Vládní návrh

ZÁKON

ze dne ……. 2017,

kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony

Parlament se usnesl na tomto zákoně České republiky:

Č Á S T P R V N Í

Změna zákona o Vojenském zpravodajství

Čl. I

Zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění zákona č. 274/2008 Sb., zákona č. 254/2012 Sb., zákona č. 273/2012 Sb., zákona č. 64/2014 Sb., zákona č. 250/2014 Sb. a zákona č. 47/2016 Sb., se mění takto:

1. V § 1 se doplňuje odstavec 3, který včetně poznámky pod čarou č. 19 zní:

„(3) Vojenské zpravodajství za podmínek stanovených tímto zákonem plní úkoly obrany České republiky v kybernetickém prostoru[19)] (dále jen „kybernetická obrana“).

[19)] § 2 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).“.

2. Za část třetí se vkládá nová část čtvrtá, která včetně nadpisu zní:

„ČÁST ČTVRTÁ

KYBERNETICKÁ OBRANA

§ 16a

Zajišťování kybernetické obrany

(1) Vojenské zpravodajství zajišťuje kybernetickou obranu jako součást obrany České republiky.

(2) Vojenské zpravodajství může při zajišťování kybernetické obrany využívat technické prostředky kybernetické obrany, kterými jsou věcné technické prostředky vedoucí

k předcházení, zastavení nebo odvrácení kybernetického útoku ohrožujícího zajišťování obrany České republiky; Vojenské zpravodajství při zajišťování kybernetické obrany společně s technickými prostředky kybernetické obrany k dosažení shodného účelu využívá také související postupy a opatření.

(3) Využívat technické prostředky kybernetické obrany na území České republiky, pokud lze očekávat, že naruší důvěrnost zpráv podle zákona o elektronických komunikacích a s nimi spojených provozních a lokalizačních údajů konkrétní osoby, lze výlučně za podmínek stanovených pro použití zpravodajské techniky tímto zákonem.

§ 16b

Předpoklady umístění a použití technických prostředků kybernetické obrany

Umístění technických prostředků kybernetické obrany podle § 16a může být provedeno výlučně na základě jeho schválení vládou, která rovněž schválí podmínky jejich používání k zajištění kybernetické obrany. Návrh na umístění technických prostředků kybernetické obrany, jehož součástí je také návrh podmínek jejich používání, předkládá vládě ministr obrany na základě návrhu ředitele Vojenského zpravodajství.

§ 16c

Součinnost

Vojenské zpravodajství může za podmínek schválených vládou podle § 16b a v rozsahu potřebném pro zajišťování kybernetické obrany požadovat od právnické nebo podnikající fyzické osoby zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací zřízení a zabezpečení rozhraní pro připojení technických prostředků kybernetické obrany.“.

Dosavadní části čtvrtá až šestá se označují jako části pátá až sedmá.

3. V § 22 se na konci odstavce 2 tečka nahrazuje čárkou a doplňuje se písmeno f), které zní:

„f) usnesení vlády, kterým vláda schválila umístění a podmínky použití technických prostředků kybernetické obrany podle § 16b.“.

4. V § 22 odst. 3 se za písmeno b) vkládá nové písmeno c), které zní:

„c) zprávu o použití technických prostředků kybernetické obrany na území České republiky, a to pouze ve věcech a v případech, ve kterých Vojenské zpravodajství svou činnost již ukončilo,“.

Dosavadní písmena c) až e) se označují jako písmena d) až f).

Č Á S T D R U H Á

Změna zákona o zajišťování obrany České republiky

Čl. II

Zákon č. 222/1999 Sb., o zajišťování obrany České republiky, ve znění zákona č. 320/2002 Sb., zákona č. 436/2004 Sb., zákona č. 413/2005 Sb., zákona č. 112/2006 Sb., zákona č. 186/2006 Sb., zákona č. 306/2008 Sb., zákona č. 281/2009 Sb., zákona č. 73/2011 Sb., zákona č. 375/2011 Sb., zákona č. 15/2015 Sb. a zákona č. 47/2016 Sb., se mění takto:

1. V § 2 odst. 1 větě druhé se za slova „Obrana státu“ vkládají slova „ , jejíž součástí je také obrana státu v kybernetickém prostoru[20)] (dále jen „kybernetická obrana“),“.

Poznámka pod čarou č. 20 zní:

„[20)] § 2 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).“.

2. V § 2 se za odstavec 1 vkládá nový odstavec 2, který zní:

„(2) Kybernetickou obranou se rozumí souhrn činností a opatření směřujících k vytvoření účinného systému obrany v kybernetickém prostoru a příprava a použití sil a technických prostředků kybernetické obrany podle zákona o Vojenském zpravodajství.“.

Dosavadní odstavce 2 až 8 se označují jako odstavce 3 až 9.

3. V § 2 odst. 9 větě druhé se slova „mobilizační plánování a“ nahrazují slovy „mobilizační plánování,“ a na konci textu odstavce 9 se doplňují slova „a plánování kybernetické obrany“.

4. V § 5 odst. 1 se na konci textu písmene d) doplňují slova „a schvaluje plán kybernetické obrany státu a jeho změny“.

5. Za § 9a se vkládá nový § 9b, který zní:

„§ 9b

Za stavu ohrožení státu vyhlášeného v souvislosti se zajišťováním obrany České republiky před vnějším napadením nebo za válečného stavu může Národní bezpečnostní úřad uložit provést reaktivní opatření nebo ochranné opatření podle zákona o kybernetické bezpečnosti, pokud to nebrání zajišťování kybernetické obrany.“.

Č Á S T T Ř E T Í

Změna zákona o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)

Čl. III

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění zákona č. 290/2005 Sb., zákona č. 361/2005 Sb., zákona č. 186/2006 Sb., zákona 235/2006 Sb., zákona č. 310/2006 Sb., zákona č. 110/2007 Sb., zákona č. 261/2007 Sb., zákona č. 304/2007 Sb., zákona č. 124/2008 Sb., zákona č. 177/2008 Sb., zákona č. 189/2008 Sb., zákona č. 247/2008 Sb., zákona č. 384/2008 Sb., zákona č. 227/2009 Sb., zákona č. 281/2009 Sb., zákona č. 153/2010 Sb., nálezu Ústavního soudu, vyhlášeného pod č. 94/2011 Sb., zákona č. 137/2011 Sb., zákona č. 341/2011 Sb., zákona č. 375/2011 Sb., zákona č. 420/2011 Sb., zákona č. 457/2011 Sb., zákona č. 468/2011 Sb., zákona č. 18/2012 Sb., zákona č. 19/2012 Sb., zákona č. 142/2012 Sb., zákona č. 167/2012 Sb., zákona č. 273/2012 Sb., zákona č. 214/2013 Sb., zákona č. 303/2013 Sb., zákona č. 181/2014 Sb., zákona č. 234/2014 Sb., zákona č. 250/2014 Sb., zákona č. 258/2014 Sb., zákona č. 318/2015 Sb., zákona č. 378/2015 Sb., zákona č. 222/2016 Sb., zákona č. 298/2016 Sb. a zákona č. …/2016 Sb., se mění takto:

1. V § 10 odst. 1 písm. o) se za slova „§ 97“ vkládají slova „a 98a“.

2. Za § 98 se vkládá nový § 98a, který zní:

„§ 98a

(1) Právnická nebo podnikající fyzická osoba zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací je povinna, je-li o to požádána za účelem plnění úkolů kybernetické obrany Vojenským zpravodajstvím na základě zákona o Vojenském zpravodajství, zřídit a zabezpečit ve vhodných bodech své sítě rozhraní pro připojení technických prostředků kybernetické obrany.

(2) Za plnění povinností podle odstavce 1 náleží právnické nebo podnikající fyzické osobě od Vojenského zpravodajství úhrada efektivně vynaložených nákladů. Způsob určení výše efektivně vynaložených nákladů a způsob jejich úhrady stanoví prováděcí právní předpis.

(3) Osoba uvedená v odstavci 1, jakož i jiné osoby podílející se na plnění povinnosti podle odstavce 1, jsou povinny zachovávat mlčenlivost o připojení technických prostředků kybernetické obrany podle odstavce 1 a s tím souvisejících skutečnostech. Tato povinnost trvá i poté, kdy tato osoba přestane být osobou podle odstavce 1 nebo osobou podílející se na plnění povinnosti podle věty první.“.

3. V § 118 se za odstavec 21 vkládá nový odstavec 22, který zní:

„(22) Právnická nebo podnikající fyzická osoba se jako osoba zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací dopustí správního deliktu tím, že

a) v rozporu s § 98a odst. 1 nezřídí nebo nezabezpečí v určených bodech své sítě rozhraní pro připojení technických prostředků kybernetické obrany na žádost Vojenského zpravodajství, nebo
b) poruší povinnost zachovávat mlčenlivost podle § 98a odst. 3.“.

Dosavadní odstavec 22 se označuje jako odstavec 23.

4. V § 118 odst. 22 úvodní části ustanovení se slova „správního deliktu“ nahrazují slovem „přestupku“.

5. V § 118 odst. 23 písm. c) se slova „odstavce 16, 17, 18, 19, 20 nebo 21“ nahrazují slovy„16 až 21 nebo 22“.

6. V § 119 se za odstavec 6 vkládá nový odstavec 7, který zní:

„(7) Fyzická osoba se jako osoba podílející se na plnění povinností právnické nebo podnikající fyzické osoby zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací dopustí přestupku tím, že poruší povinnost zachovávat mlčenlivost podle § 98a odst. 3.“.

Dosavadní odstavec 7 se označuje jako odstavec 8.

7. V § 119 odst. 8 větě první se číslo „6“ nahrazuje číslem „7“.

8. V § 150 se doplňuje odstavec 7, který zní:

„(7) Ministerstvo obrany vydá vyhlášku k provedení § 98a odst. 2.“.

ČÁST ČTVRTÁ

ÚČINNOST

Čl. IV

Tento zákon nabývá účinnosti patnáctým dnem po jeho vyhlášení, s výjimkou čl. III bodu 4, který nabývá účinnosti 1. července 2017.

DŮVODOVÁ ZPRÁVA

A) Závěrečná zpráva RIA

SHRNUTÍ ZÁVĚREČNÉ ZPRÁVY RIA

1. Základní identifikační údaje	
1. Název návrhu: **Zákon, kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony**	
Zpracovatel / zástupce předkladatele: **Ministerstvo obrany**	Předpokládaný termín nabytí účinnosti, v případě dělené účinnosti rozveďte *01.2017*
Implementace práva EU: Ne	
2. Cíl návrhu zákona	
Cílem návrhu je realizace usnesení vlády ze dne 25. května 2016 č. 382, kterým vláda schválila Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 a kterým je Ministerstvu obrany uložen úkol normativního řešení vytvoření podmínek kybernetické obrany České republiky jako součásti obrany České republiky podle zákona č. 222/1999 Sb., o zajišťování obrany České republiky, ve znění pozdějších předpisů. *Působnost v oblasti zajišťování kybernetické obrany bude svěřena Vojenskému zpravodajství.*	
3. Agregované dopady návrhu zákona	
3.1 Dopady na státní rozpočet a ostatní veřejné rozpočty: Ano	
Celkový dopad na státní rozpočet se bude odvíjet od úrovně kvality zabezpečování kybernetické obrany vyžadované po Vojenském zpravodajství státem. Jako obrana státu obecně, i kybernetická obrana může být značně nákladná. Samotný návrh zákona však přímo žádné dopady na státní rozpočet nevyvolává, jelikož úkol zabezpečovat kybernetickou obranu ukládá pouze v obecné rovině, bez konkrétních úkolů, jejichž zabezpečení by vyvolávalo přímé náklady. V základním módu lze kybernetickou obranu provádět i v rámci současného rozpočtu. Náklady proto mohou vznikat až v okamžiku, kdy vláda na základě schváleného zákona schválí konkrétní obsah a rozsah kybernetické obrany do budoucna, teprve v tomto okamžiku bude možné vyčíslit nutné náklady.	
3.2 Dopady na mezinárodní konkurenceschopnost ČR: Ne	
3.3 Dopady na podnikatelské prostředí: Ano	
Dopad na podnikatelské subjekty v působnosti zákona o elektronických komunikacích bude spočívat v jejich povinnosti strpět nasazení technických prostředků kybernetické obrany v jimi provozované infrastruktuře. Za tuto povinnost však budou státem hrazeny účelně vynaložené náklady	
3.4 Dopady na územní samosprávné celky (obce, kraje): Ne	
3.5 Sociální dopady: Ne	
3.6 Dopady na spotřebitele: Ne	

3.7 Dopady na životní prostředí: Ne
3.8 Dopady ve vztahu k zákazu diskriminace a ve vztahu k rovnosti žen a mužů: Ne
3.9 Dopady na výkon státní statistické služby: Ne
3.10 Korupční rizika: Ano
Velmi nízká. Popsána v důvodové zprávě.
3.11 Dopady na bezpečnost nebo obranu státu: Ano
Návrh se přímo dotýká bezpečnosti a obrany, jelikož upravuje výkon kybernetické obrany jako součásti zajišťování obrany státu. Dopady jsou specificky zhodnoceny v části X. obecné části důvodové zprávy.

Závěrečná zpráva o zhodnocení dopadů regulace (RIA)

1. Důvod předložení a cíle

1.1 Název

Návrh zákona, kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony

1.2 Definice problému

Problematika bezpečnosti je v českém právním řádu již řešena, přičemž jako základ lze považovat ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů. Ustanovení definuje „zajištění svrchovanosti a územní celistvosti České republiky, ochranu jejich demokratických základů a ochranu životů, zdraví a majetkových hodnot“ za základní povinnosti státu. V případě kybernetické bezpečnosti je situace poněkud odlišná. „Kybernetická bezpečnost naráží na limity klasického dělení bezpečnosti, tedy dělení na bezpečnost vnitřní a vnější nebo na bezpečnost tvrdou a měkkou. Vnitřní bezpečnost počítá s identifikací a eliminací hrozeb nacházejících se uvnitř objektu, vnější bezpečnost se pak soustřeďuje na identifikaci a eliminaci hrozeb vně objektu. Tvrdá bezpečnost se pak soustřeďuje na hrozby vojenského charakteru a měkká na ostatní. Již ze samotného popisu jednotlivých dělení je patrné, že kybernetická bezpečnost prochází napříč těmito děleními, protože postihuje vojenské i nevojenské použití informačních technologií za účelem útoku na informační systémy. Stejně tak zahrnuje vnitřní i vnější bezpečnostní rizika. Proto je potřeba přijmout ještě další kategorie, skrze které bude přesně definována. Bezpečnostní terminologie přímo počítá s přidáním adjektiva (v tomto případě adjektiva „kybernetický“), které bude specifikovat charakter ochraňovaného objektu (tedy informačních systémů).“[19]

Kybernetický prostor nabývá v moderním světě stále více na důležitosti. Na informacích a informačních technologiích je založeno velké množství lidských činností, dnes si bez nich není možné představit žádnou podstatnější aktivitu, ať už jde o obchod, zábavu, koníčky, ale také výkon státní správy respektive veřejné správy jako takové. Závislost společnosti a jejího fungování na informačních technologiích rapidně narůstá, a to ve všech oblastech (nejedná se pouze o služby informační společnosti jako je internetový obchod, ale i o fungování informačních systémů, na jejichž správné funkci je závislá celá řada základních služeb jako například řízení dopravy, výroba a přenos energií, zdravotnictví, výkon veřejné moci apod.). Se vzrůstající závislostí společnosti na informačních technologiích pak ale na straně druhé vzrůstá i riziko zneužívání těchto technologií nebo útoky na tyto technologie, které mají rozsáhlé dopady do činnosti subjektů, které s nimi pracují, a potencionálně mohou vést ke značným škodám.

