Národní úřad pro kybernetickou a informační bezpečnost
Petr Novotný
ředitel odboru kybernetických bezpečnostních politik
Mučednická 1125/31
616 00 Brno

Vážený pane řediteli,
předem mi dovolte poděkovat za možnost připomínkovat návrh podoby Mechanismu posuzování a omezování rizik spojených s dodavateli do infrastruktury elektronických komunikací (dále jen "Mechanismus"), který jste nám zaslal pod číslem jednacím č. j.: 3351/2022-NÚKIB-E/310 dne 21. 3. 2022.

Konkrétní připomínky a obecnou připomínku „Návrh řešení" v podobě obecné připomínky zasíláme v textu níže.

Přílohou „Technická analýza: Sítě páté generace z hlediska bezpečnosti".

Kontaktní osoba za VNICTP je Jakub Rejzek, MBA, LL.M, 727 938 968; jakub.rejzek@vnictp.cz

---

1. Konkrétní připomínky ke koncepci mechanismu

Jak opakovaně uvedl NÚKIB, mechanismus musí být založený na principech analýzy rizik. Současný koncept však tuto myšlenku naprosto opouští. Navrhovaný správní proces ze strany státu posuzuje **výhradně** strategická rizika spojená s osobou dodavatele. Naprosto ignoruje technické aspekty sítě i jednotlivých zařízení, umístění a funkci zařízení, zavedená bezpečnostní opatření ze strany Dodavatele, zavedená bezpečnostní opatření ze strany Odběratele a mnoho dalších individuálních okolností spojených s jednotlivýma dodávkami. **Správní proces v současném stavu hodnotí výhradně osobu dodavatele na základě výhradně strategických kritérii a zcela opomíjí technické aspekty kybernetické bezpečnosti.** Ač technické aspekty, jak uvedl NÚKIB, bude posuzovat Odběratel, dojde k jejich posouzení až ve chvíli, kdy již může být jeden či více dodavatelů vyloučen. V tu chvíli však zcela dochází k nadřazení strategických aspektů nad ty technické a může nastat situace, kdy díky technickým nedostatkům bude Dodavatel nucen zvolit fakticky rizikovějšího dodavatele. **Posuzování rizikovosti není problém čistě technický**

nebo strategický, oba aspekty kybernetické bezpečnosti musí být posouzeny společně a v závislosti na sebe.

- **Regulace se musí vztahovat pouze na kritické části sítě. Jako vhodné řešení se jeví:**

Regulaci podléhá správce nebo provozovatel informačního nebo komunikačního systému KII ve smyslu ZKB, který je zároveň operátor ve smyslu § 2 e) ZEK, avšak pouze v rozsahu, v jakém je na fungování informačního nebo komunikačního systému závislé poskytování služeb nebo sítí elektronických komunikací[1].

1) *Regulována je bezpečnostně relevantní dodávka, tzn. jakékoliv plnění, spočívající ve vývoji, výrobě, sestavení, či servisu (i) technického prostředku s výpočetní kapacitou či (ii) software, které je významné z hlediska bezpečnosti*

   a. *prvku informačního nebo komunikačního systému KII*
   b. *obsahujícího některou z kritických funkcí, které stanoví vyhláška*

2) *Odběratel identifikuje v informačních a komunikačních systémech KII, jichž je správcem či provozovatelem, takové části, které splňují podmínky dle odst. 1 a 2 výše (dále jen kritická součást systému). Zároveň je povinen proces identifikace zdokumentovat a udržovat tuto dokumentaci pro případnou ex post kontrolu ze strany NÚKIB.*

- Proces by mělo vést Ministerstvo průmyslu a obchodu

1. Konkrétní připomínka, kritická: chybějící analýzy dopadu na trh

V předkládaném návrhu Mechanismu absentuje jakákoliv analýza dopadu na trh telekomunikačních služeb. Je nutné připomenout, že samotný návrh, navzdory původním tezím, se týká regulace celého telekomunikačního průmyslu a nedotýká se prozatím velmi úzkého segmentu 5G. Zdánlivě nepodstatná změna vytváří potenciál destrukce trhu v současné podobě. I z dřívějších vyjádření samotného NUKIBu vyplývá, že **nedošlo k žádné** významné kyberbezpečností události v infrastruktuře telekomunikačních operátorů. Významný poddíl infrastruktury mobilních sítí je obsluhován formou poskytování datových okruhů „nemobilními“ operátory. Tyto společnosti, kterých v daném segmentu operují desítky, se stávají podle návrhu

Mechanismu regulovanými osobami. Kromě toho, jsme nuceni NUKIBu opakovaně připomínat přípravu návrhu Směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v celé Unii, kterou se zrušuje směrnice (EU) 2016/1148 (dále také "návrh směrnice NIS 2" nebo "směrnice NIS 2").
Tento dokument beze vší pochybnosti přesune atributy kritické infrastruktury na malé a střední podniky poskytující služby přístupu k elektronickým komunikacím. V souladu s ustanoveními článku 2 odst. 2 písm. a) návrhu směrnice NIS 2 ve spojení s bodem 8 přílohy č. I návrhu směrnice NIS 2 se tak oblast působnosti směrnice NIS 2 rozšiřuje například na poskytovatele veřejných sítí elektronických komunikací nebo poskytovatele veřejně dostupných služeb elektronických komunikací (operátory) bez ohledu na jejich velikost.
Analýzu současného návrhu NIS2 jsme zveřejnili v odkazu https://www.vnictp.cz/smernice-nis-2-vychodiska-cile-vybrane-klicove-aspekty-navrhu-smernice-nis-2-vcetne-rozsahu-0.

2. Konkrétní připomínka: chybějící analýzy dopadu na rozvoj sítí v rurálních oblastech

Masivní regulace, kterou navrhuje v podobě Mechanismu NUKIB, podepřená budoucí Evropskou regulací a tím i rozšíření rámce regulovaných podnikatelů ovlivní ve značném rozsahu tempo výstavby a modernizace všech typů telekomunikačních infrastruktur. Kromě toho pozdrží nebo přímo znemožní výstavbu v intervenčních oblastech určených pro pokrytí s přispěním veřejných prostředků – a to z důvodu nutnosti dokončení výstavby z příslušných fondů. Termíny ukončení investic jsou v roce 2025 pro fondy RRF a 2030 pro fondy OP TAK.
Neméně významným faktorem hodným analýzy je vliv takto masivní regulace na samotné záměry investic v oblastech s nižší investorskou atraktivitou. Nejenom samotní podnikatelé v investující ve výstavbě infrastruktury budou nucení směrovat svoje investice do v současnosti pokrytých částí sítě. Významným negativním inhibitorem bude nedostatečné pokrytí dodávkami komponent sítě, protože samotný proces navrhovaný v Mechanismu neumožní operativně reagovat na výpadky dodávek. Ty jsou zcela běžné. Velkým korporacím, typicky mobilním operátorům, jsou výrobci ochotní přistupovat na sankce v případě výpadků. U menších podnikatelů taková vyjednávací síla není. Vliv Mechanismu na rozvoj sítí a postupně na samotnou strukturu trhu je neoddiskutovatelný. Připomeňme, že přímo v návrhu Mechanismu NUKIB odmítá spojení s technickou relevancí rizik a regulaci navrhuje kvůli geopolitickým rizikům. NUKIB tedy požaduje změny na trhu a výrazné trvalé znevýhodnění segmentu malých a středních podniků. Trváme na zachování zřetelné provazby na technickou relevanci rizik v jakékoliv budoucí regulaci.

3. Konkrétní připomínka: chybějící analýzy dopadu na cenu koncových služeb

Každá regulace, natož takto silný zásah do trhu v podobě navrhovaného Mechanismu, vede k nárůstu variabilních a fixních nákladů. To platí pro většinu podnikatelských činností. Nákupní management podřízený dohledu státu povede zcela jistě k omezení konkurence, která je v telekomunikacích, stejně jako jinde, jedním z hlavních faktorů nastavení cen za dodávky HW. Purchasement v telekomunikacích provádějí technicky a právně vzdělaní lidé. Vytvoření složitého systému, navrhovaného NUKIBem v Mechanismu vytvoří tlak na další rozšíření nákupních oddělení a významně zvedne zejména fixní náklady – které je pro MSP stále složitější krýt z výnosů z podnikatelské činnosti. Navrhovaná regulace povede ke zdražování služeb koncových zákazníkům, podnikům, mikropodnikům, spotřebitelům a v neposlední řadě samosprávám.

