Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

SHRNUTÍ ZÁVĚREČNÉ ZPRÁVY RIA

1. Základní identifikační údaje	
Návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)	
Zpracovatel / zástupce předkladatele: Národní úřad pro kybernetickou a informační bezpečnost	Předpokládaný termín nabytí účinnosti Červenec 2024
Implementace práva EU: Ne	

2. Cíl návrhu zákona

Primárním cílem navrhovaného zákona je přispět k zajištění dlouhodobě udržitelné bezpečnosti ČR prostřednictvím zabezpečení a zvýšení odolnosti osob a institucí, jež jsou nezbytné pro naplňování základních funkcí státu. Tohoto cíle bude dosaženo prostřednictvím omezení závislosti vybraných povinných osob (dále také „povinné osoby mechanismu“) podle zákona o kybernetické bezpečnosti (dále jen „ZKB“) České republiky (dále jen „ČR“) na dodavatelích představujících strategickou hrozbu v oblasti informačních a komunikačních technologiích strategicky významné infrastruktury.

Vybrané povinné osoby, od kterých se odvíjí obsah pojmu „strategicky významná infrastruktura“, [1] byly identifikovány na základě významnosti jimi poskytované služby pro chod státu ve vybraných regulovaných odvětvích a jejich přesné vymezení je představeno v kapitole 1.4 Identifikace dotčených subjektů.

Návrh připravovaného zákona zmocní Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) k identifikaci a vyhodnocení hrozeb plynoucích z dodavatelských řetězců pro národní bezpečnost nebo veřejný pořádek. Zda jsou tyto hodnoty v ohrožení, bude vyhodnoceno na základě konkrétních kritérií stanovených právním předpisem, a to skrze vyhodnocení těchto kritérií. Mechanismus prověřování bezpečnostní spolehlivosti dodavatelů a omezování rizik spojených s dodavateli v ČR (dále jen „Mechanismus posuzování dodavatelů“) umožní NÚKIB na základě zákonného zmocnění omezit, či vyloučit z vymezených dodávek povinných osob mechanismu takové dodavatele, kteří budou vyhodnoceni jako rizikoví, v důsledku čehož dojde ke snížení dopadu negativních zahraničních vlivů na zajištění základních funkcí státu prostřednictvím dodávek technologií. Ostatní státní orgány budou NÚKIB poskytovat součinnost a informace z jejich zákonné působnosti.

Připravovaný návrh zákona doplňuje stávající systém zajišťování kybernetické bezpečnosti, založený na aktivitě a odpovědnosti správce infrastruktury. Návrh zákona má státu umožnit

[1] V minulosti byly tyto vybrané povinné osoby v materiálech předkládaných Bezpečnostní radě státu a dalších nelegislativních materiálech označovány také uvedeným pojmem „strategicky významná infrastruktura“, přičemž tak byla před předložením tohoto návrhu zákona označována infrastruktura odpovídající kritické informační infrastruktuře ve smyslu § 2 písm. b) ZKB a informačním systémům základní služby ve smyslu § 2 písm. j) ZKB.

zjišťovat strategická rizika spojená s dodavateli a omezovat vliv rizikových dodavatelů na nejkritičtějších části nejvýznamnější infrastruktury. Měl by tak vzniknout účinný systém omezování nejvýznamnějších strategických rizik spojených s dodavatelskými řetězci, který přenáší související komplikovaný bezpečnostní proces na stát, a přitom nemění osvědčené principy současné regulace kybernetické bezpečnosti.

3. Agregované dopady návrhu zákona

3.1 Dopady na státní rozpočet a ostatní veřejné rozpočty: Ano

Na poměry nových oblastí působnosti ústředního orgánu státní správy se očekává nízký dopad na státní rozpočet. Ve vztahu k návrhu zákona lze předpokládat především nutnost vyhrazení jednotek až nízkých desítek tabulkových míst u zapojených státních orgánů a rozšíření stávajících či připravovaných informačních systémů k technické obsluze procesu prověřování. V souladu s principem efektivity a cílem minimalizace ekonomických nákladů se bude maximálně využívat fungující synergie s již existujícími agendami a procesy, jakými jsou kupříkladu prověřování žadatelů o zápis do katalogu poskytovatelů služeb cloud computingu orgánům veřejné správy či prověřování zahraničních investorů dle zákona o prověřování zahraničních investic, a to včetně účelného využívání informačních systémů, které tyto agendy podporují.

Dopady na státní rozpočet pak mohou vznikat také prostřednictvím zvýšených nákladů povinných osob mechanismu z řad veřejné správy.

3.2 Dopady na mezinárodní konkurenceschopnost ČR: Ano

Návrh zákona přispěje k posílení konkurenceschopnosti ČR, a to zejména posílením její reputace v rámci mezinárodního společenství. Přijetím a implementací Mechanismu posuzování dodavatelů značně vylepší svoji mezinárodní pozici z hlediska zabezpečení investičního prostředí prostřednictvím zvýšení úrovně bezpečnosti strategicky významné infrastruktury, čímž zvýší svoji atraktivitu pro investory. Mechanismus posuzování dodavatelů mimo jiné umožní dosažení vyšší bezpečnosti dat, která, navzdory svému ekonomickému a strategickému významu, mnohdy nebývají pod plnou kontrolou subjektů, jimž patří. Namísto toho z povahy fungování kyberprostoru bývají data spravována či ukládána na infrastruktuře ovládané třetí stranou. Například pro společnosti vytvářející a vlastnící práva související s duševním vlastnictvím či know-how bude tedy přijetí navrhované úpravy znamenat lepší ochranu proti exfiltraci nebo kompromitaci těchto cenných aktiv. Je žádoucí zajistit, aby třetí strana nepředstavovala pro určitý subjekt, a tím pádem i pro stát, bezpečnostní riziko.

Zavedením takového mechanismu ČR rovněž splní některá z klíčových opatření zabezpečení 5G sítí dle Souboru opatření Evropské unie pro kybernetickou bezpečnost sítí 5G a prokáže tak vůli navyšovat kromě bezpečnosti investic také bezpečnost své strategicky významné infrastruktury obecně; tímto krokem navíc půjde ČR v Evropě příkladem vzhledem k aplikaci doporučeného opatření i na jiné sektory strategicky významné infrastruktury, než je sektor elektronických komunikací. Naopak nelze vyloučit určitý negativní dopad na konkurenční postavení podnikatelských subjektů v ČR v podobě redukce nabídky některých dodávek v důsledku omezení rizikových dodavatelů (tedy zejména dodavatelů pocházejících ze zemí mimo vnitřní trh EU), a tedy i omezený negativní dopad na mezinárodní konkurenceschopnost.

Možné omezení okruhu subjektů na trhu může vést k nárůstu cen dodávaných technologií, a tedy i ke zvýšeným nákladům na straně regulovaných subjektů. Vzhledem k možnému snížení počtu dodavatelů technologií může dojít k dočasnému poklesu vzájemného konkurenčního tlaku, a tím

pádem i ke snížení motivace k vytváření inovací.[2] Bude však zvýšena celková úroveň bezpečnosti služeb a produktů, čímž dojde ke snížení investičních rizik spojených s dodavatelským řetězcem pro potenciální investory, obzvláště ze zemí, které bezpečnost dodavatelského řetězce již právně regulují. Stejně tak povede zavedení Mechanismu posuzování dodavatelů k větší důvěře spotřebitelů a koncových uživatelů v procesy, produkty a služby subjektů, které jsou s kritickou infrastrukturou spojené. V konečném důsledku by tedy byla mezinárodní konkurenceschopnost ČR ve srovnání se zeměmi bez adekvátní právní úpravy posílena.

Ekonomika ČR závisí na vývozu dodávek zboží do okolních zemí, a to zejména do Německa (kam směřuje přes 30 % vývozu) Slovenska, Polska a Rakouska (podíl na celkovém exportu přes 50 %).[3] Všechny zmíněné státy již do různé míry dodavatelský řetězec kritické infrastruktury nebo jejích sektorů regulují nebo regulaci připravují.[4]

Absence regulace bezpečnosti dodavatelského řetězce by tak v budoucnu mohla vést ke zhoršení pozice podnikatelských subjektů působících v ČR, neboť by nemohly nabídnout stejnou míru bezpečnosti svého produktu či služby jako subjekty působící ve státech, které obdobnou regulaci přijaly. Nepřijetí předmětné právní úpravy by tedy mohlo vyvolat nucené odmítání dodávek českých společností zahraničními odběrateli kvůli bezpečnostním a strategickým hrozbám plynoucím z dodávek subdodavatelů. České společnosti by se tím de facto staly nespolehlivými dodavateli pro zahraniční obchodní partnery, kteří by byli v takovém případě nuceni svým národním legislativním systémem upřednostnit dodavatele ze zemí, které rizika dodavatelského řetězce legislativně ošetřují.

Obecně lze na mezinárodní úrovni spatřovat rostoucí tendence zavádět mechanismy bezpečnosti dodavatelského řetězce. Na úrovni EU se jedná například o závěry Rady EU ohledně bezpečnosti dodavatelského řetězce v oblasti ICT ze dne 17. 10. 2022[5]. Dalším příkladem může být sektorově zaměřený dokument „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures“[6] skupiny pro spolupráci podle Směrnice (EU) 2016/1148, která klade důraz na přijetí opatření zajišťujících bezpečnost dodavatelského řetězce v 5G sítích. Trend lze pozorovat i v legislativě evropských států, které postupně zavádějí nebo již zavedly právní nástroje k zajištění bezpečnosti dodavatelského řetězce alespoň v některých kritických odvětvích. Kromě výše zmíněných sousedních zemí se také jedná např. o Francii, Dánsko či Spojené království.

Z hlediska mezinárodní konkurenceschopnosti je vysoká úroveň kybernetické bezpečnosti a odolnosti, ať už obecně nebo ve vztahu k dodavatelskému řetězci, bezesporu přínosem. Příkladem toho je jeden ze závěrů, který zazněl na akci 12th Annual National Conference on Cyber Security, ze kterého vyplývá, že se jedná o významný faktor při rozhodování investorů.[7] Investoři se zajímají o to, jakým způsobem společnosti ke kybernetickým rizikům

[2] Podobné obavy měli např. v Dánsku (viz FOLKETINGET. L 190 Forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur. Dostupné z: https://www.ft.dk/samling/20201/lovforslag/l190/20201_l190_som_fremsat.htm

[3] ČSÚ. Zahraniční obchod ČR se zbožím – roční údaje – 2021, tab. 2.3., 2022. Dostupné z: https://www.czso.cz/csu/czso/zahranicni-obchod-cr-se-zbozim-rocni-udaje-498eu1tklj

[4] DE – Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (2021), AT – Telekommunikationsgesetz (2021), SK – Zákon o kybernetickej bezpečnosti (2021), PL – chystaná novela: Ustawa krajowym systemie cyberbezpieczeństwa

[5] COUNCIL OF THE EUROPEAN UNION. Council conclusions on ICT supply chain security. Dostupné z: https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/en/pdf, str. 2, odst. 3

[6] NIS COOPERATION GROUP. Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. Dostupné z: https://ccdcoe.org/uploads/2020/01/EU-200129-Cybersecurity-of-5G-networks-EU-Toolbox-of-risk-mitigating-measures.pdf, str. 18

[7] FT. Strengthening cyber security can boost FDI, say experts. Dostupné z: https://www.ft.lk/front-page/Strengthening-cyber-security-can-boost-FDI-say-experts/44-687887

přistupují[8].Podle globálního investorského průzkumu společnosti PricewaterhouseCoopers (PwC)[9] se investoři kybernetických hrozeb obávají více než geopolitické nestability nebo nadměrné regulace.

3.3 Dopady na podnikatelské prostředí: Ano

Za pozitivní dopad na podnikatelské prostředí lze považovat také to, že díky omezení dodávek technologií rizikových dodavatelů pro výstavbu a provoz významné strategické infrastruktury zvýší Mechanismus posuzování dodavatelů pravděpodobnost řádného poskytování regulovaných služeb prostřednictvím strategicky významné infrastruktury napříč jednotlivými sektory, jako jsou například služby elektronických komunikací či služby výroby a distribuce elektřiny, které návazně využívají jak spotřebitelé, tak podnikatelé.

Za negativní dopady na podnikatelské prostředí lze považovat zvýšení nákladů pro povinné osoby mechanismu vyplývající z povinnosti hlásit dodavatele a reagovat na vydaná omezení, omezení nabídky a konkurenčního prostředí na relevantním trhu strategicky významné infrastruktury a reputační dopady na pověst dodavatelů, vůči nimž by případně bylo uplatňováno omezení.

Administrativní zátěž navrhovaného řešení by měla být pro podnikatelské subjekty minimální, jelikož všechny nově zaváděné procesy navazují na již existující administrativní povinnosti těchto subjektů, či jsou spojeny s jinými administrativními povinnostmi subjektů regulovaných v oblasti kybernetické bezpečnosti. Administrativní zátěž způsobená výhradně navrhovaným řešením by měla být za těchto předpokladů zanedbatelná, spočívající především v nově zavedené povinnosti nahlašovat NÚKIB dodavatele specificky vymezených aktiv.

3.4 Dopady na územní samosprávné celky (obce, kraje): Ne

3.5 Sociální dopady: Ne

3.6 Dopady na spotřebitele: Ano

Přijetím Mechanismu posuzování dodavatelů dojde k navýšení úrovně bezpečnosti strategicky významné infrastruktury, což bude mít pozitivní efekt na zajištění vysoké úrovně stability a bezpečnosti služeb poskytovaných spotřebitelům napříč sektory.

Navrhované řešení zároveň počítá s mechanismy minimalizujícími negativní dopady na spotřebitele prostřednictvím omezení využitelnosti dodávek bezpečnostně rizikových dodavatelů správcem infrastruktury tak, aby nedocházelo např. k omezení všech nabízených technologických produktů v daném sektoru či k tzv. proprietárnímu uzamčení (vendor lock-in) správce regulované infrastruktury závislého na jednom dodavateli. Navrhované řešení má za cíl rovněž přispět k budování zdravého tržního prostředí, které staví na spravedlivé hospodářské soutěži soutěžitelů, motivovaných soubojem o zákazníka, a nikoliv např. omezením funkčnosti infrastruktury k dosažení geopolitických cílů státu, jež má na dodavatele vliv.

3.7 Dopady na životní prostředí: Ne

[8] DELOITTE. Governance in focus. Cyber risk reporting in the UK. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/deloitte-uk-gif-cyber-risk-reporting-uk-march-2018.pdf, str. 1

[9] PWC. 2018 Global Investor Survey. Anxious optimism in a complex world. Dostupné z: https://www.pwc.com/gx/en/ceo-survey/2018/deep-dives/pwc-global-investor-survey-2018.pdf, str. 11

3.8 Dopady ve vztahu k zákazu diskriminace a ve vztahu k rovnosti žen a mužů: Ne
3.9 Dopady na výkon státní statistické služby: Ne
3.10 Korupční rizika: Ano
Návrh zákona může mít potenciálně zásadní dopady na poptávku po zboží a službách některých dodavatelů do strategicky významné infrastruktury ČR. Tato skutečnost může vyvolat korupční tlak na změnu způsobu prověřování kritérií nebo úpravu celkového hodnocení rizikovosti dodavatele. Obdobně mohou i někteří správci regulované infrastruktury usilovat o to, aby nebyl konkrétní poskytovatel v důsledku posouzení důvěryhodnosti omezen, jelikož by to pro ně znamenalo zvýšené náklady, či naopak mohou usilovat o omezení konkrétního dodavatele za účelem zhoršení postavení svého konkurenta, který takového dodavatele využívá ve své infrastruktuře.
3.11 Dopady na bezpečnost nebo obranu státu: Ano
Mechanismus posuzování dodavatelů bude mít pozitivní vliv na národní bezpečnost a obranu. Budování odolné strategicky významné infrastruktury bez rizikových dodavatelů přispěje k její odolnosti. A právě odolná strategicky významná infrastruktura je klíčovým předpokladem pro zajištění národní bezpečnosti a obrany. S tímto předpokladem pracuje jak aktuálně platná Bezpečnostní strategie ČR, tak i Národní strategie pro čelení hybridnímu působení a Národní strategie kybernetické bezpečnosti ČR (dále jen „NSKB“). Vazbu na odolnou a bezpečnou infrastrukturu jako integrální součást národní bezpečnosti rovněž zdůrazňují strategické dokumenty NATO. Zavedením mechanismu posuzování dodavatelů se navíc podstatně sníží riziko vzniku závislosti strategické infrastruktury na jednotlivých rizikových dodavatelích.

1 Důvod předložení a cíle

1.1 Název

Návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

1.2 Definice problému

Bezpečnost a odolnost organizačních složek státu a dalších orgánů a osob, jež poskytují služby důležité pro chod státu, jsou předpokladem pro zajištění bezpečnosti ČR. Hrozby, které pro ČR plynou z prostředí, v němž se tyto subjekty nachází, jsou definovány v Bezpečnostní strategii ČR z roku 2015[10]. Jedná se zejména o hrozby spočívající v:

a) kybernetických útocích,

b) ohrožení funkčnosti kritické infrastruktury, či

c) přerušení dodávek strategických surovin nebo energie.

Počet kybernetických útoků na infrastrukturu regulovanou ZKB v posledních letech výrazně narůstá, což dlouhodobě dokládají i Zprávy o stavu kybernetické bezpečnosti ČR (dále jen „ZSKB"), naposledy ZSKB za rok 2021.[11] V té se uvádí, že rok 2021 se vyznačoval nárůstem škodlivých kybernetických aktivit, ke kterým docházelo plošně na celém území ČR.

Meziročně také vzrostl počet kybernetických incidentů evidovaných NÚKIB. Například v roce 2021 zaznamenal NÚKIB celkem 157 kybernetických bezpečnostních incidentů oproti 99 incidentům v roce 2020. V tomto ohledu aktivity státem podporovaných aktérů v kybernetickém prostoru dlouhodobě patří mezi nejvážnější hrozby pro kybernetickou bezpečnost ČR.[12] Tito aktéři jsou zpravidla vysoce sofistikovaní a k dosažení svých cílů využívají širokou škálu taktik a technik, přičemž dochází k neustálému zdokonalování používaných nástrojů.