Kybernetický prostor se stále více stává také prostorem, ve kterém mohou být vedeny konflikty jak mezi státními, tak nestátními aktéry. Výhodou je možnost značné anonymity, rychlosti, možnosti způsobit značné škody bez toho, aby pachatel sám sebe vystavil přímému riziku. Kybernetický prostor je prostor bez hranic, bez jasného určení slabších a silnějších stran, ba dokonce i bez jasného vymezení hranic „kybernetického prostoru“ jednotlivých států coby tradičních subjektů mezinárodního práva veřejného. Přitom vzhledem ke stále

[19] Harašta, Jakub 1.3 Povaha kybernetické bezpečnosti. Právní aspekty kybernetické bezpečnosti ČR [Systém ASPI] RPT. - Revue pro právo a technologie [cit. 2015-10-7] ASPI_ID LIT46505CZ. Dostupné v Systému ASPI. ISSN: 2336-517X

se rozšiřujícímu významu elektronických sítí a komunikačních prostředků je určení jednotlivých států za cíl útoku v kybernetickém prostoru stále běžnější a tím roste i důležitost jejich ochrany v tomto prostoru.

V teorii války začíná být kybernetický prostor považován za pátou dimenzi pro válčení, vedle země, moře, vzduchu a vesmíru. Je proto důležité pro ozbrojené síly každého státu brát tuto okolnost vážně a budovat v rámci svých možností kapacity na vedení operací také v rámci kybernetického prostoru. Důležitost je o to vyšší, že v kybernetickém prostoru lze zaútočit nečekaně, a prakticky odkudkoli. Na rozdíl od tradičního kinetického válčení není možné dopředu pozorovat přesuny jednotek a zbraní, není možné soustředit se jen na nejbližší nebo nejsilnější sousedy a vnější napadení může být dokonce vedeno skrze sítě nacházející se na výsostném území napadeného státu. V kybernetickém prostoru tak lze být napaden z jakékoli dálky, od stolu od počítače, a to nejen vojensky silnými státy, ale i slabými, nestátními teroristickými skupinami a dokonce i jednotlivci. Škody způsobené takovými útoky přitom mohou být nedozírné.

Kybernetické útoky lze dělit různými způsoby. Jedním z užívaných dělení je dělení na kyberkriminalitu, hacktivismus, kybernetickou válku a kybernetickou špionáž. Dělícím činitelem je motivace původců těchto útoků, kdy kyberkriminalita směřuje k vlastnímu obohacení původce, hacktivismus na upozornění na určitý problém formou apelu, kybernetická válka k poškození infrastruktury jiným státem či nestátním aktérem a kybernetická špionáž k získání jinak nedostupných informací v obchodním či mezinárodním styku. Existuje i dělení útoků podle závažnosti od nejslabších po nejsilnější, bez jasných hranic mezi jednotlivými typy, kterými mohou být porušení vnitřních nařízení, porušení právní povinnosti, kybernetická kriminalita, kybernetický terorismus, kybernetická válka.

Každý stát by proto měl budovat struktury k zajištění ochrany a obrany svých zájmů v kybernetickém prostoru před kybernetickými útoky. K budování těchto schopností je ČR zavázána svým členstvím v Organizaci Severoatlantické smlouvy (dále jen „NATO“), která mj. na svém summitu ve Walesu deklarovala, že členské státy budou budovat a vylepšovat své kapacity v kybernetické bezpečnosti. Jak plyne také ze Strategického návrhu o obraně a bezpečnosti členů NATO, přijatého v listopadu 2010 v Lisabonu, členské státy uznávají, že škodlivé kybernetické aktivity mohou překročit práh, kdy začnou ohrožovat národní a euroatlantickou prosperitu, bezpečnost a stabilitu. Poslední summit ve Varšavě pak uznal kybernetický prostor za 4. doménu válčení (vesmír se považuje za samostatnou doménu jen někdy) a kybernetický útok uznal za způsobilý aktivovat čl. 5 Severoatlantické smlouvy.

V rámci Bezpečnostní strategie České republiky, aktualizované v únoru 2015, jsou mezi identifikovanými hrozbami uvedeny kybernetické útoky. „Kybernetický prostor je velmi specifický neexistencí geografických hranic a relativizací vzdálenosti mezi zdroji hrozeb a potenciálním cílem. Díky své asymetričnosti pak umožňuje státním i nestátním aktérům poškodit strategické a významné zájmy České republiky bez využití konvenčních prostředků. Neustále se zvyšuje počet a sofistikovanost kybernetických útoků proti veřejné a soukromé sféře. Tyto útoky mohou způsobit selhání zejména komunikačních, energetických a dopravních sítí či dopravních procesů, průmyslových nebo finančních systémů, mající za následek významné hmotné škody. Závislost ozbrojených sil státu na informačních a komunikačních systémech může mít vliv na obranyschopnost státu. S kybernetickými útoky zároveň úzce souvisí problematika politické a ekonomické špionáže.“

V návaznosti na kybernetickou bezpečnost České republiky je pak nutné definovat schopnost kybernetické obrany, která by měla být aktivována převážně ve chvílích, kdy kybernetické útoky mířené proti České republice budou takové intenzity a budou směřovat proti svrchovanosti, územní celistvosti, principům demokracie a právního státu, ochrany života obyvatel a jejich majetku[20], že je již nebude možné zvládat běžnými prostředky a opatřeními kybernetické bezpečnosti, jak je v současnosti zná zákon o kybernetické bezpečnosti. Z výše uvedeného je patrné, že Česká republika potřebuje v rámci obranných kapacit prvek schopný provádět široké spektrum operací v kybernetickém prostoru, který by byl schopen aktivního využití prostředků kybernetické obrany a byl by schopen eliminace závažných kybernetických útoků mířených proti České republice a jejím zájmům. V neposlední řadě by měl mít tento prvek schopnost v případě ozbrojeného konfliktu provádět vojenské operace v kybernetickém prostoru na podporu konvenčních vojenských sil. Takový prvek by přispěl ke zvýšení odolnosti informačních a komunikačních systémů obranných složek a navýšily by se tak možnosti a kapacity v oblasti obrany státu.

Jako jeden z inspiračních zdrojů teoretických východisek pro řešení problematiky kybernetické obrany a bezpečnosti lze využít výstupy z tallinského NATO Cooperative Cyber Defence Centre of Excellence, které se zabývá v rámci NATO kybernetickou bezpečností. Jedním ze základních dokumentů je Rámcový manuál k národní kybernetické bezpečnosti, který podává poměrně vyčerpávající teoretický základ k tvorbě národních strategií kybernetické bezpečnosti.

Národní kybernetická bezpečnost může být definována jako cílené uplatňování specifických státních prostředků a principů sloužících k zabezpečení veřejných, soukromých a relevantních mezinárodních informačních a komunikačních systémů, informací v nich a souvisejícího obsahu, pokud se tyto systémy dotýkají národní bezpečnosti.

Kybernetická bezpečnost v tom nejširším slova smyslu[21] má mnoho rovin, které se vzájemně prolínají, ale současně se od sebe liší. Můžeme uvažovat o těchto rovinách:

1. Pravidla využívání infrastruktury a její ochrana
2. Ochrana kritické infrastruktury a národní krizový management
3. Boj proti kybernetické kriminalitě a kyberterorismu
4. Rozvědná a kontrarozvědná činnost v kybernetickém prostoru
5. Kybernetická obrana (ve vojenském smyslu)

Jak vyplývá z výše uvedeného, bezpečnost národního kybernetického prostředí závisí na mnoha aktérech s různými rolemi a úkoly, a na mnoha faktorech. Úspěšná ochrana tohoto prostoru se neobejde bez toho, aby úloha všech zainteresovaných subjektů byla jasně identifikována a popsána, aby si všichni tito aktéři uvědomili svoji sféru odpovědnosti a aby všichni měli k dispozici nezbytné prostředky k efektivnímu plnění svých úkolů. K naplnění těchto požadavků slouží mj. základní strategické dokumenty České republiky, Obrannou strategií počínaje (schválená usnesením vlády č. 699 ze dne 26. 9. 2012), přes Bezpečnostní strategii (usnesení vlády č. 79/2015), Národní strategii kybernetické bezpečnosti (usnesení vlády č. 105/2015) až k Akčnímu plánu k této strategii (usnesení vlády č. 382/2015).

[20] § 2 odst. 1 zákona č. 222/1999 Sb., o zajišťování obrany České republiky.

[21] Kybernetickou bezpečností v nejširším slova smyslu je nutno rozumět veškeré aktivity týkající se bezpečnosti státu, které mají souvislost s kybernetickým prostorem. Tento pojem nelze proto zaměňovat s pojmem „kybernetická bezpečnost“ vy smyslu zákona č. 181/2014 Sb., neboť ten upravuje pouze část problematiky.

Kromě těchto strategických dokumentů je důležité zásadní otázky upravit v právním řádu České republiky. Právní řád z uvedených rovin poměrně dobře upravuje první čtyři roviny kybernetické bezpečnosti. Naopak poslední rovinou, tj. problematikou kybernetické bezpečnosti a obrany ve smyslu vojensko-zpravodajském, se dosud žádným způsobem nezabývá. Vzhledem k tomu pak nelze při přípravě a samotném výkonu této činnosti využívat žádné zvláštní postupy a oprávnění, které ale jsou k této činnosti potřebné. Neexistence právní úpravy pro zajišťování kybernetické obrany jako části problematiky kybernetické bezpečnosti (v širším slova smyslu) a pochopitelně jako nedílné součásti zabezpečování obrany České republiky tak lze považovat za závažný nedostatek.

1.3 Popis existujícího právního stavu v dané oblasti

Vzhledem k tomu, že problematika kybernetických hrozeb je poměrně nová, právní řád na ni teprve v poslední době začíná reagovat. Jak bylo řečeno výše, problematika ochrany kybernetického prostoru má více rovin. Každá z těchto rovin je právně upravena na jiné úrovni, přičemž se prolíná různými právními předpisy v rámci právního řádu. Použijeme toto rozdělení při popisu právního stavu v každé z oblastí.

Ad 1) Využívání infrastruktury a rovněž zajištění její bezpečnosti řeší zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů, především hlava V., § 87 až § 104, upravující ochranu údajů, služeb a sítí elektronických komunikací. Provozovatelům této infrastruktury a služeb ukládá řadu úkolů v oblasti zajištění jejich ochrany a bezpečnosti. Působnost v této oblasti má svěřenu Ministerstvo průmyslu a obchodu a Český telekomunikační úřad.

Ad 2) Ochrana kritické informační infrastruktury, problematika kybernetického prostoru vůbec, jeho bezpečnosti a ochrany či obrany se do českého právního řádu v konkrétní podobě dostala zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Upravuje systém zajištění kybernetické bezpečnosti, a to pomocí bezpečnostních opatření, technických a organizačních, které jsou povinné osoby povinny provádět pro zajištění kybernetické bezpečnosti. Dále se stanoví definice bezpečnostních událostí a bezpečnostních incidentů, a detekce událostí a řešení incidentů. Zavádí také tzv. stav kybernetického nebezpečí. Působnost v této oblasti má svěřenu Národní bezpečnostní úřad. Přijetí zákona o kybernetické bezpečnosti bylo významných krokem vpřed, nicméně je třeba poznamenat, že tento zákon řeší kybernetickou bezpečnost v užším slova smyslu, tzn. jeho cílem je zajistit bezpečnost nejvýznamnějších informačních a komunikačních systémů (kritická informační infrastruktura a významné informační systémy), a to zejména s ohledem na zajištění důvěrnosti, integrity a dostupnosti informací. Nezabývá se situacemi, které naplňují znaky působení cizích rozvědných služeb, neřeší ani boj proti protiprávním činům v kyberprostoru a už vůbec se netýká situací, které lze z vojenského hlediska považovat za útok proti svrchovanosti státu a tedy obranou státu v kybernetickém prostoru. Kromě toho se netýká informačních a komunikačních systémů, které nakládají s utajovanými informacemi, což ale může být zejména v rámci kyberšpionáže zásadní cíl útoku (tyto systémy jsou nicméně chráněny cestou instrumentů zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů).

Ad 3) Jednou z dalších rovin zmíněných výše je boj proti kyberkriminalitě a kyberterorismu. Ačkoli se jedná o dvě odlišné věci, zejména z hlediska cíle útoků, obecně

jde o podobné jevy. Určitou působnost v této oblasti mají také zpravodajské služby, a to z hlediska získávání informací o záměrech a činnostech směřujících vůči bezpečnosti ČR, základním činitelem jsou ale zejména Policie České republiky a následně orgány činné v trestním řízení. Řada činností spadajících pod pojem kyberkriminalita nebo kyberterorismus je totiž podle českého trestního práva trestnými činy. V této oblasti je právní úprava poměrně pokročilá, české trestní právo kriminalizuje řadu jednání souvisejících s kybernetickým prostorem, a to zejména v návaznosti na mezinárodní instrumenty, zejména Úmluvu o počítačové kriminalitě z roku 2001 (v platnost vstoupila v roce 2004). Právní úpravu obsahuje trestní zákoník, konkrétně zejména § 230 (neoprávněný přístup k počítačovému systému a nosiči informací), § 231 (opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat), § 232 (poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti), § 182 (porušení tajemství dopravovaných zpráv), ale i další ustanovení odpovídající požadavkům Úmluvy. I některé jiné skutkové podstaty trestných činů mohou být naplněny jednáním, které se uskuteční v kybernetickém prostoru. Mezi nejzávažnější lze určitě zařadit např. teroristický útok (§ 311) nebo vyzvědačství (§ 316).