4. Nedostatek dodávek a MSP až v třetí řadě.

Regulace a s tím spojené náklady pro dodavatele a pro samotné podnikatele povede nutně k omezení nabídky na trhu. V segmentu MSP dojde nutně k omezení nabídky a vůbec k poklesu ochoty operovat v segmentu s nižším potenciálem obratu na podnikatelskou jednotku. Trh MSP je specifický fragmentací, obratově je však zajímavý také pro menší dodavatele specializující se na určité segmenty sítí (přístupová část sítě, přípojná část sítě, bezdrátové spoje atp.).
Všeobjímající regulace NUKIBu by způsobila nedostatek v nabídce technologií pro MSP.
Návrh mechanismu je ukázkový příklad vytvoření **bariéry** efektivního vstupu na trh společností zavádějící vývoj a výrobu technologií založené na filosofii Open Vendor Policy.
Vytvoření Mechanismu, který odmítá zahrnout relevanci technických rizik, vytváří závislost podnikatelů na jednom dodavateli. V tomto případě NUKIB kybernetická rizika nesnižuje, ale přímo exponenciálně vytváří. Cílem zadání BRS ze dne 19.10.21 bylo kybernetická rizika snížit, nikoliv je zvyšovat. Jsme toho názoru, že pro vytváření kybernetické bezpečnostní politiky bez technické relevance rizik je závažným omylem.

2. Regulace výběru dodavatelů do infrastruktury elektronických komunikací: návrh řešení formou obecné připomínky

V ČR je aktuálně připravována regulace, jejímž cílem má být minimalizace rizik spojených s dodavateli telekomunikačních sítí. V rámci této regulace má mít nově zásadní slovo stát, který by měl mít možnost autoritativně zasahovat do doposud v tomto smyslu neregulovaného výběru dodavatelů.

2.1. Současný stav a východiska

V současné době představuje klíčové ustanovení § 4 odst. 2 ZKB[2], dle kterého: *„Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zavést a provádět **bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti** informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, informačního systému základní služby a významného informačního systému a vést o nich bezpečnostní dokumentaci.“*

S tím souvisí i § 4 odst. 4 ZKB: *„Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny **zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele** pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. (…)“*.

VKB[3] jako prováděcí právní předpis k ZKB dále stanoví podrobnosti, mezi které patří mimo jiné obsah bezpečnostních opatření (§ 6 písm. a) ZKB), detaily bezpečnostních opatření pro orgány a osoby uvedené v § 3 písm. c) až f) ZKB (§ 6 písm. c) ZKB) a další problematiku. VKB obsahuje i ustanovení, která musí povinné osoby dodržovat v rámci řízení dodavatelů (§ 8 VKB).

Způsob realizace bezpečnostních opatření, která mají vybrané povinné osoby zavést a provádět ve smyslu § 4 odst. 2 ZKB, je dosud **zásadně na uvážení těchto osob**. Tyto osoby musí být připraveny si podobu těchto bezpečnostních opatření obhájit při případné kontrole ze strany NÚKIB. **Volba je však zásadně na jejich rozhodnutí a ze strany státu jim zcela konkrétní opatření zásadně není direktivně vnuceno.**

Jak vyplývá z dostupných informací, povaha regulace výběru dodavatele dosavadní paradigma ZKB (zásadně svobodné rozhodování na straně povinných osob) posouvá směrem k vrchnostenským zásahům státu, které musí povinná osoba akceptovat. Tedy do **zcela jiné roviny**.

S ohledem na intenzitu zásahu do podnikání odběratelů regulovaných dodávek, který má regulace přinést, je třeba zabývat se proporcionalitou navrženého konceptu. A to zejména v tom smyslu, jaké části sítě budou regulovány.

[2] Zák. č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů
[3] Vyhláška 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)

2.2. Uvažovaný koncept regulace a princip proporcionality

NÚKIB chce dle návrhu regulovat „*kritické součásti systému*“, kterými rozumí „*technická aktiva informačního a komunikačního systému Odběratele, na kterých je, bez ohledu na zavedení bezpečnostních opatření, závislé připojení kritické informační infrastruktury do sítě elektronických komunikací.*“

Dle NÚKIB se nemá jednat pouze o „*prvky mobilních sítí 5. generace*“, ale o veškerá „*relevantní technická aktiva celé telekomunikační infrastruktury*“, resp. taková, která z této množiny identifikuje Odběratel[4] na základě prováděcího právního předpisu, jehož vydání NÚKIB avizuje. **Uvedená definice představuje ve svém důsledku velmi široký a zároveň neurčitý pojem**.

Ve vztahu ke kritickým součástem systému mají být regulovány tzv. „*bezpečnostně relevantní dodávky*“, kterými se podle návrhu rozumí „*plnění, spočívající ve vývoji, výrobě, sestavení či servisu technického vybavení či komunikačního prostředku s výpočetní kapacitou nebo programového vybavení, směřující do Kritické součásti systému*“.

Způsob, jakým chce NÚKIB zasahovat do výběru dodavatelů, představuje pro odběratele významné omezení smluvní volnosti, resp. celé jejich podnikatelské činnosti. Fakticky se jedná o jakési „znárodnění“ celého procesu budování telekomunikačních sítí v ČR. Takový přístup je proto nutné poměřovat principem proporcionality, s nímž musí být v souladu.

Princip proporcionality je úzce spojen s celou oblastí kybernetické bezpečnosti, kdy odborníci varují před extenzivním a nepřiměřeným postupem, přičemž je třeba zejména zamezit příliš širokému nastavení pravomocí, kterým by byla neproporcionálně omezena v opozici stojící práva: „*Z toho důvodu spadají pod rozsah zákona o kybernetické bezpečnosti jen určité poměrně úzce vymezené subjekty, které jsou navíc systematicky odstupňovány podle důležitosti, která jej jim v rámci kybernetické bezpečnosti přisuzována*.“[5]

Základní právo či svobodu lze omezit pouze v zájmu jiného základního práva či svobody. Ještě před tímto omezením je však třeba i s ohledem na ustanovení čl. 4 odst. 4 Listiny základních práv

[4] Dle návrhu má být Odběratelem „orgán či osoba, která zajišťuje síť elektronických komunikací (ve smyslu § 2 písm. b) zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů) zajišťující přímé připojení ke kritické informační infrastruktuře.

[5] POLČÁK, Radim, HARAŠTA, Jakub, STUPKA, Václav: Právní problémy kybernetické bezpečnosti. Brno: Masarykova univerzita, Právnická fakulta, 2016, str. 158 - 159

a svobod využít všech možností minimalizace zásahu do druhého z nich.[6] Princip proporcionality je hojně opakován jak judikaturou Ústavního soudu[7], tak např. i Nejvyššího správního soudu.[8]

Důvodová zpráva k ZKB zdůrazňuje na několika místech **autonomii vůle povinných osob a zásadu minimalizace zásahů státu**.[9]

Princip proporcionality je široce uznáván i právem EU. **Jakékoliv omezení musí být s tímto principem v souladu.** Musí by být prokázána jeho nezbytnost k dosažení dovolávaného cíle, stejně jako že tohoto cíle nelze dosáhnout zákazy nebo omezeními menšího rozsahu nebo zákazy a omezeními méně zasahujícími obchod uvnitř Evropské unie.[10] Stanovené omezení musí být způsobilé zaručit uskutečnění daného cíle a nesmí překračovat meze toho, co je k dosažení tohoto cíle nezbytné[11]. Přijatá omezení přitom musí být doložena vhodnými důkazy či analýzou jejich způsobilosti a přiměřenosti, jakož i přesnými skutečnostmi dokládajícími takovou argumentaci[12]

Ze všeho výše uvedeného vyplývá, že volba způsobu regulace dodavatelů sítí musí projít testem proporcionality. Má-li jakýkoli omezující zásah obstát, musí být opřen o velmi závažné důvody včetně vysvětlení, proč k dosažení cíle nepostačoval mírnější nástroj. V opačném případě hrozí, že zvolené řešení s sebou přinese protiprávní následky spojené s deformací trhu, jakož i vznikem škody, jejíž náhrady by se mohly dotčené osoby v budoucnu domáhat.

