Připomínky k navrhované legislativní úpravě mechanismu prověřování bezpečnosti dodavatelského řetězce

A. Úvod

Dne 26. 1. 2023 zveřejnil Národní úřad pro kybernetickou a informační bezpečnost (dále jen „*NÚKIB*“) **návrh nového zákona o kybernetické bezpečnosti** (dále také jen „*nový ZKB*“), jakož i **8 vyhlášek** jej provádějících. Nutnost přijetí nové legislativní úpravy odůvodnil NÚKIB tím, že si přijetí směrnice NIS2[1] vyžádá provedení řady změn v oblasti regulace kybernetické bezpečnosti. Nicméně vedle uvedené transpozice směrnice NIS2 obsahují zveřejněné materiály rovněž návrh nové legislativy mechanismu prověřování rizikovosti dodavatelů, tj. problematika bezpečnosti dodavatelského řetězce (dále jen „*mechanismus*“).

Z hlediska přijetí mechanismu jsou vedle nového zákona o kybernetické bezpečnosti samého zejména důležité tyto 4 vyhlášky:

- vyhláška o regulovaných službách;
- vyhláška o nepominutelných funkcích stanoveného rozsahu (dále jen „*vyhláška o nepominutelných funkcích*“);
- vyhláška o kritériích rizikovosti dodavatele;
- vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

K předloženým legislativním návrhům může veřejnost prostřednictvím formuláře předkládat připomínky, a to do 26. 2. 2023.

B. Povinné osoby mechanismu

Kritéria pro určení povinné osoby mechanismu (dále jen „***povinné osoby***“), jakož i **nepominutelné funkce** stanoveného rozsahu a **kritéria rizikovosti dodavatele** a způsob jejich vyhodnocení **stanoví výše uvedené prováděcí předpisy - vyhláška** o kritériích rizikovosti dodavatele, vyhláška o regulovaných službách a vyhláška o nepominutelných funkcích. V této souvislosti je třeba zmínit, že uvedené **vyhlášky vydává sám NÚKIB**, **a tedy je to i NÚKIB kdo o nastavení uvedených kritérií rozhoduje a může je měnit**.

Navrhovaný mechanismus se má primárně vztahovat pouze na ty poskytovatele regulovaných služeb v režimu vyšších povinností, jejichž služby jsou výslovně uvedeny ve vyhlášce o regulovaných službách (jejím

[1] směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148.

§ 6) – **povinnou osobou se však může stát i osoba** v režimu vyšších povinností, **kterou takto NÚKIB určí svým rozhodnutím** (v případě, že by narušení bezpečnosti informací poskytovatele regulované služby mohlo způsobit závažný dopad na bezpečnost České republiky nebo vnitřní či veřejný pořádek – viz § 6 odst. 2 vyhlášky o regulovaných službách). Kompetence NÚKIB v oblasti stanovení regulovaných služeb a poměrů jejich poskytovatelů jsou značné – při splnění podmínek dle § 4 vyhlášky o regulovaných službách může sám ze své činnosti vyhodnotit naplnění kritérií pro určení regulované služby a službu určit vydáním rozhodnutí. Může také poskytovateli regulované služby změnit režim z nižších povinností na režim vyšších povinností[2].

Mechanismus má být použit v případě těch aktiv, která jsou:

1) v zákonem **stanoveném rozsahu** řízení kybernetické bezpečnosti[3], a
2) jsou tzv. **kritickou částí stanoveného rozsahu** – nový ZKB je blíže definuje jako:
    a. aktiva, u kterých poskytovatel regulované služby v režimu vyšších povinností postupem podle vyhlášky o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností (příloha č. 1 vyhlášky) ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah úrovní vysoká nebo kritická, nebo
    b. jsou to aktiva, která zajišťují nepominutelné funkce stanoveného rozsahu (tyto upravuje vyhláška o nepominutelných funkcích – vyhláška se primárně soustředí na ICT sektor).

V důvodové zprávě k vyhlášce o kritériích rizikovosti dodavatele a vyhlášky o nepominutelných funkcích lze nalézt zmínku o tom, že **povinných osob dle mechanismu by mělo dle předpokladu být cca <u>150</u>**. Současně však důvodová zpráva k vyhlášce o nepominutelných funkcích ale uvádí, že: „*Je možné, že přímo v souvislosti s navrhovanou vyhláškou dojde k rozšíření kritické části stanoveného rozsahu povinných osob mechanismu v sektoru elektronických komunikací. Z toho plyne možné rozšíření počtu dodavatelů, kteří budou moci mechanismu posuzování dodavatelů podléhat a kteří budou moci být omezeni.*“ (viz s. 5) – **<u>uvedené číslo 150 tedy není finální</u>**.

C. <u>Stručný postup využití mechanismu dle nového zákona o kybernetické bezpečnosti</u>

1) Povinné osoby (tj. primárně povinné osoby v režimu vyšších povinností NEBO osoby takto určené NÚKIB) **nahlásí NÚKIB splnění kritérií** pro identifikaci regulované služby[4], a to do 30 dnů ode dne, kdy zjistí, že došlo k naplnění k naplnění kritérií (nejpozději do 90 dnů, kdy k naplnění kritérií došlo).
2) NÚKIB provede **registraci** poskytovatele regulované služby, a to:
    - na základě nahlášení povinnou osobou;
    - na základě vlastního zjištění o naplnění kritérií, neprovede-li registraci povinná osoba ve lhůtě sama.