Podle Policie ČR (dále jen „PČR") došlo také k nárůstu kyberkriminálních aktivit. Dle PČR se i v průběhu roku 2021 potvrzuje dlouhodobý trend, a to postupný přesun trestné činnosti jako takové do kyberprostoru. V roce 2021 se počet skutků spadajících do kategorie kybernetické kriminality a ostatní kriminality páchané v kyberprostoru meziročně zvýšil o 17, 9 %.[13] Vyhodnocení NÚKIB k roku 2022 vykazuje opětovný nárůst a statistky nasvědčují tomu, že se situace ani v budoucnosti nebude měnit.

Útoky státních aktérů na systémy kritické pro chod státu se stávají běžnou realitou, ovlivňující život a fungování mnoha obyvatel a institucí. Bezpečnost těchto systémů je

[10] MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČESKÉ REPUBLIKY. Bezpečnostní strategie České republiky. 2015. Dostupná zde: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

[11] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Zpráva o stavu kybernetické bezpečnosti ČR za rok 2021. Dostupná zde: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

[12] detto

[13] POLICIE ČR. Vývoj registrované kriminality v roce 2021. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx#:~:text=V%20roce%202021%20bylo%20na,tedy%20vzrostla%20meziro%C4%8Dn%C4%9B%20o%201%20%25.

ohrožena nejen kybernetickými útoky, ale i prostřednictvím dodavatelů a dodavatelských řetězců, spadajících do sféry vlivu aktérů, jejichž zájmy a mezinárodní působení jsou v konfliktu se zájmy ČR. Dodavatelé se tak mohou stát prostředkem k prosazování politických cílů.

Jelikož ČR v rámci plnění svých základních funkcí povětšinou spoléhá na infrastrukturu vlastněnou, dodávanou či spravovanou třetími osobami, vzniká státu na těchto dodavatelích závislost (dále také „strategická závislost“). Pokud vznikne závislost na rizikovém dodavateli, plynou z toho pro stát významná rizika. Možné dopady takových rizik ukázal např. vývoj související s Ruskou invazí na Ukrajinu, která byla zahájena 24. února 2022. Válka na Ukrajině měla a má kromě nezměrných lidských, humanitárních, bezpečnostních a geopolitických dopadů také značné dopady na evropskou ekonomiku, a to především a nejcitelněji v energetice. Razantní zvýšení cen energií, zejména plynu,[14] bylo způsobeno právě onou rizikovou závislostí, jež si ČR na dovozu plynu z Ruska vytvořila.[15]

Obdobná situace strategické závislosti státu na dodavatelích může nastat, a v mnoha sektorech již nastává, v oblasti informačních a komunikačních technologií (dále jen „ICT“). V ICT je kromě již identifikovaných problémů strategické závislosti potřeba vyhodnocovat také rizika související s narušením důvěrnosti, integrity i dostupnosti dat a informací přenášených dodávanými technologiemi ze strany dodavatele.

Strategicky významná infrastruktura (viz část 1.4 Identifikace dotčených subjektů) je přitom na ICT značně závislá. S narůstající digitalizací a rozvojem této infrastruktury se rozšiřuje rozsah infrastruktury pro provádění potenciálních kybernetických útoků a tím se i značně zvyšuje riziko kybernetických útoků. Společně se zvyšující se mírou přenosu odpovědnosti za zajištění důvěrnosti, integrity a dostupnosti informací přenášených informačními systémy (dále jen „IS“) na dodavatele ICT a zvyšující se mírou složitosti jednotlivých prvků technologických systémů závislost strategicky významné infrastruktury na těchto dodavatelích dále narůstá.

Dodavatelé mají v ICT infrastruktuře výsadní postavení. Hardwarová a softwarová řešení informačních a komunikačních technologií jsou již natolik komplexní a v infrastrukturách povinných osobo mechanismu tak četně zastoupená, že je nelze technicky komplexně včas a efektivně prověřovat.

I s ohledem na časté aktualizace je technické testování ICT produktů ve velkém měřítku vysoce neefektivní. Problematika bezpečnostních záplat taktéž ztěžuje správcům infrastruktury technicky ověřit implementovaná softwarová řešení od svých dodavatelů, jelikož v případě odhalení (i zcela neúmyslných) slabin je potřeba co nejrychleji vydat softwarové aktualizace, než jich využijí útočníci (tzv. zranitelnosti nultého dne[16]). Takové aktualizace proto nemohou být podrobeny důkladné analýze, a nelze tak vyloučit riziko, že budou obsahovat například zadní vrátka, nebo jiný škodlivý kód. Klíčovým faktorem zabezpečení ICT je proto důvěra

[14] ČESKÁ NÁRODNÍ BANKA. Vývoj na evropském trhu se zemním plynem. Dostupné z: https://www.cnb.cz/cs/o_cnb/cnblog/Vyvoj-na-evropskem-trhu-se-zemnim-plynem/

[15] Eurostat uvádí 75–100% závislost ČR na ruském plynu pro první pololetí roku 2021. (Viz EUROSTAT. File:Share of Russia in national extra EU imports of each Member State, first semester 2021.png. Dostupné z: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Share_of_Russia_in_national_extra_EU_imports_of_each_Member_State,_first_semester_2021.png)

[16] Dle Zprávy o stavu kybernetické bezpečnosti za rok 2021 se jedná o typ zranitelnosti, který bývá často využíván např. státem podporovanými skupinami.

v dodavatele, že nezneužije své výsadní postavení ve prospěch svůj, státu, který má na dodavatele vliv, či jiného aktéra.

Dodavatele ze zemí mající např. nestandardní legislativní prostředí, umožňující ingerenci státních aktérů do produktů, služeb či procesů dodavatelů, jejichž zájmy jsou v konfliktu se zájmy ČR a jejích spojenců, lze považovat za rizikové. Ačkoliv výrobci či dodavatelé ICT produktů a služeb (dále jen „dodavatelé ICT“) mají s ohledem na generování zisku zájem o prodej kvalitních a bezpečných produktů, ne vždy se musí jednat o jejich jediný zájem.

Dodavatelé ICT mají sídla v různých zemích a podléhají rozličným právním řádům, mocenským strukturám a jiným neobchodním vlivům. Zvýšené riziko představují primárně dodavatelé ICT z autoritářských států, které mají silný vliv na své domácí společnosti a neváhají jej využít pro prosazování svých geopolitických cílů, jež mohou být v rozporu se zájmy ČR či jejích spojenců. Dodavatel ICT může být natolik propojený a ovlivněný státním a politickým aparátem své domovské země, že bude nezřídka činit i ekonomicky kontraproduktivní rozhodnutí v souladu se zájmy režimu, který mu potenciální reputační škodu může kompenzovat, případně jej za jednání v rozporu se svými zájmy potrestat. Navíc, vzhledem k obtížnému odhalení a ještě obtížnější atribuci (přičitatelnosti) kybernetických útoků,[17] mohou tyto aktivity představovat pro výrobce přijatelné riziko, které mu zajistí výhodné postavení v domovském státě a výrazněji neohrozí jeho zisk.

V řadě států mohou být společnosti také nuceny ke spolupráci se zpravodajskými službami státu prostřednictvím legislativy, jež na ně dopadá. V Čínské lidové republice (dále také „ČLR“) ukládá legislativa povinnost jednotlivcům i společnostem spolupracovat s čínskými státními autoritami. Jedná se např. o mechanismus, který je začleněný v zákoně o společnostech z roku 2013, jež ukládá všem společnostem povinnost ustanovit uvnitř svých struktur stranickou organizaci Komunistické strany ČLR (dále jen „KS ČLR“), pokud ve společnosti pracují nejméně tři členové Strany. V praxi to znamená přímý dosah této strany na dění v jakékoliv významné společnosti. KS ČLR vykonává skrze stranické organizace přímou kontrolu nad společnostmi a zajišťuje, že beze zbytku plní, co se od nich očekává, včetně požadavků v oblasti státní bezpečnosti[18]. Zákon o kybernetické bezpečnosti z roku 2017 pak obsahuje řadu ustanovení definujících povinnost spolupráce se státními orgány. Článek 28 určuje povinnost provozovatelů sítí poskytnout technickou podporu a spolupráci orgánům veřejné bezpečnosti a orgánům státní bezpečnosti.[19] Zákon o státní zpravodajské činnosti z téhož roku zdůrazňuje, že relevantní státní instituce jsou oprávněny vyžadovat spolupráci po jednotlivcích a organizacích: „*Národní zpravodajské služby mohou v souladu se souvisejícími státními předpisy požádat příslušné orgány, organizace a občany o poskytnutí potřebné podpory, součinnosti a spolupráce*.“[20]

[17] Atribuce dle vyjádření NÚKIB představuje proces, během něhož dochází k určení pravého zdroje útoku a samotného útočníka (Viz NÚKIB. Bezpečnější zdravotnictví i řešení rizikových dodavatelů - Vláda schválila Akční plán ke strategii kybernetické bezpečnosti. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1735-bezpecnejsi-zdravotnictvi-i-reseni-rizikovych-dodavatelu-vlada-schvalila-akcni-plan-ke-strategii-kyberneticke-bezpecnosti/)

[18] Law Bridge. 28.12.2013. Dostupné z: http://www.lawbridge.org/zhong-hua-ren-min-gong-he-guo-gong-si-fa-2013-nian-xiu-ding/

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

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

Taktéž Ruská federace (dále jen „RF“) přijala během poslední dekády několik zákonů s významným dopadem v oblasti kybernetické a informační bezpečnosti, které zásadním způsobem zasahují do fungování soukromých společností.[21] Zákon o Federální službě bezpečnosti (FSB) RF (40-FZ) poskytuje státu právní nástroje donucení ke spolupráci formálně soukromé entity, a to včetně globálně působících výrobců ICT.[22] Ustanovení § 15 tohoto zákona umožňuje FSB instalovat dodatečný software a hardware do ICT produktů ruských společností[23], stejně tak jako dosazovat důstojníky FSB do struktur soukromých firem.[24] Jedním z konkrétních případů osazeného softwaru je systém SORM (Systém pro operativní vyšetřovací činnost). Ten umožňuje FSB a dalším ruských bezpečnostním složkám monitoring síťového provozu zejména na ruském území. Slouží tak k získávání informací, sledování osob či digitální cenzuře a je primárně nasazen na síťovém provozu v rámci Ruské federace. V rámci ukrajinského konfliktu však Rusko přistoupilo k přesměrování síťového provozu na okupovaných územích právě skrze ruské poskytovatele a infrastrukturu, což ruským bezpečnostním složkám umožnilo systém SORM používat pro výše zmíněné účely i na území Ukrajiny. Okupační autority tak získaly informační kontrolu i nad tamním okupovaným obyvatelstvem.

Také Írán velmi pravděpodobně disponuje kapacitami narušit dodavatelský řetězec, nicméně limitují ho dva výrazné faktory. Těmi jsou technologická zaostalost ve srovnání s Ruskem nebo Čínou a omezení záběru útoků hlavně na Blízký východ (primárně Izrael a Saúdská Arábie) či USA. V případě technologické zaostalosti je třeba brát v potaz, že v islámské republice neleží významné výrobní kapacity hardwaru (Čína) ani softwaru (Čína i Rusko), což tak Teheránem zaštítěným aktérům ztěžuje možnost kompromitace. Přesto země disponuje ofenzivními schopnostmi a technicky vzdělanou populací, kterou ekonomické sankce a nemožnost uplatnit se na legálním trhu práce často nutí participovat na škodlivých aktivitách. Legislativní mechanismy srovnatelné s Ruskem a Čínou nejsou v Íránu veřejně známé, nicméně existují důkazy o tom, že mnoho domácích softwarových produktů je kompromitováno za účelem sledování opozice a potlačování disentu. Nelze tedy vyloučit, že Írán přijal vlastní restriktivní zákony v této oblasti.

Přestože i v ČR, stejně tak jako v dalších zemích Evropské unie a spojeneckých zemích ČR, existuje legislativa regulující vztah státu a soukromých společností pro potřeby zajišťování obrany státu a národní bezpečnosti[25], pravomoci státu jsou ve srovnání s těmi čínskými či ruskými nepoměrně nižší, případné zásahy musejí být řádně odůvodněné, podléhají soudnímu přezkumu a usilují o co nejmenší rozsah získávaných informací.

Dodavateli (či s jejich asistencí) způsobené úmyslné narušení kybernetické bezpečnosti strategicky významné infrastruktury, a to zejména nejzávažnější případy, jako je narušení dostupnosti systému ve velkém rozsahu, představuje podstatný problém pro významné ekonomické zájmy a bezpečnost státu, jelikož mohou výrazně narušit fungování státu, ekonomiky, společnosti a v krajním případě ohrozit zdraví a životy obyvatel.

[21] Human Rights Watch. 2020. Russia: Growing Internet Isolation, Control, Censorship. ttps://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship
[22] Peter B. Maggs. 2018. Report of Peter B. Maggs. Dostupné z: https://assets.documentcloud.org/documents/4386053/Report-of-Peter-B-Maggs-Russian-Surveillance-Law.pdf
[23] Федеральный закон от 03.04.1995 N 40-ФЗ (ред. от 02.12.2019) "О федеральной службе безопасности" (Federal Law on the Federal Security Service of the Russian Federation); Venice Commission. 2012. Federal Law on the Federal Security Service of the Russian Federation.
[24] FSB Dossier. 2020. Аппарат прикомандированных сотрудников. Dostupné z: https://fsb.dossier.center/prikom/
[25] V ČR se jedná zejména o Zákon č. 289/2005 Sb., o Vojenském zpravodajství.

Přestože jsou popsaná rizika spojená s dodavateli známá, v současnosti neexistuje v ČR komplexní mechanismus, který by umožnil rizika plynoucí z těchto strategických hrozeb pro strategicky významnou infrastrukturu cíleně, účinně a flexibilně vyhodnocovat a mitigovat.

Legislativní požadavky na národní i unijní úrovni v technické rovině zajišťování kybernetické bezpečnosti vedou ke zvyšování zabezpečení ICT na národní úrovni, a to především v infrastruktuře regulované zákonem o kybernetické bezpečnosti, mezi kterou je i strategicky významná infrastruktura. Útočníci tak musejí vynakládat stále vyšší úsilí směřující k narušení a nepozorovanému působení ve strategicky významných informačních systémech, což je zpravidla hlavní cíl škodlivého aktéra, jehož cílem je dlouhodobě narušovat důvěrnost, integritu či dostupnost informací přenášených těmito systémy. Takoví útočníci se musejí adaptovat na nové prostředí a vyhledávat nové vektory útoků. I to je jedním z důvodů zvyšující se atraktivity provádění útoků na dodavatelský řetězec, popř. využívání dodavatelů k prosazování cílů těchto škodlivých aktérů.

Stát by neměl rezignovat na svoji základní povinnost tím, že ji přenese na třetí, často soukromé, osoby. Stát proto nemůže ponechat výhradní výběr potenciálně rizikového dodavatele strategicky významné infrastruktury zcela v rukou soukromých firem, které nemusí být dostatečně vybaveny nebo motivovány k ochraně bezpečnosti ČR. Ačkoliv mají soukromé společnosti zájem o poskytování kvalitních a bezpečných produktů a služeb, jejich primárním cílem je dosažení zisku, přičemž tyto dva aspekty (bezpečnost versus výše zisku) mohou být v určitých případech v přímém rozporu a mohou upřednostnit vyšší zisk na úkor bezpečnosti. V souladu s čl. 1 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů, podle kterého je základní povinností státu: „*zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot“* musí stát ze své podstaty na takové riziko reagovat a usilovat o jeho mitigaci.

1.3 Popis existujícího právního stavu v dané oblasti

1.3.1 Legislativa v oblasti kybernetické bezpečnosti

V českém právním řádu je v současnosti oblast definovaného problému upravena především ZKB a jej provádějící vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

ZKB v tomto ohledu zejména ukládá v § 5 svým povinným osobám zavádět technická a organizační bezpečnostní opatření, tedy konkrétní kroky k seznámení se s aktivy svých systémů, řízení rizik s nimi spojenými, zavedení minimálních opatření k technickému zabezpečení a jiné. Ve vztahu k dodavatelskému řetězci ukládá stávající právní úprava v oblasti kybernetické bezpečnosti povinným osobám v regulované infrastruktuře toliko znát své významné dodavatele[26], informovat je o tomto jejich postavení, hodnotit rizika s významnými dodavateli spojená a smluvně své dodavatele zavazovat k přijetí některých kybernetických bezpečnostních politik.[27]

[26] Významným dodavatelem je dle § 2 písm. n) provozovatel systému dle ZKB a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti systému.
[27] § 8 VKB.

Dalším regulatorním nástrojem v oblasti definovaného problému je institut varování § 12 ZKB (dále jen „varování dle ZKB“) a další opatření dle § 11 ZKB. Varování dle ZKB slouží mimo jiné k upozornění veřejnosti na hrozbu v oblasti kybernetické bezpečnosti, o které se NÚKIB dozvěděl z vlastní činnosti nebo od jiných orgánů nebo osob. Nejen pro výkon této kompetence je NÚKIB umožněno provádět analýzu a monitoring kybernetických hrozeb a rizik.[28] Vydané varování dle ZKB pak mají povinné osoby dle ZKB v některých případech povinnost zohlednit v rámci řízení rizik spojených se svými systémy.

Právní řád tedy sice umožňuje zjišťovat a vyhodnocovat informace o hrozbách v oblasti kybernetické bezpečnosti, NÚKIB ani ostatním organizačním složkám státu, působícím v oblasti bezpečnosti, ale nedává možnost seznamovat se s informacemi o dodavatelích v regulované infrastruktuře nebo o dodavatelích, kteří se o zakázky do regulované infrastruktury uchází, způsobem, který by umožňoval odhalit a vyhodnotit hrozbu spojenou s dodavateli ještě před jejím vyhodnocením v riziko pro regulovanou infrastrukturu.

V případě, kdy se ale NÚKIB přesto podaří potřebné informace o současném či budoucím riziku spojenému s dodavatelským řetězcem získat a vyhodnotit, neumožňuje mu zákonná úprava na tato zjištění vhodně reagovat. Možnosti, které NÚKIB v takové situaci má, jsou pouze informovat o hrozbě formou varování dle ZKB nebo vydat reaktivní opatření dle § 13 ZKB – to však cílí už na určitý kybernetický bezpečnostní incident, a tedy na situaci bezprostředního narušení bezpečnosti regulované infrastruktury v konkrétní podobě. Minimalizovat zjištěnou strategickou hrozbu, spojenou s konkrétním dodavatelem prostřednictvím omezení jeho přítomnosti ve strategicky významné infrastruktuře, se organizačním složkám státu nenabízí.