Výše uvedené je třeba brát v úvahu při celém procesu tvorby zamýšlené regulace, a to zejména v kontextu otázky, na jaké části sítě se má regulace vztahovat.

2.3. Předmět regulace s ohledem na její účel

Současná právní úprava je založena na předpokladu, že za kritické části sítě lze považovat takové části, které hrají klíčovou roli pro infrastrukturu státu. V ČR takovému pojetí odpovídá tzv. kritická

[6] Nález Ústavního soudu ze dne 12. 10. 1994, sp. zn. Pl. ÚS 4/94
[7] Kromě zmíněného nálezu ze dne 12. 10. 1994, sp. zn. Pl. ÚS 4/94 též např. nálezy ze dne 17. 7. 2007, sp. zn. IV. ÚS 23/05, ze dne 11. 11. 2005, sp. zn. I. ÚS 453/03
[8] Viz např. rozsudek Nejvyššího správního soudu ze dne 5. 11. 2007, č. j. 8 As 51/2007-67 či ze dne 31. 8. 2009, č. j. 8 As 7/2008-116
[9] Viz např. důvodová zpráva k ZKB k § 3, § 4, § 11 a § 21 ZKB
[10] Srov. např. rozsudek ESD ze dne 23. 12. 2015 ve věci Scotch Whisky Association, C-333/14, bod 53
[11] Srov. např. rozsudky ESD ze dne 5. 2. 2014 ve věci Hervis Sport, C-385/12, bod 42, ze dne 25. 10. 2007 ve věci Geurts a Vögten, C-464/05, bod 24, nebo ze dne 6. 11. 2003 ve věci Piergiorgi Gambelli a další, C-243/01, bod 72
[12] Srov. např. rozsudek ESD ze dne 6. 3. 2018 ve věci SEGRO a Horváth, C-52/16 a C-113/16, bod 85

informační infrastruktura (dále jen „*KII*“).[13] Vzhledem k tomu, že se jedná o infrastrukturu nejvyššího významu, jsou s její ochranou spojeny významné povinnosti.

Má-li regulace určitým způsobem omezovat smluvní volnost určitých subjektů, mělo by takové omezení být spojeno pouze s takovým rozsahem aktiv, která tak zásadní úroveň ochrany vyžadují. Tedy nikoli plošně veškerou KII, případně širšího rozsahu.

Cílem navrhované regulace má být zmírnění **rizik spojených s dodavatelem**. Riziko je kombinací **hrozby**, **zranitelnosti** a **dopadu** na aktivum. Dopad vychází z hodnoty aktiva.[14] Jinými slovy, riziko představuje možnost či pravděpodobnost, že určitá **hrozba využije zranitelnosti aktiva a způsobí škodu**.[15]

VKB obsahuje ve své příloze č. 3 vybrané kategorie zranitelností a hrozeb. Povinná osoba v rámci řízení rizik v návaznosti na § 4 VKB s ohledem na aktiva identifikuje relevantní hrozby a zranitelnosti; přitom zvažuje zejména kategorie hrozeb a zranitelností uvedených v této příloze VKB.[16]

VKB ve spojení s ZKB tak ukládá povinným osobám zohledňovat rozsáhlý katalog hrozeb. **S dodavatelem jsou však spojeny pouze některé hrozby**.

NÚKIB se katalogem hrozeb spojených s dodavateli ve svém návrhu podrobněji nezabývá. Lze mít za to, že s dodavateli mohou být teoreticky spojeny zejména následující hrozby:

- **porušení smluvních závazků dodavatelem, zejména odepření dodávek, servisu či aktualizací** (k tomu např. viz hrozba *nedodržení smluvního závazku ze strany dodavatele* v příloze č. 3 VKB),

[13] Kritickou informační infrastrukturou ZKB se dle § 2 písm. b) ZKB rozumí „*prvek nebo systém prvků kritické infrastruktury* ***v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti***“. Kritická infrastruktura je upravena v zákoně č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. Dle jeho § 2 písm. g) se kritickou infrastrukturou rozumí „*prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.*“
Prvek kritické infrastruktury musí splňovat průřezová a odvětvová kritéria, která jsou upravena v nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů.

[14] Metodika k varování ze dne 17. prosince 2018, dostupné na https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

[15] Tamtéž

[16] § 5 odst. 1 písm. b) VKB

- **poškození technického či programového vybavení dodavatelem** pomocí integrované zranitelnosti či v průběhu servisu či aktualizace (k tomu např. viz hrozba *poškození nebo selhání technického anebo programového vybavení* v příloze č. 3 VKB),
- **integrace špionážního backdoor** (k tomu např. viz hrozba *škodlivý kód (například viry, spyware, trojské koně)* a *napadení elektronické komunikace (odposlech, modifikace)*). v příloze č. 3 VKB)

Mnoho jiných hrozeb působí naopak ze **zcela odlišných zdrojů**, např. *pochybení ze strany zaměstnanců* či *nedostatek zaměstnanců s potřebnou odbornou úrovní*.

Řadu hrozeb je navíc povinná osoba schopna efektivně minimalizovat. Je proto otázkou, zda je nezbytné vztáhnout uvažovanou regulaci plošně tak, jak navrhuje NÚKIB, či pouze na vybrané prvky, které lépe odrážejí výše uvedené specifické hrozby a berou ohled na míru přijatelného rizika. S ohledem na zásady ZKB jakož i českého právního řádu obecně lze říci, že uvažovaná regulace by se měla vztahovat pouze na:

- **součásti KII, které**
- **jsou ohroženy hrozbou spojenou s dodavatelem, přičemž**
- **tuto hrozbu není schopna povinná osoba účinně minimalizovat,**
- **a míra rizika opravňuje zásah státu do svobody podnikání.**

Je-li připravován specifický proces týkající se analýzy rizik spojených výhradně s dodavateli, v souladu s principem proporcionality by se tento mechanismus měl vztahovat výhradně na kritické části sítě, jejichž vymezení odpovídá účelu předmětné regulace. KII jakožto právní pojem blíže neurčující prvky či kritické funkce sítě se v tomto ohledu jeví jako nevhodný. Je proto na místě zabývat se bližší specifikací kritických částí sítě, které mají podléhat regulaci.

V tomto ohledu se jako vhodný jeví koncept, podle kterého by byly kritické části dále podrobněji vymezeny (omezeny) s tím, že jejich identifikace by byla na samotném Odběrateli. Tak směrem se udává i návrh NÚKIB: „*Konkrétní rozsah Kritických součástí systému bude v souladu se stávající systematikou řízení aktiv dle § 4 VKB založen primárně na identifikaci aktiv Odběratelem. Základem Kritické součásti systému sice budou povinná typová aktiva stanovená prováděcím předpisem, konkrétní rozsah aktiv spadajících do Kritické součásti systému však bude vždy individuální a bude vycházet z identifikace aktiv svého informačního a komunikačního systému Odběratelem.*“

Pokud jde o konkrétní způsob vymezení kritických součástí systému, jako inspirace se nabízí některý z přístupů, které zvolily členské státy EU.

2.4. Předmět regulace v dalších členských státech

Pokud by měla být zavedena nová regulace dodavatelů předpokládaná ze strany NÚKIB, měla by být nastavena tak, aby vyhovovala principům, na kterých stojí jak ZKB, tak pojetí EU. V tomto kontextu se lze inspirovat přístupy jiných států EU. Typické je pojetí, kdy jsou definovány kritické části sítě[17], které požívají vyšší úrovně ochrany. Ta je spojena se specifickými povinnostmi, kterými jsou zatíženi správci, resp. provozovatelé těchto (částí) sítí. Odkázat lze např. na právní regulaci ve Finsku či Německu.

2.4.1. Podstata finského modelu s ohledem na předmět regulace

Finsko disponuje pokročilou legislativou v oblasti telekomunikačních sítí. Již dříve zde byla zavedena většina opatření, které doporučuje tzv. EU 5G Toolbox, vydaný v lednu 2020. Dosavadní legislativu doplňuje novela zákona o elektronických komunikačních službách (dále také jen „**ZEKS**"), která nabyla účinnosti k 1. 1. 2021.