[2] § 5 odst. 3 vyhlášky o regulovaných službách.
[3] Viz Hlava II nového ZKB, § X Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby.
[4] Viz Hlava II nového ZKB, § X Registrace poskytovatele regulované služby.

Povinné osoby mechanismu jsou povinny zjišťovat informace o dodavatelích bezpečnostně významných dodávek a hlásit je prostřednictvím Portálu NÚKIB.[5] Zejména rizikovost těchto dodavatelů NÚKIB posléze hodnotí.

3) **NÚKIB shromažďuje a vyhodnocuje informace** a údaje spojené s orgánem nebo osobou, které se týkají možné hrozby pro bezpečnosti České republiky, vnitřního nebo veřejného pořádku nebo naplnění kritérií rizikovosti dodavatele.[6] NÚKIB pro tyto účely vychází jak z informací zjištěných v rámci vlastní činnosti, tak z informací, kterými disponují jiné orgány či osoby (tyto poskytují NÚKIB informace a součinnost[7] - vždy na žádost NÚKIBu, **NÚKIB si tedy sám volí, zda dotyčný orgán osloví**). Při hodnocení kritérií bere NÚKIB v úvahu také utajované a jiné neveřejné a citlivé informace.

   Při hodnocení rizik NÚKIB reflektuje kritéria stanovená vyhláškou o kritériích rizikovosti dodavatele, což jsou **strategická kritéria založená zejména na zemi původu dodavatele** (tj. jsou posuzovány z hlediska, zda je v zemi původu dodavatele demokratický politický systém, dělba moci, dodržována lidská práva, nezávislý soudní přezkum, není zde povinnost spolupráce se zpravodajskými službami apod.)[8].

4) NÚKIB je následně v rámci **omezení rizik**[9] oprávněn vydat **opatření obecné povahy (OOP)**, ve kterém stanoví podmínky nebo zakáže použití plnění dodavatele bezpečnostně důležité dodávky v kritické části stanoveného rozsahu (pokud zjistí možné významné ohrožení bezpečnost České republiky nebo vnitřní či veřejný pořádek v důsledku vyhodnocení kritérií rizikovosti dodavatele).

   - proti opatření obecné povahy **není možné podat opravný prostředek** (odvolání ani rozklad),
   - z podmínek nebo zákazu stanoveného opatřením obecné povahy může NÚKIB povolit **výjimku**, pokud by plnění OOP mohlo ohrozit poskytování regulované služby (výjimku však nepovolí, pokud by to zcela mařilo účel OOP) - řízení o výjimce probíhá pouze z moci úřední a výsledek se odvíjí od vlastního posouzení NÚKIB.

D. Problematické aspekty mechanismu

Jakkoli se z informací prezentovaných NÚKIB má jevit, že mechanismus je zcela komplementární a takřka bezproblémovou součástí nové právní úpravy připravované v souvislostí s implementací směrnice NIS2, není to pravdou. Rozhodnutí NÚKIB spojit v návrhu nového zákona o kybernetické bezpečnosti

[5] Detaily stanoví vyhláška o technických a organizačních podmínkách používání Portálu NÚKIB a požadavcích na úkony vykonávané prostřednictvím Portálu NÚKIB (vyhláška o Portálu NÚKIB).
[6] Viz Hlava II nového ZKB, § X Prověřování rizik spojených s dodavatelem.
[7] Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí, Ministerstvo vnitra, Nejvyšší státní zastupitelství, Policie České republiky, Národní bezpečnostní úřad, Úřad pro ochranu hospodářské soutěže, Finanční analytický úřad a zpravodajské služby České republiky. O poskytnutí informací či součinnosti může NÚKIB z téhož účelu požádat také jiné orgány či osoby.
[8] Jako problematické jsou v důvodové zprávě k vyhlášce o kritériích rizikovosti dodavatele (s. 2-3) výslovně zmíněna Čína (ČLR), Rusko (RF) a Írán.
[9] Viz Hlava II nového ZKB, § X Omezení rizik spojených s dodavatelem.

implementaci evropské směrnice NIS2 s obsahově nesouvisející a rozsah směrnice NIS2 překračující mechanismus prověřování bezpečnosti dodavatelských řetězců, může přímo ohrozit implementaci směrnice NIS2. V postupu NÚKIB lze zcela jasně shledávat účelovost spojení implementace směrnice NIS2 s implementací připravovaného mechanismu.

Tendenční postup NÚKIB potrhuje i skutečnosti, že zatímco implementační principy ke směrnici NIS2 NÚKIB s odbornou veřejností obsáhle sdílel, návrh úpravy mechanismu prověřování bezpečnosti dodavatelských řetězců a jeho konkrétní podoba byly oznámeny až 26. 1. 2023.

Navrhovaný mechanismus přitom bez řádného odůvodnění **zásadně přesahuje rámec implementované směrnice NIS2**, a to tak, že přijetí mechanismu by pravomoci NÚKIB rozšířilo do takové míry, že by se z něj stal svého druhu „superúřad“, jehož pravomoci by významně překračovaly jeho jemu příslušející vymezenou pozici ústředního správního úřadu, a dávaly mu pravomoci, které jinak náležejíc výlučně do gesce vlády, tajných služeb či ministerstva vnitra.

