-a-media/huawei-technologies.html

117 "Stanovisko k implementaci 5G Toolbox", AK Toman, Devátý a partneři, https://www.5gvcesku.cz/DATA/dokumenty/A_Toman_Pravni_stanovisko_Implementace_EU_Toolbox.pdf

118 "Ze špionáže podezřelý Huawei vede kampaň za 5G. Využil nezávisle se tvářící institute." Aktuálně.cz, 14. duben https://zpravy.aktualne.cz/domaci/site-5g-se-bez-huawei-prodrazi-o-38-miliard-tvrdi-studie-cis/r~6e44780078bb11ea9d74ac1f6b220ee8/

119 "Význam budování 5G sítí v ČR". CETA, https://www.5gvcesku.cz/DATA/dokumenty/CETA_Studie_5G_key.pdf

120 "Vybudování infrastruktury na vysokorychlostní internet bude stát 120 až 150 miliard korun". Hospodářská komora ČR, https://www.komora.cz/press_release/vybudovani-infrastruktury-vysokorychlostni-internet-bude-stat-120-az-150-miliard-korun/

121 "Jsme šokováni, volali Číňané do Černínského paláce. Babišova dohoda s USA je prý proti jejich zájmům". Deník N, https://denikn.cz/365793/jsme-sokovani-volali-cinane-do-cerninskeho-palace-babisova-dohoda-s-usa-je-pry-proti-jejich-zajmum/.

122 "Připomínky k návrhu textu Vyhlášení výběrového řízení za účelem udělení práv k využívání rádiových kmitočtů pro zajištění sítí elektronických komunikací v kmitočtových pásmech 700 MHz a 3440–3600 MHz". Český telekomunikační úřad, https://www.ctu.cz/sites/default/files/obsah/ctu/vyzva-k-uplatneni-pripominek-k-navrhu-textu-vyhlaseni-vyberoveho-rizeni-za-ucelem-udeleni-prav-k/obrazky/20200504pripominkymvcr.pdf

že vliv na konečnou podobu sítě budou mít i doporučení vyplývající z EU 5G Toolbox.[123]

Technologie čínských firem v ČR

Na rozdíl od technologií firem Huawei a ZTE české instituce možná bezpečnostní rizika spojená s používáním dalších výrobků čínských technologických firem, které spojenecké státy označily za rizikové, zatím oficiálně neřešily. Ve zprávách v českých médiích byly však několikrát zmíněny kvůli svému podílu na budování internačních táborů pro Ujgury v provincii Sin-ťiang. Stejně jako v jiných státech jsou výrobky firem DJI, Dahua a Hytera velice populární a rozšířené ve státní sféře, včetně z hlediska bezpečnosti důležitých rezortů jako je ministerstvo vnitra a ministerstvo obrany.

Drony DJI nakoupilo v roce 2018[124] a znovu pak v roce 2019 pro své Středisko psychologických a informačních operací[125] ministerstvo obrany, dále pak Policejní prezidium[126] a generální ředitelství Hasičského záchranného sboru[127].

České bezpečnostní složky používají i komunikační techniku společnosti Hytera, jejichž radiostanice používá Hasičský záchranný sbor[128]. 50 radiostanic této značky určených pro skryté nošení si pořídilo i Policejní prezidium ČR.[129] Stejná instituce nakoupila i kamery a záznamová zařízení firmy Hikvision pro vozidla využívaná ochrannou službou a pro speciální intervenční vozidlo. Tyto kamery využívá dále i Správa hmotných rezerv[130]

Vojenská policie nakoupila v roce 2017 kamery firmy Hikvision za 2,75 mil. korun.[131] Kamery stejné firmy za 6 milionů korun pořídila i Vězeňská služba ČR, jejíž mluvčí uvedla, že kamery používají v uzavřeném okruhu (tedy bez přístupu na internet), obdobně se vyjádřil i mluvčí vojenské policie.[132] Tato instituce využívá i záznamová zařízení značky Dahua.[133] Zajímavou zmínku o firmě Hikvision obsahuje smlouva o dodávce kamerového systému pro Český rozhlas: „kamery a zařízení čínského výrobce Hikvision (Wonderex) nejsou standardně v systému Genetec Security Center (i.e. dodávaného bezpečnostního systému, pozn. aut.) podporovány, neboť představují bezpečnostní riziko pro celý systém a proto je nelze akceptovat."[134] Termokamera společnosti Dahua byla také využita pro snímaní teploty českých zákonodárců během koronavirové pandemie, když ji do Sněmovny zapůjčil senátor Ivo Valenta.[135]