Ad 4) Další rovinou je rozvědná činnost v kybernetickém prostoru, resp. kontrarozvědná činnost jako její opak. Kybernetický prostor je výjimečné prostředí k provádění špionáže kvůli své relativní anonymitě, možnosti přenášet velké objemy dat a možnosti maskovat místo původu „útoku“ (ve většině případů však nejde o ozbrojený útok zakládající právo státu na sebeobranu podle mezinárodního práva). Pro zejména zpravodajské služby je tedy kybernetický prostor velmi důležitou sférou, a to jak z hlediska možností získávat informace, tak z hlediska ochrany vlastních informací před obdobnou činností protivníka. V této oblasti zatím žádné specifické právní předpisy Česká republika nemá (s výjimkou toho, že některé jednání může být postihováno v trestněprávní rovině, jak je popsáno výše), uplatní se tedy standardní pravidla pro zpravodajskou činnost a kontrarozvědnou činnost platná i pro jiné oblasti, ať už se jedná o postupy zpravodajských služeb a policie, nebo o trestní stíhání těchto činů. Je však nutné poznamenat, že znění těchto zákonů, zejména ohledně tzv. specifických prostředků získávání informací, zdaleka nestíhá překotný vývoj v této oblasti a nepostihuje tak všechny možnosti, které dnešní kybernetický prostor nabízí. Tento problém však vyžaduje hlubší analýzy a důkladnější změny právní úpravy zpravodajských služeb a není proto součástí předkládaného návrhu zákona.

Ad 5) Obrana státu je v právním řádu řešena dosud spíše na bázi kinetického válčení v podobě klasického konvenčního konfliktu. Pokud se ovšem soustředíme na právní úpravu pak již ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, nerozlišuje případné napadení na vnější a vnitřní, nýbrž obecně umožňuje pro případy, je-li bezprostředně ohrožena svrchovanost, územní celistvost, demokratické základy České republiky nebo ve značném rozsahu vnitřní pořádek a bezpečnost, životy a zdraví, majetkové hodnoty nebo životní prostředí anebo je-li třeba plnit mezinárodní závazky o společné obraně, vyhlásit podle intenzity, územního rozsahu a charakteru situace nouzový stav, stav ohrožení státu nebo válečný stav. Bezpečnost České republiky zajišťují ozbrojené síly, ozbrojené bezpečnostní sbory, záchranné sbory a havarijní služby. Státní orgány, orgány územních samosprávných celků a právnické a fyzické osoby jsou povinny se podílet na zajišťování bezpečnosti České republiky. Rozsah povinností a další podrobnosti stanoví zákon.

Na tento ústavní zákon pak ovšem navazují další zákony, které spojují a zaměřují institut obrany státu na hrozbu vnějšího napadení, tedy zejména zákon č. 219/1999 Sb., o ozbrojených silách, ve znění pozdějších předpisů, podle něhož „K zajišťování své

bezpečnosti vytváří Česká republika ozbrojené síly. Základním úkolem ozbrojených sil je připravovat se k obraně České republiky a bránit ji proti vnějšímu napadení.“. Obdobně je obrana státu zaměřena proti vnějšímu napadení podle § 2 odst. 1 zákona č. 222/1999 Sb., o zajišťování obrany České republiky, který stanoví, že se jedná o „souhrn opatření k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením. Obrana státu zahrnuje výstavbu účinného systému obrany státu, přípravu a použití odpovídajících sil a prostředků a účast v kolektivním obranném systému“. Zapomenout ale nelze ani na zákon č. 153/1994 Sb., o zpravodajských službách, podle jehož § 2 zpravodajské služby jsou státní orgány pro získávání, shromažďování a vyhodnocování informací důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnost a obranu České republiky, a tedy se na zajišťování obrany státu také významně podílejí.

Konkrétní zmínka o kybernetickém prostoru a jeho obraně v těchto zákonech zatím není. V rámci uvedených právních předpisů by činnosti obsahově odpovídající kybernetické obraně mohly být prováděny, byť s určitým omezením, vyplývajícím z přece jenom značně odlišného prostředí, v němž by docházelo k aktivitám ohrožujícím bezpečnost České republiky. Pokud by se v oblasti kybernetického prostoru jednalo čistě o obranu státu proti vnějšímu napadení, pak by ozbrojené síly, resp. armáda, mohly vyvíjet činnost i bez novelizace příslušných zákonů, stejně tak i další orgány mající za úkol zajišťovat bezpečnost státu. Vzhledem k povaze kybernetického prostoru však není vždy jednoznačně možné okamžitě odlišit vnější a vnitřní napadení, a stejně tak není možné zcela přesně vyhodnotit, zda již jde o ozbrojený útok zakládající právo státu na sebeobranu ve smyslu mezinárodního práva nebo zda se jedná o čin charakteru teroristického, kriminálního nebo např. špionážního. Právní posouzení každé vzniklé situace jako vnějšího napadení opravňujícího ozbrojené síly k vojenské reakci by tedy bylo značně komplikované.

1.4 Identifikace dotčených subjektů

Dotčeným subjektem bude zejména Vojenské zpravodajství. Nepřímo se návrh zákona dotkne Armády České republiky, Bezpečnostní informační služby, Úřadu pro zahraniční styky a informace a Národního bezpečnostního úřadu, které mají rovněž podíl na zajišťování bezpečnosti a obrany České republiky a s nimiž se předpokládá úzká spolupráce. V návaznosti na novou roli Vojenského zpravodajství a nová oprávnění pak budou dotčeni podnikatelé v oblasti elektronických komunikací. Bude se jednat o dopady přímé, bude-li konkrétní podnikatel určen vládou a poté vyzván k součinnosti. Jelikož součinnost bude vždy vyžadována za finanční náhradu, neměly by tyto subjekty být vyžadováním součinnosti poškozovány.

1.5 Popis cílového stavu

Návrh si klade za cíl v základní podobě upravit problematiku chybějících oblastí zajišťování obrany České republiky a kybernetické bezpečnosti České republiky v širším smyslu, tj. kybernetické obrany, a tím docílit komplexního pojetí právní úpravy obrany státu a kybernetické bezpečnosti. Jelikož ústavním požadavkem je, aby státní moc byla uplatňována jen v případech, v mezích a způsoby, které stanoví zákon, bude zákonem upraveno, co se považuje za provádění kybernetické obrany, kdo je za její výkon odpovědný, a jaké prostředky k tomu bude mít. Jelikož je nutná k této činnosti i součinnost některých fyzických a právnických osob, bude jim k tomu uložena patřičná povinnost. Návrh žádným způsobem neupravuje konkrétní podmínky pro používání obranných aktivit v kybernetickém prostoru, jelikož tyto situace budou, obdobně jako je tomu u klasického kinetického konfliktu, řešeny

předem připravenými plány obrany státu a ad hoc posuzovány před vydáním konkrétních rozkazů k provedení určité aktivity v případě aktuálního ohrožení.

1.6 Zhodnocení rizika

Riziko spojené s nepřijetím navržené úpravy spočívá zejména v tom, že činnosti, které dosud nejsou výslovně právními předpisy upraveny, tj. kybernetickou obranu, nelze plnohodnotně provádět bez součinnosti s některými soukromými subjekty, přičemž tuto součinnost a její pravidla lze nastavit jedině zákonnou cestou. Při nepřijetí úpravy by tak činnosti kybernetické obrany mohly sice být prováděny, ale ve značně omezeném, a tedy poměrně neúčinném režimu. Kromě toho by nebyl výslovně určen žádný orgán odpovědný za tuto oblast obrany státu, což by mohlo vést k tomu, že by se této činnosti řádně nevěnoval žádný státní orgán, anebo naopak by si tuto činnost osvojilo orgánů více. Ochrana kybernetického prostoru v České republice před narušením jak špionážními aktivitami, tak i dalšími útoky, by tak byla značně omezená, nesourodá a nesystémová (viz zákon č. 22/1999 Sb.).

2. Návrh variant řešení

Varianta I. (nulová)

Znamená zachování současného stavu. Kybernetická obrana nebude nikomu výslovně svěřena a nebudou upraveny žádné zvláštní prostředky k jejímu výkonu. Zajištění kybernetické obrany tak zůstane v obecné rovině na Ministerstvu obrany a Armádě České republiky, jelikož jejím úkolem je bránit Českou republiku před vnějším napadením. Tato činnost však nebude mít žádná zákonná pravidla, Armádě nebude k provádění této činnosti svěřeno žádné speciální oprávnění. Kontrašpionáž, a tedy i kontrašpionáž v kybernetickém prostoru, zůstane úkolem BIS a Vojenského zpravodajství. Tyto služby však prozatím mají za úkol jen sběr informací, tj. budou pouze zjišťovat, kdo, jak a proč se pokouší nelegálně v kybernetickém prostoru získávat informace, a o těchto zjištěních informovat oprávněné adresáty. Oproti současnému stavu nebudou mít svěřena rovněž žádná oprávnění, což vzhledem ke skutečnosti, že znění zákonů upravujících jejich činnost má původ v první polovině devadesátých let minulého století a jejich ustanovení o zpravodajské technice současný stav kybernetického prostoru nereflektují, znamená, že jejich schopnost reagovat na hrozby v kybernetickém prostoru zůstane značně omezená. Kybernetická bezpečnost v podobě, která je popsána v zákoně o kybernetické bezpečnosti, pochopitelně zůstane v působnosti NBÚ, tento zákon však upravuje zajišťování kybernetické bezpečnosti zásadně v pasivním módu, nepočítá tedy s žádnými prvky obrany aktivní, bez níž se v případě závažnějších útoků obejít nelze.

Varianta II.

Další z variant je svěřit zákonem výkon kybernetické obrany Armádě ČR, a kontrarozvědnou činnost ponechat zpravodajským službám. Všem pak je možné zákonem přiznat některá nutná oprávnění k provádění této činnosti. Nevýhodou této varianty je větší okruh subjektů, které by vyvíjely činnost v kyberprostoru, riziko vzájemných střetů při této činnosti a v neposlední řadě mnohem vyšší ekonomická náročnost, jelikož prostředky pro tyto činnosti by bylo nutné pořizovat několikrát. Nikoli nevýznamnou pak je i otázka lidských zdrojů, jejichž nabídka je pochopitelně omezená. Působnost NBÚ zůstává stejná jako u varianty I.

Varianta III.

Jednou z variant by mohlo být také rozšíření pravomocí Národního bezpečnostního úřadu i na sféru kybernetické obrany. Výhodou by bylo využití stejné vědomostní i technické základny, nicméně nevýhodou by bylo nežádoucí prolínání různých rovin a úrovní zajišťování kybernetické bezpečnosti v České republice. Kybernetická obrana nastupuje až jako ultima ratio, ve chvílích, kdy běžný systém zajištění kybernetické bezpečnosti, jak jej zná současný zákon o kybernetické bezpečnosti, již nepostačuje, respektive již není na tento typ nebezpečí zaměřen, tedy ve všech případech, kdy je bezprostředně ohrožena svrchovanost, územní celistvost, demokratické základy České republiky nebo ve značném rozsahu vnitřní pořádek a bezpečnost, životy a zdraví, majetkové hodnoty nebo životní prostředí anebo je-li třeba plnit mezinárodní závazky o společné obraně, přičemž nelze vyloučit ani působení v rámci jednoho ze základních principů mezinárodního práva, tj. povinnost bdělosti (due diligence). Jde o podobný vztah, jako je při zajišťování bezpečnosti mezi policií a armádou. Obrana kybernetického prostoru bude aplikována při takových útocích, které již spadají do kategorie kyberterorismus nebo kybernetická válka (viz výše dělení kybernetických útoků), naopak by její aplikace a uplatnění pravomocí s kybernetickou obranou spojených v žádném případě neměla zasahovat do oblasti vymezené zákonem o kybernetické bezpečnosti, což navrhovaná právní úprava naopak plně respektuje. Varianta III. proto není vhodná zejména právě z hlediska rozdělení kompetencí.

Varianta IV. (podle návrhu)

V této variantě by zajišťování kybernetické obrany bylo svěřeno Vojenskému zpravodajství. V tomto smyslu hovoří i Akční plán k Národní strategii kybernetické bezpečnosti, v němž vláda uložila Vojenskému zpravodajství vybudovat Národní centrum kybernetických sil. Návrh zákona proto, v návaznosti na již přijaté usnesení vlády, obsahuje záměr svěřit kybernetickou obranu Vojenskému zpravodajství.

Důvodem pro preferenci této varianty je, že kyberprostor není typické „kinetické“ válčiště, ale spíše prostor informační, kde velkou roli tradičně mají zpravodajské služby. Kromě toho vzhledem k povaze kybernetického prostoru není vždy jednoznačně možné odlišit vnější a vnitřní napadení, a stejně tak není možné zcela přesně vyhodnotit, zda již jde o ozbrojený útok zakládající právo na sebeobranu ve smyslu mezinárodního práva nebo zda se jedná o čin charakteru teroristického, kriminálního nebo např. špionážního. Z těchto hledisek se jeví jako nejvhodnější svěřit tento úkol zpravodajským službám, které jsou určeny k tomu, aby se podílely na zajišťování bezpečnosti státu v celém spektru hrozeb. Z ekonomických a praktických důvodů se pak jeví jako vhodné, aby to byla jen jedna ze služeb. Vzhledem k povaze kybernetické obrany z principu jako souhrnu opatření, prováděných v kybernetickém prostoru, směřujících k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením[22] pak konkrétně Vojenské zpravodajství jakožto vojenská zpravodajská služba, integrální součást Ministerstva obrany, podílející se na systému zabezpečování obrany státu[23], což nabízí i další výhody, a sice jednodušší spolupráci s Armádou a z toho vyplývající snadné pokračování v činnosti v případě přechodu státu do mimořádných stavů. Podstatným argumentem pro tuto variantu je dále skutečnost, že zpravodajské služby jsou zvyklé své

[22] § 2 odst. 1 zákona č. 222/1999 Sb., o zajišťování obrany České republiky.

23 § 16 odst. 2 písm. e) zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky: „Ministerstvo obrany jako orgán pro zabezpečování obrany řídí Vojenské zpravodajství“.

činnosti vykonávat v utajeném režimu, k čemuž jim právní řád již nyní dává i mnohé nástroje, které tak nebude nutné nově zavádět či měnit. Vojenské zpravodajství je navíc službou s vnitřní i vnější působností, což může být při činnostech v kybernetickém prostoru rovněž výhodou. Vojenské zpravodajství tak může při kybernetické obraně využít informací, které má k dispozici z jiných zdrojů.