Návrh mechanismu jde do extrémní míry nad rámec směrnice NIS2, a to bez jakéhokoliv vysvětlení. Přitom cílem směrnice NIS2 je podporovat harmonizaci a standardizaci v oblasti kybernetické bezpečnosti na úrovni EU, což mechanismus zcela neguje. V této souvislosti zcela absentuje odůvodnění, proč by daná problematika nemohla být řešena mírnějším zásahem, než jaký představuje mechanismus. NÚKIB sám přitom nepředkládá a nedefinuje žádná konkrétní rizika či zranitelnosti, která by takový to zásah do základních lidských práv soukromých osob ospravedlňovala. Hovoří pouze o obecných hrozbách, které i přes to, že se pohybujeme v oblasti kybernetické bezpečnosti, blíže nerozvádí. Proč pro řešení těchto obecných hrozeb není současná úprava (či úprava stanovená směrnicí NIS2) dostačující, není řádně odůvodněno a je pouze stručně zmíněno, že navrhovaná úprava je v souladu se zásadou proporcionality – **konkrétní naplnění zásady proporcionality však není blíže osvětleno, zřejmě proto, že navrhovaná úprava zcela proporcionální není.**

Uvedený postup NÚKIB, kdy došlo k rozhodnutí spojit implementaci směrnice NIS2 se současným začleněním mechanismu do českého právního řádu, tak lze považovat za zcela nevhodný.

<u>Zásadní připomínky k předkládané legislativě v souvislosti s mechanismem lze shrnout následovně</u>:

1) **Mechanismus není a priori prostředkem k zajištění kybernetické bezpečnosti**

   Tato skutečnost je zřejmá již ze samotného textu nového zákona o kybernetické bezpečnosti. V § X odst. 1 Prověřování rizik spojených s dodavatelem je výslovně uvedeno:

   „*Úřad shromažďuje a vyhodnocuje informace a data spojená s orgánem či osobou, která se* ***týkají možné <u>hrozby</u> pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele*** *podle odstavce 4.(…)*“

A není to pouze výše uvedené ustanovení, které hovoří výlučně o hrozbě, nikoli kyberbezpečnostní či kybernetické hrozbě, ale celá pasáž nového ZKB upravující mechanismus prověřování bezpečnosti dodavatelského řetězce neobsahuje jedinou zmínku o kybernetické bezpečnosti.

O kybernetické bezpečnosti nehovoří ani text vyhlášky o regulovaných službách a ve vyhlášce o nepominutelných funkcích je kybernetická bezpečnost zmíněna pouze stručně v rámci popisu jedné nepominutelné funkce. V textu vyhlášky o kritériích rizikovosti dodavatele najdeme zmínku pouze v § 4: „*Pro vyhodnocení kritérií rizikovosti dodavatele podle § X odst. 4 [Prověřování rizik spojených s dodavatelem] zákona se dle zjištěných poznatků o naplnění jednotlivých kritérií dodavatelem určí hodnota rizikovosti dodavatele, která stanoví možnou kybernetickou hrozbu spojenou s dodavatelem nebo možné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku.(…)*“ I z tohoto znění je zřejmé, že mechanismus nesměřuje čistě k zajištění kybernetické bezpečnosti.

Z výše uvedeného je zřejmé, že mechanismus a priori není nástrojem kybernetické bezpečnosti, ale směřuje do sféry jiných bezpečnostních opatření, které ale nenáleží do gesce NÚKIB, ale spíše Ministerstva vnitra či tajných služeb. Jeho začlenění do nového ZKB tak nedává pojmově smysl a nesmyslné je též to, aby hlavním rozhodujícím orgánem byl NÚKIB, když jeho kompetence mají být právě v oblasti kybernetické bezpečnosti.

2) Kritéria rizikovosti dodavatelů nejsou primárně spojena s kybernetickou bezpečností

Jak v rámci přípravy mechanismu opakovaně uvedl NÚKIB, návrh mechanismu by měl vycházet z koncepce tzv. analýzy rizik. Analýzu rizik netvoří pouze identifikace hrozeb na straně dodavatele, kterou zmiňuje důvodová zpráva k novému ZKB, avšak také dalších 5 nezbytných kroků pro objektivní vyhodnocení rizik a efektivní zavedení **přiměřených bezpečnostních opatření**.
Analýzu rizik dle aktuálně účinné vyhlášky o kybernetické bezpečnosti (VKB) a mezinárodně uznávaných standardů tvoří následující kroky:

1) Identifikace aktiv (§ 5 písm. g) VKB „informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém“)
2) Identifikace hrozby (§5 písm. e) VKB: „potenciální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, která může způsobit škodu“)
3) Identifikace rizik (§5 písm. h) VKB: „rizikem možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu“)
4) Identifikace zranitelností (§5 písm. p) VKB: „slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami“)
5) Hodnocení rizik (§ 5 písm. h) VKB: „možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu“)
6) Řízení rizik (§ 5 písm. i) VKB: „řízením rizik činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik“)