V kontextu varování NÚKIB stran společnosti Huawei jsou zajímavé smlouvy uzavřené po jeho vydání. Jedná se např. o dodávky páteřního routeru[136] včetně firewallu[137], směrovače pro havarijní linku[138] a dodávku perimetrických prvků[139] pro Českou televizi. Stejně zajímavou je smlouva o poskytnutí pozáruční podpory pro dodávku pevných disků stejné firmy pro Správu železniční dopravní cesty do roku 2021 za téměř 10 mil. korun. [140]

Čínské firmy nejsou jen významným dodavatelem ICT technologií, ale zajímají se i o dostavbu nového jaderného bloku v JE Dukovany. Čínská státní společnost CGN nabízí[141] postavit v Dukovanech vlastní

[123] "Vyhlášení výběrového řízení za účelem udělení práv k využívání rádiových kmitočtů pro zajištění sítí elektronických komunikací v kmitočtových pásmech 700 MHz a 3440–3600 MHz". Český telekomunikační úřad, https://www.ctu.cz/sites/default/files/obsah/ctu/vyzva-k-uplatneni-pripominek-k--navrhu-textu-vyhlaseni-vyberoveho-rizeni-za-ucelem-udeleni-prav-k/obrazky/20200316-vyhlaseniczvk.pdf

[124] "Česká republika - Ministerstvo obrany". Registr smluv, https://smlouvy.gov.cz/smlouva/6105735

[125] "Česká republika - Ministerstvo obrany". Registr smluv, https://smlouvy.gov.cz/smlouva/10855672

[126] "Policejní prezidium České republiky". Registr smluv, https://smlouvy.gov.cz/smlouva/4717620

[127] "MV - generální ředitelství HZS ČR". Registr smluv, https://smlouvy.gov.cz/smlouva/10772072

[128] "MV - generální ředitelství HZS ČR". Registr smluv, https://smlouvy.gov.cz/smlouva/11645540

[129] "Policejní prezidium České republiky". Registr smluv, https://smlouvy.gov.cz/smlouva/10622932

[130] "Správa státních hmotných rezerv". Registr smluv, https://smlouvy.gov.cz/smlouva/12063388

[131] "Čínské kamery v Americe zakázali. V Česku dál hlídají vězně, slouží policii i armádě". Deník N, https://denikn.cz/64942/cinske-kamery-v-americe-zakazali-v-cesku-dal-hlidaji-vezne-slouzi-policii-i-armade/

[132] Ibid.

[133] "Vězeňská služba České republiky" Registr smluv, https://smlouvy.gov.cz/smlouva/5216408

[134] "Český rozhlas", Registr smluv. https://smlouvy.gov.cz/smlouva/9711999

[135] "Poslancům měří teplotu kamera od čínské firmy, která sleduje utlačované Ujgury. Zdarma ji zapůjčil Valenta". Deník N, https://denikn.cz/351852/poslancum-meri-teplotu-kamera-od-cinske-firmy-ktera-sleduje-utlacovane-ujgury-zdarma-ji-zapujcil-valenta/

[136] "Česká televize". Registr smluv, https://smlouvy.gov.cz/smlouva/8102039

[137] "Česká televize". Registr smluv, https://smlouvy.gov.cz/smlouva/11147528

[138] "Česká televize". Registr smluv. https://smlouvy.gov.cz/smlouva/11033704

[139] "Česká televize". Registr smluv. https://smlouvy.gov.cz/smlouva/12092008

[140] "Správa železniční dopravní cesty, státní organizace". Registr smluv, https://smlouvy.gov.cz/smlouva/10824456

[141] Česká jaderná horečka. Plánovaná stavba bloku v Dukovanech vyvolává u odborníků skepsi". Euro.cz, https://www.euro.cz/byznys/ceska-jaderna-horecka-1475148

model reaktoru Hualong One (HPR1000), který mimo vlastní Čínu staví v pákistánském Karáčí a o jehož využití usiluje také v plánované britské jaderné elektrárně Bradwell B. Jak je však uvedeno výše, čínská expanze v britském jaderném sektoru byla kvůli obavám o dopad na národní bezpečnost zpochybněna kabinetem Theresy May a CGN byla navíc Spojenými státy obviněna z krádeže duševního vlastnictví a tajné podpory vojenského jaderného výzkumu.[142]