Možnost omezovat přítomnost rizikových dodavatelů ve strategicky významné infrastruktuře je tak zcela ponechána na povinných osobách dle ZKB. S ohledem na rozdělení pravomocí a povinností mezi státem a soukromým sektorem, jakož i mezi jednotlivými organizačními složkami státu, ale tyto povinné osoby nejsou motivovány analyzovat a omezovat hrozby pro větší množinu systémů strategicky významné infrastruktury, než za jaké jsou odpovědné. I pokud takovou hrozbu ale některá povinná osoba ve svém řízení rizik dle VKB reflektovat chce, nemá zpravidla oprávnění, nástroje ani kapacitu shromažďovat a vyhodnocovat informace k tomu potřebné.

Tzv. strategické hrozby spojené s dodavateli, tedy například možnost nepřezkoumatelných zásahů cizích států do aktivit dodavatele či neformální působení na dodavatele směřující k poškození jiného státu (viz část **Chyba! Nenalezen zdroj odkazů. Chyba! Nenalezen zdroj odkazů.**), vyžadují pro svoji sofistikovanost a komplexitu seznámení se s velkým množstvím informací, často zpravodajského či jiného charakteru. K těmto informacím má z podstaty věci povětšinou přístup pouze stát, resp. jeho bezpečnostní aparát, a neoprávněná dispozice s takovými informacemi, byť subjektem jednajícím v dobré víře (jako například zmiňovaná povinná osoba, mající vůli strategickou hrozbu reflektovat), je právními předpisy přísně sankcionována.[29]

[28] § 22 písm. u) ZKB.

[29] Např. zajištění si přístupu k utajované informaci bez současného splnění zákonných předpokladů umožňuje zákon č 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, dle § 148 odst. 4 písm. d) a § 155a odst. 2 potrestat pokutou až do 1 000 000 Kč.

Správci regulované infrastruktury tak stojí před opačným problémem než NÚKIB – mají přehled o užívaných dodavatelích (tzn. informace, které NÚKIB schází), mají možnost omezit v infrastruktuře přítomnost vysoce rizikových dodavatelů, nemají ale možnost získat a vyhodnotit veškeré potřebné informace pro to, aby mohli hrozbu spojenou s dodavatelem účinně redukovat. Nezřídka se navíc stává, že identifikovaná hrozba, před níž NÚKIB vydal varování dle ZKB, není v analýze rizik povinných osob dle ZKB dostatečně, či dokonce jakkoliv, reflektována. Dle výstupů z kontrol a auditů povinných osob prováděných dle ZKB je úskalím tohoto přístupu nejčastěji samotná maturita povinných osob v oblasti řízení rizik, kdy povinná osoba nesplňuje samotnou procesní prerekvizitu vykonávání analýzy rizik. V případě, kdy je varování dle ZKB v analýze rizik náležitě zohledněno, často nejsou řízeny následné procesy a alokovány zdroje pro ošetření daného rizika doložitelné formou např. plánu zvládání rizik.

Pro řešení definovaného problému nepostačuje ani současné zmocnění NÚKIB k zajišťování metodické podpory v oblasti kybernetické bezpečnosti dle § 22 písm. j) ZKB. V rámci této pravomoci vydal ve snaze adresovat definovaný problém NÚKIB v únoru 2022 Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice (dále jen „5G Doporučení“).

5G Doporučení představuje podpůrný materiál pro výběr dodavatelů subjektů budujících a provozujících sítě a poskytujících služby elektronických komunikací, které jsou kritickou informační infrastrukturou. Cílem 5G Doporučení je nabídnout operátorům, potažmo celému odvětví elektronických komunikací, pohled NÚKIB, Ministerstva průmyslu a obchodu (dále jen „MPO“), Ministerstva zahraničních věcí (dále jen „MZV“), Bezpečnostní informační služby (dále jen „BIS“), Úřadu pro zahraniční styky a informace (dále jen „ÚZSI“) a Vojenského zpravodajství (dále jen „VZ“) na základní východiska posuzování důvěryhodnosti dodavatelů technologií do 5G sítí a navrhnout kritéria, která mohou přispět k výběru důvěryhodných dodavatelů.

Přestože však byla vodítka tohoto druhu ze strany správců této infrastruktury dlouhodobě požadována, k reflexi 5G Doporučení jeho adresáty po jeho vydání prakticky nedošlo; mnozí správci kritické informační infrastruktury v sektoru elektronických komunikací nadále uzavírají kontrakty na dodávky technologií do bezpečnostně citlivých částí své infrastruktury s dodavateli, kteří po vyhodnocení kritérií 5G Doporučení na první pohled nevychází jako důvěryhodní.[30]

Na základě této zkušenosti se jeví neregulatorní působení na zohledňování strategické roviny důvěryhodnosti dodavatele v sektoru elektronických komunikací jako nedostatečné. Lze se domnívat, že ani v jiných sektorech hospodářství nebudou podnikatelské subjekty ochotny upřednostňovat strategickou důvěryhodnost dodavatele před bezprostředními ekonomickými aspekty dodávek, jako je například nabídková cena, nebudou-li existovat závazná regulatorní pravidla.

Problematika posuzování subjektů na základě mj. také vyhodnocování kritérií netechnického charakteru je v současnosti již zavedena v právním řádu pro vymezené skupiny

[30] T-MOBILE CZECH REPUBLIC, A.S. T-Mobile pokračuje s rozšiřováním 5G sítí – spustil dalších 270 vysílačů. Dostupné z: https://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/t-mobile-pokracuje-s-rozsirovanim-5g-siti-spustil-dalsich-270-vysilacu.html; SEDLÁK, Jan. Varování navzdory. Vodafone a T-Mobile budou dál v 5G sítích nasazovat zařízení od Huawei. Dostupné z: https://www.e15.cz/byznys/technologie-a-media/varovani-navzdory-vodafone-a-t-mobile-budou-dal-v-5g-sitich-nasazovat-zarizeni-od-huawei-1389914

subjektů. Jedná se zejména o zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (dále jen „zákon o IS veřejné správy“), který v §6m odst. (1) písm. c) stanovuje mezi požadavky na poskytovatele cloud computingu poskytujícího cloud computing orgánu veřejné správy, jako osobu nebo jiné právní uspořádání, která je způsobilá pro poskytnutí cloud computingu orgánu veřejné správy z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob. Poskytovatel cloud computingu musí zákonem definované požadavky splnit, jestliže má být zapsán v katalogu cloud computingu pro orgány veřejné správy (dále jen „katalog cloud computingu“). Pouze poskytovatelé zapsaní v katalogu cloud computingu mohou poskytovat služby cloud computingu orgánům veřejné správy.

1.3.2 Legislativa v ostatních oblastech

Kromě nedostatečného zmocnění NÚKIB k řešení definovaného problému nemají ani orgány a osoby v postavení zadavatele dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, (dále jen „ZZVZ“), reálnou možnost zohlednit aspekt strategické bezpečnostní rizikovosti dodavatele v zadávacích podmínkách a při následném hodnocení nabídek. Stanovení a následné posuzování netechnických aspektů dodavatele vyžadují specifickou expertízu a informace, kterými zadavatelé zpravidla nedisponují. V konečném důsledku tak zpravidla dochází k výběru dodavatele veřejné zakázky na základě nabídkové ceny, případně jiných, snadno vyhodnotitelných kritérií.

Další regulací je zákon č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů (dále jen „zákon o prověřování zahraničních investic“). Zákon o prověřování zahraničních investic v § 1 písm. a) uvádí, že předmětem této právní úpravy je mj. stanovení pravidel prověřování některých zahraničních investic z důvodu ochrany bezpečnosti ČR nebo vnitřního či veřejného pořádku. Zahraniční investoři do cílových osob definovaných § 7 zákona tak budou podrobeni prověření s cílem získat povolení zahraniční investice, bez nějž tuto investici nebudou moci uskutečnit.

K účelu udržení nebo obnovení mezinárodního míru a bezpečnosti, boje proti terorismu, dodržování mezinárodního práva, ochraně lidských práv a svobod a podpoře demokracie a právního státu směřuje zákon č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů (dále jen „zákon o mezinárodních sankcích“). Na základě tohoto zákona je možné nařízením či rozhodnutím vlády při splnění jedné z podmínek vymezených v § 2 uplatnit omezení či zákazy v oblastech stanovených v § 4 odst. 2 zákona o mezinárodních sankcích. K omezení či zákazu využívání ICT produktů na území ČR může dojít na základě:

a) § 5, odst. 1 písm. a) zákona o mezinárodních sankcích, kdy může dojít k omezení nebo zákazu dovozu anebo koupě zboží, na které se vztahují mezinárodní sankce, jeho prodeje nebo jakéhokoli jiného nakládání s ním.

b) § 7 zákona o mezinárodních sankcích, kdy mohou sankce také v oblasti technické infrastruktury spočívat v omezení či zákazu dodávek energie nebo dodávek surovin, strojů nebo zařízení potřebných k její výrobě subjektu, osobě či celému území, na které se mezinárodní sankce vztahují.

Stávající právní úprava umožňuje omezit či zakázat produkty či služby poskytované určitými osobami, a to z důvodu možnosti existence strategického rizika spojeného s těmito osobami majícího negativní vliv na zajištění ochrany bezpečnosti, veřejného pořádku či bezpečnosti a dodržování práv třetích osob v ČR. Poskytovatelé cloud computingu či zahraniční investoři jsou na základě platné právní úpravy v současnosti regulováni a

prověřování mj. i na základě hodnocení tzv. netechnických kritérií. Obdobná regulace je v současnosti potřebná taktéž pro dodavatele ICT do strategicky významné infrastruktury ČR, a to z důvodu nedostatečnosti existující právní úpravy pro řešení problému definovaného v části 1.2. Zákon o mezinárodních sankcích umožňuje dokonce omezení či zákaz dodávek zboží, popř. v oblasti dodávek energií taktéž veškerá zařízení potřebná k její výrobě, a to nejen zboží určitého subjektu či osoby, nicméně celému území, na které se sankce vztahují. Ačkoliv tento sankční režim umožňuje regulovat dodávky mj. také do strategické infrastruktury, z povahy věci jsou omezení spojená s udělováním sankcí především reaktivního charakteru na vývoj na mezinárodní úrovni. Jejich využívání pro potřeby mitigace rizika úmyslného narušení kybernetické bezpečnosti strategicky významné infrastruktury či vzniku strategické závislosti na rizikovém dodavateli tedy není dostačující. Plánovaná regulace dodavatelů nicméně počítá s využitím informací a poznatků těchto existujících mechanismů pro proces hodnocení důvěryhodnosti dodavatelů do strategické infrastruktury státu, a to z důvodu zvýšení efektivnosti tohoto procesu.

V současnosti je na úrovni Evropské unie plánováno zavedení evropského systému certifikace kybernetické bezpečnosti[31], např. certifikační schéma pro 5G sítě. Evropský certifikační systém zahrnuje pouze technickou certifikaci produktů, služeb a procesů a nevyhodnocuje rovinu strategické důvěryhodnosti dodavatele. Prověřování strategické důvěryhodnosti dodavatelů však především nelze aplikovat na úrovni Evropské unie z důvodu vyloučení problematiky vnitřní bezpečnosti z úpravy primárního práva Evropské unie[32]. Evropský systém certifikace kybernetické bezpečnosti se tedy v současnosti jeví pouze jako vhodný doplněk k navrhovanému řešení, avšak nemůže a ani nemá ambice jej nahradit.

1.4 Identifikace dotčených subjektů

Navrhovaný zákon bude mít přímý dopad jak na vybrané povinné osoby ZKB, tak na jejich dodavatele, jejichž specificky vymezené typy dodávek do strategicky významné infrastruktury ČR mohou být po zavedení regulace omezeny. V neposlední řadě budou regulací významné ovlivněny taktéž státní orgány, které budou do procesu prověřování bezpečnostní spolehlivosti dodavatelů zapojeny.

1.4.1 Povinné osoby mechanismu

Dotčenými subjekty návrhu zákona jsou v prvé řadě správci strategicky významné infrastruktury. Konkrétně se jedná o poskytovatele regulované služby v režimu vyšších povinností, kterým plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, a to dle vyhlášky o regulovaných službách. Jedná se o poskytovatele takových regulovaných služeb, které naplňují kritéria pro určení regulované služby v režimu vyšších povinností, a zároveň by narušení bezpečnosti informací poskytovatele regulované služby mohlo způsobit závažný dopad na bezpečnost České republiky nebo vnitřní či veřejný pořádek. Odhadem počtu těchto povinných subjektů mechanismu je 150 subjektů. V tomto dokumentu je množina poskytovatelů těchto regulovaných osob označována jako „strategicky významná infrastruktura“ nebo „povinné osoby mechanismu“.

[31] Tento systém je zaváděn na základě nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“).
[32] Viz např. čl. 72 Smlouvy o fungování EU.

Hlavní přímý dopad návrhu zákona na povinné osoby mechanismu spočívá ve stanovení několika nových povinností, a to zejména povinnosti nahlašovat NÚKIB specificky vymezený okruh dodavatelů, jejichž dodávky využívají v rámci vymezené regulované části infrastruktury. Dále bude povinným osobám mechanismu uložena povinnost reflektovat opatření obecné povahy vydaná NÚKIB ve vztahu ke svým dodavatelům. Dle výsledků dotazníkového šetření[33] respondenti uvedli, že mají v průměru 9 dodavatelů plnění do infrastruktury tvořící informační nebo komunikační systém regulovaný zákonem o kybernetické bezpečnosti.[34] Průměrně 5 dodavatelů dodává respondentům aktiva (kromě objektů), která jsou hodnocena jako vysoká nebo kritická dle přílohy č. 1 k vyhlášce o kybernetické bezpečnosti (dále jen „kritická a vysoká aktiva“).[35] 5 dodavatelů je v průměru také zapojených do vývoje, výroby, sestavení, servisu či dodávek do vysokých a kritických technických aktiv respondentů.[36]

Dojde ke zvýšení nákladů povinných osob mechanismu. Náklady mohou mít podobu jak finanční, tak personální, ty však lze rovněž převést na finanční, dále se proto zvažují již jen finanční náklady. Zvýšené náklady vyplývají z povinnosti hlásit přímé dodavatele a vyvinout přiměřenou snahu k zjišťování nepřímých dodavatelů, tedy vyžadují odpovídající kapacity pro zmapování dodavatelského řetězce, udržování a aktualizaci této informace.

Další ze zvýšených nákladů vyplývají z povinnosti reagovat na vydaná omezení, ke splnění této povinnosti je tak třeba uvažovat kapacity pro sledování vydaných omezení, vyhodnocení nezbytných zdrojů pro reakci na omezení (např. vyčíslení finančních nákladů na implementaci omezení), nastavení plánu reakce na konkrétní omezení (např. rozplánování jednotlivých kroků projektu implementace omezení s ohledem na stanovenou lhůtu pro splnění omezení) a zejména kapacity nezbytné pro snížení hrozby v případě mírnějšího omezení dodavatele (např. přijetí technického bezpečnostního opatření – pořízení nového prvku, úprava nastavení prvku atp.), nebo obměnu plnění poskytovaného dodavatelem v případě zákazu využívání konkrétního dodavatele (např. náklady spojené s ukončením smlouvy, odpisem nevyužitého majetku, pořízením nového majetku).

Cílem možnosti udělování takovýchto výjimek je předejít paralýze infrastruktury (resp. ohrožení poskytování regulované služby podstatným způsobem) v důsledku zákazu nenahraditelné technologie. Zároveň ovšem udělování výjimek bude prováděno až na základě podnětu některé povinné osoby, která bude mít povinnost uvést vysvětlit důvody, které by k udělení výjimky měly vést, vč. řádného podložení svých tvrzení důkazy. NÚKIB následně získané informace vyhodnotí z pohledu potřeby stanovení výjimky ze zákazu daného vysoce rizikového dodavatele, a to v procesu připomínek k návrhu opatření obecné povahy (dále jen „OOP“), prostřednictvím kterého budou rozhodnutí o identifikované míře rizikovosti dodavatele sdělována veřejnosti a na základě kterého budou povinným osobám mechanismu plynout povinnosti související s využíváním plnění daného identifikovaného dodavatele.

Vyčíslení nákladů není dobře možné, protože do něj vstupuje řada neznámých proměnných, a to zejména jak často bude nutné přistoupit k omezení některého z dodavatelů,

[33] Dotazníkové šetření bylo adresovaného všem orgánům a osobám dle § 3 c), d), f) a g) zákona o kybernetické bezpečnosti (odesláno prostřednictvím datové schránky 1. 11. 2022 s žádostí o sdílení vyplněného dotazníku do 30. 11. 2022). Následně NÚKIB vyhodnotil odpovědi orgánů a osob, kteří se stanou poskytovateli regulované služby v režimu vyšších povinností, kterým plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, přičemž některé orgány či osoby spravující či provozující více systémů poskytli odpovědi za každý takový systém zvlášť. NÚKIB obdržel 65 takových odpovědí (dále jen „respondenti“).

[34] Na tento dotaz poskytlo kvantifikovatelnou odpověď 64 respondentů.

[35] Na tento dotaz poskytlo kvantifikovatelnou odpověď všech 65 respondentů.

[36] Na tento dotaz poskytlo kvantifikovatelnou odpověď všech 65 respondentů.

v jakém rozsahu bude omezovaný dodavatel ve strategické infrastruktuře zastoupen a jaký způsob reakce na dané omezení přijme konkrétní povinná osoba mechanismu.

Za další dopad je možné považovat omezení nabídky a konkurenčního prostředí na trhu. Při využití některého z omezených dodavatelů bude nezbytné vynaložit vyšší finanční náklady (viz první negativní dopad) ke snížení jeho hrozby nebo bude přímo zakázáno využití konkrétního dodavatele. Tento stav povede ke snížení významu nebo odstranění omezeného dodavatele z relevantního trhu (trh s plněním do strategické infrastruktury) což bude mít za následek omezení nabídky a v některých oblastech i konkurenčního prostředí, a tedy zvýšení ceny plnění ostatních dodavatelů.