NÚKIB teoreticky identifikoval hrozbu ve smyslu rizikového dodavatele. Součástí mechanismu však stále musí být identifikace aktiv, identifikace konkrétních rizik spojených s konkrétními dodavateli, identifikace zranitelností těchto aktiv, které může určitá hrozba využít, hodnocení rizik, kdy se hodnotí, zda konkrétní identifikovaná rizika mohou využít konkrétně identifikované zranitelnosti aktiv a způsobit škodu a v neposlední řadě **řízení rizik, kdy budou zavedena přiměřená bezpečnostní opatření ke zvládání rizik. Tímto způsobem je také zajištěno dodržení principu proporcionality.**

V současném znění mechanismu však NÚKIB na koncepci analýzy rizik zcela rezignuje. Blíže nedefinovanou hrozbu spojenou s dodavateli řeší jediným bezpečnostním opatřením, a to plošným zákazem daného dodavatele ve smyslu OOP. **NUKIB tak nemůže argumentovat, že řeší konkrétní rizika u konkrétních dodávek, když chce případně rizikové dodavatele plošně zakazovat.**

Je tak velmi reálné, že k potencionálně miliardovým škodám na straně povinných osob může dojít bez jakéhokoli posouzení toho, zda opravdu hrozí bezprostřední riziko, které nelze ošetřit jinak než plošným zákazem.

V této souvislosti je třeba podotknout, že kritéria pro posuzování rizikovosti dodavatelů nemají nic společného s kybernetickou bezpečností (např. dodržování lidských práv), jedná se čistě o geopolitická kritéria, která ač mohou mít význam v politických rozhodnutích vlády, nemohou hrát roli při řízení konkrétních rizik v oblasti kybernetické bezpečnosti. Připravovaný mechanismus je tak spíše nástrojem (geo)politickým než kyberbezpečnostním, byť se jako takový snaží prezentovat.

O to více je evidentní nelogické směšování výsostně kyberbezpečnostní normy NIS 2 s mechanismem, kdy se NÚKIB navíc nijak nezabývá otázkou, proč nově zavedená kyberbezpečnostní opatření v rámci NIS 2 nejsou dostatečným řešením obecných hrozeb spojených s dodavateli.

3) Vznik „superúřadu“ NÚKIB a překročení kompetencí NÚKIB jako ústředního správní úřadu

NÚKIB by se v návaznosti na předkládanou legislativu stal jakými „superúřadem“, který by měl mít kontrolu nad dodavatelským řetězcem kritických odvětví, která však on sám současně definuje a může jejich rozsah modifikovat dle svého uvážení. N**ÚKIB pro sebe v předkládaném návrhu totiž mj. požaduje pravomoc určovat napříč obory činnosti rozsah regulace a povinných osob vlastními vyhláškami, tj. bez širší diskuse a kontroly ze strany vlády anebo Parlamentu České republiky.** Do pravomoci NÚKIB by tak spadala možnost na základě vlastního uvážení omezovat či **zakazovat obchodní dodávky a transakce v oborech činností a týkající se dodavatelů a zemí, které by NÚKIB sám určil. Toto rozhodování, které hrozí arbitrárností, je nepřijatelné.**

Pokud by byla přijata právní úprava v předložené podobě, NÚKIB by přebíral kompetence vlády, když by ve své podstatě mohl určovat zahraniční politiku České republiky a zasahovat i do oblasti národní bezpečnosti (v rámci mechanismu by doslova určoval, které země jsou demokratické, a které nikoli). Úkolem NÚKIB je provádění činností v oblasti kybernetické bezpečnosti, v zákonem vymezených mantinelech, a v rámci regulované infrastruktury řízení regulovaných subjektů a nápomoc zvyšovat kybernetickou odolnost těchto subjektů. Určování zahraniční politiky (byť nepřímo) do jeho kompetencí nenáleží. Tímto **postupem by NÚKIB mohl zhoršit jak mezinárodní, tak hospodářské postavení České republiky.**

Pro ilustraci rozsahu nově navrhovaných kompetencí NÚKIB – tyto by tedy měly zahrnovat:

- **určení povinných osob mechanismu,**
- určení rozsahu mechanismu (sám NÚKIB avizuje, že se mechanismus bude rozšiřovat),
- určení posuzovaných dodavatelů,
- určení kritérií rizikovosti dodavatelů, na jejichž základě budou posuzováni,
- určení koho osloví pro poskytnutí informací pro hodnocení dodavatelů (a koho ne),
- vyhodnocení kritérií rizikovosti dodavatelů na základě vlastního uvážení,
- vydání OOP, proti němuž není přípustný řádný opravný prostředek.

Celý proces prověření, hodnocení a případného omezení či zakázání dodavatele je tak od počátku čistě ve výlučné režii NÚKIB.

4) Vágnost odůvodnění připravované legislativy

Lze shrnout, že argumentace NÚKIB v důvodových zprávách k připravované legislativě (to platí jak pro nový ZKB, tak prováděcí vyhlášky) je velmi vágní, obecné a většina uváděných údajů zůstává v rovině ničím nepodložených tvrzení.