Jak bylo popsáno výše, návrh tohoto zákona má za cíl doplnit systém kybernetické bezpečnosti v České republice o další rozměr, a sice vojensko-zpravodajský. Pojem „kybernetická obrana“ (angl. cyber defence) bývá obvykle používán ve vojenském kontextu, nicméně může se dotýkat také kriminálních nebo špionážních záležitostí. NATO používá různé definice pro bezpečnost (security) a obranu (defence). První je používána ve vztahu k bezpečnosti komunikačních a informačních systémů (KIS), přičemž bezpečnost je definována jako schopnost přiměřeně chránit důvěrnost, dostupnost a integritu KIS a informací v nich zpracovávaných, uložených a přenášených. Obrana je potom schopnost zabezpečit dostupnost a správu služeb v operačních KIS proti potencionálním, bezprostředním i probíhajícím škodlivým jednáním, které mají původ v kyberprostoru. US Cyber Command definuje obranné kybernetické operace jako zaměřování a synchronizování opatření k zjištění, analyzování, odvrácení a zmírnění kybernetických hrozeb a slabých míst, vyřazení protivníků provádějících nebo majících v plánu provádět útočné operace a jinak chránit zásadní prvky, které slouží k zajištění americké svobody jednání v kyberprostoru.

Současný právní řád ČR kybernetickou obranu nezná a ani ji nijak nedefinuje. Z toho vyplývá, že ji také žádný státní orgán nemůže provádět, zejména mohlo-li by přitom dojít k zásahům do základních lidských práv a svobod. Pokud bychom se drželi čisté definice obrany státu, pak by i obranu kybernetického prostoru mohly zabezpečovat ozbrojené síly. Ve chvíli, kdy si ale uvědomíme, že kybernetická obrana není jen čistá obrana proti vnějšímu útoku v tradičním smyslu tohoto pojmu, ale že tyto aktivity mají několik podob a dimenzí, z nichž čistě vojenská (sebeobrana na základě ozbrojeného útoku podle mezinárodního práva) je pouze jedna z nich, pak nutně musíme dojít k závěru, že zákonné vymezení kybernetické obrany, určení státního orgánu, který za ni bude odpovědný, a vymezení alespoň základních prostředků sloužících k této činnosti, je nezbytné.

Vojenské zpravodajství má prozatím působnost jen k zabezpečování informací, ne k aktivní obraně ČR, zatímco provádění kybernetické obrany by alespoň v určitém rozsahu aktivní činností přesahující rámec zabezpečování informací bylo. Státní moc lze uplatňovat jen na základě zákona a v jeho mezích. V okamžiku, kdy v rámci zajišťování kybernetické obrany bude nutné vyžadovat po fyzických či právnických osobách jakoukoli součinnost nebo bylo-li by touto činností jakkoli zasahováno do základních práv a svobod osob, je nezbytně nutné tuto činnost normovat zákonem.

Navrhovaná úprava pak v sobě při zajištění věcných aspektů kybernetické obrany současně vychází z nezbytnosti zajistit proporcionalitu mezi svěřenými technickými prostředky a opatřeními jejího výkonu a dostatečnými zárukami proti jejich zneužití (pro jiné účely nebo proti nežádoucímu osobnímu nebo časovému rozsahu jejich účinků). Připravovaný právní rámec proto poskytuje záruky bránící jejímu zneužití, a to jednak v rámci jejího začlenění do podmínek a systému zajišťování obrany České republiky, jednak jednoznačným a předvídatelným nastavením rozsahu a podmínek užití technických prostředků kybernetické obrany, pro které – jsou-li užity ve smyslu zpravodajské techniky – platí stejné mantinely a právní limity, jako je tomu u zpravodajské činnosti.

Doba trvání jednotlivých opatření užitých v rámci výkonu kybernetické obrany, limity zneužití technických prostředků kybernetické obrany ve vztahu k ochraně demokratických principů a vyloučení svévole jejich užití nad stanovený zákonný rámec stanovením podmínek užití technických prostředků kybernetické obrany vládou České republiky.

Novela zákona o Vojenském zpravodajství přitom stanoví povinnosti Vojenského zpravodajství související s prováděním kontroly dodržování vládou stanovených podmínek výkonu kybernetické obrany, a to v zájmu ochrany základních práv a svobod, která v demokratickém státě mohou pro stanovené účely (veřejného zájmu, tedy včetně obrany a bezpečnosti) dotčena, avšak nikoliv bezbřehou diskrecí svěřenou orgánům moci výkonné. Návrh zákona však záruky nezneužití svěřené působnosti obsahuje, a to včetně začlenění oblasti kybernetické obrany do existujících systémů, pro něž uvedená ochrana platí obdobně.

3. Vyhodnocení nákladů a přínosů

3.1 Identifikace nákladů a přínosů

Přínosem varianty II., III. i IV. je legislativní zakotvení a vymezení pojmu kybernetické obrany, včetně přiřazení odpovídající působnosti subjektům kybernetickou obranu vykonávajícím, čímž dojde ke zvýšení bezpečnosti České republiky. Tato činnost s sebou samozřejmě nese náklady, které mohou být jak na personál, tak na technické prostředky. Přímý přínos varianty I. není žádný, nicméně také kybernetická obrana prováděná bez konkrétních zákonem zakotvených instrumentů by určitý přínos k zabezpečení obrany České republiky měla, ale rovněž by nesla i určité náklady.

3.2 Náklady

Varianta I. s sebou pochopitelně žádné okamžité přímé náklady nenese. Je však třeba si uvědomit, že i bez výslovné úpravy kybernetické obrany v zákoně by tato činnost v omezeném rozsahu stejně musela být někým prováděna, přičemž náklady by tak následně vznikaly i v této nulové variantě. Vzhledem k tomu, že při neexistenci zákonné úpravy by se o určitou formu kybernetické obrany pravděpodobně pokoušela řada subjektů, zpravodajskými službami počínaje, přes NBÚ a Armádou ČR konče, náklady by mohly být i v případě nepřijetí právní úpravy značné, neboť by docházelo k vynakládání veřejných prostředků na tutéž činnost, jakož i personální a technické vybavení vícekrát. Je ovšem otázkou zda by vůbec takto pojatá a vykonávaná kybernetická obrana byla funkční, neboť by každému ze subjektů pokoušejících se o její výkon stále chybělo zakotvení odpovídajících pravomocí.

Varianta II. by znamenala, že by u AČR, BIS i VZ byla postupně vybudována pracoviště pro zajišťování kybernetické obrany. Vzhledem k omezené možnosti koordinace této činnosti je pravděpodobné, že by náklady byly vyšší, než kdyby tato činnost byla svěřena jen jednomu subjektu. Efektivita se naopak dá předpokládat jako nižší, což by pramenilo z roztříštěnosti této činnosti. Je samozřejmě možné, že „konkurence“ mezi jednotlivými subjekty kybernetickou obranu provádějícími by mohla mít jistý efekt v podobě vyšší „kvality“ této činnosti ze strany jednotlivých subjektů, ovšem nelze předpokládat, že by tento přínos, který je pouze hypotetický, vyvážil negativa mnohem vyšší finanční nákladnosti. Také lze pochybovat, zda Česká republika disponuje dostatečnou personální základnou v potřebných profesích umožňující vybudování odpovídajícího prvku kybernetickou obranu provádějícího vícekrát.

Varianta III. by znamenala rozšíření oprávnění Národního bezpečnostního úřadu o činnosti kybernetické obrany. Je pravděpodobné, že tato varianta by byla levnější než varianta IV., jelikož by bylo možné využít část personálních i technických aktiv, jež má NBÚ k dispozici. Vzhledem k rozšíření úkolů o další, odlišný směr činnosti by nicméně bylo nutné i v této variantě personální stavy posílit a nákupu technických prostředků by se Česká republika také nevyhnula. Nevýhody této varianty z hlediska praktického byly popsány výše.

Varianta IV. znamená postupné vybudování pracoviště pro kybernetickou obranu v rámci Vojenského zpravodajství. Náklady budou spočívat jednak v prostředcích na kvalifikované pracovníky a jednak v nákupu sofistikovaných technických prostředků. Konkrétní výši nákladů nelze přesně určit, jelikož pracoviště bude budováno postupně a vždy v závislosti na dostupných rozpočtových prostředcích. Náklady tedy budou vždy výhradně záviset na ochotě vlády podporovat kybernetickou obranu České republiky. Zákon samotný proto žádné přímé náklady nepřináší, jelikož pouze otevírá možnost provádění činností kybernetické obrany. Až teprve samotný faktický výkon této činnosti a budování schopností bude vyžadovat finanční prostředky, ale lze říci, že jejich výše bude flexibilní a bude záviset jedině na možnostech státních financí, obdobně jako je tomu u jiných oblastí zabezpečování obrany. V počátku půjde zejména o nákup technických prostředků a platové prostředky na první zaměstnance. V pozdějším období budou pravděpodobně klesat nutné výdaje na technické prostředky a vzhledem ke zvyšujícímu se počtu zaměstnanců budou růst platové výdaje. Odhady učiněné v rámci Vojenského zpravodajství počítají z počátku s náklady přibližně 300 milionů korun ročně, samotný návrh právní úpravy však žádné konkrétní náklady nevyvolává, dokud nebude fakticky započato s budováním příslušného pracoviště, jelikož návrh zákona pouze svěřuje zajišťování kybernetické obrany Vojenskému zpravodajství, což se v určitém, byť minimálním, rozsahu dá provádět i v rámci současného rozpočtu. Bude záležet zásadně na navazujících rozhodnutích o podobě a rozsahu tohoto pracoviště, přičemž vzhledem k citlivému charakteru této činnosti nelze v neutajované důvodové zprávě uvádět bližší údaje o jeho předpokládané podobě.

Jiným subjektům než státu náklady ani v jedné z variant nevznikají, resp. se počítá s tím, že budou kompenzovány.

3.3 Přínosy

Varianta I. nemá žádný prokazatelný přínos. Varianty II., III. a IV. mají očekávané přínosy v tom smyslu, že dobře prováděná kybernetická obrana může zabránit škodám vzniklým kybernetickými útoky či špionáží. Finančně však tento přínos nelze vyčíslit. Konkrétním přínosem zvolené varianty IV. pak je vybudování vysoce specializovaného pracoviště, které umožní České republice držet krok v oblasti obrany proti sofistikovaným úmyslným kybernetickým útokům, které přímo mohou zasáhnout základní bezpečnostní zájmy státu.

3.4 Vyhodnocení nákladů a přínosů variant

	I.	II.	III.	IV.
Finanční náklady	4	1	3	2
Přínos pro obranu	2	5	4	5

Využití technických kapacit	1	2	4	5
Využití personálních zdrojů	1	2	5	4
Využití dosavadních schopností daného subjektu	1	1	3	5
celkem	9	11	19	21

Poznámka: 1 – žádné, 2 – nižší, 3 – střední, 4 – vyšší , 5 – nejvyšší (u finančních nákladů naopak)

Klady a zápory možných variant řešení byly popsány výše. Návrh vychází v souladu s úkolem uloženým vládou v Akčním plánu k Národní strategii kybernetické bezpečnosti z varianty IV. Úkol zajišťovat kybernetickou obranu v České republice bude svěřen Vojenskému zpravodajství, které k tomuto účelu vybuduje Národní centrum kybernetických sil (jedná se o pracovní název), jež bude jeho součástí. Vojenskému zpravodajství tak přibude nový úkol, který na rozdíl od dosavadních úkolů nebude již jen čistě informační, ale bude mít částečně také charakter aktivního působení.

Novela zákona č. 289/2005 Sb., o Vojenském zpravodajství, rozšíří působnost Vojenského zpravodajství o zabezpečování kybernetické obrany, upraví některé konkrétní podmínky provádění kybernetické obrany, schvalovací proces u opatření majících charakter zásahu do práv třetích osob, a dále stanoví oprávnění požadovat po podnikatelích v oblasti elektronických komunikací součinnost spočívající v umožnění nasazení technických prostředků kybernetické obrany.

Novela zákona č. 222/1999 Sb., o zajišťování obrany České republiky, definuje kybernetickou obranu a výslovně ji zařadí jako součást zajišťování obrany státu. V důsledku toho bude možné využít při zajišťování kybernetické obrany též nástroje tohoto zákona. Upraví také výslovně existenci plánu kybernetické obrany státu schvalovaného vládou, který bude stěžejním řídícím dokumentem pro oblast kybernetické obrany. Novela zákona č. 127/2005 Sb., o elektronických komunikacích, pak stanoví povinnosti odpovídající oprávněním Vojenského zpravodajství.

Hospodářský dopad předkládaného návrhu lze očekávat pouze u úzké skupiny osob, které jsou subjekty zajišťujícími sítě nebo služby elektronických komunikací a které budou osloveny s žádostí o součinnost. Tyto osoby budou pravděpodobně částečně ovlivněny právě nutností tuto součinnost poskytnout, nicméně návrh předpokládá úhradu účelně vynaložených nákladů těmto osobám vzniklých. Na druhou stranu je možné očekávat pozitivní hospodářský dopad v případech, kdy činností Národního centra kybernetických sil dojde k odvrácení nebo minimalizování kybernetického útoku, který by jinak měl na hospodářství škodlivé následky. Finanční dopad bude návrh mít pouze na státní rozpočet, a to jedině v případě, že dojde k rozhodnutí o vybudování pracoviště zajišťujícího kybernetickou obranu v takové podobě, které Vojenské zpravodajství resp. Ministerstvo obrany nebude již schopné finančně pokrýt v rámci rozpočtu stávajícího.

Dopady na podnikatelské prostředí jsou totožné s dopady hospodářskými popsanými v předchozím odstavci. Návrh nemá žádné sociální dopady ani dopady na rodiny nebo specifické skupiny obyvatel. Nejsou ani žádné dopady na životní prostředí. Navrhované řešení se žádným způsobem nedotýká zákazu diskriminace ani rovnosti mužů a žen. Návrh nemá dopady na státní statistickou službu.

Dopady ve vztahu k ochraně osobních údajů a k ochraně soukromí jsou blíže vyhodnoceny v rámci důvodové zprávy k návrhu. Rovněž korupční rizika jsou posouzena v rámci důvodové zprávy.

Pokud jde o dopady na bezpečnost a obranu státu, návrh se samozřejmě přímo dotýká zabezpečování obrany a bezpečnosti státu, neboť upravuje novou oblast zajištění obrany státu, a to v kybernetickém prostoru. Návrh zákona definuje kybernetickou obranu jako součást zajišťování obrany státu, nastavuje pravidla jejího plánování, budování a přímého výkonu, čímž ve svém souhrnu významně přispívá k zajišťování obrany a bezpečnosti České republiky (blíže k tomu viz také popis a vyhodnocení jednotlivých variant, zejména pak varianty IV.).

Na aktiva zpravodajských služeb nebo bezpečnostních sborů, ani na jejich příslušníky návrh nemá žádný dopad.

4. Stanovení pořadí variant a výběr nejvhodnějšího řešení

Na základě vyhodnocení nákladů a přínosů v jednotlivých variantách tak, jak je provedeno v kapitole 3, byla zvolena k realizaci normativního řešení varianta IV.