Povinné osoby mechanismu mají právo v průběhu procesu vydávání OOP (kterým bude zakázáno využívání plnění konkrétního dodavatele) podávat připomínky nebo námitky. Cílem regulace je zvýšení odolnosti a bezpečnosti strategicky významné infrastruktury v ČR, v žádném případě však cílem není ohrožení poskytování regulované služby. Pokud dodavatel poskytuje bezpečnostně relevantní dodávky, která je nezbytná pro poskytování regulované služby v požadované kvalitě a zároveň neexistuje žádný jiný dodavatel, který by takovou dodávku mohl poskytnout, NÚKIB může udělit výjimku pro využívání bezpečnostně relevantní dodávky. V některých případech může jít např. o zajištění minimálního fungování služby, v některých případech o zajišťování služby na úrovni odpovídající posledním poznatkům – high-end technologie. Jedná se např. možnost využívat unikátní (např. patentované) technologie od dodavatele vyhodnoceného jako vysoce rizikového, které jsou nezbytné pro poskytování regulované služby.

Dojde-li k udělení výjimky a využije-li tuto výjimku některá z povinných osob mechanismu, stane se ČR závislá na vysoce rizikovém dodavateli. Tato závislost bude umocněna tím, že NÚKIB potvrdí, že pro danou typovou dodávku na trhu neexistuje alternativní dodavatel. Toto riziko bude mít povinná osoba povinnost mitigovat určitými bezpečnostními opatřeními, nicméně jak bylo popsáno v části 1. 2 Definice problému, strategické riziko plynoucí ze závislosti na rizikovém dodavateli není možné uspokojivě mitigovat technickými či organizačními opatřeními. Vhodně nastavená opatření mohou značně snížit míru rizika pro důvěrnost a integritu informací, nicméně rizika plynoucí pro dostupnost informací, a tedy i služby jako takové, příslušnými opatřeními uspokojivě mitigovat nelze.

1.4.2 Dodavatelé povinných osob mechanismu

Dalšími přímo dotčenými subjekty pak jsou dodavatelé plnění do strategicky významné infrastruktury. Budou-li tito dodavatelé vyhodnoceni jako bezpečnostně rizikoví či vysoce rizikoví, NÚKIB vydáním varování dle § X zákona o kybernetické bezpečnosti nebo vydáním OOP omezí či zakáže využití jejich zboží či služeb ve výše uvedené infrastruktuře.

Ačkoliv samotným dodavatelům Mechanismus posuzování dodavatelů nestanoví žádné povinnosti, návrh zákona by na ně měl nepřímý dopad, jelikož může zasáhnout do jejich podnikatelských aktivit. NÚKIB omezí možnost využití dodávek správci infrastruktury takových dodavatelů, kteří budou dle kritérií stanovených v prováděcím právním předpisu vyhodnoceni jako rizikoví z hlediska ochrany bezpečnosti České republiky, veřejného pořádku a dodržování práv třetích osob.

Negativním dopadem je pak reputační dopad na dodavatele, na kterého bude veřejně aplikováno omezení. Lze předpokládat, že i ostatní zákazníci omezeného dodavatele, kteří nejsou povinnými osobami mechanismu, budou vydané omezení vnímat negativně, což může

vést v konečném důsledku ke snížení poptávky po plnění poskytovaném omezeným dodavatelem, a tedy zvýšení poptávky na trhu, a tedy nárůstu ceny obdobného plnění.

1.4.3 Státní orgány

Dalšími nepřímo dotčenými subjekty jsou státní orgány, které by měly být přímo zapojeny do procesu shromažďování informací o rizikovosti dodavatelů.

Jmenovitě se jedná o NÚKIB, Bezpečnostní informační službu (dále jen „BIS“), Finanční analytický úřad (dále jen „FAÚ“), Ministerstvo průmyslu a obchodu (dále jen „MPO“), Ministerstvo vnitra (dále jen „MV“), Ministerstvo zahraničních věcí (dále jen „MZV“), Národní bezpečnostní úřad (dále jen „NBÚ“), Nejvyšší státní zastupitelství (dále jen „NSZ“), PČR, Úřad pro ochranu hospodářské soutěže (dále jen „ÚOHS“), Úřad pro zahraniční styky a informace (dále jen „ÚZSI“), Vojenské zpravodajství (dále jen „VZ“) a další státní orgány, které budou osloveny k poskytnutí informací a součinnosti v případě potřeby.

Tyto státní orgány shromažďují informace o rizikovosti dodavatelů a tyto informace poskytují NÚKIB, a to vždy na základě své zákonné působnosti a expertízy v dané oblasti prověřování. NÚKIB dále tyto obdržené informace vyhodnotí a v případě identifikace rizika vydává omezení vztahující se k danému dodavateli.

1.5 Popis cílového stavu

Vrcholným cílem návrhu zákona je omezit závislost strategicky významné infrastruktury ČR na rizikových dodavatelích představujících strategickou hrozbu v oblasti kybernetické bezpečnosti, a přispět tak k zajištění dlouhodobě udržitelné bezpečnosti a odolnosti strategicky významné infrastruktury. Při dosažení cílového stavu by měla být ve strategicky významné infrastruktuře omezena přítomnost rizikových a potenciálně rizikových dodavatelů, jež mohou představovat bezpečnostní hrozbu pro Českou republiku. Mělo by tak dojít k významnému omezení možnosti negativního zahraničního působení na zajištění základních funkcí státu prostřednictvím zneužití závislosti v dodavatelsko-odběratelských vztazích, jako je proprietární uzamčení odběratele, tzv. vendor lock-in, nevynucené omezení dodávek či zneužití infrastruktury nebo neoprávněný zásah do ní.

Zákon si dále klade za cíl prostřednictvím intenzívnějšího informování povinných osob mechanismu o hrozbách spojených s rizikovými dodavateli přispívat k tomu, že i povinné osoby začnou samy klást vyšší důraz na bezpečnost, a to vč. aspektů rizikovosti, které posuzuje stát. Dlouhodobým cílem zákona je tak také změnit přístup samotných povinných osob k výběru dodavatelů. Povinné osoby by měly klást vyšší důraz na bezpečnost a nižší důraz pouze na pořizovací cenu ICT produktů a služeb. Dodavatelé, kteří budou nabízet bezpečná ICT řešení, a to jak z pohledu technického, tak strategického, by tak získávali konkurenční výhodu oproti dodavatelům, kteří nejsou schopni takové záruky poskytnout.

Rizika v oblasti kybernetické bezpečnosti nelze zcela eliminovat. Akceptace míry rizika, která je uvedena v kapitole 1.2, je ovšem nepřijatelná a cílem tohoto zákona je umožnit státu disponovat takovými nástroji, které toto riziko sníží na akceptovatelnou úroveň. Návrh zákona si mj. dává za cíl přispět k výběru takových dodavatelů do strategicky významné infrastruktury, kteří při jakémkoliv zjištění zranitelnosti či narušení dodávaného technologického řešení budou se svými odběrateli tyto informace ihned sdílet, flexibilně a

transparentně postupovat při řešení a nápravě identifikovaných zranitelností a vynakládat úsilí k dosažení opětovného zabezpečení takových produktů či služeb.

Konkrétně prostřednictvím zákona dojde k plnění:

d) Bezpečnostní strategie ČR[37], a to především při čelení hrozbám jako jsou kybernetické útoky, ohrožení funkčnosti kritické infrastruktury, či přerušení dodávek strategických surovin nebo energie.

a) NSKB[38], konkrétně v provádění systematického a pečlivého hodnocení rizik, které zahrnuje technické i netechnické aspekty kybernetické bezpečnosti, které je nezbytné pro vytvoření a udržení skutečně odolné infrastruktury. Stěžejní otázkou v této problematice je pak bezpečnost dodavatelského řetězce, tedy nutnost zajistit, že externí subjekty a osoby mající vliv na nejdůležitější infrastruktury státu nejsou z bezpečnostního hlediska rizikovými. Návrh zákona je i plněním konkrétního úkolu v Akčním plánu NSKB, který zní „Vytvořit návrh posuzování rizikového profilu dodavatelů na národní úrovni a uplatňování omezování vysoce rizikových dodavatelů do systémů regulovaných ZKB“.

b) Národní strategie pro čelení hybridnímu působení[39], a to konkrétně prostřednictvím posilování odolnosti státu a společnosti na základě komplexního, celospolečenského přístupu k bezpečnosti, jehož účelem je omezování zranitelností, jichž původci hybridního působení využívají. ČR dále taktéž touto právní úpravou bude posilovat schopnosti prvků kritické infrastruktury uchovávat svoji dostatečnou funkčnost pro případ svého vystavení hybridnímu působení. V neposlední řadě zákon přispívá k snižování strategické závislosti ČR na zemích s odlišnou ideově-hodnotovou orientací. Takováto závislost by mohla být zneužita v působení proti zájmům ČR.

c) Programového prohlášení vlády České republiky[40], a to konkrétně při naplňování cílů „Kritická infrastruktura bude stát na bezpečných, otevřených a auditovatelných technologiích“ (…) (v části „Kybernetická bezpečnost“) a „nedemokratickým státům nebyl umožněn přístup ke klíčové infrastruktuře ČR.“

d) Souboru opatření EU pro bezpečnost sítí 5G[41] (tzv. EU 5G Toolboxu), a to zejména strategického opatření 03, jež požaduje stanovení rámce na národní úrovni k posouzení rizikového profilu dodavatelů a uplatňování omezování u dodavatelů považovaných za vysoce rizikové, včetně jejich vyloučení pro účinné zmírnění rizik v nezbytných případech, pokud jde o klíčová aktiva (dále jen „SM03“). Přijetím zákona bude ČR disponovat nástrojem, který SM03 naplní a zařadí se tak mezi další státy EU, jako je např. Německo.

[37] MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČESKÉ REPUBLIKY. Bezpečnostní strategie České republiky. 2015. Dostupná zde: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

[38] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Národní strategie kybernetické bezpečnosti. Dostupná zde: https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

[39] MINISTERSTVO OBRANY ČR. Národní strategie pro čelení hybridnímu působení. Dostupná zde: https://mocr.army.cz/assets/informacni-servis/zpravodajstvi/narodni-strategie-pro-celeni-hybridnimu-pusobeni.pdf

[40] VLÁDA ČR. Programové prohlášení vlády České republiky. 2022. Dostupné zde: https://www.vlada.cz/assets/jednani-vlady/programove-prohlaseni/programove-prohlaseni-vlady-Petra-Fialy.pdf

[41] NIS COOPERATION GROUP. Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. 01/2020. Dostupné zde: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468

e) Závěrů Rady EU o bezpečnosti dodavatelského řetězce IKT[42], které vyzývají členské státy EU k posílení bezpečnosti dodavatelského řetězce IKT s cílem řešení hrozeb nežádoucí strategické závislosti v rámci dodavatelských řetězců IKT.

f) Strategického konceptu NATO[43], a to zejména odstavce 26, který upozorňuje na důležitost identifikace a mitigace strategické závislosti a zranitelností mimo jiné ve své kritické infrastruktuře a dodavatelských řetězcích.

g) Článku 3 Severoatlantické smlouvy[44], který uvádí, že zajištění bezpečného a odolného dodavatelského řetězce přispívá k plnění spojeneckého závazku rozvíjení kolektivních i individuálních kapacit ČR k odolávání jakékoliv formě útoků, včetně těch kybernetických.

h) tzv. Strengthened Resilience Commitment[45], kdy se v roce 2021 členské státy NATO dohodly na závazku posílit odolnost s cílem neustále zvyšovat národní, kolektivní odolnost a civilní připravenost. Členské státy NATO se mimo jiné dohodly, že zvýší úsilí v zabezpečení a diverzifikaci dodavatelských řetězců a zajistí odolnost kritické infrastruktury a klíčových průmyslových odvětví.

i) Prague Proposals[46], které upozorňují mimo jiné na důležitost provádění systematického a pečlivého posuzování rizik, jež je nezbytné pro vytvoření a udržení skutečně odolné infrastruktury. Takové posuzování zahrnuje technické i netechnické aspekty kybernetické bezpečnosti.

1.6 Zhodnocení rizika spojeného s nečinností

Současný stav je nedostatečný a může způsobit závislost státu prostřednictvím strategicky významné infrastruktury na rizikových dodavatelích, což by v důsledku mohly vést až k nenaplňování základních funkcí státu a ohrožení bezpečnosti České republiky či veřejného pořádku.

Při zachování současného stavu, kdy nemá stát nástroje k hodnocení a omezování rizik spojených s dodavateli do strategicky významné infrastruktury, by dodavatelé do této infrastruktury byli na základě proběhnuvšího dotazníkového šetření[47] i nadále vybíráni pouze na základě posouzení povinných osob mechanismu a jeho vyhodnocení kritérií souvisejících zejména s požadavky zákona o kybernetické bezpečnosti (resp. vyhlášky o kybernetické bezpečnosti) (41 % respondentů), cenou (14 % respondentů), kvalitou nabízeného řešení a

[42] RADA EVROPSKÉ UNIE. Závěry Rady o bezpečnosti dodavatelského řetězce IKT. Říjen 2022. Dostupné zde: https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/cs/pdf

[43] NATO. NATO 2022 Strategic Concept. Dostupné zde: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

[44] NATO. Severoatlantická Smlouva. 1949. Dostupné zde: https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=cs

[45] NATO. Strengthened Resilience Commitment. 2022. Dostupné z: https://www.nato.int/cps/en/natohq/official_texts_185340.htm

[46] PRAGUE 5G SECURITY CONFERENCE. The Prague Proposals. The Chairman Statement on cyber security of communication networks in a globally digitalized world. 2019. Dostupné z: https://www.nukib.cz/en/infoservis-en/conferences/prague-5g-security-conference-2019/

[47] Dotazníkové šetření bylo adresovaného všem orgánům a osobám dle § 3 c), d), f) a g) zákona o kybernetické bezpečnosti (odesláno prostřednictvím datové schránky 1. 11. 2022 s žádostí o sdílení vyplněného dotazníku do 30. 11. 2022). Následně NÚKIB vyhodnotil odpovědi orgánů a osob, kteří se stanou poskytovateli regulované služby v režimu vyšších povinností, kterým plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, přičemž některé orgány či osoby spravující či provozující více systémů poskytli odpovědi za každý takový systém zvlášť. NÚKIB obdržel 65 takových odpovědí (dále jen „respondenti“).

technologickou způsobilostí dodavatele (44 % respondentů) a dalšími požadavky zákona o veřejných zakázkách pro ty orgány a osoby, které se tímto zákonem jsou povinni řídit.[48]

Nutno podotknout, že i správci strategicky významné infrastruktury vyhodnocují některá kritéria související s netechnickými aspekty dodavatelů či nabízených technických řešení. Jedná se zejména o posuzování a vyhodnocování kritérií souvisejících se sídlem dodavatele (zdali má dodavatel sídlo v zemi EU či NATO vyhodnocuje 73 % respondentů[49], zdali dodavatel podléhá právním řádům zemí, na které veřejně upozorňují bezpečnostní instituce ČR vyhodnocuje 68 % respondentů[50]. Vlastnickou strukturu dodavatele zná a vyhodnocuje 80 % respondentů[51]. Zdali byl dodavatel pravomocně odsouzen pro trestný čin zajímá 56 % respondentů[52], o poznání méně respondentů[53] (44 %) pak hodnotí, zdali je dodavatel pod výkonem účinné míry kontroly hospodářské činnosti cizího státu, resp. zdali dodavatel jedná eticky, v souladu s pravidly mezinárodního obchodu a s péčí řádného hospodáře (36 %)[54]. Další hrozby spojené s dodavatelským řetězcem jako hrozba nedodržení smluvního závazku ze strany dodavatele nevyhodnocuje 9 % respondentů[55], hrozbu zneužití vnitřních prostředků či sabotáž nevyhodnocuje 19 % respondentů[56] a hrozbu použití špionážních technik ze strany či prostřednictvím dodavatele nevyhodnocuje dokonce 40 % respondentů[57].

Posuzování a vyhodnocování takovýchto kritérií či hrozeb by ovšem i nadále zůstalo zcela na vůli a míře posouzení samotných správců strategicky významné infrastruktury a nebylo by vyžadováno, aby k posuzování takového typu kritérií docházelo. Absence posuzování strategických rizik plynoucích ze strany dodavatelů do významné strategické infrastruktury by tak nebyla výjimečná, a jelikož značná část dotázaných subjektů takovou analýzu neprovádí nyní, existuje velice nízká pravděpodobnost, že by došlo ke změně jejich přístupu k této problematice bez regulatorních nástrojů. V krajních případech by tak mohlo dojít k narušení až ochromení fungování některé strategicky významné infrastruktury, což by mělo celospolečenský dopad.

Dalším problémem současného stavu související s bezpečností dodavatelského řetězce je to, že ačkoliv dle výsledků dotazníkového šetření[58] povinné osoby mechanismu dle zákona o kybernetické bezpečnosti smluvně zavazují své dodavatele k plnění požadavků na kybernetickou bezpečnost, pouze 80 % potvrdilo, že po dodavatelích vyžaduje plnění těchto požadavků i jejich subdodavateli. Ačkoliv 92 % respondentů[59] získává informace

[48] Na tento dotaz poskytlo vyhodnotitelnou odpověď 63 respondentů.
[49] Na tento dotaz poskytlo odpověď 64 respondentů.
[50] Na tento dotaz poskytlo odpověď 63 respondentů.
[51] Na tento dotaz poskytlo odpověď 64 respondentů.
[52] Na tento dotaz poskytlo odpověď 64 respondentů.
[53] Na tento dotaz poskytlo odpověď 62 respondentů.
[54] Na tento dotaz poskytlo odpověď 64 respondentů.
[55] Na tento dotaz poskytlo odpověď 64 respondentů.
[56] Na tento dotaz poskytlo odpověď 64 respondentů.
[57] Na tento dotaz poskytlo odpověď 62 respondentů.
[58] Dotazníkové šetření bylo adresovaného všem orgánům a osobám dle § 3 c), d), f) a g) zákona o kybernetické bezpečnosti (odesláno prostřednictvím datové schránky 1. 11. 2022 s žádostí o sdílení vyplněného dotazníku do 30. 11. 2022). Následně NÚKIB vyhodnotil odpovědi orgánů a osob, kteří se stanou poskytovateli regulované služby v režimu vyšších povinností, kterým plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, přičemž některé orgány či osoby spravující či provozující více systémů poskytli odpovědi za každý takový systém zvlášť. NÚKIB obdržel 65 takových odpovědí (dále jen „respondenti“).
[59] Na tento dotaz poskytlo odpověď 63 respondentů.

i o subdodavatelích svých významných dodavatelů, pouze 5 % z nich získává informace o subdodavatelích 2. úrovně, přičemž žádný z respondentů nezískává informace o subdodavatelích 3. a další úrovně. V průměru má přitom každý významný dodavatel 4 až 5 subdodavatelů[60].