Podstata finského modelu spočívá v **technologicky neutrální** definicí kritických částí informační infrastruktury, **spolupráci veřejného a soukromého sektoru** a cílení bezpečnostního posouzení na **konkrétní zařízení** komunikační sítě. Finské právní předpisy neumožňují vstup státu do procesu sjednávání smlouvy na dodávky telekomunikačních služeb.

ZEKS poskytuje podrobné informace o tom, jak musí telekomunikační společnosti a další příslušní operátoři jednat, aby zajistili bezpečnost informací ve svých sítích. § 243 ZEKS zejména stanoví rozsáhlé **požadavky na kvalitu komunikačních sítí a služeb** (např. technická úroveň, možnost detekovat významná narušení a ohrožení bezpečnosti informací, interoperabilita a komunikace sítí).

Podle § 244a odst. 1 ZEKS, zařízení komunikační sítě nesmí být používáno **v kritických částech veřejné komunikační sítě**, pokud existují *vážné důvody k podezření, že používání zařízení ohrožuje národní bezpečnost nebo národní obranu státu* takovým způsobem, který by umožňoval:

[17] Obdobně tzv. EU Toolbox, tedy *„Souboru opatření EU pro kybernetickou bezpečnost sítí 5G", hovoří o tzv. klíčových aktivech – „key assets".*

a) činnost zahraničních zpravodajských služeb, nebo
b) činnosti, které by mohly narušit, ochromit, nebo mít jinak nepříznivý dopad na důležité zájmy Finska, základní funkce společnosti nebo demokratický společenský řád.

Popsané ustanovení § 244a odst. 1 se dle § 244a odst. 2 **vztahuje také na kritické oddělené sítě**, jako jsou sítě připojené k veřejné komunikační síti jaderných elektráren, přístavů, letišť a dalších společenských subjektů.

Posouzení případného bezpečnostního rizika se vztahuje pouze na zařízení komunikační sítě. Zařízení komunikační sítě je definováno v § 3 odst. 1 bodu 38 ZEKS. Podle této definice je zařízení komunikační sítě zařízením, které je určeno k použití přenosu nebo řízení zpráv prostřednictvím komunikační sítě.

Zařízení komunikační sítě je tedy součástí komunikační sítě, jako je přepínač, rozbočovač a směrovač. Za používání zařízení komunikační sítě se považuje také údržba, správa nebo monitorování tohoto zařízení.

V souladu s § 244a odst. 6 ZEKS vydala Finská dopravní a komunikační agentura (dále jen „**Traficom**“) **nařízení o kritických částech komunikační sítě** TRAFICOM/161584/03.04.05.00/2020 (dále jen „**Nařízení**“). Toto Nařízení napomáhá telekomunikačním operátorům a provozovatelům oddělených sítí interpretovat, **které technické části** veřejné komunikační sítě nebo kritické části oddělené sítě **představují kritickou část**, na kterou odkazuje § 244a odst. 1 ZEKS.

Na základě článku 3 Nařízení jsou telekomunikační operátoři a provozovatelé oddělených sítí povinni **samostatně identifikovat kritické části své komunikační sítě a komponenty komunikační sítě nebo služby, které v nich používají**. Telekomunikační operátoři a provozovatelé sítí jsou povinni proces posouzení identifikace kritické části komunikační sítě **zdokumentovat** a současně udržovat tuto dokumentaci aktuální k případnému posouzení ze strany Traficomu.

Traficom předpokládá, že pro telekomunikační operátory a provozovatele oddělených sítí nebude představovat identifikace sítí, které spravují delší dobu, přílišnou zátěž. Je tak **primárně odpovědností telekomunikačních operátorů a provozovatelů oddělených sítí vymezit, které části svých sítí lze posoudit jako kritické.**

2.4.2. Definice kritických částí komunikační sítě

Nařízení **definuje kritické části** komunikačních sítí **technologicky neutrálním způsobem**. To je doplněno o přesnější definici kritických částí sítí 4G a 5G. Článek 4 Nařízení obsahuje **seznam síťových funkcionalit**, které jsou vždy považovány za kritickou část komunikační sítě.

Tento článek se v zásadě vztahuje na všechny druhy komunikačních sítí, jako jsou mobilní sítě a pevné linky (circuit-switched and packet switching mobile networks and fixed broadband networks). **Podle definice v článku 4 Nařízení je část komunikační sítě označena za kritickou i v případě implementace pouze části funkcionality komunikační sítě, která je považována za kritickou část.**

O kritickou část veřejné komunikační sítě se jedná vždy, pokud komunikační síť obsahuje alespoň některou z následujících funkcionalit:

a) klíčové funkce sítě související s kontrolou nebo správou v komunikační síti koncových uživatelů, které mohou mít významný dopad na provoz v komunikačních sítí, včetně:
   i. součásti komunikační sítě nebo služby, pokud jim je na základě počtu uživatelů nebo oblasti geografického pokrytí přidělena priorita 1 nebo 2 v souladu s Nařízením o odolnosti komunikačních sítí a služeb a synchronizaci komunikačních sítí.
   ii. součásti komunikační sítě nebo služby, pokud kontrolují nebo řídí významnou část provozu celé sítě; a
   iii. součásti komunikační sítě nebo služby v síti datového centra, pokud jsou nezbytné.
b) správa přístupu koncových uživatelů, autentizace a autorizace a přidělování síťových zdrojů koncovým uživatelům a správa připojení a relací koncových uživatelů;
c) registrace, autentizace a autorizace komunikační sítě a servisních funkcí;
d) infrastrukturní služby nezbytné pro podporu provozu komunikační sítě a služby;
e) funkce pro realizaci rozhraní mezi komunikačními sítěmi nebo službami, včetně roamingu;
f) funkce, kterými se propojují komunikační sítě nebo služby, jestliže taková funkce může mít významný dopad na přístup ke komunikační síti nebo na provoz v síti;
g) centralizovaná správa šifrování komunikační sítě, jejích funkcí a provozu koncových uživatelů a šifrovacích klíčů;
h) funkce zabezpečení informací, které ovlivňují kritické části komunikační sítě;

i) řídící a monitorovací systémy sítě, pokud se týkají řízení nebo monitorování kritických částí komunikační sítě, nebo pokud mohou mít jinak významný dopad na přístup k síti nebo na provoz v síti, jakož i další účetní, podpůrné a back-endové systémy, které mohou mít významný dopad na přístup ke komunikační síti nebo na provoz v ní;
j) provádění odposlechu nebo sledování telekomunikací;
k) virtualizace, pokud je použita pro implementaci funkce nebo opatření, které jsou považovány za kritickou část komunikační sítě;
l) jakoukoli jinou funkci nebo opatření, pokud jsou realizovány prostřednictvím takové virtualizace, která je považována za kritickou část komunikační sítě v souladu s odstavcem 11 tohoto seznamu a
m) klíčové funkce a opatření umožňující přístup k údajům o zeměpisné poloze předplaceného nebo koncového zařízení zpracovávaného v komunikační síti nebo umožňující určení polohy pomocí komunikační sítě.

Seznam v článku 4 Nařízení je pouze demonstrativní a je odpovědností telekomunikačních operátorů a provozovatelů oddělených sítí, aby posoudili, zda části komunikační sítě, které spravují, mohou obsahovat i další kritické části, které nejsou definovány v Nařízení.

Seznam v článku 4 Nařízení je pouze demonstrativní a je odpovědností telekomunikačních operátorů a provozovatelů oddělených sítí, aby posoudili, zda části komunikační sítě, které spravují, mohou obsahovat i další kritické části, které nejsou definovány v Nařízení.