Zveřejněný návrh mechanismu je překvapivý, nejasný a nevysvětluje hrozby (reálné hrozby, z nichž má NÚKIB obavu a odůvodňují zavedení nové regulace), zranitelnosti (tj. jak konkrétní hrozba může být realizována) ani rizika (tj. potenciální následky), kterým má nová regulace čelit. Problematické a zmatečné je také neustálé směšování kyberbezpečnostních rizik a strategických rizik tak, jak to zrovna vyhovuje argumentaci NÚKIB. Kupříkladu, tvrdí-li NÚKIB v důvodové zprávě k mechanismu (s.2), že: „*Právní sice umožňuje zjišťovat a vyhodnocovat informace o hrozbách v oblasti kybernetické bezpečnosti, NÚKIB ani ostatním státním orgánům, působícím v oblasti bezpečnosti, ale dává pouze velmi limitovanou 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 její realizací.*“, pak pokud jde o kybernetická rizika, tak již současná úprava zjištění těchto informací již umožňuje. Pokud jde o strategické a obecně bezpečnostní rizika, tato jsou v gesci tajných služeb, je tedy opravdu proporcionální zavedení nového mechanismu, jak NÚKIB tvrdí?

5) Netransparentnost

Rozhodování NÚKIB o potenciální rizikovosti dodavatelů je dle navržené úpravy zcela netransparentní. Problémem je v tomto směru **zejména jednostranný (možno až svévolný) způsob určování regulovaných odvětví, netransparentní hodnocení významu kritérií rizikovosti dodavatelů a zemí, utajování informací, z nichž se při rozhodování vychází, jakož i parametrů jejich hodnocení.**

NÚKIB v důvodové zprávě k vyhlášce o kritériích rizikovosti dodavatele (s.5) tvrdí, že *účelem zavedení kritérií je zajištění transparentnosti všech obecných hledisek, které mají význam pro posouzení, zda konkrétní dodavatel představuje hrozbu pro bezpečnost ČR nebo vnitřní či veřejný pořádek. Důraz je tak kladen nejen na význam hrozby plynoucí ze strany bezpečnostně rizikového dodavatele pro povinné osoby mechanismu, ale i pro bezpečnost státu jako takového*." Existence kritérií má dle názoru NÚKIB též posilovat právní jistotu dodavatelů a povinných osob tím, že stanovují, jaké skutečnosti stát považuje za významné pro posouzení rizikovosti dodavatele. V důsledku proto dojde k eliminaci úřední svévole a k vytvoření spravedlivého a transparentního procesu, jelikož k omezení dodavatele (ať už formou varování nebo opatření obecné povahy) může dojít jen při naplnění konkrétně stanovených kritérií.
V důvodové zprávě k mechanismu (s. 7) NÚKIB dokonce uvádí: „*Návrh zákona zmocní NÚKIB a další organizační složky státu k* ***identifikaci a vyhodnocení hrozeb plynoucí z dodavatelských řetězců*** *pro národní bezpečnost nebo veřejný pořádek. Zda jsou tyto hodnoty v ohrožení bude* ***vyhodnoceno na základě transparentních kritérií stanovených v prováděcím právním předpise – vyhlášce o kritériích rizikovosti dodavatele****, k prověřování kritérií bezpečnostní spolehlivosti dodavatelů povinných osob mechanismu, a to skrze vyhodnocování kritérií a případné omezování bezpečnostních rizik spojených s těmito dodavateli*."

Kritéria rizikovosti stanovená zejména vyhláškou o kritériích rizikovosti dodavatele, jakož i způsob vyhodnocení těchto kritérií, jsou ale zcela obecná, vágní a objektivně neměřitelná, **o tvrzené řádné transparentnosti hodnotících kritérií tak nelze ani uvažovat**. Řádná metodika vyhodnocení absentuje, lze si tedy i stěží představit, jak příslušný úředník bude například posuzovat, zda je v předmětné zemi zavedena dělba moci či zda je v dané zemi vykonávána státní moc pouze na základě zákona.

6) Nereflektování již zavedených bezpečnostní opatření, snižování kompetence povinných osob

NÚKIB v důvodové zprávě k návrhu mechanismu prověřování dodavatelského řetězce výslovně zpochybňuje erudici a odpovědnost povinných osob, když tvrdí, že: „*Nezřídka se navíc stává, že identifikovaná hrozba, před níž NÚKIB vydal varování podle ZKB, není v analýze rizik povinných osob podle ZKB dostatečně, či dokonce jakkoliv, reflektována. Podle výstupů z kontrol a auditů povinných osob prováděných podle 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 v analýze rizik náležitě zohledněno, často nejsou řízeny následné procesy a alokovány zdroje pro ošetření daného rizika doložitelné formou např. plánu zvládání rizik.“

Dále NÚKIB podotýká, že ze strany povinných osob prakticky nedošlo k reflexi Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice a obdobně není reflektováno ani varování vydané NÚKIB v prosinci 2018. Dle dostupných informací však nikdy ze strany klíčových operátorů nedošlo k pochybení či jakémukoliv postihu v souvislosti řízením aktiv, rizik či dodavatelů. Nicméně pokud NÚKIB tvrdí, že varování či doporučení pro hodnocení důvěryhodnosti dodavatelů nebyla reflektována patřičně, nabízí se otázka, jaké nápravné kroky v tomto směru učinil sám NÚKIB, aby dodržování zajistil**? NÚKIB takto v podstatě místo postupu dle účinné právní úprava zavádí „donucovací“ prostředek pro povinné osoby, které doporučující úkony NÚKIB reflektovaly způsobem, který se NÚKIB nezdá jako dostatečný (např. diverzifikace dodavatelů, což je jeden z kroků doporučených mj. i EU Toolboxem).**