Navíc pro identifikaci rizikovosti dodavatele je kromě vyhodnocení uvedených netechnických kritérií konkrétním dodavatelem nutné také zhodnocení dalších informací (vč. zpravodajských) o možných strategických hrozbách a rizicích spojených s konkrétním dodavatelem. Jedná se tedy o kritéria, která není schopen adekvátně vyhodnotit správce strategicky významné infrastruktury, a to ani pokud se o to vyhodnocováním alespoň dílčích aspektů sám pokouší. Z takového důvodu nejsou současné nástroje státu cílící na omezení rizika spojeného s rizikovými dodavateli dostatečná (více viz kapitola 1.3 Popis existujícího právního stavu v dané oblasti).

Evropská agentura pro bezpečnost sítí a informací (dále jen „ENISA“) ve výroční zprávě Threat Landscape pro rok 2022[61], která sleduje stav kybernetické bezpečnosti v zemích EU a identifikuje hlavní hrozby, trendy či aktéry útoků v této oblasti uvádí, že ve sledovaném období (červenec 2021–červenec 2022) byl opět pozorován nárůst tohoto typu útoků, přičemž se jednalo o druhý nejrozšířenější typ kompromitace. Ze zprávy dále vyplývá, že dochází k nárůstu útoků na dodavatelské řetězce státem podporovanými aktéry a zároveň rostou i jejich schopnosti a motivace. V souvislosti s válkou na Ukrajině se ukázalo, že geopolitický kontext má zcela zásadní dopad na operace v kyberprostoru a dle předpovědí ENISA bude tento trend nadále pokračovat. Zpráva zmiňuje i nárůst útoků na dodavatelský řetězec softwaru prostřednictvím kompromitace oblíbených softwarových balíčků, platforem nebo open-source knihoven pro vývoj softwaru. Útoky tohoto typu mohou mít dle ENISA zcela zásadní dopad v případě narušení kritických služeb nebo i služeb, které nejsou přímo zasaženy.

Konflikt na Ukrajině dále jasně poukazuje na důležitost pochopení bezpečnosti a odolnosti všech dodavatelů v našich strategicky důležitých dodavatelských řetězcích. V dnešním nejistém globalizovaném bezpečnostním prostředí lze rozumně předpokládat možné náhlé zhoršení vztahů s jakýmkoliv státem, jehož zájmy nejsou v souladu se zájmy ČR či jejími spojenci. Je tedy důležité, aby stát měl nástroje pro omezení využívání dodavatelů s vazbami na takové státy. V případě eskalace vztahů či vzniku konfliktu by závislost strategicky významné infrastruktury na takových dodavatelích mohla mít pro ČR nepředstavitelné důsledky.

Další rizika spojená s nečinností jsou:

a. vytvoření strategické hrozby státu v podobě závislosti na rizikových dodavatelích. V případě realizace hrozby by došlo k ohrožení strategicky významné infrastruktury, jejíž narušení by mohlo mít dopad na fungování celé ČR.

b. existence nepředvídatelného prostředí a nejistota povinných osob mechanismu, kteří ačkoliv mají přehled z ostatních států o rizikovosti vybraných dodavatelů, mohou při výběru i nadále upřednostňovat jiné, zejména ekonomické aspekty nabízeného řešení, což je podněcováno zejména obavou z nekonkurenceschopnosti na trhu a taktéž podmínkami, které jim jsou v ČR nabízeny.

[60] Na tento dotaz poskytlo odpověď 51 respondentů.

[61] ENISA. ENISA Threat Landscape 2022. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

c. reputační dopad ČR, kdy absence regulatorního rámce dodavatelů do strategicky významné infrastruktury bude řadit ČR mezi státy, jež zaostávají, a proto je důležité zachovat své jméno a vybudovat 5G sítě na bezpečném základu s adekvátně nastavenou regulací. Absence regulace bezpečnosti dodavatelského řetězce by tak v budoucnu mohla vést ke zhoršení pozice podnikatelských subjektů působících v ČR, kteří by nemohli nabídnout stejnou míru bezpečnosti svého produktu či služby jako subjekty ve státech, které obdobnou regulaci přijaly. Nepřijetí předmětné právní úpravy by tedy mohlo vyvolat nucené odmítání dodávek českých společností zahraničními odběrateli kvůli bezpečnostním a strategickým hrozbám plynoucím z dodávek subdodavatelů. České společnosti by se tím de facto staly nespolehlivými dodavateli pro zahraniční obchodní partnery, kteří by byli v takovém případě nuceni svým národním legislativním systémem upřednostnit dodavatele ze zemí, které rizika dodavatelského řetězce legislativně ošetřují.

d. Vznik strategické hrozby v podobě závislosti na rizikových dodavatelích či přítomnosti technologií vysoce rizikových dodavatelů ICT ve strategické infrastruktuře. Může také dojít k omezení volnosti strategického rozhodování ČR, kdy bude nutné vzít v potaz možnost zneužití přítomnosti rizikových dodavatelů cizím státem.

e. Může docházet k výskytu vícero závažných zranitelností a tím k navýšení počtu kybernetických incidentů a útoků ze strany států, které mohou zneužívat svého vlivu nad dodavateli operujícími pod jejich jurisdikcí. Tito dodavatelé poskytující hardware či software do strategické infrastruktury ČR mohou cíleně narušit důvěrnost, integritu a dostupnost dat.

f. Vznik nepřiměřených finančních dopadů pro ČR, jelikož sanace kybernetických incidentů s sebou může přinášet náklady pohybující se v řádech desítek miliónů až miliard korun. Dále je nutné zmínit nežádoucí finanční dopady spojené se situací, kdy může být nezbytné produkty strategicky rizikových dodavatelů bezodkladně nahradit až ve chvíli, kdy se již hrozba bezprostředně realizovala. A to navíc pouze v případě, že by takové odstranění bylo po technické, finanční a legislativní stránce vůbec proveditelné. Časový rámec potřebný pro nahrazení pak navíc může násobně překračovat lhůtu pro efektivní reakci, což jen podtrhuje potřebu včasného a proaktivního řešení, nikoli až reakci ex post.

g. Sekundárně dochází k nepřímému financování států, které mohou tyto prostředky následně využívat pro narušování zájmů ČR a jejích spojenců. Tuto situaci lze nyní pozorovat například při nákupu plynu či ropy pocházejících z Ruské federace, kdy jsou získané finance vynakládány na vedení ozbrojeného konfliktu na Ukrajině.

h. V neposlední řadě může docházet k poškození reputace ČR, která je dlouhodobě v Evropě považována za vedoucí stát v oblasti kybernetické bezpečnosti.

2 Návrh variant řešení

2.1 Varianta I – nulová varianta: Zachování současného stavu

Varianta zachování současného stavu by znamenala nečinit žádné legislativní změny k omezení strategických bezpečnostní rizik spojených s důvěryhodností dodavatelů do strategicky významné infrastruktury.

Zachování současného stavu bude i nadále podporovat existenci strategické hrozby v podobě závislosti na rizikových dodavatelích či přítomnosti technologií rizikových dodavatelů ICT ve strategicky významné infrastruktuře. Výběr dodavatelů do strategicky významné infrastruktury bude i nadále probíhat pouze na základě kritérií definovaných, posuzovaných a vyhodnocených správci této infrastruktury. Rozhodování o tom, na jakých dodavatelích si strategicky významné subjekty prostřednictvím dodávek kritických součástí systémů vytvoří závislost, je tak zcela v rukou správců této infrastruktury (jak soukromoprávních, tak veřejnoprávních subjektů). V případě veřejných subjektů se pro výběr technologických dodávek musejí veřejní zadavatelé řídit zákonem o veřejných zakázkách. Jelikož ovšem veřejní zadavatelé nemají vhodné nástroje, kapacity a častokrát ani dostatečné zmocnění k nastavení zadání veřejných zakázek tak, aby snížily riziko přítomnosti rizikových dodavatelů ICT ve strategické infrastruktuře ČR, nezřídka kdy dochází k hodnocení nabídek dle § 115 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, na základě ceny a vyhodnocení dalších kritérií je upozaděno, popř. zcela absentuje.

Nástroje a zmocnění jsou nedostatečná především při posuzování netechnických aspektů vyžadujících specifickou expertízu a informace, kterými veřejný sektor často nedisponuje. Strategicky významná infrastruktura v rukou soukromoprávních subjektů se může potýkat s obdobnými problémy, které byly identifikovány u veřejných zadavatelů, tedy absence nástrojů či kapacit identifikovat, posuzovat a vyhodnocovat rizika (zejména rizika netechnického charakteru) spojená s dodavateli. U subjektů, které dostatečné kapacity i nástroje ke komplexnější identifikaci, posouzení a vyhodnocení rizik spojených s dodavateli mají, může být požadavek na vyšší bezpečnost v konfliktu s jejich primárním cílem, kterým je dosažení zisku. Vyšší zisk tak může být upřednostňován na úkor bezpečnosti.

Dalším aspektem, který správci strategicky významné infrastruktury neberou, a z podstaty své činnosti (a vzhledem k distribuci pravomocí mezi stát a soukromý sektor) ani nemohou, brát v potaz, je dopad nefunkčnosti regulované služby, kterou spravují, na další subjekty, na stát jako takový, a na národní bezpečnost ČR.

Strategicky významné subjekty mají mj. společné to, že pokud přestanou poskytovat regulovanou službu, ohrozí poskytování dalších regulovaných služeb dle [určovací vyhlášky]. Tedy i v případě, že by poskytovatelé regulovaných služeb měli jak kapacity a nástroje pro vyhodnocování hrozeb netechnického charakteru pro infrastrukturu, kterou spravují, nebudou schopni adekvátně vyhodnotit všechna rizika plynoucí ze strategické závislosti na rizikovém dodavateli pro ČR a její národní bezpečnost, a to ani pokud se o to vyhodnocováním alespoň dílčích aspektů sami pokouší. Pro identifikaci rizikovosti dodavatele je kromě vyhodnocení netechnických kritérií spojených s daným dodavatelem nutné také zhodnocení dalších informací (vč. zpravodajských) o možných strategických hrozbách a rizicích spojených s konkrétním dodavatelem.

Výběr dodavatelů do strategicky významné infrastruktury v případě nulové varianty kromě výše zmíněného zákona o veřejných zakázkách reguluje pouze ZKB, jeho prováděcí předpisy, zejména vyhláška o kybernetické bezpečnosti. Ačkoliv tyto předpisy stanovují regulovaným subjektům, mezi kterými jsou i správci strategicky významné infrastruktury, určité povinnosti týkající se bezpečnosti dodavatelského řetězce, nicméně jejich zaměření cílí na obecné seznámení se s dodavateli, stanovení minimálních smluvních ujednání a zavedení technických a organizačních opatření.

Regulované subjekty jsou povinny před uzavřením smlouvy s dodavatelem provést hodnocení technických rizik souvisejících s plněním smlouvy, zahrnout do smlouvy ujednání podle požadavků vyhlášky a stanovit mechanismy smluví odpovědnosti za zavedení a kontrolu plnění daných ujednání a v průběhu plnění smlouvy pravidelně provádět hodnocení rizik a zavedených bezpečnostních opatření. Stávající normy nekladou na správce strategicky významné infrastruktury požadavky týkající se identifikace, posuzování a vyhodnocování strategického rizika plynoucího ze závislosti na rizikovém dodavateli. Toto strategické riziko nelze uspokojivě mitigovat technickými či organizačními opatřeními. Vhodně nastavená opatření mohou značně snížit míru rizika pro důvěrnost a integritu informací, nicméně rizika plynoucí pro dostupnost informací, a tedy i služby jako takové, příslušnými opatřeními uspokojivě mitigovat nelze.

V případě nulové varianty bude snaha o strategického rizika ze strany státu i nadále realizována především prostřednictvím varování podle ZKB. Varování podle ZKB vydává NÚKIB v případě, že se dozví o hrozbě v oblasti kybernetické bezpečnosti. Několik takových varování podle ZKB již bylo vydáno (viz část 1.3). Správci strategicky významné infrastruktury, jelikož jsou povinnými osobami dle zákona o kybernetické bezpečnosti, jsou povinni zohledňovat varování, a to v rozsahu vyhodnocení hrozeb spojené s jejich ICT systémy a na tyto hrozby reagovat. Výše identifikovaný problém tohoto přístupu ve vztahu k vyhodnocování netechnického rizika ovšem přetrvává i nyní. V případě identifikace hrozby netechnického charakteru z podstaty své činnosti (a vzhledem k distribuci pravomocí mezi stát a soukromý sektor) je pro značnou část povinných osob vyhodnocování rizika spojeného s touto hrozbou pro systém, který spravují či provozují, obtížné vyhodnotit, a není výjimkou, že identifikovaná hrozba, před níž NÚKIB vydá varování podle ZKB, v analýze rizik povinných subjektů není adekvátně reflektována.

Zákon o IS veřejné správy dále umožňuje omezit či zakázat produkty či služby poskytované poskytovateli cloud computingu, a to z důvodu možnosti existence strategického rizika spojeného s těmito poskytovateli majícího negativní vliv na zajištění ochrany bezpečnosti, veřejného pořádku či bezpečnosti a dodržování práv třetích osob v ČR. Poskytovatelé cloud computingu jsou tedy jedinými dodavateli, kteří jsou v případě nulové varianty regulováni a prověřováni organizačními složkami státu v čele s Ministerstvem vnitra, a to mj. i na základě vyhodnocování netechnických kritérií. V případě nulové varianty žádní další dodavatelé nebudou muset být ze zákona posouzeni z hlediska strategických rizik souvisejících s využitím dodavatelů kritických částí systémů strategicky významné infrastruktury. Nedojde tak k naplnění, a to ani k částečnému, stanoveného cíle, kterým je omezení závislosti strategicky významné infrastruktury ČR na rizikových dodavatelích představujících strategickou hrozbu v oblasti kybernetické bezpečnosti a přispět tak k v zajištění dlouhodobě udržitelné bezpečnosti a odolnosti strategicky významné infrastruktury.

NÚKIB dále bude zajišťovat metodickou podporu v oblasti kybernetické bezpečnosti podle § X zákona o kybernetické bezpečnosti. Poskytování metodické podpory ovšem nepostačuje k dosažení sledovaného cíle. Pojí se s ní totiž stejné překážky a problémy, jako byly identifikovány výše při vydání varování podle ZKB, tj. obtížnost poskytovatelů strategicky významné infrastruktury vyhodnotit a aplikovat doporučení NÚKIB pro jimi spravovaný systém, příp. vědomé nereflektování doporučení a upřednostňování jiných aspektů při výběru dodavatele. NÚKIB spolu s MPO, MZV, BIS, ÚZSI a VZ poskytl v únoru 2022 podpůrný

materiál pro výběr dodavatelů subjektů budujících a provozujících sítě a poskytujících služby elektronických komunikací prostřednictvím 5G Doporučení. Přestože však byla vodítka tohoto druhu ze strany správců této infrastruktury dlouhodobě požadována, nedošlo po jejich vydání k reflexi doporučení mezi jejich adresáty.

Nulová varianta nevede k mitigaci identifikovaných rizik současného stavu, která tak zůstávají neřešena. Tato rizika jsou identifikována a podrobně popsána v kapitole 1.6. Nulová varianta se tak zpracovává pouze pro porovnání dopadů jiných variant.

2.2 Varianta II: Mechanismus posuzování dodavatelů ve strategicky významné infrastruktuře

Varianta II cílí na rozšíření pravomoci relevantních státních orgánů v oblasti kybernetické bezpečnosti tak, aby byl zaveden komplexní Mechanismus posuzování dodavatelů do strategicky významné infrastruktury napříč jejími sektory, a to vč. možnosti omezování či zákazu využití dodavatelů, kteří budou vyhodnoceni jako rizikoví či vysoce rizikoví.

S ohledem na zachování proporcionality zajištění národní bezpečnosti a ochrany svobody podnikání, jakož i s ohledem na minimalizaci státního donucení a ekonomických dopadů navrhovaného řešení na veřejný i soukromý sektor, je nezbytné omezit prověřování pouze na vymezenou strategicky významnou infrastrukturu[62], a to pouze na její část, která je kritická pro bezpečnost daného prvku vymezené infrastruktury. Prověřováni by měli být také pouze dodavatelé dodávek, které jsou relevantní z hlediska bezpečnosti daného prvku.

2.2.1 Rozsah regulované infrastruktury

Mechanismus posuzování dodavatelů vychází z principů a hodnot zákona o kybernetické bezpečnosti. Respektuje tak v maximální možné míře stávající performativní povahu pravidel řízení dodavatelů a jiných ustanovení vyhlášky o kybernetické bezpečnosti a zaměřuje prověřování ze strany státu toliko na ty strategické aspekty důvěryhodnosti dodavatelů, jež povinné osoby mechanismu z podstaty své činnosti (a vzhledem k distribuci pravomocí mezi stát a soukromý sektor) nemohou provádět.

Při vymezování části infrastruktury, stejně jako rozsahu dodávek, jejichž dodavatelé budou posuzováni prostřednictvím mechanismu, byl kladen důraz na vyvážený přístup, který jednak respektuje princip, kdy bezpečnost systémů má být v maximální možné míře v rukou jejich správců, a jednak poskytuje povinným subjektům dostatečná vodítka, aby byla aplikace mechanismu u všech povinných subjektů obdobná. Základním předpokladem pro vymezení posuzovaného dodavatele přitom je, že by se mělo jednat pouze o takové dodavatele, jejichž dodávka má či může mít vliv na bezpečnost regulované služby.

Základní tezí tohoto přístupu je, že mechanismem by měli být prověřeni jen dodavatelé poskytující plnění do kritické součásti systému strategicky významné infrastruktury, které má zároveň vliv na bezpečnost regulovaného systému. Taková kritická část systému je soubor aktiv regulovaného systému, i) u kterých správce regulované služby postupem dle prováděcího právního předpisu ohodnotil dopad narušení bezpečnosti informací úrovní vysoká nebo kritická

[62] povinné osoby mechanismu jsou identifikovány a podrobně představeny v části 1.4.

nebo, ii) které zajišťují funkce regulovaného systému, stanovené prováděcím právním předpisem.