Bezpečnostních rizik spojených s možnou účastí této firmy (a také ruského Rosatomu) si byli vědomi členové meziresortní vládní skupiny, kteří nepřímo doporučili, aby nový jaderný blok výše zmíněné firmy nestavěly. Jejich závěr je podložen vyhodnocením pěti kritérií, mezi nimiž se objevilo i hodnocení netechnických rizik. Konkrétně šlo o způsob, jakým státy, ze kterých možný dodavatel pochází, referují ve svých strategických dokumentech o spojeneckých organizacích (např. NATO), kterých je ČR součástí.[143] Bezpečnostní pravidla založená na tomto dokumentu pak schválila vláda v květnu 2020 jako součást veřejné soutěže na výstavbu nového bloku.[144]Případným rizikem by bylo i financování stavby z čínské strany (jako v případě Hinkley Point). Stavba jaderných zdrojů je finančně nákladná dlouhodobá investice, která se velmi zřídka podaří uskutečnit v původně plánovaném termínu a rozpočtu a v tomto ohledu je nutné připomenout obecné využívání čínských půjček k prosazování politických cílů (tzv. debt trap diplomacy).[145]

NETECHNICKÁ RIZIKA A SOUKROMÝ SEKTOR

Současná česká debata o netechnických rizicích a aplikaci jejich analýzy ke zvýšení bezpečnosti se týká především kritické kybernetické infrastruktury, tedy systémů, jejichž narušení by významně poškodilo fungování státu a ekonomiky. Mnoho důležitých systémů ve státní i soukromé sféře však do KII nespadá a je pouze na vlastním uvážení manažerů a jejich IT odborníků, zda vezmou při nákupu ICT zařízení a technologií v potaz varování státních institucí, či se rozhodnou pro pořízení daného vybavení pouze na základě ceny.

Používání rizikových technologií však může mít významné dopady i z čistě podnikatelského hlediska. (1) Produkty čínských společností často obsahují více bezpečnostních chyb než produkty jejich konkurentů.[146]A je vlastně jedno, jestli těchto chyb využije čínská zpravodajská služba, nebo „obyčejný" kyberútočník. (2) Využívání těchto produktů může mít časem dopad i na cenu pojištění kybernetických rizik, jehož využívání neustále roste. Podle nedávno zveřejněného průzkumu Českého statistického úřadu je proti kyberútokům pojištěno 17% velkých firem, z hlediska sektorů pak 32% ICT firem a 19% telekomunikačních firem.[147] Jedno z obecných pravidel pojištění je to, že čím rizikověji se pojistník chová, tím vyšší pojištění platí, a v některých případech pak nemusí být plnění vyplaceno vůbec. (3) Citlivá je dostupnost služeb, ať už technické podpory nebo softwarových updatů. Čína velice často používá embarga či bojkoty jako součást své zahraniční politiky k potrestání jiného státu, který se dotkl jejích zájmů.[148] Tato forma nátlaku může dopadnout i na soukromé firmy. Samozřejmě, že se proti rizikům spojeným s takzvaným „vendor lock-in" dá bránit pořízením záložních řešení od nečínských firem, ale toto řešení je zbytečně finančně nákladné. (4) Dalším rizikem je možné poškození reputace: pokud firma, na rozdíl od svých konkurentů, používá rizikové technologie, může to pro ni znamenat podstatnou konkurenční nevýhodu, která např. může způsobit i to, že firma nedostane nějakou zakázku, pokud zadavatel požaduje bezpečnostní záruky v dodavatelském řetězci. Dalším faktorem reputačního hlediska mohou být úzké vazby některých čínských

[142] "US warns Britain against Chinese alliances on nuclear plants". Financial Times, https://www.ft.com/content/84ab26f6-d7a5-11e8-a854-33d6f82e-62f8#myft:saved-articles:page

[143] "Dva z kola ven". Týdeník Respekt, https://www.respekt.cz/tydenik/2018/48/dva-z-kola-ven

[144] "Vláda schválila tajný dokument, který může z dostavby Dukovan vyřadit Rusko a Čínu". Deník N, https://denikn.cz/361816/vlada-schvalila-tajny-dokument-ktery-muze-z-dostavby-dukovan-vyradit-rusko-a-cinu/

[145] "Poor countries borrowed billions from China. They can't pay it back." The New York Times, https://www.nytimes.com/2020/05/18/business/china-loans--coronavirus-belt-road.html.