2.4.3. Kritické části veřejné telekomunikační sítě 4G a 5G sítí

Článek 5 a 6 Nařízení doplňuje obecnou definici kritických částí komunikační sítě obsaženou v článku 4. Tyto části obsahují **výčet jednotlivých funkcionalit jádra (core) 4G a 5G sítě**, které jsou považovány za kritické. **Za kritickou část komunikačních sítí tak nejsou považovány 4G a 5G sítě jako celek, ale pouze konkrétní funkcionality částí jádra těchto sítí, které jsou vyjmenovány níže:**

Kritické části 4G sítě:

Funkce	Popis
Home Subscriber Server (HSS)	Uživatelská databáze, která ukládá data pro zpracování uživatelských relací a připojení

Equipment Identity Register (EIF)	Registr mobilních zařízení, který obsahuje informace o oprávněních používat mobilní zařízení
Subscription Locator Function (SLF)	Funkce, která přenáší do jiných síťových funkcí název centrální databáze obsahující uživatelská data (HSS)
Mobile Management Entity (MME)	Entita, která zajišťuje ověření přihlášení do sítě a sleduje pohyb účastníků v síti
Serving Gateway (SGW)	Obslužná brána, která převádí data na úrovni uživatele
Packet Data Network Gateway (PDN GW)	Paketová přepojovací síť mezi interní IP sítí operátora a externí IP sítí
Evolved Packet Data Gateway (ePDG)	Brána zabezpečující přenos mezi uživateli mimo 3GPP
3GPP AAA Server and 3GPP AAA Proxy	Server a proxy server zajišťující ověřování a autorizaci uživatelů mimo přístupové 3GPP
Access Network Discovery and Selection Function (ANDSF)	Funkce zajišťující správu uživatelského provozu mezi mobilní sítí a sítí mimo 3GPP
Policy and Charging Rules Function (PCRF)	Funkce, která dohlíží na zásady připojení uživatelů a pravidla pro výši účtování za jednotlivé služby

Kritické části 5G sítě:

Funkce	**Popis**
Access and Mobility Management Function (AMF)	Odpovídá za zpracování signalizačních dat, registraci koncových zařízení a správu mobility
User Plane Function (UPF)	Odpovědnost za směrování, správu a řízení provozu v uživatelské rovině
Policy Control Function (PCF)	Odpovědnost za řízení provozu a provádění politiky správy přístupu
Authentication Server Function (AUSF)	Odpovědnost za ověřování koncových zařízení uživatelů

Unified Data Management (UDM)	Odpovědnost za správu přístupu uživatelů a vytváření a správu šifrovacích klíčů
Application Function (AF))	Podporuje rozhodování o směrování v síti
Network Exposure Function (NEF) and Intermediate NEF (I-NEF)	Umožňuje poskytovat funkce páteřní sítě 5G třetím stranám a externím aplikacím
Network Repository Function (NRF)	Odpovědnost za dostupnost, registraci a autorizaci síťových služeb
Network Slice Selection Function (NSSF)	Odpovědnost za služby rozdělování sítě a specifikace
Network Slice Specific Authentication and Authorisation Function (NSSAAF)	Odpovědnost za autentizaci a autorizaci síťového segmentu
Session Management Function (SMF)	Odpovědnost za správu relací uživatelů
Security Edge Protection Proxy (SEPP)	Proxy server, který zabezpečuje propojení k jiným sítím
Unstructured Data Storage Function (UDSF)	Funkce sloužící k ukládání a načítání nestrukturovaných dat
Unified Data Repository (UDR)	Úložiště dat schopné ukládat a vyhledávat mimo jiné informace o předplatitelích
UE Radio Capability Management Function (UCMF)	Funkce pro ukládání a uchovávání údajů o rádiových schopnostech UE
Non-3GPP InterWorking Function (N3IWF)	Funkce umožňující přístup k funkcím sítě pro uživatele mimo mobilní síť

5G Equipment Identity Register (5G-EIR)	Registr identity zařízení, který obsahuje informace o oprávnění k používání mobilních zařízení
Service Communication Proxy (SCP)	Směruje zprávy do jiných síťových funkcí
Network Data Analytics Function (NWDAF), excluding its decentralised feature insofar as it does not control or manage access	Shromažďuje a analyzuje údaje pro kontrolu sítě

V článku 7 Nařízení je navíc **definována výjimka**, na základě které funkcionality jádra 4G a 5G sítí, které jsou vyjmenované ve výše uvedených tabulkách, **nejsou považovány za kritické** za předpokladu, že telekomunikační **operátor** nebo provozovatel oddělené sítě řádně **odůvodní** splnění těchto podmínek:

a) funkcionalita se primárně vztahuje k poskytování nekomunikačních služeb,
b) funkcionalita má dopad pouze na omezený počet koncových uživatelů,
c) funkcionalita přenáší pouze informace na okraji komunikační sítě a
d) **kritické části komunikační sítě jsou zabezpečeny spolehlivými mechanismy, které zabrání případnému narušení způsobenému touto funkcionalitou**.

Telekomunikační operátor nebo provozovatel oddělené sítě uplatňující výjimku je vždy povinen prokázat a zdokumentovat naplnění výše uvedených podmínek.

Článek 8 Nařízení doplňuje výše uvedené vymezení kritické části informační infrastruktury. Podle tohoto článku jsou za kritickou část komunikační sítě považovány všechny telefonní služby založené na IP.

2.4.4. Posuzování zařízení pro komunikační sítě ve Finsku

Hlavními orgány pro oblast kyberbezpečnosti ve Finsku jsou:

a) **Finská dopravní a komunikační agentura** (dále jen „**Traficom**“) – odborný garant technických záležitostí souvisejících s 5G, jde o národního telekomunikačního regulátora;
b) **Národní centrum kybernetické bezpečnosti Finska** – v rámci Traficomu, působí jako národní komunikační bezpečnostní úřad;

c) **Poradní výbor pro zabezpečení sítí** – v souvislosti s implementací 5G sítí došlo ke zřízení nového poradního výboru pro zabezpečení sítí. Tento výbor se skládá ze zástupců orgánů veřejné správy a zástupců telekomunikačního průmyslu. Úkolem výboru je posouzení otázek ve vztahu k národní bezpečnosti v telekomunikačních sítích a v případě potřeby je výbor oprávněn vydat doporučení ke zlepšení zabezpečení těchto sítí. Výbor je současně oprávněn vydat doporučení pro legislativní změny ve vztahu ke zlepšení kybernetické bezpečnosti, zejména aktualizovat § 244a ZEKS.

Proces posouzení toho, zda může použití konkrétního telekomunikačního zařízení v kritických částech sítě vážně ohrozit bezpečnost státu, závisí na **kontrole ex post ze strany Traficomu**. **Finský přístup k posouzení bezpečnostní stránky je tedy založen na zásadě minimalizace státních zásahů**, jelikož Traficom žádným způsobem **nezasahuje do procesu kontraktace** telekomunikačního operátora.

Traficom může zahájit kontrolu buď z vlastní iniciativy (ex offo) nebo z podnětu jakékoliv jiné osoby. Na základě § 315 ZEKS má Traficom právo vyžádat si od telekomunikačních operátorů a provozovatelů oddělených sítí dokumentaci vztahující se k posouzení kritických částí komunikační sítě, kterou byli povinni připravit na základě čl. 3 Nařízení. Současně má také právo vyžádat si jakékoliv informace k posuzovanému zařízení.

Má-li Traficom důvod domnívat se, že určité telekomunikační zařízení představuje potenciální riziko pro zdraví nebo bezpečnost lidí nebo pro jiné aspekty veřejného zájmu, provede úplné posouzení, zda je předmětné zařízení v souladu s právními požadavky (§ 260 ZEKS). Současně by Traficom měl o jakémkoliv podezření informovat ostatní veřejné orgány plnící úkoly související s národní bezpečností nebo obranou státu. V tomto případě by měly orgány možnost společně posoudit, zda má být zahájeno správní řízení.

Pokud má Traficom na základě tohoto 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 potencionální bezpečnostní problém, který Traficom zjistil (takovou nápravou může být například aktualizace softwaru).

V případě, že telekomunikační operátor nepřijme přiměřená nápravná opatření ve stanovené lhůtě, může Traficom přijmout nezbytná prozatímní opatření, aby zamezil používání potencionálně nebezpečného zařízení v kritických částech komunikační sítě.

Pouze poslední možnost představuje rozhodnutí Traficomu o odstranění předmětného zařízení z telekomunikační 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.**

2.4.5. Shrnutí finského modelu

Finský model přístupu ke kritické informační infrastruktuře spočívá v **jasné definici kritických částí** komunikačních sítí. Za tuto kritickou část není považována telekomunikační síť jako celek, nýbrž pouze **vybrané funkcionality** části jádra (core) sítě. Seznam kritických částí je založen na definicích 3GPP a pokrývá funkce jádra sítě – v tomto kontextu je významná skutečnost, že rádiová přístupová síť není v tomto seznamu zahrnuta.[18]

Je **povinností samotných telekomunikačních operátorů identifikovat a zdokumentovat** části telekomunikační sítě, které jsou považovány za kritické. Tuto dokumentaci následně musí **udržovat aktuální** pro následné možné posouzení ze strany finských bezpečnostních orgánů.