Dodavatel, který může být omezen prostřednictvím mechanismu posuzování pak bude takový dodavatel, který poskytuje bezpečnostně relevantní dodávku do kritické součásti systému strategicky významné infrastruktury. Bezpečnostně relevantní dodávkou se rozumí plnění, spočívající ve vývoji, výrobě, sestavení či servisu technického vybavení s výpočetní kapacitou nebo programového vybavení nebo ve vývoji, sestavení, poskytnutí či servisu informační či komunikační služby směřující do Kritické části systému.

Kritická část systému je určená poskytovatelem regulované služby, jež má již před přijetím této právní úpravy povinnost podle zákona o kybernetické bezpečnosti, a především jeho prováděcího právního předpisu, vyhlášky o kybernetické bezpečnosti, stanovit metodiku pro identifikaci aktiv, hodnocení aktiv, identifikovat a evidovat aktiva, provádět řízení rizik, vč. analýzy rizik a další související povinnosti. Identifikace aktiv prováděná správcem regulované služby, tak již probíhá v současnosti, tato právní úprava v této souvislosti správcům strategicky významné infrastruktury neurčuje nové povinnosti a navazuje na jejich stávající povinnosti.

Popisovaná varianta řešení dále umožňuje prováděcím právním předpisem stanovit funkce regulovaného systému, jež budou příslušnými správci povinně do kritické části systému zahrnuty. Důvod pro existenci takového prováděcího systému je umožnit minimalizovat rozdílnost přístupů identifikace vysokých a kritických aktiv v případech, kdy jsou aktiva dané identifikované funkce nesporně spojená s dopadem narušení bezpečnosti informací úrovní vysoká nebo kritická. Tento prováděcí předpis umožní NÚKIB identifikaci takových funkcí, a tedy zamezení rozdílného přístupu k identifikaci aktiv v těch případech, kdy o míře jejich významnosti pro zajištění kybernetické bezpečnosti poskytované služby není pochyb.

2.2.2 Kritéria rizikovosti dodavatele

Kritéria rizikovosti dodavatele směřují k prověření strategických bezpečnostních hrozeb, resp. strategických bezpečnostních rizik netechnického charakteru, vycházejících bezprostředně od osoby dodavatele a souvisejících s jeho aktivitami.

Jedná se první řadě o kritéria související se zemí, která má na dodavatele vliv. Takovou zemí může být země, kde má dodavatel sídlo, nicméně i další země, která může na dodavatele efektivně vyvíjet nátlak, rozhodujícím významným způsobem jej ovlivnit či uplatňovat rozhodující vliv. Pro identifikaci takových zahraničních vlivů tak bude zkoumána a posuzována např. vlastnická struktura dodavatele. Z hlediska rizikovosti dodavatele pro bezpečnost ČR je důležité analyzovat a posoudit kritéria reflektující souladnost právních norem, zásad a zvyklostí, kterými je dodavatel dle různých právních řádů vázán, s normami, zásadami a zvyklostmi českého právního řádu.

Kromě zemí, které mají na dodavatele vliv a kritérií, která je nezbytná vyhodnotit a posoudit směrem k těmto zemím budou posuzována také kritéria, která souvisejí přímo s osobou samotného dodavatele. Identifikace nekalých praktik dodavatele či jednání v rozporu s pravidly hospodářské soutěže č má taktéž negativní dopad na úroveň možné rizikovosti daného dodavatele.

2.2.3 Povinnosti povinného subjektu mechanismu prověřování

Povinné osoby mechanismu budou povinny nahlašovat NÚKIB dodavatele, kteří jim poskytují bezpečnostně relevantní dodávku. Nahlášení dodavatele bude znamenat poskytnout NÚKIB základní identifikační údaje o dodavateli, předkladatel má tak snahu minimalizovat administrativní náklady na straně povinných osob mechanismu pro tuto novou povinnost.

Povinné osoby mechanismu jakožto povinné osoby podle ZKB podléhají ze zákona také kontrole NÚKIB. S ohledem na zachování principu efektivity a principu minimalizace nákladů bude kontrolní činnost související s mechanismem prověřování zařazena mezi standardní kontrolní činnost, kterou NÚKIB (Odbor kontroly) provádí a jejíž systém i metodika je nastavená a fungující.

Kromě nahlášení přímých dodavatelů bezpečnostně relevantních dodávek budou mít povinné osoby povinnost také vynaložit přiměřené úsilí na to, aby se dozvěděli o dalších (nepřímých) dodavatelích poskytujících bezpečnostně relevantní dodávku. V neposlední řadě budou mít povinnost dodržovat omezení vydaná NÚKIB.

Na rozdíl od varianty III v této variantě tak povinné subjekty mechanismu nemají povinnost využívat pouze „certifikované“ či „schválené“ dodavatele a jejich podnikatelské procesy tak při výběru a kontraktaci nejsou omezeny a prodlouženy čekáním na schválení daného dodavatele pro danou bezpečnostně relevantní dodávkou.

2.2.4 Proces posuzování dodavatele

Varování podle § X zákona o kybernetické bezpečnosti bude vydáno, vyhodnotí-li NÚKIB naplnění jednoho či více kritérií rizikovosti dodavatele, které může znamenat ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku.

Zákaz využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu bude vydán, vyhodnotí-li státní orgány zapojené do prověřování dodavatelů ve vztahu k orgánu či osobě naplnění jednoho či více kritérií rizikovosti dodavatele, které může znamenat významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku.

Dodavatelé, kteří budou omezeni či vyloučeni z budování kritické části strategicky významné infrastruktury budou pravidelně přezkoumáváni co do naplňování kritérií rizikovosti. Dojde-li k rozdílnému vyhodnocení kritérií či dopadu u daného dodavatele, které bude mít vliv na ohrožení bezpečnosti ČR nebo vnitřního či veřejného pořádku spojeného s daným dodavatelem spojena, neprodleně dojde ke změně, příp. ke zrušení omezení vztahujících se k danému dodavateli. Tímto mechanismem je zaručeno, že omezeni budou skutečně pouze ti dodavatelé, kteří mohou ohrozit bezpečnosti ČR nebo vnitřního či veřejného pořádku.

Podle výsledků dotazníkového šetření[63] 74 % respondentů[64] určuje ekonomickou životnost aktiv. Ekonomická životnost aktiv je nejčastěji (v 49 % případů) určována dle stanovené délky podpory (výrobce) daného aktiva. Dalšími faktory pro stanovení ekonomické životnosti aktiva je v 24 % případů stanovována s přihlédnutím k technické životnosti aktiva či ekonomickou výhodnost užívání aktiva. 39 % respondentů[65] aktiva po uplynutí doby poskytované podpory (výrobcem) dále v provozované či spravované infrastruktuře nevyužívá. Respondenti, kteří taková aktiva využívají, poté činí různorodé kroky k mitigaci rizik v podobě zneužití zranitelností, které se u takto nepodporovaných aktiv mohou objevit, a to zejména implementací vhodných technických a organizačních opatření (např. provedením segmentace sítě, omezení přístupu k nepodporovanému aktivu, zvýšený monitoring či úplná izolace takového aktiva či zajištění redundance). NÚKIB se dotazoval i na délku ekonomické životnosti vysokých a kritických technických aktiv v tvořící informační nebo komunikační systém regulovaný ZKB. Taková aktiva mají nejdelší ekonomickou životnost v sektoru energetiky (jedná se o průměrnou nejnižší životnost 7 let[66], průměrnou životnost 10-11 let[67] a nejdelší životnost až 20 let[68], přičemž jeden z respondentů uvedl životnost aktiva až 50 let). Respondenti z ostatních sektorů v průměru uváděli délky ekonomické životnosti od minima 3 let[69], přes průměr 6-7 let[70], po maximální délku životnosti 10 let[71], přičemž pouze 3 respondenti uvedli maximální délku ekonomické životnost delší než 10 let (jednalo se o 12, 14 a 20 let).

V případě zákazu dodavatele bude stanovena přechodná lhůta, do jejíž uplynutí musejí povinné osoby tento zákaz reflektovat, která bude reflektovat životní cyklus dodávaných technologií a bude v řádech několika let. Tato lhůta ovšem nemůže být fixní, ale musí být stanovována individuálně při vydávání OOP, a to z důvodu vysoké variability délky ekonomické životnosti aktiv, jejichž dodavatelé budou regulováni a na něž se zákaz využívání jejich plnění může vztahovat.

Tento postup minimalizuje dopady omezení identifikovaných rizikových dodavatelů na povinné subjekty mechanismu, které plnění takového dodavatele v době identifikace rizika s ním spojeného, ve vymezené části svojí infrastruktury využívají.

Dodavatelé jsou prověřováni dle stanoveného prioritizačního mechanismu. Kromě dodavatelů nahlášených povinnými osobami mechanismu má NÚKIB, stejně tak jako ostatní státní orgány zapojené do posuzování dodavatelů, možnost posoudit rizikovost i dalších subjektů, které mají potenciál poskytovat bezpečnostně relevantní dodávky do strategicky významné infrastruktury a působit tak i preventivně.

[63] Dotazníkové šetření bylo adresovaného všem orgánům a osobám dle § 3 c), d), f) a g) zákona o kybernetické bezpečnosti (odesláno prostřednictvím datové schránky 1. 11. 2022 s žádostí o sdílení vyplněného dotazníku do 30. 11. 2022). Následně NÚKIB vyhodnotil odpovědi orgánů a osob, kteří se stanou poskytovateli regulované služby v režimu vyšších povinností, kterým plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, přičemž některé orgány či osoby spravující či provozující více systémů poskytli odpovědi za každý takový systém zvlášť. NÚKIB obdržel 65 takových odpovědí (dále jen „respondenti“).
[64] Na tento dotaz poskytlo odpověď 61 respondentů.
[65] Na tento dotaz poskytlo odpověď 62 respondentů.
[66] Na tento dotaz poskytlo odpověď 16 respondentů.
[67] Na tento dotaz poskytlo odpověď 18 respondentů.
[68] Na tento dotaz poskytlo odpověď 15 respondentů.
[69] Na tento dotaz poskytlo odpověď 21 respondentů.
[70] Na tento dotaz poskytlo odpověď 21 respondentů.
[71] Na tento dotaz poskytlo odpověď 22 respondentů.

Varianta II cílí na omezení strategicky rizikových dodavatelů do strategicky významné infrastruktury v ČR, přičemž dbá na principy minimalizace státního donucení a proporcionalitu zajištění národní bezpečnosti a ochrany svobody podnikání. Omezováni tak budou pouze dodavatelé bezpečnostně relevantních dodávek do kritické části systému strategicky významné infrastruktury. Dodavatel bude omezen či zakázán do této vymezené infrastruktury na základě vyhodnocení transparentních kritérií, které může znamenat ohrožení bezpečnosti ČR nebo vnitřního či veřejného pořádku. V případě vyloučení dodavatele budou mít dotčené osoby možnost k návrhu zákazu vznést připomínky, a v odůvodněných případech mohou uplatnit žádost o výjimku. Povinné osoby, které zakázaného dodavatele využívají, budou mít na vyřazení dodavatele z bezpečnostně relevantních dodávek přechodnou lhůtu v řádu několika let.

2.3 Varianta III: Mechanismus plošného posuzování bezpečnostní spolehlivosti dodavatelů ve strategicky významné infrastruktuře

Účelem tohoto přístupu je ex ante prověřování všech dodavatelů vymezených dodávek do vymezené části regulované infrastruktury. Správci této infrastruktury by tak pro dané dodávky do dané strategické infrastruktury nemohli využít jiné než předem prověřené dodavatele. Rozsah regulované infrastruktury (část 2.2.1.) i Kritéria rizikovosti dodavatele (část 2.2.2.) by byly shodné s variantou II. Hlavní rozdíl této varianty a varianty II je ten, že ve variantě III prověřování probíhá na žádost přímého dodavatele ve správním řízení, přičemž prověřován není jenom žadatel – přímý dodavatel, který je smluvní stranou správce regulované strategické infrastruktury – nýbrž celý jeho relevantní dodavatelský řetězec.

2.3.1 Povinnosti povinného subjektu plošného mechanismu prověřování

Povinná osoba plošného mechanismu prověřování bezpečnostní spolehlivosti dodavatelů (dále jen „plošný mechanismus prověřování“) má povinnost pro bezpečnostně relevantní dodávky využívat pouze dodavatele, resp. dodavatelské řetězce, které byly vyhodnoceny jako bezpečnostně spolehlivé. Pokud byl dodavatel, resp. jeho dodavatelský řetězec, identifikován jako potenciálně bezpečnostně rizikový, v případě využití jeho bezpečnostně relevantní dodávky musí povinný subjekt identifikovanou hrozbu reflektovat v analýze rizik. Povinná osoba plošného mechanismu prověřování nemůže využívat bezpečnostně relevantních dodávek dodavatele, který byl identifikován jako vysoce rizikový, popř. v jehož relevantním dodavatelském řetězci byl identifikován vysoce rizikový poddodavatel.

Povinná osoba mechanismu má dále povinnost NÚKIB nahlašovat dodavatele, resp. dodavatelský řetězec, kterého pro bezpečnostně relevantní dodávky využívá.

Povinné osoby mechanismu jakožto povinné osoby podle ZKB podléhají ze zákona také kontrole NÚKIB. S ohledem na zachování principu efektivity a principu minimalizace nákladů bude kontrolní činnost související s mechanismem prověřování zařazena mezi standardní kontrolní činnost, kterou NÚKIB (Odbor kontroly) provádí a jejíž systém i metodika je nastavená a fungující.

Pokud by bylo v rámci kontroly u povinného subjektu plošného mechanismu prověřování zjištěno, že existuje orgán či osoba, kteří naplňují definici dodavatele, ale nebyl

povinným subjektem plošného mechanismu prověřování předložen k prověření, uloží NÚKIB předmětnému povinnému subjektu opatření k nápravě a též sankci za spáchání přestupku.

2.3.2 Proces posuzování dodavatele

Prověřování probíhá v této variantě na žádost dodavatele ve správním řízením vedeném NÚKIB, přičemž prověřován není jenom žadatel – přímý dodavatel, který je smluvní stranou správce regulované infrastruktury – ale celý jeho dodavatelský řetězec, který odpovídá definici bezpečnostně relevantní dodávky.

Pakliže by byl zvolen přístup, kdy by o prověření mohl zažádat jakýkoliv dodavatel, bylo by vysoce pravděpodobné, že by o prověření žádalo velké množství subjektů, které potenciál plnit bezpečnostně relevantní dodávku nemají. Jejich prověření by představovalo pro zapojené státní instituce nepřiměřenou zátěž. Motivací takových subjektů k podání žádosti o prověření by přitom mohlo být například zvýšení prestiže získáním statusu bezpečnostně spolehlivého dodavatele, aniž by však takový subjekt měl ve svém portfoliu produkty, které jsou způsobilé stát se součástí bezpečnostně relevantní dodávky.

Zahájení procesu prověřování by tudíž bylo podmíněno dvěma podmínkami:

a) bezpečnostní prověření dodavatele, resp. dodavatelského řetězce, je vázáno na konkrétní plánovanou bezpečnostně relevantní dodávku,

b) dodavatel, resp. dodavatelský řetězec, mají potenciál dodávku povinnému subjektu mechanismu poskytnout.

Po splnění podmínek[72] dodavatel zahájí správní řízení podáním žádosti o bezpečnostní prověření dodavatele, resp. svého dodavatelského řetězce.

Do procesu prověřováváni a správního řízení jsou zapojeny tyto orgány státu: NÚKIB, FAÚ, MPO, MV, MZV, NBÚ, NSZ, PČR, ÚOHS a zpravodajské služby ČR. Tyto státní orgány shromažďují informace o rizikovosti orgánů a osob z hlediska ochrany bezpečnosti ČR, veřejného pořádku a dodržování práv třetích osoba za tímto účelem prověřují naplnění kritérií rizikovosti dodavatele. Orgány státu poskytují součinnosti a informace NÚKIB ke zhodnocení a rozhodnutí. NÚKIB na základě obdržených informací vyhodnotí (ne)naplnění kritérií rizikovosti a vydá rozhodnutí. Rozhodnutí by bylo veřejné a obsahovalo by jeden ze tří následujících závěrů:

1. nebylo identifikováno riziko spojené s prověřovaným dodavatelem
   - v tomto případě bude prověřovanému subjektu umožněno uskutečňovat bezpečnostně relevantní dodávky bez dalších omezení,
2. prověřovaný dodavatelem byl vyhodnocen jako potenciálně bezpečnostně rizikový
   - v tomto případě bude využití prověřovaného subjektu pro uskutečňování bezpečnostně relevantní dodávky podmíněno reflektováním identifikované hrozby v analýze rizik povinné osoby mechanismu,
3. prověřovaný dodavatelem byl vyhodnocen jako vysoce bezpečnostně rizikový
   - v tomto případě nebude dodavateli umožněno podílet se na bezpečnostně relevantní dodávce.

[72] Dodavatel doloží splnění podmínek prostřednictvím čestného prohlášení jednoho z povinných subjektů.

Lhůta celého správního procesu od podání žádosti až do vydání správního rozhodnutí je stanovena na maximálně 4 měsíce. Tato lhůta byla stanovena na základě porovnání přístupů k prověřování dodavatelů v okolních státech a také s ohledem na vyvážený přístup, který by na jedné straně měl ponechat dostatečný prostor pro jednotlivé instituce zapojené do procesu prověřování a na druhé straně by neměl zdržovat povinnou osobu při výběru dodavatele bezpečnostně relevantní dodávky. Navrhovaná lhůta je kompromisem těchto dvou přístupů. V každém případě by měla být zachována možnost prodloužení lhůty k vydání rozhodnutí v obzvláště složitých případech.

2.3.3 Přechodná doba

V momentě účinnosti zákonné úpravy dojde k bezpečnostnímu prověření všech dodavatelů (tedy přímých dodavatelů i dalších dodavatelů v dodavatelském řetězci), jejichž bezpečnostně relevantní dodávky povinné osoby v okamžiku nabytí účinnosti právní úpravy využívají. K prověření stávajících dodavatelů dojde obdobně také v případě, že se některý orgán či osoba nově stane povinným subjektem mechanismu.

Přechodná doba má za cíl stanovit takové časové období, během kterého dojde k přirozené obnově technologického řešení v souvislosti s jeho ekonomickou životností, aby nedocházelo k nutnosti předčasného vyřazení bezpečnostně relevantních dodávek rizikových dodavatelů z provozu a v souvislosti s tím k vzniku nároků povinných subjektů mechanismu na náhradu nákladů spojených s předčasnou obměnou technologie.