5. Implementace doporučené varianty a vynucování

Za implementaci řešení bude odpovědné Ministerstvo obrany a jeho součást Vojenské zpravodajství. Implementace doporučeného řešení si v rámci tohoto orgánu nevyžádá žádné zvláštní postupy. Po některých vybraných podnikatelích a dalších osobách v oblasti elektronických komunikací bude do budoucna vyžadována součinnost ohledně připojení technických prostředků kybernetické obrany. K nasazení technických prostředků bude docházet postupně, po dohodě s dotčenými subjekty a za jejich součinnosti. Návrh nenařizuje přijetí žádných okamžitých opatření, pouze umožňuje do budoucna tato opatření přijmout.

Vynucování by přicházelo v úvahu jedině u předpokládané součinnosti podnikatelů a dalších osob v oblasti elektronických komunikací. Návrh předpokládá spolupráci na bázi vzájemné dohody. Pouze v případě, že by praxe ukázala problémy s ochotou poskytovat Vojenskému zpravodajství součinnost při plnění úkolů spojených se zajišťováním kybernetické obrany, zákon obsahuje i donucovací mechanismy ve formě nové skutkové podstaty správního deliktu. Dále může být cestou správních deliktů a přestupků vynucována povinnost mlčenlivosti zúčastněných osob. Jedná se nástroje, které v obdobném provedení již nyní obsahuje zákon o elektronických komunikacích pro vynucení celé řady povinností. O těchto správních deliktech (*resp. od 1.7.2017přestupcích*) bude rozhodovat Český telekomunikační úřad.

6. Přezkum účinnosti regulace

Přezkum účinnosti novelizace bude probíhat postupně. Jelikož jde v zásadě o novou problematiku, jež prozatím právní úpravu neměla a jejíž faktické naplňování bude probíhat postupně, není vyloučeno, že po nějaké době dojde k identifikaci oblastí, jejichž úprava se ukáže jako potřebná nebo nedostatečná, a bude provedena revize úpravy.

7. Konzultace a zdroje dat

Před přípravou návrhu zákona byla provedena řada konzultací se zahraničními subjekty, které mají v působnosti kybernetickou bezpečnost a obranu. Zejména se jednalo o National Cyber Bureau (Izrael), Joint Sigint Cyber Unit (Nizozemí) a GCHQ (Velká Británie).

V České republice byl návrh a jeho podoba konzultovány zejména s Národním bezpečnostním úřadem jako gestorem problematiky kybernetické bezpečnosti, s Českým telekomunikačním úřadem, zpravodajskými službami a dále s hlavními subjekty provozujícími sítě elektronických komunikací zejména ve smyslu nezbytné budoucí spolupráce.

8. Kontakt na zpracovatele RIA

Závěrečnou zprávu zpracoval a kontaktní osobou pro případné připomínky a dotazy je:
Mgr. Martin Fliegel
Vojenské zpravodajství
tel.: 973 200 429
e-mail: martin.fliegel@uvoz.cz.

B) Obecná část

I. Zhodnocení platného právního stavu, včetně zhodnocení současného stavu ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen

Kybernetická obrana, kterou je v návrhu zákona myšlena obrana státu v kybernetickém prostoru, není prozatím v právním řádu České republiky výslovně řešena. Zákony je řešena obrana státu obecně, avšak jelikož v době přijetí těchto právních předpisů nebyl kybernetický prostor tak zásadní pro fungování společnosti a státu, není řešena ta složka obrany, která se má odehrávat právě v kybernetickém prostoru. Tento deficit má za cíl napravit právě předkládaný návrh novely zákona o Vojenském zpravodajství a souvisejících právních předpisů. Bližší vyhodnocení platného právního stavu obsahuje závěrečná zpráva RIA.

Současný právní stav nemá žádný vztah k zákazu diskriminace ani k rovnosti mužů a žen.

II. Odůvodnění hlavních principů navrhované úpravy, včetně dopadů navrhovaného řešení ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen

S ohledem na fakt, že kybernetická obrana České republiky v právním řádu není prozatím žádným způsobem vymezena, není určen ani státní orgán, který by ji měl za úkol zajišťovat. Návrh zákona tedy jde cestou definování pojmu kybernetické obrany, svěření jejího zajišťování Vojenskému zpravodajství jako součásti Ministerstva obrany a úpravy prostředků, které budou sloužit k zajišťování kybernetické obrany.

Navrhovaná úprava pak v sobě při zajištění věcných aspektů kybernetické obrany současně vychází z nezbytnosti zajistit proporcionalitu mezi svěřenými technickými prostředky a opatřeními jejího výkonu a dostatečnými zárukami proti jejich zneužití (pro jiné účely nebo proti nežádoucímu osobnímu nebo časovému rozsahu jejich účinků). Připravovaný právní rámec proto poskytuje záruky bránící jejímu zneužití, a to jednak v rámci jejího začlenění do podmínek a systému zajišťování obrany České republiky, jednak jednoznačným a předvídatelným nastavením rozsahu a podmínek užití technických prostředků kybernetické obrany, pro které – jsou-li užity ve smyslu zpravodajské techniky – platí stejné mantinely a právní limity, jako je tomu u zpravodajské činnosti.

Doba trvání jednotlivých opatření užitých v rámci výkonu kybernetické obrany, limity zneužití technických prostředků kybernetické obrany ve vztahu k ochraně demokratických principů a vyloučení svévole jejich užití nad stanovený zákonný rámec užití technických prostředků kybernetické obrany, tedy podmínky pro tyto účely stanovené vládou ČR.

Bližší vysvětlení navrhované právní úpravy obsahuje závěrečná zpráva RIA.

Navrhovaná právní úprava nemá žádný vztah k zákazu diskriminace ani k rovnosti mužů a žen.

III. Vysvětlení nezbytnosti navrhované právní úpravy v jejím celku

Jak bylo řečeno, kybernetická obrana není zatím v právním řádu definována a ani předpisy upravující zajišťování obrany státu s ní nepočítají. Jelikož se jedná o součást obrany státu, bez přijetí zvláštní úpravy by úkol zajišťovat kybernetickou obranu automaticky připadl Ministerstvu obrany, které je v souladu se zákonem č. 2/1969 Sb. ústředním orgánem státní správy zejména pro zabezpečování obrany České republiky, resp. na jím řízenou Armádu České republiky. Bez přijetí zvláštního zákona by však tyto orgány neměly k dispozici žádné zvláštní prostředky k jejímu zajišťování. Jako nejlepší řešení se tedy jeví přijmout novelu příslušných zákonů, které kybernetickou obranu svěří konkrétnímu orgánu, vybráno bylo Vojenské zpravodajství jako součást Ministerstva obrany, a dají mu k tomu dostatečné prostředky. Tím se umožní vznik a vybudování kvalitního pracoviště, které bude v budoucnu schopno reagovat na všechny formy ohrožení bezpečnosti České republiky, které budou mít původ v kybernetickém prostoru. Bližší vysvětlení nezbytnosti navrhované právní úpravy obsahuje závěrečná zpráva RIA.

IV. Zhodnocení souladu navrhované právní úpravy s ústavním pořádkem České republiky

Základním principem navrhované právní úpravy je dostát ústavnímu pravidlu, že státní moc lze uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon. Kybernetická obrana jakožto součást obecně pojaté obrany (sebeobrany) státu je právem státu a rovněž povinností státu vůči občanům (čl. 1 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky) a jako taková je samozřejmě v souladu s ústavním pořádkem. Je nicméně nezbytné, aby samotný výkon takové obrany, tedy výkon státní moci, byl normován zákonem, a to zejména v případech, kdy by při výkonu takové obrany bylo zasahováno do základních lidských práv a svobod. Ústava České republiky vyžaduje, aby působnost správních úřadů, a obecně vzato i jiných státních orgánů, byla stanovena zákonem. Z tohoto důvodu je kybernetická obrana určena zákonem do působnosti Vojenského zpravodajství a jsou stanovena její základní pravidla a meze. Dále platí, že nikdo nesmí být nucen činit, co zákon neukládá, a proto je zákonem upraveno, jaké povinnosti budou právnickým a fyzickým osobám v souvislosti s plněním úkolů kybernetické obrany uloženy.

Navrhovaný zákon nemá umožnit Vojenskému zpravodajství zasáhnout do základních práv a svobod a soukromé sféry osob ve větší míře, než mohlo zasahovat podle zákona o Vojenském zpravodajství v dosavadním znění. Vojenské zpravodajství je v současnosti oprávněno zasahovat do základních lidských práv a svobod, chráněných zejména ustanoveními čl. 7 a čl. 10 odst. 2 a 3 Listiny základních práv a svobod, čl. 8 Evropské úmluvy o ochraně lidských práv a základních svobod a čl. 17 Mezinárodního protokolu o občanských a politických právech, a to při použití specifických prostředků získávání informací, zejména zpravodajské techniky a sledováním osob a věcí[24]. Tyto prostředky mohou být využity po povolení předsedou senátu Vrchního soudu v Praze, resp. ministrem obrany, a to v případech, kdy Vojenské zpravodajství potřebuje získat informace o konkrétní osobě (nebo o telefonním čísle, popřípadě o jiném konkrétním objektu) nebo věci a za předpokladu, že by odhalování nebo dokumentování činností, pro něž má být použita, bylo jiným způsobem neúčinné nebo podstatně ztížené anebo v daném případě nemožné. Návrh zákona nepředpokládá zásahy do těchto práv ve větším rozsahu, než tomu je dosud. Technické prostředky kybernetické obrany, které nově zavádí navržená novelizace zákona

[24] § 8 a § 15 zákona č. 289/2005 Sb., o Vojenském zpravodajství.

o Vojenském zpravodajství, nemají za cíl narušovat soukromí nebo tajemství zpráv a - to je třeba zdůraznit - rozhodně neopravňují Vojenské zpravodajství sledovat obsah komunikace konkrétních osob (pro tento typ jednání nadále a výhradně platí pravidla pro použití zpravodajské techniky), ale pouze signalizovat určité přesně definované negativní jevy související s kybernetickým prostorem (k technickým prostředkům blíže viz zvláštní část důvodové zprávy). Bylo-li by na základě těchto signálů nutné zaměřit se na konkrétní osoby a jejich chování v kybernetickém prostoru, bude tak činěno v rozsahu povolení na zpravodajskou techniku tak jako dosud. Monitoring kybernetického prostoru je při provádění kybernetické obrany nezbytný, jelikož umožňuje včas identifikovat určité jevy, jež mohou nasvědčovat přípravě kybernetického útoku či dokonce již jeho průběhu. Pokud jde o rozsah zásahů do práv na ochranu soukromí nebo tajemství dopravovaných zpráv, monitoring není určen k tomu, aby se zaměřoval na obsah konkrétních informací nebo komunikaci konkrétních osob. Lze jej přirovnat např. k úsekovému měření rychlosti na silnicích. Kamerový systém změří a zaznamená rychlost (tj. chování) všech vozidel bez rozdílu a bez identifikace, a správní orgány se poté zaměří jen na ta vozidla, jež jsou automaticky vyhodnocena jako vozidla porušující pravidla, přičemž ostatní zůstanou bez povšimnutí.

Zákon o Vojenském zpravodajství dále již nyní zasahuje do práva vlastnit majetek podle čl. 11 Listiny, jelikož některé subjekty ve sféře elektronických komunikací nutí strpět některá opatření v jimi vlastněné infrastruktuře[25]. Návrh tyto povinnosti jenom rozšiřuje, přičemž ale zachovává pravidlo, že omezení vlastnického práva je možné ve veřejném zájmu, a to na základě zákona a za náhradu.

Pro každý zásah do základních práv a svobod platí obecná zásada, že k němu může dojít pouze za podmínky, že ochrany tohoto jiného zájmu nelze dosáhnout šetrnějším způsobem. Omezení, resp. zásah do těchto práv může být připuštěn pouze za účelem ochrany jiného zájmu, který bude shledán v konkrétní věci důležitějším. Evropská úmluva dovoluje zásahy do práva na respektování soukromého a rodinného života, obydlí a korespondence v případech, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.

Ústavní soud používá k poměření těchto zájmů tzv. test proporcionality. Při něm jsou postupně posuzována tři kritéria. Prvním je **kritérium vhodnosti**, tj. odpověď na otázku, zdali institut, omezující určité základní právo, umožňuje dosáhnout sledovaný cíl (ochranu jiného základního práva). Zde je potřeba si uvědomit, že návrh zákona tak, jak je formulován, nepochybně povede ke zvýšení míry bezpečnosti České republiky a jejích občanů a k ochraně shora zmíněných hodnot, zejména práva na informační sebeurčení (tj. zejm. práva na ochranu soukromí, soukromého života, na svobodu projevu, na přístup k informacím a dalších informačních práv člověka), bezpečnosti a integrity (nedistributivních[26] práv) České republiky a mezinárodních závazků České republiky.

---

[25] § 9 odst. 5 zákona č. 289/2005 Sb., o Vojenském zpravodajství.

[26] Srov. oponentní posudek Pavla Holländera k nálezu pléna Ústavního soudu ze dne 3.4.1996, č.j. Pl.ÚS 32/95, 112/1996 Sb., N 26/5 SbNU 215, dostupný z: www.nalus.usoud.cz: „Ústavní úprava postavení jedince ve společnosti obsahuje ochranu individuálních práv a svobod, jakož i ochranu veřejných statků (public goods, kolektive Gütter). Rozdíl mezi nimi spočívá v jejich distributivnosti. Pro veřejné statky je typické, že prospěch z nich je nedělitelný a lidé nemohou být vyloučeni z jeho požívání. Příklady veřejných statků jsou národní bezpečnost, veřejný pořádek, zdravé životní prostředí. Veřejným statkem se tudíž určitý aspekt lidské existence stává

Dosavadní zkušenosti ukazují, že kybernetické útoky se stávají stále závažnější hrozbou, přičemž je nezbytné, aby stát byl pokud možno připraven jim čelit, což lze v případě nejzávažnějších kybernetických útoků zajistit jen předběžným budováním kapacit schopných se s takovými útoky vypořádat. Návrh zákona vychází z aktuálního vývoje v oblasti budování orgánů pro zabezpečování kybernetické obrany a vybírá tak ty nejefektivnější nástroje obrany kybernetického prostoru při zachování minimální zátěže směrem k osobám soukromého práva. Lze proto konstatovat, že určení jednoho státního orgánu odpovědným za zajišťování kybernetické obrany a jeho vybavení nezbytnými prostředky pro plnění tohoto úkolu, při poměrně malém omezení základních práv a svobod výměnou za ochranu jiných, významných práv a svobod, je vhodné řešení.