Finské orgány v oblasti kyberbezpečnosti současně na základě **principu minimalizace státních zásahů** žádným způsobem nezasahují do procesu kontraktace mezi telekomunikačními operátory a dodavateli těchto zařízení. Proces posouzení bezpečnostních rizik ve vztahu k telekomunikačním sítím spočívá v **dodatečné kontrole** konkrétního telekomunikačního zařízení.

Má-li Traficom důvod domnívat se, že určité zařízení představuje bezpečnostní riziko, zahájí konzultaci s telekomunikačním operátorem a v návaznosti na to může nařídit vhodná nápravná opatření. Krajní řešení představuje odstranění potencionálně nebezpečného zařízení z komunikační sítě. V takovém případě však má telekomunikační operátor nárok na veškerou náhradu nákladů, které jsou s tím spojeny.

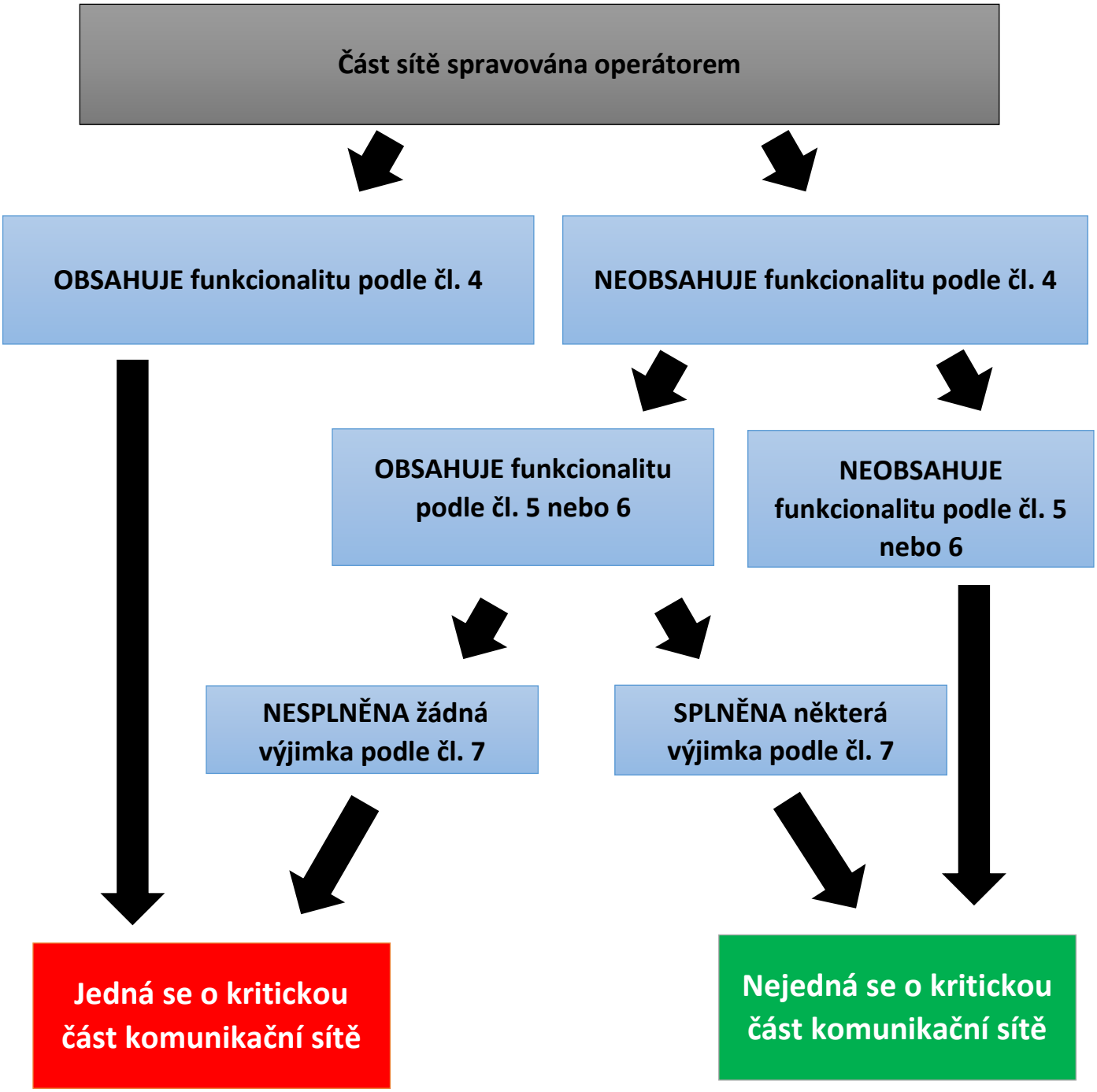
Pro přehlednost zpracovatel níže doplňuje tabulku významných ustanovení finské legislativy:

[18] Avance: Implementing the 5G toolbox: Could Finland serve as a model for the other EU countries?, dostupné na https://www.avance.com/wp content/uploads/2021/05/AVANCE-Insight-01-2021.pdf

	Ustanovení	Povinnosti telekomunikačního operátora
1.	Článek 3 Nařízení	Operátoři jsou povinni samostatně identifikovat a zdokumentovat kritické části své komunikační sítě. Operátor je povinen označit za kritické i ty části sítě, které nejsou definovány v Nařízení, ale o níž se domnívá, že by mohly být považovány za kritické.
2.	Článek 4 Nařízení	Článek 4 obsahuje seznam funkcionalit (generální klauzuli), který se vztahuje na všechny druhy komunikační sítě. Pokud operátor zjistí, že telekomunikační síť, ve které působí, obsahuje funkce uvedené v tomto článku, jedná se o kritickou část komunikační sítě.
3.	Článek 5 a 6 Nařízení	Článek 5 a 6 obsahuje jednotlivé funkce jádra (core) 4G a 5G sítě, které jsou považovány za kritické. Pokud operátor zjistí, že telekomunikační síť, ve které působí, obsahuje funkce uvedené v tomto článku a současně nedojde k naplnění výjimek definovaných v čl. 7 Nařízení, jedná se o kritickou část komunikační sítě.
4.	Článek 7 Nařízení	Výjimky, na základě kterých nejsou funkce jádra (core) 4G a 5G sítí uvedené v článcích 5 a 6 považovány za kritické části komunikační sítě. Telekomunikační operátor musí řádně odůvodnit a zdokumentovat splnění bezpečnostních podmínek.
5.	Článek 8 Nařízení	Na základě tohoto článku je operátor povinen označit jako kritické části sítě i všechny telefonní služby založené na IP.
6.	§ 315 ZEKS	Operátoři jsou povinni na vyžádání předložit Traficomu dokumentaci vztahující se k výše uvedenému procesu identifikace a zabezpečení kritických částí sítě.

Výbor Nezávislého ICT průmyslu

SCHÉMA IDENTIFIKACE KRITICKÝCH ČÁSTÍ KOMUNIKAČNÍ SÍTĚ (FINSKO)



2.4.6. Předmět regulace

Jak již bylo uvedeno výše, účelem nové regulace je zmírnění **rizik spojených s dodavatelem.** Regulaci by proto měly podléhat pouze ty části KII, které vykazují zranitelnosti, jichž by mohly využít hrozby mající svůj původ na straně dodavatelů. Má-li totiž regulace reagovat na hrozby spojené s dodavateli, je třeba vzít v úvahu, že různé části KII vykazují jiné zranitelnosti a nelze je proto regulovat zcela mechanicky.

Zásadní je pojmenování **kritických funkcí**, jejichž strategická hodnota v uvedeném smyslu vyžaduje zvýšenou úroveň ochrany.

Lze odkázat na zprávu EU „*Koordinované posouzení rizik v oblasti kybernetické bezpečnosti sítí 5G ze zemí EU*“.[19] Zde jsou popsány v souvislosti s klíčovými aktivy mimo jiné i různé kategorie prvků a funkcí sítě, přičemž jim připisuje určitou **úroveň citlivosti**. Zde mimo jiné odděluje **funkce jádra sítě** (*core network functions*) a **rádiovou přístupovou síť** (*Radio Access network*). Zatímco v prvním případě uvádí úroveň citlivosti jako **kritickou** (*critical*), ve druhém případě hovoří o **vysoké** (*high*).