2.4 Varianta IV: Mechanismus posuzování bezpečnostní spolehlivosti dodavatelů v sektoru elektronických komunikací

Varianta IV cílí na rozšíření pravomoci relevantních státních orgánů v oblasti kybernetické bezpečnosti tak, aby byl zaveden komplexní mechanismus posuzování bezpečnostní spolehlivosti dodavatelů do strategicky významné infrastruktury v sektoru elektronických komunikací, a to vč. možnosti omezování či zákazu využití dodavatelů, kteří budou vyhodnoceni jako rizikoví či vysoce rizikoví.

Sektor elektronických komunikací, resp. sítě elektronických komunikací představují kritickou infrastrukturu ČR, na jejichž dostupnosti je závislá celá řada služeb, stejně tak jako celá řada dalších odvětví. V současné době dochází k budování páté generace sítí elektronických komunikací (dále jen „5G sítě“). Význam této infrastruktury pro společnost je zcela zásadní a míra závislosti se v budoucnu bude nadále zvyšovat, a to zejména z důvodu digitalizace společnosti, vzniku nových technologií a jejich implementaci do nových ekosystémů. Ačkoliv debata o bezpečnosti dodavatelského řetězce a bezpečnosti a odolnosti nastupujících 5G sítí probíhá na mezinárodní úrovni již dlouho, zásadní posun v ní přineslo až varování před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation ze dne 16. prosince 2018, které vydal NÚKIB v rámci své pravomoci vydávat opatření podle ZKB. Toto varování reagovalo mimo jiné i na rostoucí využívání technologií rizikových dodavatelů ve strategické informační a komunikační infrastruktuře nezbytné pro chod státu. Dále byla v květnu 2019 uspořádána v ČR první globální konference (Prague 5G Security Conference) zabývající se tématem 5G sítí a dalších sítí budoucích generací, jakožto komunikační infrastrukturou strategického a bezpečnostního významu, které

státy musí věnovat pozornost. Na závěr této konference byly přijaty tzv. Pražské návrhy[73], jež jako první globální dokument shrnuly možné perspektivy a principy, které by státy měly brát v potaz při budování 5G sítí, a nabídly je celému mezinárodnímu společenství. Důležitým předpokladem pro bezpečné budování, zavádění a správu 5G sítí byla v dokumentu identifikována i důvěryhodnost dodavatele technologií.

V prvním pololetí roku 2019 byly zároveň přijaty závěry Evropské rady, na které navazovalo Doporučení Evropské komise (EU) 2019/534 ze dne 26. března, Kybernetická bezpečnost 5G sítí[74]. Tím byl nastartován proces koordinovaného přístupu k zajištění bezpečnosti 5G sítí v celé EU. Jedním z výsledků tohoto procesu bylo mimo jiné tzv. Koordinované posouzení rizik v oblasti kybernetické bezpečnosti sítí 5G ze zemí EU ze dne 9. října 201975 a následně 29. ledna 2020 i Sdělení Komise Evropskému Parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů k bezpečnému zavádění sítí 5G v EU – Implementace souboru opatření EU, kterým byl představen 5G EU Toolbox[76].

Na národní úrovni došlo v návaznosti na mezinárodní vývoj ve druhém a třetím čtvrtletí roku 2020 k vyhodnocení plnění všech opatření a podpůrných kroků z 5G EU Toolboxu. Pracovní skupinou složenou z relevantních státních institucí byla vyhodnocena jako významná zejména strategická opatření ke zmírnění rizik spojených s dodavateli SM03, SM05 a SM06, která se zaměřují na rizikový profil dodavatelů, rozmanitost dodavatelů a odolnost dodavatelsko-odběratelských vztahů. Jako jedno z prioritních strategických opatření k další implementaci bylo přitom identifikováno opatření SM03, které stanoví, aby byl posuzován rizikový profil dodavatelů a byla uplatňována omezení u dodavatelů považovaných za vysoce rizikové, včetně vyloučení těchto vysoce rizikových dodavatelů u klíčových aktiv. Opatření SM03 bylo vyhodnoceno jako částečně naplňované v prostředí ČR. Český právní řád disponuje nástroji, které mohou určitá rizika spojená s dodavateli, jež jsou považováni za rizikové, účinně snižovat. Neexistují však obecně závazná pravidla, která by posuzování rizikovosti či důvěryhodnosti dodavatele upravovala komplexně a jednoznačně.

I na základě výše uvedených dokumentů se začalo problematikou bezpečnosti dodavatelského řetězce 5G sítí zabývat vícero států po celém světě. Přístup k posuzování rizikového profilu dodavatelů a k problematice bezpečnosti 5G sítí obecně se přitom napříč státy liší. Některé státy, jako např. Velká Británie, Francie, Švédsko, Austrálie či Spojené státy americké, zvolily cestu přímého zákazu konkrétně identifikovaných vysoce rizikových dodavatelů technologií 5G, popř. dodavatelů do sektoru elektronických komunikací. Jiné státy, mezi něž patří například Německo, Belgie či Polsko, naopak zavedly či plánují zavést komplexní mechanismy pro prověřování a omezování dodavatelů ze strany státu, a to včetně posuzování kritérií vztahujících se k důvěryhodnosti dodavatele (tedy obdobně dle varianty II).

V únoru roku 2022 bylo vydáno také 5G doporučení. 5G sítě mají potenciál stát se digitální komunikační páteří naší ekonomiky a společnosti a umožnit rozvinutí a využití

[73] PRAGUE 5G SECURITY CONFERENCE. The Prague Proposals. The Chairman Statement on cyber security of communication networks in a globally digitalized world. 2019. Dostupné z: https://www.nukib.cz/en/infoservis-en/conferences/prague-5g-security-conference-2019/

[74] EVROPSKÁ KOMISE. Doporučení Komise (EU) 2019/534 ze dne 26. března 2019. Kybernetická bezpečnost sítí 5G. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32019H0534&from=EN

[75] NIS COOPERATION GROUP. EU coordinated risk assessment of the cybersecurity of 5G networks. 2019. Dostupné z: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132

[76] NIS COOPERATION GROUP. Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. 01/2020. Dostupné zde: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468

nových technologií do zcela nových ekosystémů. Dlouhodobě udržitelná bezpečnost a odolnost těchto sítí je strategickým zájmem státu i společnosti jako celku. Jedním ze zásadních předpokladů zajištění kybernetické bezpečnosti technologických řešení 5G sítí je bezpečnost dodavatelského řetězce. Hardware i software technologických řešení 5G sítí jsou již natolik komplexní, že snižovat rizika spojená s dodavateli 5G sítí pouze technickými prostředky je nedostatečné; zásadním faktorem je tudíž důvěryhodnost dodavatele. Významnou součástí kybernetické bezpečnosti 5G sítí je bezpečnost dodavatelského řetězce. V případě 5G sítí je z důvodu jejich vysoké komplexity a nákladnosti typickým fenoménem na trhu těchto technologií závislost odběratele, tedy subjektu budujícího a provozujícího 5G síť, na dodavateli technologie a jeho dodavatelském řetězci. Tato závislost s sebou přináší nové kybernetické hrozby a zvyšuje riziko spojené s některými stávajícími hrozbami, a to například možností implementovat do dodávaného technologického řešení zranitelnost, která umožňuje narušení důvěrnosti, dostupnosti nebo integrity přenášených dat. Důvěra v dodavatele a jím dodávaná technologická řešení je v tomto ohledu zásadní. Narušení kybernetické bezpečnosti 5G sítí, a to zejména jeho nejzávažnější případy, jako je narušení dostupnosti sítě ve velkém rozsahu vedoucí ke značným škodám či kybernetická špionáž, představuje podstatný problém jak pro významné ekonomické zájmy a bezpečnost státu, tak pro operátory a jejich uživatele. Vzhledem k roli, jakou budou 5G sítě v následujících letech hrát v souvislosti s rozvojem nových technologií, komunikačních ekosystémů a zvyšováním počtu připojených zařízení, by mělo naplnění výše uvedených hrozeb dalekosáhlé celospolečenské důsledky. Dlouhodobě udržitelná bezpečnost a odolnost těchto sítí je proto strategickým zájmem státu i společnosti jako celku.

Vzhledem k důležitosti a klíčovému postavení sítí elektronických komunikací pro fungování státu a vlivu na zajišťování národní bezpečnosti, tato varianta počítá se zavedením Mechanismu posuzování bezpečnostní spolehlivosti dodavatelů, ve stejné formě, jako je představena ve variantě II. Jediný rozdíl by byl rozsah povinných osob. Ve variantě IV na rozdíl od varianty II by se povinné osoby mechanismu omezily pouze na poskytovatele veřejně dostupné služby elektronických komunikací.

Na základě zhodnocení uvažovaných variant ve smyslu naplnění cíle regulace, kterým je omezit závislost strategicky významné infrastruktury ČR na rizikových dodavatelích představujících strategickou hrozbu v oblasti kybernetické bezpečnosti a přispět tak k v zajištění dlouhodobě udržitelné bezpečnosti a odolnosti strategicky významné infrastruktury, se jako zcela nevhodná jeví nulová varianta, jež je stanovenému cíli nevede. Nulová varianta, která ke stanovenému cíli nevede, je tedy vyřazena. Varianta II i varianta III směřují ke stanovenému cíli zcela a varianta IV ke stanovenému vede pouze částečně.

3 Vyhodnocení nákladů a přínosů

3.1 Identifikace nákladů a přínosů

V této části jsou formou kvalifikovaného odhadu vyčísleny a popsány náklady a přínosy jednotlivých variant, a to jak pro povinné osoby mechanismu, dodavatele, jichž se prověřování a případné omezené může dotknout, pro instituce zapojené do procesu posuzování, i pro stát a jeho obyvatele. Zejména pro vyčíslení nákladů pro instituce zapojené do procesu posuzování a pro povinné osoby mechanismu bylo využito dotazníkového šetření s cílem získání dat, která jsou předkladateli jinak nedostupná.

3.2 Náklady

3.2.1 Nulová varianta

Nulová varianta neřeší problémy, které jsou základním důvodem předložení věcného záměru. Jejím jediným přínosem je absolutní kontinuita současného stavu, která pochopitelně není spojena s novými přímými náklady na výkon veřejné správy.

Nepřijetí legislativních změn může přinést náklady spojené s náhradou či nápravou škod, které by vyplynuly z činnosti rizikového dodavatele, jenž by poškodil významnou strategickou infrastrukturu ČR. V první řade je nutné zmínit nevyčíslitelnou strategickou hrozbu v podobě závislosti na rizikových dodavatelích či přítomnosti technologií vysoce rizikových dodavatelů ICT této infrastruktuře. Může také dojít k omezení volnosti strategického rozhodování ČR, kdy bude nutné vzít v potaz možnost zneužití přítomnosti rizikových dodavatelů cizím státem, což může zamezit strategické autonomii ČR.

Dále lze idenfitikovat vznik nepřiměřených finančních dopadů pro ČR a subjekty působící v její jurisdikci ze sanace kybernetických incidentů, což s sebou může přinášet náklady pohybující se v řádech miliónů, a to na základě možného výskytu vícero závažných zranitelností a tím k navýšení počtu kybernetických incidentů a útoků ze strany států nebo státem sponzorových kriminálních aktérů, které mohou zneužívat svého vlivu nad dodavateli operujícími pod jejich jurisdikcí. Tito dodavatelé poskytující hardware či software do strategické infrastruktury ČR mohou cíleně narušit důvěrnost, integritu a dostupnost dat. Mezi náklady spojené s nulovou variantou by mohly náležet škody způsobené nečinností státu v oblasti zajišťování kybernetické bezpečnosti ze strany rizikových dodavatelů. Z veřejně dostupných informací a dat např. vyplývá, že škody kybernetického útoku na nemocnici Rudolfa a Stefanie Benešov z roku 2019 byly vyčísleny na více než 23 milionů Kč[77], kybernetický útok na Fakultní nemocnici Brno z roku 2020 měl za důsledek škody v řádech desítek milionů Kč.[78] Kybernetický útok v roce 2022 na Ředitelství silnic a dálnic způsobil škody v minimální hodnotě 30 milionů Kč.[79] Ekonomické vyčíslení škod ovšem nejsou jedinými dopady kybernetických útoků na strategickou infrastrukturu státu. V zahraničí jsou již známy případy, kdy v důsledku kybernetického útoku nemohla nemocnice v Düsseldorfu poskytnout péči pacientovi, což mělo za důsledek i škodu na lidském životě.[80]

V neposlední řadě je nutné zmínit možné poškození reputace ČR, která je dlouhodobě v Evropě považována za vedoucí stát v oblasti kybernetické bezpečnosti.

[77] ČTK. Benešovská nemocnice získá 12,5 milionů na úhradu nákladů spojených s kyberútokem. Dostupné z: https://www.seznamzpravy.cz/clanek/regiony-zpravy-stredocesky-kraj-benesovska-nemocnice-ziska-125-milionu-na-uhradu-nakladu-spojenych-s-kyberutokem-182158

[78] ČTK, IDNES.CZ. Kybernetický útok stál nemocnici v Brně desítky milionů, klesly odběry krve. Dostupné z: https://www.idnes.cz/brno/zpravy/fakultni-nemocnice-brno-kyberneticky-utok-skody-odber-krve.A200417_093436_brno-zpravy_krut

[79] ČTK. Obnova systémů ŘSD po kyberútoku stála desítky milionů. Brzy má opět fungovat i web s dopravními informacemi. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3518463-obnova-systemu-rsd-po-kyberutoku-stala-desitky-milionu-brzy-ma-opet-fungovat-i-web-s

[80] NOVINKY. Úmrtí kvůli hackerskému útoku? Byla to jen otázka času, míní bezpečnostní expert. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-umrti-kvuli-hackerskemu-utoku-byla-to-jen-otazka-casu-mini-bezpecnostni-expert-40337662

3.2.2 Varianta II

Při volbě druhé varianty vznikají přímé a nepřímé náklady na straně státu a povinných osob, a potenciální nepřímé náklady dodavatelů povinných osob.

Nový právní předpis rozšíří pravomoci relevantních státních orgánů v oblasti kybernetické bezpečnosti tak, aby byl zaveden komplexní mechanismus posuzování bezpečnostní spolehlivosti dodavatelů do strategicky významné infrastruktury napříč jejími sektory, a to vč. možnosti omezování či zákazu využití dodavatelů, kteří budou vyhodnoceni jako rizikoví či vysoce rizikoví. V pro zabezpečení výkonu těchto nových pravomocí bude nutné přijmout jednotky až nízké desítky nových pracovníků pro posuzování rizikovosti a prověřování rizikových dodavatelů. Mechanismus posuzování je ovšem navržen tak, aby v maximální možné míře využíval již stávajících kapacit jednotlivých státních orgánů, které jsou v současnosti využívány pro posuzování

Ve vztahu k návrhu zákona lze předpokládat nutnost vyhrazení jednotek až nízkých desítek tabulkových míst u zapojených organizačních složek státu a rozšíření stávajících či připravovaných informačních systémů k technické obsluze procesu prověřování. Na straně NÚKIB a spolupracujících institucí budou muset být vynaloženy náklady související s rozšířenými pravomocemi státních orgánů tak, aby mohlo docházet k systematickému a koordinovanému prověřování dodavatele do strategicky významné infrastruktury. V souladu s principem efektivity a cílem minimalizace ekonomických nákladů se bude maximálně využívat fungující synergie s již existujícími agendami a procesy, jakými jsou kupříkladu prověřování žadatelů o zápis do katalogu poskytovatelů služeb cloud computingu orgánům veřejné správy či prověřování zahraničních investorů dle zákona o prověřování zahraničních investic, a to včetně účelného využívání informačních systémů, které tyto agendy podporují.

Noví pracovníci NÚKIB a spolupracujících institucí budou dle nařízení vlády č. 222/2010 Sb., o katalogu prací ve veřejných službách a správě, ve znění pozdějších předpisů, provádět šetření rizikových dodavatelů a tuto rizikovost vyhodnocovat.

Náklady vzniknou také povinným osobám mechanismu. S ohledem na návaznost procesů spojených s mechanismem prověřování na stávající procesy, které povinné osoby podle ZKB mají již v současnosti povinnost provádět, jako je identifikace a hodnocení aktiv, analýza rizik apod., dochází k minimálnímu zásahu, a tedy i k minimálnímu vzniku dodatečných nákladů při zavádění nové regulace do právních předpisů. Nové povinnosti povinných osob mechanismu budou sestávat z povinnosti NÚKIB hlásit přímé dodavatele bezpečnostně relevantních dodávek, vynaložit přiměřené úsilí ke zjišťování nepřímých dodavatelů bezpečnostně relevantních dodávek a zjištěné nepřímé dodavatele taktéž hlásit NÚKIB. Tyto nové povinnosti generují na straně povinných osob mechanismu minimální administrativní náklady.

Potenciální významnější náklady povinným osobám mechanismu generuje povinnost dodržovat opatření vydaná NÚKIB. V případě vydání varování podle ZKB se bude jednat o reflexi identifikované hrozby v analýze rizik, což je opět proces, který je u povinných osob mechanismu již nastavený a fungující. Případný zákaz dodavatele má potenciální vysoký dopad na povinné osoby. Pokud by povinná osoba identifikovaného zakázaného vysoce rizikového dodavatele využívala v bezpečnostně relevantní dodávce, bude muset takového dodavatele ze

své infrastruktury vyloučit. Z dotazníkového šetření[81] plyne, že vyloučení a nahrazení významného dodavatele může pro povinnou osobu mechanismu generovat náklady až ve výši[82] jednotek milionů Kč (3 % respondentů), desítek milionů Kč (34 % respondentů), stovek milionů Kč (16 % respondentů). Tyto náklady spočívají ve výměně stávajícího řešení, pořízení nového řešení a jeho integraci mezi stávající infrastrukturu a procesy, přičemž vždy ale bude záležet o jakého dodavatele se jedná a jaké podmínky nabízí dodavatelé alternativní. 22 % respondentů uvedlo, že vyloučení takového dodavatele nebude mít žádný dopad. 25 % respondentů uvedlo náklady vyšší než 1 miliarda Kč, nicméně náklady byly vyčísleny na takové výše z důvodu, že dané orgány či osoby uvažovaly o vyloučení dodavatelů, kteří jako jediní jsou schopni dané plnění poskytnout. Do kalkulace nákladů tak započítávali mj. dopady ukončení či omezení poskytování regulované služby, vč. ušlého zisku. Pro případ unikátnosti dodávky daného vysoce bezpečnostně rizikového dodavatele NÚKIB umožňuje v rámci procesu připomínkování návrhu OOP povinným osobám mechanismu tento fakt NÚKIB sdělit. V případě dostatečného odůvodnění a podložení tvrzení důkazy může NÚKIB udělit výjimku pro typovou bezpečnostně relevantní dodávku a povinným osobám mechanismu za podmínek reflektování identifikované hrozby v analýze rizik umožní bezpečnostně relevantní dodávku využívat i nadále, čímž jsou případné náklady plynoucí ze zákazu takového dodavatele pro povinnou osobu minimalizovány. Jelikož tedy navrhovaná právní úprava pro případy existence jediného možného dodavatele poskytujícího bezpečnostně relevantní dodávku umožňuje získat výjimku ze zákazu takového dodavatele pro danou bezpečnostně relevantní dodávku, s generací respondenty udaných vysokých nákladů (vyšších než 1 miliardu Kč) předkladatel nepočítá.