7) Absence opravného prostředku proti OOP

Výstupem procesu prověřování bezpečnosti dodavatelských řetězců má být opatření obecné povahy (OOP) vydané NÚKIB, kterým NÚKIB povinným osobám dle mechanismus stanoví podmínky (tj. omezí) nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu. OOP je specifickým správním aktem na pomezí normativního a individuálního správního aktu, který má konkrétně určený předmět (vztahuje se na konkrétní situaci) a s obecně vymezeným okruhem adresátů**.**

Co je však v případě OOP zásadní, je nemožnost podání řádného opravného prostředku. Proti omezení či zákazu obchodních vztahů stanovených OOP je tak není možnost bránit se opravným prostředkem (proti OOP nelze podat odvolání ani rozklad), což dále přispívá k netransparentnosti a možné arbitrárnosti rozhodování NÚKIB.

Bylo by žádoucí, aby v rámci procesu, který může mít zcela zdrcující dopad na povinné osoby i dodavatele, byly tyto subjekty účastníkem řízení (tak jak je tomu v drtivé většině zemí, které implementoval bezpečností opatření v oblasti řízení dodavatelského řetězce). Tedy nikoli, že bez jejich účasti bude o nich vrchnostensky rozhodnuto NÚKIBem, a proti tomuto rozhodnutí nebude ani dán řádný opravný prostředek.

8) Zásadní narušení legitimního očekávání podnikatelů a podnikatelského prostředí

V důsledku připravované legislativy by také bylo narušeno legitimní očekávání podnikatelů, neboť doslova každý aspekt mechanismu (včetně rozsahu regulace a povinných subjektů) může být ze strany NÚKIB kdykoli jednostranně změněn (vzhledem k tomu, že NÚKIB přijímá vyhlášky tyto

oblasti blíže upravující) a rovněž může dojít k zákazu či významnému omezení jeho dodavatelů. Takto rozsáhlá rozhodovací pravomoc poskytuje velký prostor pro libovůli při rozhodování NÚKIB a představuje tak rozsáhlé riziko.

NÚKIB sám si je vědom toho, že návrh mechanismu má zásadní dopad na povinné osoby, tak i na dodavatele – viz s. 6 důvodové zprávy k vyhlášce o kritériích rizikovosti dodavatele:

„Byť vydání varování a OOP svým charakterem vytváří povinnosti jen pro dotčené poskytovatele regulované služby, fakticky má velmi citelný ***dopad i na samotné dodavatele, kteří mohou být nepřímo vyloučeni z dodávání plnění pro konkrétní množiny poskytovatelů regulovaných služeb****. Zákon, a v důsledku i navrhovaná vyhláška, proto zasahuje i do práva na podnikání dodavatelů, kteří budou shledáni rizikovými a bude proti nim vydáno varování či opatření obecné povahy*."

S tímto argumentem se NÚKIB pouze stručně vyrovnává tvrzením, že podle čl. 1 rozsahu ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, je zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot základní povinností státu a zákon lze považovat za jeden z prostředků plnění této povinnosti státu. Dle tvrzení NÚKIB zákon zároveň reflektuje postavení kybernetické bezpečnosti jako nedílného předpokladu rozvoje digitální společnosti a ekonomiky, o nějž ČR jako členský stát Evropské unie usiluje, a tento účel a smysl zákona pak sledují prováděcí právní předpisy. **Jakým způsobem navrhovaná právní úprava splňuje zásadu proporcionality, NÚKIB nikde neuvádí, zřejmě proto, že zřetelně splněna není.**

Konečným důsledkem mechanismu tak může být úplné dlouhodobé zastrašení podnikatelských subjektů od spolupráce s dodavateli z vybraných zemí. Je zapotřebí si také uvědomit, že při takto obecně nastavených kritériích může dojít k tomu, že „rizikovou" zemí se v okamžiku změny politické reprezentace v ČR náhle stane stát, u nějž by to navrhovaná právní regulace v tuto chvíli absolutně nepředpokládala.

9) Nereflektování zásadních finančních dopadů navrhované právní úpravy

Ačkoli jsou NÚKIB velmi dobře známy možné finanční a hospodářské dopady navrhované právní úpravy (mechanismu), což dokládá i níže uvedená citace ze shrnutí závěrečné zprávy RIA k návrhu zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), která byla převzata např. i do odvodnění vyhlášky o nepominutelných funkcích, NÚKIB tyto zcela lakonicky přechází a projevuje ignoraci a nezájem k potřebám povinných subjektů, kdy je zcela evidentní, že jej možné (prokazatelné) ztráty povinných osob nezajímají a udané předpokládané ztráty převyšující 1 miliardu Kč přímo ignoruje s odkazem na možnost výjimky (jejíž udělení závisí výlučně na uvážení NÚKIB a řízení o výjimce může být zahájenou pouze z moci úřední).

*„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 plyne, že **vyloučení a nahrazení významného dodavatele může pro povinnou osobu mechanismu generovat náklady až ve výši 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 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.“*

Finanční a administrativní dopady připravované regulace přitom byly ze strany předpokládaných povinných osob dlouhodobě a intenzivně komunikovány i s NÚKIBem.