S ohledem na výše uvedené se tak v kontextu uvažované regulace nabízí **posouzení citlivosti a strategického významu různých částí KII. Pouze u takových částí, u nichž je regulace dodavatelů nezbytná, by měli být omezeni vysoce rizikoví dodavatelé ve svém přístupu k dodávkám, které by mohly mít vliv na bezpečnost a funkčnost těchto kritických částí sítě – *bezpečnostně relevantním dodávkám*.**

Regulovány by tedy měly být bezpečnostně relevantní dodávka, tzn. jakékoliv plnění, významné z hlediska bezpečnosti

a. **prvku informačního nebo komunikačního systému KII,**
b. **obsahujícího některou z funkcí, které stanoví vyhláška.**

[19] EU coordinated risk assessment of the cybersecurity of 5G networks (9 October 2019), zpráva dostupná na https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049

2.4.7. Identifikace kritických částí sítě a vedení dokumentace

Jsou-li definovány právním předpisem objektivní znaky kritických částí sítě, je třeba je identifikovat v konkrétním případě. Tento proces je nejsnáze proveditelný pro povinnou osobu, která zná nejlépe části KII, jichž je správcem, resp. provozovatelem.

Povinná osoba je zároveň povinna proces identifikace zdokumentovat a udržovat tuto dokumentaci pro případnou ex post kontrolu ze strany NÚKIB.

Pro povinnou osobu se v zásadě nejedná o zcela novou povinnost, neboť již dle platné právní úpravy má povinnost provádět řízení aktiv[20], kdy je mimo jiné povinna svá aktiva identifikovat a evidovat zajišťovat ve spojení s nimi řadu dalších činností. Identifikace, hodnocení a evidence primárních a podpůrných aktiv je součástí bezpečnostní politiky[21], kterou povinná osoba stanoví.[22]

V souvislosti s bezpečnostní politikou vede povinná osoba dle platné právní úpravy rovněž tzv. bezpečnostní dokumentaci.[23]

2.5. Německý přístup

Německo přijalo zákon o bezpečnosti IT 2.0. Zákon je mimo jiné zaměřen na kybernetickou bezpečnost telekomunikačních sítí.

Zákon nově zavádí proces posuzování důvěryhodnosti dodavatele. Zákon předem žádného dodavatele technologii nevylučuje, zanechává však možnost státu do budoucna blokovat operátory od spolupráce s tzv. nedůvěryhodnými dodavateli.

Proces posuzování rizikovosti dodavatelů se v souladu s principy proporcionality, volné hospodářské soutěže a minimalizace zásahu státu vztahuje pouze na předem určené kritické komponenty definované v § 2 odst. 13 BSIG, pro které je stanovena povinnost certifikace. Ostatní komponenty tomuto procesu nepodléhají. Kritické komponenty jsou komponenty, které jsou

[20] § 4 VKB
[21] Příloha č. 5, bod 1.2. VKB
[22] § 30 VKB
[23] § 30 VKB, obsah bezpečnostní dokumentace je upraven v bodu 2 přílohy č. 5 VKB

součástí tzv. strategické části sítě. Strategickou část sítě předem určí stát. Kritické komponenty posléze ve svých sítích identifikují samotní operátoři.

Samotný proces posuzování rizikovosti dodavatelů je postaven na principech analýzy rizik. Až při prokázání rizikovosti daného dodavatele v kritických částech sítě v rámci předem nastaveného procesu může dojít k blokaci jeho spolupráce s operátorem na dané zakázce.

Pro zachování objektivity celého procesu začíná evaluace důvěryhodnosti dodavatele u samotného dodavatele. Ten v případě prodeje tzv. kritických komponent musí operátorovi předložit rozsáhlou písemnou záruku, ve které uvede, zda a jak může dostatečně zajistit bezpečnost svých kritických komponent a důvěryhodnost celého svého dodavatelského řetězce tak, aby nebyla ohrožena bezpečnost, integrita, dostupnost nebo chod kritické infrastruktury státu. Je tak na dodavateli, aby uvedl co nejvyšší míru důkazů prokazujících bezpečnost své technologie a dokázal státu, ve kterém chce podnikat, svou celkovou důvěryhodnost. Operátor posléze záruku společně se svou vlastní analýzou rizik předloží Ministerstvu vnitra k jejímu zkoumání a verifikaci.

Zásadní je, že záruka je předkládána **v rámci oznámení provozovatele kritické infrastruktury, který hodlá příslušné technologie daného dodavatele používat**. Důvodová zpráva k novele uvádí: *„V rámci způsobu použití technologie je třeba upřesnit funkci a umístění (lokalizace, bezpečnostní relevance, zejména možné dopady na bezpečnost kritické infrastruktury, funkčnost, rozsah nasazení atd.) v kritické infrastruktuře. Oznámení je podáváno provozovatelem, neboť pouze on má vědomost o těchto skutečnostech (např. na základě analýzy požadavků na ochranu určité části komunikační sítě dle telekomunikačního zákona).“* Německý zákonodárce uvedeným klade důraz na zohlednění individuálních okolností konkrétní dodávky.

Ministerstvo vnitra spolu s dotčenými orgány předem stanoví minimální požadavky na prohlášení o záruce. Dodavatel musí zejména zaručit, že jeho technologie nemají nekalé technické vlastnosti (pro účely sabotáže, špionáže nebo terorismu) a svou zárukou pokrýt i možná rizika vyplývající z organizační struktury dodavatele a případných povinností z ní vyplývajících.

Po předložení záruky dodavatele následuje proces jejího zkoumání a verifikace. Smyslem verifikace a zkoumáním této záruky (zkoumání důvěryhodnosti) je identifikovat rizika, která nelze identifikovat zkoumáním pouze technické stránky komponent dodavatele (zejména v rámci certifikačního procesu.) Tím Německo implementuje strategické opatření SM03 z EU Toolboxu.

Dotčené orgány ověřují, zda tvrzení dodavatele jsou pravdivá a v případě identifikace rizik zkoumají, zda dodavatel ve své záruce tato rizika společně s operátorem dostatečně eliminuje.

V případě, kdy je používání kritických komponent v rozporu se zájmy bezpečnostní politiky státu, je ministerstvo vnitra po konzultaci s dotčenými orgány (ministerstvo hospodářství a energetiky, ministerstvo zahraničních věcí a úřad spolkového kancléře) oprávněno zakázku (danou koupi kritických komponent dodavatele operátorem) zakázat. Takový případ lze předpokládat zejména v případě, že se ukáže, že prohlášení v záruce jsou nepravdivá, nebo panují-li podložené obavy z narušení bezpečnosti státu.

Používání kritických komponent může ministerstvo dle § 9b odst. 4 zakázat i později, pokud se prokáže, že dodavatel není nadále důvěryhodný. Povinnosti vyplývající z předložené záruky totiž nesouvisejí pouze s dobou instalace, ale musí být dodržovány trvale, tj. při provozu kritických komponent. To vyžaduje průběžné vyhodnocování dodržování záruky. Ministerstvo vnitra proto může zakázat používání kritických komponent tehdy, pokud se dodavatel kritických komponent ukáže nedůvěryhodným. To nastane v případech (§ 9b odst. 5), kdy:

- porušil závazky a ujištění uvedené v záruce,
- skutečnosti uvedené v záruce jsou nepravdivé,
- nepodporuje odpovídajícím způsobem kontroly zabezpečení a penetrační analýzy svých produktů a prostředí výroby v požadovaném rozsahu,
- bezodkladně neoznámil provozovateli kritické infrastruktury a neodstranil známé nedostatky či manipulace,
- kritické komponenty disponují či disponovaly vlastnostmi, které jsou nebo byly schopny negativně ovlivnit bezpečnost, integritu, dostupnost nebo funkčnost kritické infrastruktury; toto neplatí, pokud dodavatel prokáže, že tuto technickou vlastnost nerealizoval nebo ji odstranil.