56 % respondentů[83] jako nejzávažnější možný dopad na poskytování služby identifikuje omezení či ukončení poskytování služby. Právě riziko ohrožení poskytování regulované služby podstatným způsobem také umožňuje poskytovateli regulované služby zažádat o výjimku ze zákazu plnění identifikovaného vysoce rizikového dodavatele. Pro dalších 32 % respondentů jsou nejzávažnější dopady ty finanční a 12 % respondentů v případě aplikace lhůty respektující ekonomickou životnost daného aktiva vyloučení stávajícího dodavatele identifikuje s absencí dopadů vyšších než ty, které jsou s obnovou technologie a přechodem na alternativní technologická řešení standardně spojena.

V případě, že povinná osoba vysoce rizikového dodavatele v současnosti nevyužívá, nicméně v budoucnu by o bezpečnostně relevantních dodávkách tohoto dodavatele uvažovala, z důvodu vyloučení možnosti bezpečnostně relevantní dodávku od vysoce rizikového dodavatele pořídit může docházet k obdržení vyšší ceny od alternativních dodavatelů dodávek. Tento přístup a zvýšené náklady se mohou objevit obzvláště v případě, že na trhu není dostatečná konkurence a danou dodávku poskytuje pouze omezený počet dodavatelů.

[81] Dotazníkové šetření bylo adresovaného všem orgánům a osobám dle § 3 c), d), f) a g) zákona o kybernetické bezpečnosti (odesláno prostřednictvím datové schránky 1. 11. 2022 s žádostí o sdílení vyplněného dotazníku do 30. 11. 2022). Následně NÚKIB vyhodnotil odpovědi orgánů a osob, kteří se stanou poskytovateli regulované služby v režimu vyšších povinností, kterým plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, přičemž některé orgány či osoby spravující či provozující více systémů poskytli odpovědi za každý takový systém zvlášť. NÚKIB obdržel 65 takových odpovědí (dále jen „respondenti“).

[82] Na otázku uvedení maximálního finančního dopadu na zastupovanou organizaci v případě zákazu využívání plnění nejvýznamněji zastoupeného významného dodavatele dle § 2 písm. n) vyhlášky o kybernetické bezpečnosti po uplynutí ekonomické životnosti poskytovaného aktiva obdržel NÚKIB 32 odpovědí, které lze kvantifikovat.

[83] Na tento dotaz poskytlo odpověď 64 respondentů.

V neposlední řadě varianta II přináší dodatečné nepřímé náklady taktéž dodavatelům bezpečnostně relevantních dodávek. V případě vyloučení vysoce bezpečnostně rizikového dodavatele z možnosti poskytovat bezpečnostně relevantní dodávky do strategicky významné infrastruktury dojde k omezení hospodářské soutěže. Takový dodavatel nicméně i nadále může poskytovat ostatní dodávky do strategické infrastruktury, stejně tak jako dalším subjektům v ČR. Tato varianta nicméně nevyžaduje iniciativu či jinou součinnost od dodavatelů.

Vzhledem k tomu, že varianta II nevyžaduje ex ante prověření všech dodavatelů, resp. dodavatelských řetězců do strategicky významné infrastruktury, minimalizuje také nároky na personální a administrativní kapacity státu i soukromého sektoru, jakož i zásah prověřování do podnikatelských procesů, nehrozí tedy zdržení investic a zpomalení rozvoje z důvodu zpomalení výběrových řízení.

3.2.3 Varianta III

Náklady varianty III jsou ve srovnání s variantou II pro všechny dotčené subjekty vyšší. Všechny náklady identifikované ve variantě II jsou přenositelné do varianty III, přičemž varianta III přináší také další náklady.

Vzhledem k tomu, že proces prověřování probíhá ex-ante před poskytnutí bezpečnostně relevantní dodávky každým novým dodavatelským řetězcem, nároky na intenzitu prověřování jsou výrazně vyšší. Zátěž bude extrémně vysoká především na začátku účinnosti tohoto zákonného předpisu, jelikož do předem stanovené lhůty bude nutné prověřit všechny stávající dodavatelské řetězce, které momentálně poskytují bezpečnostně relevantní dodávky do strategicky významné infrastruktury státu. Tato varianta tak předpokládá velmi vysoké personální a administrativní nároky na stát z důvodu vedení velkého a nepředvídatelného množství správních řízení a z toho možné plynoucí náhrady škody za nesprávný úřední postup z důvodů nesplnění zákonných lhůt.

Náklady na straně státu by tak byly značně zvýšené.

Zvýšené nároky byly taktéž na dodavatele bezpečnostně relevantních dodávek. Ti by jakožto prerekvizitu pro poskytování bezpečnostně relevantních dodávek museli získat „certifikaci“ jak sebe sama, tak každého dodavatelského řetězce, který by využívali pro poskytování bezpečnostně relevantních dodávek. Varianta III klade vysoké nároky co do poskytovaných informací o samotném přímém dodavateli, ale i o jeho poddodavatelích. Tento certifikační proces zvyšuje bariéry trhu.

Varianta III má také výraznější dopady a náklady na povinné osoby mechanismu. Povinnost využívat pouze certifikované dodavatele, resp. dodavatelské řetězce pro poskytování bezpečnostně relevantních dodávek má značný dopad na podnikatelské procesy povinných osob mechanismu. Dojde k prodloužení kontraktačního procesu a dalších procesů souvisejících s pořizováním nových bezpečnostně relevantních dodávek vč. zpomalení výběrových řízení a v důsledku toho může dojít ke zdržení investic a zpomalení rozvoje, což může způsobit také časové prodlení při realizaci výstavby dané strategicky významné infrastruktury.

3.2.4 Varianta IV

Náklady varianty IV jsou zcela shodné s náklady varianty II. Jediný rozdíl mezi těmito dvěma variantami je v rozsahu povinných osob mechanismu, kdy varianta IV reguluje pouze

sektor elektronických komunikací. Náklady se tak budou dotýkat menšího počtu povinných osob mechanismu i dodavatelů.

Dále budou i menší náklady na straně státu, jelikož bude posuzován značně menší počet dodavatelů, a to vzhledem k tomu, že povinnými osobami mechanismu dle varianty IV jsou pouze jednotky subjektů. Náklady na straně státu by tak byly sníženy zhruba na desetinu nákladů Varianty II.

3.3 Přínosy

3.3.1 Nulová varianta

K této variantě se z hlediska dosažení cíle regulace nepojí žádné přínosy.

3.3.2 Varianta II

Přínos této varianty spočívá v přijetí komplexního Mechanismu posuzování dodavatelů, jenž umožní NÚKIB na základě zákonného zmocnění omezit či vyloučit z vymezených dodávek povinných osob mechanismu takové dodavatele, kteří budou vyhodnoceni jako rizikoví, v důsledku čehož dojde ke snížení dopadu negativních zahraničních vlivů na zajištění základních funkcí státu prostřednictvím dodávek technologií.

Realizace varianty II přispěje ke stabilitě a zabezpečení poskytování služeb jednotlivých strategických sektorů, a také k zajištění dlouhodobě udržitelného zabezpečení a odolnosti infrastruktury, jež je nezbytná pro naplňování základních funkcí státu. Dojde k omezení závislosti strategicky významné infrastruktury ČR na rizikových dodavatelích představujících strategickou hrozbu v oblasti kybernetické bezpečnosti. Dojde tak také k významnému omezení možnosti negativního zahraničního působení na zajištění základních funkcí státu prostřednictvím zneužití závislosti v dodavatelsko-odběratelských vztazích, jako je proprietární uzamčení odběratele, tzv. vendor lock-in, nevynucené omezení dodávek či zneužití infrastruktury nebo neoprávněný zásah do ní.

Dále díky intenzivnějšího informování povinných osob mechanismu o hrozbách spojených s rizikovými dodavateli bude realizace varianty II přispívat k tomu, že povinné osoby začnou i samy klást vyšší důraz na bezpečnost, a to vč. aspektů rizikovosti, které posuzuje stát. Tato varianta má také ambici změnit přístup samotných povinných osob k výběru dodavatelů. Povinné osoby by měly klást vyšší důraz na bezpečnost a nižší důraz pouze na pořizovací cenu ICT produktů a služeb. Dodavatelé, kteří budou nabízet bezpečná ICT řešení, a to jak z pohledu technického, tak strategického, by tak získávali konkurenční výhodu oproti dodavatelům, kteří nejsou schopni takové záruky poskytnout.

3.3.3 Varianta III

Přínos této varianty spočívá v přijmutí komplexního Mechanismu posuzování dodavatelů, jenž umožní NÚKIB na základě zákonného zmocnění omezit či vyloučit z vymezených dodávek povinných osob mechanismu takové dodavatele, kteří budou vyhodnoceni jako rizikoví, v důsledku čehož dojde ke snížení dopadu negativních zahraničních vlivů na zajištění základních funkcí státu prostřednictvím dodávek technologií. To přispěje ke stabilitě a zabezpečení poskytování služeb jednotlivých strategických sektorů, a také k zajištění

dlouhodobě udržitelného zabezpečení a odolnosti infrastruktury, jež je nezbytná pro naplňování základních funkcí státu.

Přínosem této varianty je taktéž to, že do vymezené strategicky významné infrastruktury nebudou mít přístup žádní dodavatelé, kteří nebudou předem systematicky a předvídatelně prověřeni.

3.3.4 Varianta IV

Přínos této varianty spočívá v přijmutí komplexního Mechanismu posuzování dodavatelů, jenž umožní NÚKIB na základě zákonného zmocnění omezit či vyloučit z vymezených dodávek povinných osob mechanismu takové dodavatele, kteří budou vyhodnoceni jako rizikoví, v důsledku čehož dojde ke snížení dopadu negativních zahraničních vlivů na zajištění základních funkcí státu prostřednictvím dodávek technologií. To přispěje ke stabilitě a zabezpečení poskytování služeb v sektoru elektronických komunikací, a také k zajištění dlouhodobě udržitelného zabezpečení a odolnosti infrastruktury v sektoru elektronických komunikací, jež se podílí na naplňování základních funkcí státu.

Dále díky intenzívnějšího informování povinných osob mechanismu o hrozbách spojených s rizikovými dodavateli bude realizace varianty II přispívat k tomu, že povinné osoby začnou i samy klást vyšší důraz na bezpečnost, a to vč. aspektů rizikovosti, které posuzuje stát. Tato varianta má také ambici změnit přístup samotných povinných osob k výběru dodavatelů. Povinné osoby by měly klást vyšší důraz na bezpečnost a nižší důraz pouze na pořizovací cenu ICT produktů a služeb. Dodavatelé, kteří budou nabízet bezpečná ICT řešení, a to jak z pohledu technického, tak strategického, by tak získávali konkurenční výhodu oproti dodavatelům, kteří nejsou schopni takové záruky poskytnout.

4 Stanovení pořadí variant a výběr nejvhodnějšího řešení

Varianta I – Zachování současného stavu neumožňuje dosažení cílového stavu, neřeší definovaný problém a ponechává tím prostor pro jeho další prohloubení.

Varianta II – Mechanismus posuzování bezpečnostní spolehlivosti dodavatelů ve strategicky významné infrastruktuře adresuje navrhovaný problém v celé jeho šíři a dosahuje cílového stavu. Zároveň minimalizuje dodatečné náklady dotčených subjektů spojené s navrhovanou právní úpravou, čímž zachovává proporcionalitu mezi dosažením cílového stavu a minimalizací zásahu do práv osob.

Varianta III – Mechanismus plošného posuzování bezpečnostní spolehlivosti dodavatelů ve strategicky významné infrastruktuře navrhovaný problém adresuje v celé jeho šíři a dosahuje cílového stavu. Na druhou stranu ovšem přináší významné zvýšení nákladů jak na straně státu, tak na straně ostatních dotčených subjektů.

Varianta IV – Mechanismus posuzování bezpečnostní spolehlivosti dodavatelů v sektoru elektronických komunikací adresuje definovaný problém pouze částečně, a to ve vybraném sektoru elektronických komunikací. Nemá tak potenciál plně dosáhnout požadovaného cílového stavu, ačkoliv k jeho plnění přispívá za vynaložení minimálních nákladů.

S ohledem na míru naplnění požadovaného cílového stavu a minimalizaci nákladů s tím spojených se navrhuje přijmout variantu II.

5 Implementace a vynucování

Národní úřad pro kybernetickou a informační bezpečnost bude řídit proces prověřování důvěryhodnosti a rizikovosti dodavatelů do strategicky významné infrastruktury ve spolupráci se spolupracujícími státními orgány jakož i omezovat či vylučovat tyto rizikové dodavatele v rámci svých nově nabytých zákonných povinností.

6 Přezkum účinnosti

Vyhodnocení a přezkum účinnosti navrhovaného právního předpisu budou prováděny průběžně ve spolupráci s ostatními orgány veřejné moci a na základě přijatých dotazů veřejnosti a orgánů veřejné moci.

7 Konzultace a zdroje dat

V rámci příprav návrhu zákona byly s žádostí o konzultace, vyjádření a následnou spolupráci s podílením se na procesu posuzování bezpečnostní spolehlivosti dodavatelů osloveny tyto státní orgány: FAÚ, MPO, MV, MZV, NBÚ, NÚKIB, NSZ, PČR, ÚOHS a zpravodajské služby ČR.

Vybraným organizačním složkám státu byl představován mechanismus posuzování dodavatelů v několika fázích přípravy, přičemž došlo na vzájemné sdílení informací a připomínek jak k dílčím částem mechanismu - tzn. právní, strategická i technická stránka – tak k jeho funkčnímu celku. Vybrané státní orgány dále poskytly cenné podklady v podobě informací z hlediska pracovních kapacit a celkových nákladů souvisejících s fungováním a podílením se na mechanismu posuzování dodavatelů, a to formou vyplňování relevantních dotazníků Úřadu.

Problematika právních, strategických, politických a dalších aspektů mechanismu rizikovosti dodavatelů, včetně návrhů možných řešení byla také v rámci otevřených diskuzí konzultována s akademickou obcí (například Masarykova univerzita), zájmovými svazy, komorami a soukromým sektorem (například sdružení právnických osob CZ.NIC). Pro potřeby dopadů regulace a mechanismu jako takového na regulované subjekty Úřad dále oslovil zástupce širokého spektra subjektů[84] s žádostí o poskytnutí informací do dotazníků k dopadům připravované regulace. Pro potřeby identifikace těchto dopadů se vyjádřili zástupci odvětví, jako jsou odvětví energetické, odvětví dopravní, bankovnictví včetně infrastruktury finančních trhů, zdravotnictví, vodohospodářství, digitální infrastruktura, chemický průmysl, potravinářství a zemědělství, komunikační a informační systémy, nouzové služby a veřejná správa.

Problematika mechanismu rizikovosti dodavatelů byla rovněž konzultována a diskutována na mezinárodním poli s relevantními úřady (analogie Národního úřadu pro kybernetickou a informační bezpečnost) převážně Německa, Spojeného království či

[84] Dle § 3 zákona o kybernetické bezpečnosti z těch odvětví, ve kterých je určený regulovaný systém dle vyhlášky č. 437/2017 Sb. a nařízení vlády č. 432/2010 Sb.

Spojených států amerických, které vzhledem ke své expertíze a svým mechanismům ochrany dodavatelských řetězců poskytly významné informace a zkušenosti s nastavováním mechanismu rizikovosti dodavatelů.

Jako relevantní zdroje použitelných dat posloužily zejména strategické dokumenty a dokumenty politik, zákonné či podzákonné předpisy a jiné koncepční dokumenty nebo zkušenosti relevantních států Evropské unie a NATO související s tamními obdobami mechanismů rizikových dodavatelů, jak v rozsahu telekomunikačního sektoru, tak i napříč bezpečnostně relevantními sektory obsahujícími kritickou informační infrastrukturu. Jako další písemné podklady využitelné k tvorbě mechanismu rizikovosti dodavatelů posloužily Soubor opatření EU pro kybernetickou bezpečnost sítí 5G (tzv. EU 5G Toolbox), Zvláštní zpráva Evropského účetního dvora č. 3/2022: Spouštění sítí 5G v EU a data Úřadu a spolupracujících organizačních složek státu.

Celková podoba budoucího právního rámce mechanismu a spolu s tím i budoucí rozsah úpravy byla také představena a konzultována skrz odborné semináře a konference, jakými byly:

Konference v Poslanecké sněmovně Parlamentu ČR na téma „Bezpečnost dodavatelského řetězce v sítích elektronických komunikací a další strategické infrastruktuře České republiky“ ze dne 13. července 2022, konference „CyberCon 2022“ ze dnů 13. – 15. září 2022, konference CEVRO institutu k bezpečnosti dodavatelského řetězce v sítích elektronických komunikací v České republice ze dne 20. září 2022, konference v Poslanecké sněmovně Parlamentu ČR k budování 5G sítí ze dne 19. října 2022, konference EU Secure and Innovative Digital Future ze dnů 3. - 4. listopadu 2022 či Seminář k bezpečnosti dodavatelského řetězce ze dne 7. prosince 2022.

Národní úřad pro kybernetickou a informační bezpečnost rovněž opakovaně vyzýval odbornou i širokou veřejnost k zasílání podnětů týkajících se mechanismu rizikovosti dodavatelů, ať už formou připomínek v rámci dotazníků, možnosti účastnit se a diskutovat na konferencích či odborných seminářích k mechanismu rizikovosti dodavatelů, tak prostřednictvím plošné konzultace s širokou veřejností, na jejímž základě vzniklo mnoho podkladů pro konečné úpravy mechanismu.

8 Kontakty na zpracovatele RIA