V tomto směru lze v důvodové zprávě k zavedení mechanismu nalézt výslovně protichůdná tvrzení:

- s.6: „*Výstup z mechanismu posuzování dodavatelů má sloužit toliko jako jeden ze vstupů do procesu řízení rizik a* ***neměl by pro povinné osoby mechanismu představovat významnou administrativní či jinou zátěž.*** *Navrhovaný mechanismus prověřování je vytvářen s cílem* ***minimalizovat ekonomické náklady*** *pro soukromé subjekty i pro stát na úroveň nezbytnou pro zajištění účelu mechanismu*."
- s.19: „*Potenciální* ***významnější náklady povinným osobám mechanismu generuje povinnost dodržovat opatření vydaná NÚKIB****. V případě upozornění na riziko spojené s dodavatelem 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***."

E. Protichůdná a nepodložená tvrzení v důvodové zprávě k zavedení mechanismu v novém ZKB

1) Řešení strategických hrozeb dle současné právní úpravy a pozice povinných osob

Dle NÚKIB je možnost omezovat přítomnost rizikových dodavatelů ve strategicky významné infrastruktuře primárně ponechána na povinných osobách podle ZKB, které ale dle názoru NÚKIB prezentovaného v důvodové zprávě (viz s.3) zřejmě nejsou dostatečně způsobilé, aby toto hodnocení prováděly.

Povinné osoby totiž dle názoru NÚKIB: „*nejsou motivovány analyzovat a omezovat hrozby pro větší množinu systémů strategicky významné infrastruktury, než za jaké jsou odpovědné. Nicméně i pokud by se povinná osoba chystala takovou hrozbu ve svém řízení rizik podle VKB reflektovat, nemá zpravidla oprávnění, nástroje ani kapacitu shromažďovat a vyhodnocovat informace k tomu potřebné*.(…)

(…) *Nezřídka se navíc stává, že* ***identifikovaná hrozba, před níž NÚKIB vydal varování podle ZKB, není v analýze rizik povinných osob podle ZKB dostatečně, či dokonce jakkoliv, reflektována****. Podle výstupů z kontrol a auditů povinných osob prováděných podle 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 v analýze rizik náležitě zohledněno, často nejsou řízeny následné procesy a alokovány zdroje pro ošetření daného rizika doložitelné formou např. plánu zvládání rizik***."

Současně ale NÚKIB na s. 6 důvodové zprávy uvádí:

„*Problematika komplexního zajištění bezpečnosti nicméně zůstává věcí správce systému či sítě. V souladu se stávajícím nastavením systému zajišťování kybernetické bezpečnosti v České republice je klíčovým prvkem systém řízení rizik podle VKB.* ***Ačkoliv navrhovaný mechanismus přichází s novým vstupem státu***

do tohoto systému, komplexní analýzu hrozeb a rizik v oblasti kybernetické bezpečnosti ponechává na odpovědnosti povinných osob mechanismu.“

NÚKIB tedy na jedné straně tvrdí, že povinné osoby nedisponují dostatečnou „maturitou“ v oblasti řízení rizik, současně však na nich údajně ponechává samotnou analýzu rizik, která je zcela zásadní. Lze se domnívat, že (jak je uvedeno i výše) v textu, má mechanismus sloužit jako **donucovací prostředek pro povinné osoby**, které např. k varování vydanému NÚKIBem přistupují způsobem, který se NÚKIB nejeví jako „ten správný“. Zřejmě jediným „správným“ přístupem dle NÚKIB je úplné vyloučení předmětného dodavatele a není-li k němu přistoupeno a využití dotyčného dodavatele je pouze omezeno, není tento přístup z pohledu NÚKIB dostatečně vyspělý a zodpovědný. Je ale třeba mít na paměti, že varování je institutem upozorňujícím (povahou doporučujícím), nikoli zavazujícím.

V tomto kontextu je také zcela nepochopitelné, že NÚKIB, který má být odborníkem v oblasti kybernetické bezpečnosti, označuje výše uvedený jednostranný zákaz dodavatele ze strany státu jako vstup státu do systému komplexního zajištění bezpečnosti postaveném na analýze rizik, kterou „*ponechává na odpovědnosti povinných osob mechanismu*“. NÚKIB naopak zcela znehodnocuje analýzu rizik ze strany povinných osob a jimi zavedená bezpečnostní opatření, kdy si vyhrazuje pravomoc zakázat povinnými osobami užívaného dodavatele bez možnosti jejich odborného vstupu či zhojení nedostatků.

2) Existující legislativa

Důvodová zpráva uvádí výčet právních předpisů, které v současnosti umožňují reagovat na NÚKIBem uváděná strategická rizika – zejména jde o:

- zákon č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
- zákon č. 69/2006 Sb., o provádění mezinárodních sankcí

Důvodová zpráva k tomuto výslovně uvádí:

„***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 České republice***.*(…) 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 pro zvýšení efektivnosti tohoto procesu."

Shrneme-li výše uvedené, dojdeme k závěru, že v ČR v současné době existuje právní úprava, která je způsobilá účinně mitigovat strategická rizika a vzhledem k její povaze jí lze postihnout i oblast ICT, NÚKIB však tvrdí, že není dostačující, dostatečně však neodůvodňuje proč.