Druhým kritériem poměřování základních práv a svobod je **kritérium potřebnosti**, spočívající v porovnávání legislativního prostředku, omezujícího základní právo resp. svobodu, s jinými opatřeními, umožňujícími dosáhnout stejného cíle, avšak nedotýkajícími se základních práv a svobod. Návrh zákona bude omezovat, byť ne více než dosud, právo vlastnit majetek a právo na soukromí, to ale v zájmu zajištění výkonu práva na informační sebeurčení a práva na osobní bezpečnost. V tomto případě má návrh zákona jasně vymezený účel, který spočívá v zabezpečení kybernetického prostoru, tj. v zabezpečení fungování služeb informační společnosti, ať soukromých nebo veřejných. Právě prostřednictvím těchto služeb, tj. jejich dostupnosti, spolehlivosti a bezpečnosti, lze v době rostoucího významu informační společnosti svobodně realizovat právo na informační sebeurčení. Obecným cílem zákona pak je zajistit prostřednictvím obrany kybernetického prostoru fungování státu ve všech jeho aspektech a jeho bezpečnost, což je povinností státu a což samozřejmě umožňuje občanům faktický výkon jejich práva na informační sebeurčení, ale i dalších práv a svobod. Jelikož je nezpochybnitelné, že kybernetické útoky se stávají stále závažnější hrozbou, je potřebnost opatření kybernetické obrany a tím zajištění fungování státu i jeho občanů v kybernetickém prostoru zřejmá. Vedle závazků České republiky plynoucích z členství v mezivládních organizacích představuje zásadní důvod k úpravě kybernetické bezpečnosti (to i včetně shora uvedeného omezení vlastnického práva) základní princip mezinárodního práva, tj. povinnost bdělosti (due diligence). Je v tomto směru jen otázkou času, kdy začne Mezinárodní soudní dvůr řešit odpovědnost státu za jednání, kterého se sice stát sám neúčastní, ale které je mu přičitatelné, neboť má původ v jeho suverénní doméně. Typicky tak může dojít k situaci, kdy budou zneužity počítače na území České republiky k útoku na cizí stát (takové případy se u rozsáhlých útoků vyskytují běžně) – Česká republika, přestože útok neorganizuje ani se na něm nepodílí, může být pohnána k odpovědnosti za to, že takovému útoku, byť k tomu měla prostředky (nebo je měla mít), účinně nezabránila.

Třetím kritériem je **porovnání závažnosti** obou v kolizi stojících základních práv. V posuzovaném případě jedním z nich je právo na soukromí a na tajemství dopravovaných zpráv, na druhé straně pak právo na informační sebeurčení a na bezpečnost. Ke střetu obdobných práv se vyjádřil Ústavní soud v nálezu sp. zn. Pl. ÚS 11/2000 takto: „Ústavní soud zastává názor, že při střetu uvedených dvou hodnot nelze přirozeně abstrahovat

za podmínky, kdy není možno jej pojmově, věcně i právně rozložit na části a tyto přiřadit jednotlivcům jako podíly. (-) Pro základní práva a svobody je, na rozdíl veřejných statků, typická jejich distributivnost. Aspekty lidské existence, jakými jsou např. osobní svoboda, svoboda projevu, účast v politickém dění a s tím spjaté volební právo, právo zastávat veřejné funkce, právo sdružovat se v politických stranách atd., lze pojmově, věcně i právně členit na části a tyto přiřadit jednotlivcům.“

od bezpečnostních zájmů státu, které je třeba respektovat. Je totiž zřejmé, že výše definovaný státní zájem představuje zájem existenční, který legitimizuje určité omezení privátní sféry jedince; ostatně ve svém důsledku je to stát, jenž postavení jedince chrání. Jestliže Ústavní soud judikoval, že ústava moderního demokratického právního státu představuje společenskou smlouvu, založenou na minimálním hodnotovém a institucionálním konsensu (srov. nález sp. zn. Pl. ÚS 33/97, in: Ústavní soud ČR: Sbírka nálezů a usnesení, sv. 9, str. 407), lze pod tímto pojmem mimo jiné chápat jak zájem státu, tak i jím chráněných osob na jeho vlastní bezpečné existenci; k ochraně tohoto zájmu musí stát disponovat příslušnými nástroji. Jedním z nich je i oblast ochrany utajovaných skutečností.“. Nález se týkal ochrany utajovaných informací, ale lze jej použít i při obdobném střetu v předmětné oblasti zajišťování kybernetické obrany. I zde může docházet k obdobnému střetu práva jedince s právem státu a jeho občanů. Stát musí mít možnost disponovat též nástroji k zajištění své obrany.

Navrhovaná úprava bezprostředně nezasahuje negativně do práva na informační sebeurčení člověka, neboť primárně nezasahuje do obsahové stránky komunikace a nezakládá ani přímé pravomoci státu direktivně zasahovat do běžného života informační společnosti – návrh zákona tedy nepředpokládá žádný státní zásah do soukromí uživatelů při zajišťování kybernetické obrany a v zásadě ani do jejich možností komunikovat prostřednictvím služeb informační společnosti. Právo na informační sebeurčení člověka je naopak návrhem zákona zpracováno jako hodnota, k jejíž ochraně návrh zákona primárně směřuje. Vzhledem k tomu, že technické prostředky kybernetické obrany nicméně mohou svými technickými parametry být schopné zasáhnout do práva na soukromí, návrh zákona takový zásah předvídá a výslovně jej považuje za zpravodajskou techniku s požadavkem na soudní povolení jejího použití, tedy nastavuje stejná pravidla jako pro jiné typy zpravodajské techniky.

Výše zmíněný zásah do vlastnického práva soukromoprávních subjektů je ve struktuře proporcionality odůvodněn z hlediska vhodnosti, a to jako jediné možné řešení kybernetické obrany, dané nutností nasazení technických prostředků kybernetické obrany do soukromoprávními subjekty vlastněných sítí a služeb elektronických komunikací. Zároveň je ovšem přistoupeno k refundaci nákladů soukromoprávních subjektů, které těmto subjektům vzniknou ve spojení s nutností nasazení technických prostředků kybernetické obrany, kdy jsou tak dopady zásahu do vlastnického práva soukromoprávních subjektů dále minimalizovány. Bez součinnosti s těmito subjekty, a tedy zásahu do jejich vlastnického práva, přitom není v praxi reálné a ani možné účinně bránit kybernetický prostor.

Pokud jde o potřebnost, provedenými studiemi a konzultacemi nebylo zjištěno alternativní řešení, které by mohlo naplnit základní cíl záměru, tj. obranu kybernetického prostoru. Byť je většina poskytovatelů služeb elektronických komunikací primárně pozitivně motivována k dobrovolné účasti na zajištění kybernetické obrany státu prostřednictvím ekonomických motivů (jen fungující síť může generovat ekonomický efekt), je třeba sekundárně umožnit, a to i z důvodu zákonné povinnosti zajistit důvěrnost komunikací, formou zákonných povinností vynutit součinnost těch subjektů, které by dobrovolnou spolupráci akceptovat případně odmítly, a to s důrazem na subjekty, jejichž infrastruktura je pro stát kriticky důležitá. Jinak by vznikala hluchá místa v kybernetické obraně, která by umožňovala potencionálnímu útočníkovi případné obejití kybernetické obrany, a tedy její negaci.

Zásah do vlastnického práva je tedy co do své intenzity ve zřejmém nepoměru s rizikem zásahu do distributivních i nedistributivních práv, k jejichž ochraně zákon vzniká.

Povinnost umožnit nasazení technických prostředků kybernetické obrany, nad to za náhradu, tak zdaleka nedosahuje intenzity rizik ekonomických ztrát, společenských otřesů či ztráty mezinárodní důvěryhodnosti České republiky, ani hrozby případného narušení např. právě práva na informační sebeurčení osob. Povinnosti zamýšlené tímto zákonem jsou tedy plně odůvodněny chráněnými zájmy a omezují své adresáty jen v naprosto nezbytně nutné míře. Lze tedy konstatovat, že navrhovaná úprava je poměrná.

Vzhledem k tomu, že zákon, jak uvedeno shora, přináší jen minimum povinností osobám soukromého práva, nezatěžuje jejich právo na informační sebeurčení (tj. předkládaný návrh nedává státním orgánům nové právo zasahovat do soukromí ani do aktivní komunikace uživatelů služeb informační společnosti) a naopak zvyšuje míru ochrany základních práv (včetně práva na informační sebeurčení) a nedistributivních veřejných statků (např. kybernetické bezpečnosti), lze konstatovat, že vyhovuje požadavkům ústavní proporcionality a je tedy ústavně konformní.

Právní úprava je navrhována tak, aby byla v souladu se zásadami zákonnosti, legitimity cílů a přiměřenosti zásahu do základních práv a svobod. Předkládaný návrh směřuje k tomu, aby stát zajistil informace o činnostech, které ohrožují jeho bezpečnost, aby byl připraven detekovat aktivity, jež ohrožují jeho bezpečnost a v rámci možností byl schopen se jim bránit nebo alespoň minimalizovat následky.

Lze tedy konstatovat, že navrhovaná právní úprava je v souladu s ústavním pořádkem České republiky.

V. Zhodnocení slučitelnosti navrhované právní úpravy s právem Evropské unie, judikaturou soudních orgánů Evropské unie nebo obecnými právními zásadami práva Evropské unie

Činnost zpravodajských služeb není právem Evropské unie upravena, přičemž naopak spadá pod pojem tzv. národní bezpečnosti, o němž Smlouva o Evropské unii stanoví v čl. 4 odst. 2 větě poslední výslovně, že „zejména národní bezpečnost zůstává výhradní odpovědností každého členského státu“. Pojem národní bezpečnosti se dotýká ochrany samotných základů státu, tedy ochrany před činnostmi ohrožujícími nebo narušujícími takové hodnoty jako jsou ústavní zřízení, významné ekonomické zájmy, bezpečnost a obrana státu. Tento pojem je třeba považovat za zvláštní vůči obecnému pojmu bezpečnosti, který je součásti prostoru svobody, bezpečnosti a práva a který se týká předcházení trestným činům nebo správním deliktům, jejich odhalování a objasňování (srov. hlavu V Smlouvy o fungování Evropské unie – Prostor svobody, bezpečnosti a práva) – v této oblasti Evropská unie naopak s členskými státy část pravomocí sdílí (čl. 4 odst. 2 písm. j) Smlouvy o fungování Evropské unie).

Smlouva o EU se obrany členských států dotýká v čl. 42 a následujících, týkajících se společné bezpečnostní a obranné politiky. Příprava členských států k obraně, včetně obrany v kybernetickém prostoru, bude-li v souladu se společnou obrannou a bezpečnostní politikou EU, nemůže v takovém případě být v rozporu s právem EU. Návrh je tedy s právem EU slučitelný.

Nad rámec problematiky kybernetické obrany je však možné poznamenat, že doposud se EU věnuje pouze oblasti kybernetické bezpečnosti v rozsahu, který působností odpovídá našemu zákonu o kybernetické bezpečnosti.

Oblast bezpečnosti sítí a informací v Evropské unii je od července roku 2016 regulována směrnicí Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii[27].

Jak již bylo uvedeno výše, sub II., navrhovaná úprava zasáhne, byť ne více než tomu je dosud, do soukromé sféry osoby, která je chráněna čl. 7 Listiny základních práv Evropské unie a dále – ve vztahu k navrhované úpravě – rozvinuta v čl. 8 této Listiny, jenž upravuje ochranu osobních údajů osoby. Stejně jako v rámci zhodnocení navrhované právní úpravy s ústavním pořádkem České republiky také zde platí, že právní úprava je navrhována tak, aby byla v souladu se zásadami zákonnosti, legitimity cílů a přiměřenosti zásahu do základních práv a svobod; odpovídá proto podmínkám pro omezení podle čl. 52 uvedené Listiny.

VI. Zhodnocení souladu navrhované úpravy s mezinárodními smlouvami, jimiž je Česká republika vázána

Navrhovaná úprava není v rozporu s mezinárodními smlouvami, jimiž je Česká republika vázána. Zároveň je ovšem třeba poznamenat, že tyto mezinárodní smlouvy se vzhledem k datu svého vzniku eo ipso ani problematikou kybernetické obrany (ani kybernetické bezpečnosti) zabývat nemohou. Toto ovšem neznamená, že není možné dohledat ustanovení, která mohou být potencionálně aplikována i na tuto oblast.

Soulad s Úmluvou o ochraně lidských práv a základních svobod a Mezinárodním paktem o občanských a politických právech byl posouzen výše v kapitole II.

Do otázek týkajících se práva na sebeobranu státu, tedy rovněž na sebeobranu v kybernetickém prostoru, zasahuje zejména Charta Spojených národů, která státům výslovně přiznává v čl. 51 právo na sebeobranu. Dále se bude jednat o prameny mezinárodního humanitárního práva. Jelikož však návrh zákona nijak nespecifikuje způsob provádění této (kybernetické) sebeobrany, sám o sobě není a nemůže být s Chartou ani dalšími prameny mezinárodního práva v rozporu. Konkrétní akce a opatření, jež budou při výkonu kybernetické obrany konány, budou schvalovány ad hoc, a to vždy po důkladném posouzení, že jsou jak v souladu s pravidly stanovenými Chartou, tak v souladu s ostatním mezinárodním právem, přičemž posuzován bude též soulad jak s ius ad bellum tak i ius in bello. Jako jeden z inspiračních zdrojů jak pro zpracování návrhu zákona, tak následně pro vytváření vlastních podmínek výkonu kybernetické obrany - alespoň do doby, než dojde k dalšímu vývoji v této oblasti mezinárodního práva - bude využit tzv. Tallinský manuál, který vyjadřuje expertní názory na aplikaci mezinárodního humanitárního práva ve sféře kybernetického prostoru.

[27] Dostupný on-line na adrese: http://eur-lex.europa.eu/legal-content/CS/TXT/uri=CELEX%A52013PC0048

VII. Předpokládaný hospodářský a finanční dopad navrhované právní úpravy na státní rozpočet, ostatní veřejné rozpočty, na podnikatelské prostředí České republiky, dále sociální dopady, včetně dopadů na rodiny a dopadů na specifické skupiny obyvatel, zejména osoby sociálně slabé, osoby se zdravotním postižením a národnostní menšiny, a dopady na životní prostředí

Hospodářský a finanční dopad návrhu je vyhodnocen v závěrečné zprávě z hodnocení dopadů regulace (RIA).

Obecně lze konstatovat, že aby úkol zajišťovat kybernetickou obranu mohl být plněn, bude nutné navýšit rozpočet Vojenského zpravodajství. Konkrétní náklady lze pouze odhadovat, protože budou záviset zejména na rozhodnutích vlády o tom, v jakém rozsahu bude pracoviště kybernetické obrany budováno a jaké podmínky pro užívání technických prostředků kybernetické obrany budou vládou České republiky stanoveny.