2.5.1. Inspirace Německým přístupem

Inspirací v Německém modelu je zejména regulace **výhradně kritických částí sítě a princip analýzy rizik, na kterém je postaveno posouzení důvěryhodnosti dodavatele.**

Posouzení důvěryhodnosti dodavatele vychází z posuzování jím předložené záruky, kde dodavatel může prokázat svou důvěryhodnost a podpořit ji konkrétními důkazy. Tím jsou

chráněna práva dodavatele, neboť právě jeho aktivita je klíčová pro to, zda bude shledán důvěryhodným.

Současně se při posuzování dodavatele dle strategických kritérii bere ohled na *„funkci a umístění (lokalizace, bezpečnostní relevance, zejména možné dopady na bezpečnost kritické infrastruktury, funkčnost, rozsah nasazení atd.) v kritické infrastruktuře“* Tím celý mechanismus ctí pravidla analýzy rizik, kdy jsou rizika hodnocena na základě identifikace aktiv, zranitelností a konkrétních rizik spojených s dodavateli.

2.6. Význam analýzy rizik v mechanismu

Jak opakovaně uvedl NÚKIB, návrh mechanismu by měl vycházet z **koncepce analýzy rizik**. Analýzu rizik netvoří pouze identifikace rizik na straně dodavatele, kterou obsahuje návrh NÚKIB, avšak také dalších **5 nezbytných kroků pro objektivní vyhodnocení rizik a efektivní zavedení přiměřených bezpečnostních opatření.**

Analýzu rizik dle vyhlášky o kybernetické bezpečnosti a mezinárodně uznávaných standardů tvoří následující kroky:

1) **Identifikace aktiv**

(§ 5 písm. g „informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém“)

2) **Identifikace hrozby**

(§5 písm. e vyhlášky: „potenciální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, která může způsobit škodu“)

3) **Identifikace rizik**

(§5 písm. h vyhlášky: „rizikem možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu“)

4) **Identifikace zranitelností**

(§5 písm. p vyhlášky: „slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami“)

5) **Hodnocení rizik**

(§ 5 písm. h vyhlášky: „možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu“)

6) **Řízení rizik**

(§ 5 písm. i vyhlášky: „řízením rizik činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik,“)

NÚKIB již identifikoval hrozby spojené s dodavateli. Součástí mechanismu tak 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 poslední řadě **řízení rizik**, kdy budou zavedena přiměřená bezpečnostní opatření ke zvládání rizik.

Pro identifikaci aktiv, které by měly být regulovány, se jako vhodná inspirace jeví Finský model, který definuje tzv. kritické funkce. Na základě nich posléze Odběratelé ve svých sítích identifikují kritické části systému, které podléhají v případě bezpečnostně relevantní dodávky potřebě prověření dodavatele ze strany státu.

Pro fázi identifikace konkrétních rizik spojených s konkrétními dodavateli se jako vhodný model naopak jeví Německý model, který zavádí koncept tzv. záruky ze strany dodavatele. V rámci správního řízení se v tomto ohledu jeví jako žádané, aby Dodavatel měl možnost předložit konkrétní důkazy, prokazující svou důvěryhodnost. Záruka je také dobrým podkladem pro samotný orgán vedoucí řízení o prověření, na jehož základě mohou být efektivně prověřována a případně identifikována konkrétní rizika spojená s dodavatelem.

Následný proces identifikace zranitelností vyžaduje participaci ze strany Odběratele. Je proto žádoucí, aby osvědčení o prověření mohlo být vydáno již před touto fází, za předpokladu, že na straně Dodavatele **nebudou identifikována žádná rizika**. V případě identifikace konkrétních rizik na straně dodavatele je dobrou inspirací Německý i Finský model, kdy v obou případech jsou v rámci hodnocení rizik brána v potaz již zavedená bezpečnostní opatření ze strany Odběratele a technické aspekty konkrétní dodávky. Strategická kritéria, jejichž význam zde není zpochybňován, jsou tak hodnocena v rámci technických aspektů kybernetické bezpečnosti.
Na základě výše uvedeného procesu také současně vzniknou obsáhlé podklady i k samotné fázi **řízení rizik**. Kdy se znalostí konkrétních zranitelností a konkrétních rizik bude zavedení efektivních bezpečnostních opatření zásadně snadnější.

2.7. Role NÚKIB v mechanismu

Řízení o prověření vedeno Ministerstvem průmyslu a obchodu

V souvislosti s procesem prověřování dodavatelů je zásadní otázkou, u kterého správního orgánu by mělo být příslušné řízení vedeno. Ačkoli se jedná o záležitost týkající se kybernetické bezpečnosti, nelze přehlédnout, že věc má i další roviny. Následující skutečnosti vedou k závěru, že **nejvhodnějším orgánem pro vedení příslušného řízení je Ministerstvo průmyslu a obchodu** (dále jen „*ministerstvo*“).

Předně, problematika výběru (a omezování výběru) dodavatelů se zásadně dotýká hospodářské soutěže a ekonomiky. Jakékoli omezení či dokonce vyloučení některých dodavatelů může mít zásadní dopad na rychlost rozvoje telekomunikačních sítí a náklady s tím spojené. Věc je tedy **úzce spojena se státní průmyslovou a obchodní politikou**, pro kterou představuje ministerstvo ústřední orgán státní správy dle § 13 odst. 1 písm. a) zákona č. 2/1969 Sb., ve znění pozdějších předpisů.

Stejné ustanovení uvádí, že ministerstvo je ústředním správním orgánem rovněž pro **zahraničně ekonomickou politiku**. Dle § 13 odst. 3 mimo jiné koordinuje zahraničně obchodní politiku České republiky ve vztahu k jednotlivým státům, zabezpečuje sjednávání dvoustranných a mnohostranných obchodních a ekonomických dohod včetně komoditních dohod, realizuje obchodní spolupráci s ES, ESVO, GATT a jinými mezinárodními organizacemi a integračními seskupeními. Ministerstvo je tedy zásadně **předurčeno k řešení veškerých zahraničně-obchodních záležitostí**. Mezi ně posuzování dodavatelů majících své mateřské subjekty v zahraničí nepochybně patří.

Do působnosti ministerstva navíc dle platné právní úpravy patří prověřování zahraničních investic. Ministerstvo je k tomuto zmocněno jednak v § 13 odst. 1 písm. d) zákona č. 2/1969 Sb., jednak zvláštním zákonem č. 34/2021 Sb., který toto prověřování podrobně upravuje. Prověřování zahraničních investic se svojí povahou a účelem prověřování dodavatelů do infrastruktury elektronických komunikací blíží, neboť zákon 34/2021 Sb. dle § 1 písm. a) stanoví *„pravidla prověřování některých zahraničních investic z důvodu ochrany bezpečnosti České republiky a vnitřního či veřejného pořádku*“. Součástí posouzení tak jsou i politická kritéria – obdobně, jak zvažuje ve svém návrhu NÚKIB.

Jak vyplývá z výše uvedeného, **ministerstvo má** k vedení řízení o prověření dodavatelů nejen **zákonné předpoklady**, ale zároveň i **personální aparát** odpovídající **odbornosti a zkušeností**,

neboť dlouhodobě řeší povahově obdobné záležitosti. **Je tedy zcela přirozeným a efektivním řešením, aby i prověřování dodavatelů bylo v jeho gesci**.

Role NÚKIB má v řízení rovněž svou váhu, a to s ohledem na účel řízení, kterým je posilování kybernetické bezpečnosti. S ohledem na převažující zahraničně-obchodní povahu věci by mělo zaujímat primární roli ministerstvo. Pokud by měl do řízení určitým způsobem zasahovat NÚKIB, jeví se jako vhodné řešení jeho zapojení formou vyžádání stanoviska k určité otázce, která spadá do jeho působnosti.

S přátelským pozdravem,
Jakub Rejzek, MBA, LL.M.
Předseda prezidia Výboru nezávislého ICT průmyslu z.s.

V kopii paní A. Dobyšarová; a.dobysarova@nukib.cz

Jakub Rejzek
Digitally signed by Jakub Rejzek
Date: 2022.04.07 12:28:42 +02'00'

Disclaimer: Výbor nezávislého ICT průmyslu z.s. nezastupuje společnost Vodafone v záležitostech týkající se mobilních sítí. Připomínky týkající se mobilních sítí nejsou názorem společnosti Vodafone a jejich text nebyl se společností Vodafone Czech Republic a.s. konzultován.