[146] "Huawei telecom gear much more vulnerable to hackers than rivals' equipment, report says". Wall Street Journal, https://www.wsj.com/articles/huawei--telecom-gear-much-more-vulnerable-to-hackers-than-rivals-equipment-report-says-11561501573

[147] "Kyberzločinnost roste. Každá pátá firma v ohrožení". oPojištění, https://www.opojisteni.cz/technologie/kyberneticka-rizika/kyberzlocinnost-roste--kazda-pata-firma-v-ohrozeni/c:17941/

[148] "A geopolitical row with China damages South Korean business further". The Economist, https://www.economist.com/business/2017/10/19/a-geopolitical-row-with-china-damages-south-korean-business-further

firem na represivní aparát čínského státu, který se lehce může stát zásadním bodem současné debaty o celospolečenské odpovědnosti firem. (5) Zásadní je též je ochrana vlastního know-how/duševního vlastnictví firem. Očekávané využití internetu věcí zvýší počet aktivních prvků a periférií, které budou firmy využívat ve svém fungování, ale dojde tím i ke zvýšení počtu zranitelných bodů, kterými se může útočník dostat k cenným firemním datům a technologiím.

DOPORUČENÍ

Zvýšit povědomí o komplexních rizicích spojených se stále větším využíváním moderních technologií a především o jejich netechnických aspektech je dlouhodobá práce a role státu je v ní omezená. I když se stát může pokusit donutit soukromé firmy ke komplexnějšímu uvažování o kybernetické bezpečnosti, jako např. v případě návrhu amerického zákona, který by u veřejně obchodovaných společností vyžadoval v rámci povinně poskytovaných informací uvádět, zda je v jejich nejvyšším vedení expert na kybernetickou bezpečnost[149], měl by se především soustředit na osvětovou činnost. O tom, že nemáme sdílet svá hesla či otevírat podezřelé emaily ví každý, i když se mnoho lidí touto radou neřídí. Je zapotřebí aby se povědomí o možných rizicích spojených s používám čínských technologií rozšířilo mezi co největší a nejrůznorodější skupinu uživatelů. Označení jistého dodavatele za riziko by mělo být doplněno různými scénáři bezpečnostních, finančních a reputačních dopadů, které jsou snadno pochopitelné i pro netechnicky vzdělané uživatele.

V případě upozornění na netechnická rizika by bylo dobré podpořit stanovisko NÚKIB relevantními institucemi jako jsou zpravodajské služby, které stejně na tato rizika dlouhodobě upozorňují i ve veřejných verzích ročních zpráv a NÚKIB sám na nich svou analýzu rizik částečně zakládá. Společné stanovisko zástupců bezpečnostní komunity by oslovilo širší skupinu uživatelů ICT technologií, kteří nemusí nutně sledovat prohlášení NÚKIB, když se jich bezprostředně netýká. Důležitým krokem by bylo také navázání komunikace mezi státními úřady a pojišťovnami/zajišťovnami, které by pak mohly posuzovat bezpečnost systému svých pojistníků informovaněji a komplexněji.

Současná definice kritické informační infrastruktury zatím dostačuje současné struktuře ekonomiky. Na druhou stranu je však nutné sledovat obecný vývoj nových technologických sektorů především v souvislosti s rozvojem sítí páté generace a na ni napojených periferních zařízení, neboť některé z nich se mohou stát pro českou ekonomiku a společnost natolik významná, že rizika spjatá s jejich napadnutím mohou být pro náš stát zásadní. Pokud se má ČR stát zemí budoucnosti, která bude založená na využití moderních technologií, musí také dbát o jejich bezpečnost, i když to může vyžadovat vyšší náklady a mnoho dlouhodobé práce. Budoucnost není zadarmo.

[149] "Companies must start taking cyber risk seriously". Financial Times, https://www.ft.com/content/2f886ce8-b9f3-11e9-8a88-aa6628ac896c

Prague Security Studies Institute
Pohořelec 6, 118 00 Prague 1
Czech Republic
Tel./fax: +420 233 355 735
pssi@pssi.cz
www.pssi.cz