Návrh zákona nepředstavuje vzhledem k předmětu úpravy a nositeli působnosti pro výkon kybernetické obrany žádné nároky na rozpočty krajů a obcí.

Dopad na podnikatelské prostředí bude spočívat pouze v tom, že vybraným podnikatelům v oblasti elektronických komunikací vznikne povinnost součinnosti při používání prostředků kybernetické obrany. Tato součinnost však bude vždy za adekvátní finanční náhradu.

Sociální dopady, dopad na rodiny ani na specifické skupiny obyvatel návrh zákona vzhledem k předmětu jeho úpravy nemá.

Návrh zákona rovněž není způsobilý vzhledem k povaze jím prováděné úpravy vyvolat dopady do životního prostředí.

VIII. Zhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů

Dopad na ochranu osobních údajů návrh zákona nemá. Nepředpokládá se zpracování osobních údajů nad rámec současného zpracování osobních údajů při plnění úkolů Vojenského zpravodajství a nenavrhuje se ani žádná změna právní úpravy tohoto zpracování.

Určitý dopad na soukromí návrh zákona bude mít, jelikož technické prostředky kybernetické obrany, jejichž používání má návrh umožnit, budou mít schopnost monitorovat provoz sítí elektronických komunikací. Bez takového monitoringu není totiž zajišťování kybernetické obrany v praxi proveditelné. Při takovémto monitoringu však nepůjde o sledování komunikace konkrétních osob (k tomuto účelu Vojenské zpravodajství může stejně jako dosud využívat institutu zpravodajské techniky, kterou nově bude i případné využití technických prostředků kybernetické obrany, bude-li jimi narušena důvěrnost zpráv konkrétní osoby), ale jedině o neadresný, necílený monitoring, jehož účelem bude zachytit a signalizovat nestandardní chování na monitorovaných sítích, a tím včas upozornit a reagovat na ohrožení bezpečnosti kybernetického prostoru. Jelikož nepůjde o cílené sledování, nebylo možné do návrhu zákona vložit jakékoli mechanismy kontroly a nezávislé povolovací

procesy. Konkrétní nasazování a používání technických prostředků tak bude alespoň stanovovat vláda jako kolektivní orgán, čímž bude zajištěna nezbytná míra kontroly nad činností Vojenského zpravodajství v této oblasti.

IX. Zhodnocení korupčních rizik

Navržená zákonná úprava je pojata tak, aby zásahy do pokojného stavu byly co nejmenší a aby rozhodování o těchto zásazích bylo vždy víceúrovňové a nekoncentrovalo se v jedné osobě. Tyto kroky jsou pak základní pojistkou vedoucí k minimalizaci korupčních rizik. Předpis kompetence Vojenského zpravodajství rozšiřuje jen v nezbytné míře, která mu umožní plnit úkoly nově právně zakotvených činností v rámci kybernetické obrany. Neupravuje žádný nový proces formálního rozhodování. Schvalování plánu kybernetické obrany státu bude probíhat standardním procesem formou vládního usnesení, přičemž návrh zákona byl zpracován v Ministerstva obrany s využitím odborných znalostí a zkušeností pracovní skupiny vytvořené za účelem posouzení všech souvisejících vztahů vyplývajících z kybernetické obrany jako integrální součásti obrany České republiky a zpracování co nejúčelnější normativní právní úpravy podmínek výkonu kybernetické obrany; pracovní skupina byla vytvořena ze zástupců Ministerstva vnitra, Národního bezpečnostního úřadu, Bezpečnostní informační služby, Úřadu pro zahraniční styky a informace a Českého telekomunikačního úřadu. Návrh zákona je předkládán vládě České republiky cestou ministra obrany, přičemž vláda České republiky bude poté moci po jeho přijetí opět prostřednictvím ministra obrany kontrolovat jeho faktické plnění a efektivitu přijatých opatření. Na základě tohoto plánu a souvisejících vyhodnocení faktického stavu sítí a služeb elektronických komunikací v České republice bude opět vláda jakožto kolektivní orgán schvalovat nasazení konkrétních prostředků kybernetické obrany a rovněž základní pravidla jejich použití.

Návrh zákona přímo neupravuje opravné prostředky proti těmto usnesením (lze se však dovolat například úpravy provedené Jednacím řádem vlády). Je však třeba dodat, že teprve na základě těchto usnesení bude Vojenské zpravodajství oslovovat příslušné právnické nebo fyzické osoby zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací s žádostmi o součinnost, přičemž se předpokládá s každým takovým subjektem uzavření dohody o způsobu nasazení technických prostředků. Každý subjekt přímo dotčený nasazením technických prostředků tak bude moci se k realizovanému opatření vyjádřit, a v případě nedohody si případně i stěžovat nebo požadovat změnu příslušných usnesení (byť samozřejmě neformálně a bez nároku na změnu). Zároveň navrhovaná právní úprava žádným způsobem neomezuje právnické nebo fyzické osoby zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací, vůči kterým bylo vládou rozhodnuto o povinnosti zřízení technického rozhraní pro připojení technických prostředků kybernetické obrany, v podání žaloby podle § 82 soudního řádu správního[28]. Obdobně nelze vyloučit ani podání ústavní stížnosti.

Byť není korupční potenciál předkládaného návrhu zákona zcela zanedbatelný, je velice nízký.

Teoreticky je tak možné si představit možnost snahy některých osob zajišťujících síť elektronických komunikací nebo poskytujících službu elektronických komunikací ovlivnit ať

[28] Každý, kdo tvrdí, že byl přímo zkrácen na svých právech nezákonným zásahem, pokynem nebo donucením (dále jen "zásah") správního orgánu, který není rozhodnutím, a byl zaměřen přímo proti němu nebo v jeho důsledku bylo proti němu přímo zasaženo, může se žalobou u soudu domáhat ochrany proti němu nebo určení toho, že zásah byl nezákonný.

už pozitivně nebo negativně své zařazení mezi subjekty, u nichž bude realizováno nasazení technických prostředků. Lze ovšem říci, že toto riziko je velmi nízké.

Taktéž lze teoreticky uvažovat o možnosti snahy některých osob zajišťujících síť elektronických komunikací nebo poskytujících službu elektronických komunikací ovlivnit výši náhrady nákladů spojených se zřízením rozhraní pro připojení technických prostředků kybernetické obrany. Ani v tomto případě ovšem nelze považovat takovéto korupční riziko za příliš reálné, jelikož výši a podmínky poskytování těchto náhrad by měl stanovit prováděcí právní předpis v podobě nařízení vlády, jenž by měl garantovat dostatečnou ochranu před možným korupčním rizikem.

X. Zhodnocení dopadů na bezpečnost a obranu státu

Návrh zákona má přímý dopad na obranu a bezpečnost státu. Definuje kybernetickou obranu jako součást zajišťování obrany státu, nastavuje pravidla jejího plánování, budování a přímého výkonu, čímž ve svém souhrnu významně přispívá k zajišťování obrany a bezpečnosti České republiky. Návrh zákona nemá dopady na aktiva zpravodajských služeb ani bezpečnostních sborů ani na jejich příslušníky. Podrobnosti obsahuje závěrečná zpráva RIA.

B) Zvláštní část

K části první – novela zákona o Vojenském zpravodajství
K čl. I

K bodu 1

Do § 1 zákona o Vojenském zpravodajství, který vymezuje Vojenské zpravodajství jako jednotnou ozbrojenou zpravodajskou službu České republiky, se doplňuje nový odstavec 3, a to jako formulování úkolu (*nové působnosti*) Vojenského zpravodajství, kterým je plnění úkolů obrany České republiky v kybernetickém prostoru.

Uvedené doplnění plnění odpovídá ustanovení § 5 odst. 4 zákona o zpravodajských službách České republiky, kterým je stanoveno, že zpravodajské služby společně se svým základním posláním kterým je získávání, shromažďování a vyhodnocování informací důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnost a obranu České republiky, mohou plnit také další úkoly, pokud tak stanoví zvláštní zákon nebo mezinárodní smlouva, jíž je Česká republika vázána.

Navrhovaná úprava je pak provázána na zákon o zajišťování obrany České republiky (viz část druhá návrhu zákona), a to tak, aby bylo zřejmé, že obrana České republiky v kybernetickém prostoru je přímou součástí zajišťování obrany státu.

Pojem „kybernetický prostor“ je pak odkázán na jeho definici v zákoně o kybernetické bezpečnosti, neboť se jedná o totéž prostředí s týmiž znaky.

K bodu 2

Do zákona o Vojenském zpravodajství se navrhuje vložit novou část třetí, a to za účelem provedení úpravy podmínek výkonu kybernetické obrany, a to včetně předpokladů pro umístění a použití technických prostředků kybernetické obrany a součinnosti právnických a podnikajících fyzických osob zajišťujících sítě elektronických komunikací nebo poskytujících službu elektronických komunikací.

K § 16a

Kybernetická obrana je v první řadě definována jako nedílná součást obrany České republiky, tedy včetně využívání všech jejich aspektů přípravy, organizace a strukturálních vazeb.

Za zásadní úpravu je nepochybně nutné považovat definování technických prostředků kybernetické obrany, jíž jsou stanoveny jednoznačné meze pro povahu nástrojů, jimiž může být kybernetická obrana zajišťována. Podle definice provedené v navrhovaném znění § 16a odst. 2 budou technickými prostředky kybernetické obrany technická zařízení a s nimi související opatření vedoucí k předcházení, zastavení nebo odvrácení kybernetického útoku ohrožujícího schopnosti zajišťování obrany České republiky. Půjde tedy jednak o věcné prostředky, ale také s nimi související činnosti, tedy jejich vlastní použití, mj. v určitých mezních situacích např. i prvky aktivní obrany. Aby jejich použití bylo účinné, není možné vyčerpávajícím způsobem v důvodové zprávě ani v jiných veřejně dostupných dokumentech objasňovat způsoby jejich využití, jejich schopnosti, možnosti a slabiny (souvisí s nutností

utajovat aktiva zpravodajských služeb, k tomu srov. usnesení vlády č. 343D ze dne 6. května 2015). Na druhou stranu je nezbytné, aby Vojenské zpravodajství mělo nastavena jasná pravidla a limity svého působení, které se v rámci využívání těchto technických prostředků smí a současně musí dodržet.

Není primárním účelem technických prostředků kybernetické obrany zjišťovat obsah datového provozu konkrétních uživatelů, tyto aktivity, budou-li to technické prostředky kybernetické obrany vůbec umožňovat, bude moci Vojenské zpravodajství i nadále provádět výhradně a pouze v intencích pravidel pro použití zpravodajské techniky[29], a tedy na základě povolení soudce, který takovéto povolení vydá jedině při splnění zákonných předpokladů.

V souladu s dosavadní koncepcí zákonů upravujících činnost zpravodajských služeb, tedy i zákona o Vojenském zpravodajství, je na úrovni zákona o Vojenském zpravodajství upravena z oblasti kybernetické obrany jen ta problematika, jíž lze označit jako uplatňování státní moci, tedy jen ty záležitosti, které se dotýkají osob a jejich práv a svobod. Ostatní záležitosti, jež zákonnou úpravu nevyžadují, budou součástí plánu kybernetické obrany státu schváleného vládou, anebo součástí Statutu Vojenského zpravodajství, který rovněž schvaluje vláda. Jedná se o standardní legislativní přístup k problematice obrany státu a zpravodajské činnosti, který byl i dosud používán.

Navrhovaná úprava stanoví limity pro používání technických prostředků kybernetické obrany pro případy, kdy lze předpokládat, že takovou činností může dojít k narušení důvěrnosti zpráv (*tedy jakákoliv informace, která se vyměňuje nebo přenáší mezi konečným počtem účastníků nebo uživatelů prostřednictvím veřejně dostupné služby elektronických komunikací, s výjimkou informace přenášené jako součást veřejného rozhlasového nebo televizního vysílání sítí elektronických komunikací, nelze-li ji přiřadit k určitelnému účastníkovi nebo uživateli, který tuto informaci přijímá*) a s nimi spojených provozních a lokalizačních údajů konkrétní osoby; těmito limity jsou omezení stanovená pro použití zpravodajské techniky v zákoně o vojenském zpravodajství.

K § 16b

Jelikož není navrhovanou úpravou primárně sledováno umožnění Vojenskému zpravodajství zjišťování obsahu datového provozu konkrétních uživatelů, není obecně navrhován u nasazení a používání technických prostředků obdobný povolovací režim jako u zpravodajské techniky, jelikož tyto prostředky nejsou určeny k monitorování datové komunikace konkrétní osoby, nýbrž toliko obecných znaků datového provozu odůvodňujících možné následné užití obranných aktivit, a tudíž není účelné a ani možné je takto povolovat. Naopak, zákon o Vojenském zpravodajství i dosud stanovuje, že použitím zpravodajské techniky, pokud jím není zasahováno do základních práv a svobod, není monitorování telekomunikačního, radiokomunikačního nebo jiného obdobného provozu bez odposlechu jeho obsahu, popřípadě zjišťování údajů o tomto provozu[30], to znamená, že k monitorování provozu sítí bez soudního povolení je Vojenské zpravodajství oprávněno již nyní.

Rozhodnutí o umístění technických prostředků kybernetické obrany (tedy de facto „co a kam“) je v § 16b svěřováno vládě, která bude o případném umístění rozhodovat na základě návrhu ředitele Vojenského zpravodajství předloženého cestou ministra obrany. Vláda bude rovněž mít, na základě téhož § 16b pravomoc prioritně rozhodovat o podmínkách použití

[29] § 10 zákona č. 289/2005 Sb., o Vojenském zpravodajství.
[30] § 8 odst. 2 písm. d) zákona č. 289/2005 Sb., o Vojenském zpravodajství.

technických prostředků kybernetické obrany. Takové rozhodnutí bude mít podobu pravidel, „manuálu“, který bude určovat Vojenskému zpravodajství, za jakých podmínek a jakým způsobem smí určené technické prostředky použít. V případech, kdy to okolnosti dovolí, může vláda rozhodovat i o použití těchto technických prostředků v konkrétních jednotlivých případech.

Z vymezení situací, za nichž je možné tyto technické prostředky použít, pak jednoznačně vyplývá conditio sine qua non těchto postupů, tedy že budou moci být použity jen tehdy, kdy standardní opatření pro bezpečnost České republiky v kybernetickém prostoru stačit nemohou.