F. Mechanismus navržený NÚKIB v Evropě nemá obdoby

Ač NÚKIB argumentuje, že v mnoha ohledech se při přípravě Mechanismu inspiroval v zahraničí, nejedná se o pravdivé tvrzení. Prvky mechanismu lze najít v zahraničí, NÚKIB si však ve všech ohledech vzal z každého zahraničního přístupu ten prvek, který mu dává nejvíce pravomocí a nejvíce oslabuje postavení soukromého sektoru. Nikde bohužel nedohledáme odůvodnění, proč méně invazivní zahraniční přístupy nebyly dostačující a NÚKIB musel přistoupit k více invazivní regulaci (opět se vracíme k principu proporcionality a jeho nedodržení).

NÚKIB v důvodové zprávě odkazuje mimo jiné na Finský model. Právě na Finském modelu lze velmi dobře demonstrovat, jak se možná NÚKIB v některých ohledech inspiroval, avšak ve všech ohledech omezil práva soukromých osob nad rámec Finského modelu.

Finský model	**Mechanismus navržený NÚKIB**
Oba modely pro definování kritické části sítě používají tzv. funkcionality (v návrhu nového ZKB tzv. nepominutelné funkce). Funkcionality, které definují rozsah regulace, se vztahují pouze na **jádro sítě.**	Nepominuté funkce se vztahují na **jádro sítě + prvky RAN.** **Kritickou částí stanoveného rozsahu jsou nad rámec nepominutelných funkcí také aktiva definovaná povinnými osobami jako kritická.** NÚKIB může definovat kritickou část sítě. Má tedy naprostou kontrolu nad rozsahem a povinnými osobami.
Posuzuje se **konkrétní zařízení dodavatele v rámci konkrétní dodávky.**	Posuzuje se země původu dodavatele, na základě strategických kritérii (demokracie, dělba moci či lidská práva). Případný zákaz dodavatele se vztahuje na všechny povinné osoby.
Kontrola **ex post**	Kontrola **ex ante**

Traficom přistupuje k posuzování zařízení pouze v případě, kdy **identifikuje případné riziko.**	NÚKIB posuzuje dodavatele dle vlastního uvážení.
Na počátku procesu posuzování zařízení si Traficom vyžádá **tzv. bezpečnostní dokumentaci** vztahující se k posouzení kritických částí komunikační sítě, kterou jsou povinni připravit a aktualizovat povinné osoby. Pouze na základě této bezpečnostní dokumentace, která obsahuje seznam veškerých bezpečnostních opatření implementovaných ze strany povinných osob, je Traficom schopný hodnotit konkrétní riziko.	NÚKIB si od povinných osob vyžádá (pokud uzná za vhodné) základní informace k osobě dodavatele. Poté hodnotí osobu dodavatele na základě informací zejména od tajných služeb a hodnotí je v kontextu obecných strategických kritérii. NÚKIB neuvádí, zda při posuzování bere v potaz již zavedená bezpečnostní opatření ze strany operátorů. S ohledem na fakt, že se však případný zákaz vydaný ve formě OOP vztahuje na všechny povinné osoby, nelze předpokládat, že konkrétní dodávka či bezpečnostní opatření hrají v procesu posuzování jakoukoli roli.
Pokud má Traficom na základě posouzení podezření, že zařízení představuje **bezpečnostní hrozbu**, informuje nejprve příslušného telekomunikačního operátora. Následně musí být dána telekomunikačnímu operátorovi možnost **vyjádřit se** k předmětnému posouzení a musí mu být dána také možnost v přiměřené lhůtě **napravit potenciální bezpečnostní problém**, který Traficom zjistil (takovou nápravou může být například aktualizace softwaru).	Pokud NÚKIB vyhodnotí osobu dodavatele jako rizikovou, vydá veřejné OOP, kterým může osobu dodavatele plošně zakázat. Neposuzuje se tedy riziko v konkrétním případě, ale pouze obecná hrozba. Povinné osoby nemají možnost se bránit jinak, než žalobou.
V případě, že telekomunikační operátor nepřijme **přiměřená nápravná opatření ve** stanovené lhůtě, může Traficom přijmout nezbytná prozatímní opatření, aby zamezil používání potenciálně nebezpečného zařízení v kritických částech komunikační sítě.	Povinné osoby nemají možnost přijmout odpovídající bezpečnostní opatření. NÚKIB může přistoupit k zákazu zařízení bez komunikace s povinnou osobou.

V případě, že telekomunikační operátor nepřijme přiměřená **nápravná opatření** ve stanovené lhůtě, může Traficom přijmout nezbytná prozatímní opatření, aby zamezil používání potenciálně nebezpečného zařízení v kritických částech komunikační sítě. Telekomunikační operátor, kterému byla uložena povinnost odstranit telekomunikační zařízení z kritických částí komunikační sítě má na základě § 301a ZEKS právo na náhradu veškerých nákladů na odstranění a výměnu předmětného zařízení, jakož i na náhradu dalších finančních ztrát, jako jsou náklady na opravy či úpravy zařízení nebo náklady na koupi náhradního zařízení. Pouze poslední možnost představuje rozhodnutí Traficomu o odstranění předmětného zařízení z telekomunikační sítě.	Žádná náhrada povinným osobám nenáleží.