K § 16c

Navrhovaným ustanovením § 16c je Vojenské zpravodajství oprávněno v souladu s usnesením vlády o umístění technických prostředků kybernetické obrany, jakož i v rozsahu potřebném pro plnění úkolů zajišťování kybernetické obrany požadovat od právnické nebo fyzické osoby zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací zřízení rozhraní pro připojení technických prostředků kybernetické obrany. Jde o obdobu v současnosti platného ustanovení § 9 odst. 5 písm. a) zákona o Vojenském zpravodajství, podle něhož Vojenské zpravodajství je oprávněno v rozsahu potřebném pro plnění konkrétního úkolu požadovat od právnické nebo fyzické osoby zajišťující veřejnou komunikační síť anebo poskytující veřejně dostupnou službu elektronických komunikací zřízení, popřípadě zabezpečení rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech nebo záznam zpráv v určených bodech jejich sítě. Navrhované znění § 16c upravuje obdobné oprávnění k součinnosti pro účely kybernetické obrany.

K bodu 3

V § 22 odst. 2 se navrhuje řediteli Vojenského zpravodajství uložit, aby vedle již stanovených dokumentů jím předkládaných kontrolnímu orgánu, tedy Stálé komisi pro kontrolu činnosti Vojenského zpravodajství, byl povinen předkládat rovněž usnesení vlády České republiky o schválení umístění a podmínek použití technických prostředků kybernetické obrany.

Navrhovaná úprava opět směřuje k zajištění vyloučení svévole v použití technických prostředků kybernetické obrany, když veškeré související činnosti podléhají kontrole Poslanecké sněmovny, a to právě prostřednictvím (*s využitím*) kontroly základního dokumentu, který bude Vojenskému zpravodajství stanovovat pravidla pro výkon kybernetické obrany.

K bodu 4

Navrhovanou úpravou je do § 22 odst. 3 zákona o Vojenském zpravodajství doplňován další dokument, který je ředitel Vojenského zpravodajství povinen na požádání předkládat kontrolnímu orgánu. Tímto dokumentem je zpráva zprávu o použití technických prostředků kybernetické obrany na území České republiky, přičemž obsah dokumentu je omezen pouze na ty případy, ve kterých Vojenské zpravodajství svou činnost již ukončilo. Navrhované ustanovení ve vztahu k výkonu kybernetické obrany opět posiluje vymezení mantinelů užití

technických prostředků kybernetické obrany tak, aby byly vytvořeny garance zamezení případné svévole jejich užití jednotlivých a poskytnuty garance zachování demokratických zásad ve fungování státu.

K části druhé – změna zákona o zajišťování obrany

K čl. II

K bodu 1

Navrhovaným doplněním § 2 odst. 1 zákona o zajišťování obrany České republiky se obrana kybernetického prostoru stává integrální součástí obrany státu, a je tedy na ni nutné pohlížet v kontextu tohoto zákona, a tedy na ni uplatňovat jím stanovení zásady přípravy, organizace i výkonu obrany.

K bodu 2

Zákon o zajišťování obrany vymezuje[31] základní pojem obrana státu, jako souhrn opatření k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením. Obrana státu zahrnuje výstavbu účinného systému obrany státu, přípravu a použití odpovídajících sil a prostředků a účast v kolektivním obranném systému. Je přitom nepochybné, zejména ve vazbě na výše uvedenou zákonnou definici pojmu obrana státu (coby souhrn opatření činěných za určitým účelem), že tento souhrn opatření lze uplatňovat taktéž ve sféře kybernetického prostoru, jak jej definuje zákon o kybernetické bezpečnosti[32].

Návrh zákona proto explicitně doplňuje do výčtu toho, co zahrnuje obrana státu a její systém, též kybernetickou obranu, jelikož se jedná o novou, velmi specifickou oblast obranných aktivit, odlišnou od současných forem „kinetické“ obrany (pozemní, vzdušná apod.), kterou je vhodné samostatně zdůraznit a jednoznačně konstatovat její reálnost a určit její nezadatelné místo v systému obrany státu.

V důsledku výslovného doplnění kybernetické obrany jako součásti systému obrany státu se dává jasně najevo, že veškeré aktivity týkající se obrany státu mohou a musí počítat také s kybernetickou obranou jako její nedílnou součástí. I plnění úkolů kybernetické obrany tak bude součástí zajišťování obrany státu, pročež bude možné využít i všech nástrojů, které poskytuje zákon o zajišťování obrany.

Navrhovanou úpravou (vložením nového odstavce 2 do § 2) zajištěn účel výkonu kybernetické obrany, který musí být shodný s výkonem obrany klasické a kterým je zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrana života obyvatel a jejich majetku před vnějším napadením.

[31] § 2 odst. 1 zákona č. 222/1999 Sb., o zajišťování obrany České republiky.

[32] § 2 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Ve spojení s progresivním zahrnutím dimenze kyberprostoru do oblastí, v nichž je realizován souhrn opatření tvořících obranu státu, je navrhovaným doplněním § 2 odst. 1 zákona o zajišťování obrany České republiky provedeno doplnění základní definice obsahu kybernetické obrany. Obsah kybernetické obrany je tvořen činnostmi směřujícími k vytvoření účinného systému obrany v kybernetickém prostoru a příprava a použití sil a technických prostředků. Jedná se tedy jednak o přípravu, vývoj, výstavbu a výcvik, a jednak o samotné použití všech sil a prostředků, které v dané chvíli budou potřebné, vhodné, nezbytné a k dispozici k tomu, aby byla zajištěna obrana České republiky.

K bodu 3

Zahrnutím kybernetické obrany do systému obrany České republiky jako celku vyvolává potřebu systémově doplnit tuto její součást do dalších ustanovení zákona o zajišťování obrany České republiky tak, aby byly vyloučeny výkladové pochybnosti o rozsahu činností, které z tohoto zákona dopadají také na přípravu, věcné zajištění, organizaci a výkon kybernetické obrany.

Plánování kybernetické obrany státu se proto zařazuje do definičního výčtu toho, co tvoří plány obrany státu, čímž je současně zdůrazněna jeho specifická povaha a role v celém komplexním systému.

K bodu 4

Jelikož je obrana státu, jak ji definuje zákon o zajišťování obrany České republiky[33], nově výslovně doplněna o oblast obrany vykonávané ve sféře kybernetického prostoru, tedy kybernetickou obranu státu, která se stává nedílnou byť specifickou součástí obrany státu, dochází tak, jako je tomu u obrany státu obecně, také u kybernetické obrany k navázání tohoto institutu na proces plánování obrany státu, a to formou samostatného podzákonného obranně – plánovacího dokumentu v podobě plánu kybernetické obrany státu. Vzhledem k faktu, že činnost zpravodajských služeb, a tedy i Vojenského zpravodajství, podléhá kontrole vlády (§ 12 zákona č. 153/1994 Sb., o zpravodajských službách České republiky), jeví se jako vhodné a dostatečné, aby základní pravidla a meze činnosti byly primárně stanoveny vládou prostřednictvím schválení plánu kybernetické obrany státu. Tento plán bude jedním z plánů obrany státu podle zákona o zajišťování obrany[34], kdy Ministerstvo obrany k zajišťování obrany státu podle § 6 odst. 1 písm. a) tohoto zákona navrhuje vládě základní opatření k přípravě a organizování obrany státu; k tomu zejména zpracovává obranné koncepce a požadavky na zabezpečení obrany státu. Proces zpracování a schválení plánu je tak zcela v souladu s již běžně zavedenými formami podzákonných obranně – plánovacích dokumentů, schvalovaných vládou, která odpovídá za přípravu a zajišťování obrany státu[35]. Plán bude samozřejmě vzhledem k velké citlivosti obsahu utajovanou informací příslušného stupně. Bude nicméně dokumentem, který bude přesně vymezovat pravidla přípravy a zajišťování kybernetické obrany v České republice, a jedině postupy a činnosti, které budou v souladu s plánem, budou moci být považovány za souladné se zákonem.

[33] § 2 odst. 1 zákona č. 222/1999 Sb., o zajišťování obrany České republiky.
[34] § 5 odst. 1 písm. c) zákona č. 222/1999 Sb., o zajišťování obrany České republiky.
[35] § 4 zákona č. 222/1999 Sb., o zajišťování obrany České republiky.

K bodu 5

V souvislosti s úpravou podmínek zajišťování kybernetické obrany je nutné zajistit proporcionalitu oprávnění k provádění dalších, pro stát zásadních činností prováděných v kybernetickém prostoru. Kybernetická obrana byla proto i pro přípravu návrhu zákona zvažována v kontextu činností (resp. stanovených práv a povinností) vykonávaných za účel zajištění bezpečnosti kybernetického prostoru. Navrhovaná úprava proto stanoví limity pro výkon oprávnění Národního bezpečnostního úřadu při zajišťování bezpečnosti kybernetického prostoru za stavu ohrožení státu nebo za válečného stavu, a to v obecné rovině tak, aby upřednostněno bylo zajištění obrany státu, když v kybernetickém prostoru bude vždy souběžně zajišťována jeho bezpečnost i obrana státu, avšak s omezením, že kybernetická obrana nesmí bránit zajišťování kybernetické obrany.

Národní bezpečnostní úřad je proto do budoucna pro případy stavu ohrožení státu vyhlášeného v souvislosti se zajišťováním obrany České republiky před vnějším napadením nebo válečného stavu omezen co do ukládání provedení reaktivních opatření nebo ochranných opatření „nerušeným výkonem kybernetické obrany“, což v praxi bude představovat úzkou součinnost Vojenského zpravodajství a Národního bezpečnostního úřadu.

K části třetí – změna zákona o elektronických komunikacích

K čl. III

K bodu 1

Navrhovanou úpravou je provedeno legislativně- technické opatření vyvolané úpravou provedenou podle bodu 2 této části návrhu zákona. Podle dosavadní právní úpravy je České telekomunikační úřad zmocněn k tomu, aby všeobecným oprávněním stanovil konkrétní podmínky týkající kromě jiného také plnění povinností podle § 97 zákona o elektronických komunikacích, přičemž nově je nutné zajistit, aby se tato povinnost týkala také nově navrhované úpravy podle bodu 2 (nově navrhované znění § 98a), a to kromě jiného pro obdobnost obou úprav (viz čl. 4 odst. 3 Listiny základních práv a svobod).

K bodu 2

K odstavci 1

Nově vkládaný § 98a odst. 1 je provázán k nově navrhovanému znění § 16c zákona o Vojenském zpravodajství. Podle něj je právnická nebo podnikající fyzická osoba zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací povinna Vojenskému zpravodajství podle § 16c zákona o Vojenském zpravodajství zřídit a zabezpečit v určených bodech své sítě rozhraní pro připojení technických prostředků kybernetické obrany. Jde o obdobu ustanovení § 97 odst. 1, který je odpovídající k § 9 odst. 5 zákona o Vojenském zpravodajství, a ukládá určeným osobám povinnost součinnosti.

K odstavci 2

V navrhovaném znění § 98a odst. 2 je provedena úprava náhrady nákladů právnických nebo fyzických osob zajišťujících síť elektronických komunikací nebo poskytujících službu elektronických komunikací, spojených s povinností zřídit a zabezpečit v určených bodech jejich sítě rozhraní pro připojení technických prostředků kybernetické obrany, a to k tíži

Vojenského zpravodajství, a dále upravuje zmocnění k vydání prováděcího předpisu, který následně stanoví výši a způsob určení úhrady za takto vynaložené náklady.

K odstavci 3

Navrhovaná úprava § 98a odst. 3 stanoví povinnost mlčenlivosti právnických nebo podnikající fyzických osob zajišťujících síť elektronických komunikací nebo poskytujících službu elektronických komunikací, jakož i dalších osob podílejících se na plnění jejich povinností uložených jim v zájmu zajišťování kybernetické obrany, týkající se připojení technických prostředků kybernetické obrany a s tím souvisejících skutečnostech. Tato mlčenlivost není časově omezená a trvá i potom, kdy tyto osoby přestanou být nositeli povinnosti zřídit a zabezpečit ve vhodných bodech své sítě rozhraní pro připojení technických prostředků kybernetické obrany, a to jako právnická nebo podnikající fyzická osoba zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací nebo osoba s nimi spolupracující.

K bodu 3

Navrhovaná úprava doplňuje novou skutkovou podstatu správního deliktu spočívající v neposkytnutí součinnosti (ve smyslu bodu 2) a v porušení mlčenlivosti. Vojenské zpravodajství bude oslovovat příslušné právnické nebo fyzické osoby zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací s žádostmi o součinnost na základě rozhodnutí vlády o nasazení technických prostředků kybernetické obrany, vždy s předpokladem „dobrovolnosti“ takovéto spolupráce (zvláště pokud náklady spojené s poskytnutou součinností těmto subjektům vznikající budou Vojenským zpravodajstvím refundovány), a tedy se záměrem uzavřít dohodu o způsobu nasazení technických prostředků s každým takovýmto subjektem. Jako ultima ratio je zde ovšem konstruována sankční povinnost dotčených subjektů, spojená s případným neposkytnutím zákonem stanovené součinnosti. O sankcích za tyto delikty bude rozhodovat Český telekomunikační úřad, který tak bude moci nezávisle posoudit, zda je neposkytnutí součinnosti oprávněné či nikoli.

K bodu 4

Dnem 1. července 2017 nabude účinnosti zákona č. 252/2016 Sb., o odpovědnosti za přestupky a řízení o nich, který mění koncepci správního trestání. Proto je kromě doplnění skutkové podstaty podle bodu 4, s níž je spojena odpovědnost za její porušení, přizpůsobit začlenění nově navrhovaného ustanovení do právního řádu také po 1. červenci 2017. Navrhovaná úprava je proto svázána s odloženou účinností práva od 1. července 2017, jež je zajištěna úpravou uvedenou v části čtvrté čl. IV návrhu zákona.

K bodu 5

Jedná se o legislativně technické změny provedené v návaznosti na novelizační bod 3.

K bodu 6

Navrhované znění § 119 odst. 7 doplňuje novou skutkovou podstatu přestupku spočívající v porušení mlčenlivosti uložené podle navrhovaného znění § 98a odst. 3 (povinnost mlčenlivosti fyzických osob o připojení technických prostředků kybernetické obrany a s tím souvisejících skutečnostech).

K bodu 7

Jedná se o legislativně technické změny provedené v návaznosti na novelizační bod 6.

K bodu 8

Ministerstvo obrany se zmocňuje k vydání vyhlášky, kterou se stanoví způsob určení výše efektivně vynaložených nákladů za zřízení a zabezpečení rozhraní a způsob jejich úhrady.

K části čtvrté – ÚČINNOST

K čl. IV

Navrhovanou úpravou se stanoví, že návrh zákona nabývá účinnosti patnáctým dnem po jeho vyhlášení ve Sbírce zákonů, a to s výjimkou úpravy navrhované v části třetí bodě 4 (viz odůvodnění bodu 4).

V Praze dne 5. října 2016

Předseda vlády:

Mgr. Bohuslav Sobotka v. r.

Ministr obrany:

MgA. Martin Stropnický v. r.