##  IV.

## DŮVODOVÁ ZPRÁVA

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

## Obecná část

Poznámka k obecné části:

V souladu s čl. 9 odst. 3 Legislativních pravidel vlády jsou dále uvedené kapitoly I. až III. a V. až IX. obsahově rozpracovány v Závěrečné zprávě z hodnocení dopadů regulace k návrhu zákona (část V. celého materiálu), následující text je proto nutné vnímat jako základní informaci ke každé z kapitol uvedených názvem příslušné oblasti odůvodnění zpracovatelského přístupu k návrhu zákona, kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony (dále jen „návrh zákona“).

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

I. 1 Zhodnocení platného právního stavu

Vláda České republiky svým usnesením ze dne 25. května 2016 č. 382, kterým schválila Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020, současně uložila Ministerstvu obrany úkol předložit návrh normativního řešení vytvoření podmínek kybernetické obrany České republiky.

Ministerstvo obrany na základě tohoto úkolu připravilo ve spolupráci s MV, NBÚ, ÚZSI, BIS a ČTÚ návrh zákona, kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony (dále jen „návrh neprojednaného zákona“). Cílem návrhu neprojednaného zákona bylo umožnit splnění úkolu C. 9.01 uvedeného Akčního plánu, tedy zajistit podmínky výkonu kybernetické obrany a vybudování Národního centra kybernetických sil v rámci Vojenského zpravodajství.

Předkládaným návrhem neprojednaného návrhu zákona byly navrženy změny těchto právních předpisů v působnosti MO:

* zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů,
* zákon č. 222/1999 Sb., o zajišťování obrany České republiky, ve znění pozdějších předpisů;

dále se návrhem mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

Návrh neprojednaného zákona schválila vláda České republiky na svém jednání dne 5. října 2015, přičemž návrh byl po zapracování schválených úprav předán k dalšímu legislativnímu projednání Poslanecké sněmovně Parlamentu České republiky. Legislativní proces k návrhu neprojednaného zákona však byl po široké diskusi ukončen, neboť v něm nebyly shledány dostatečné záruky pro ochranu soukromí a osobních údajů fyzických osob, jako problémový pak byl shledán rovněž způsob řešení svěření provádění kybernetické obrany do výlučné působnosti Vojenskému zpravodajství mimo rámec jemu svěřené působnosti zpravodajské služby, tedy mimo rámec činností prováděných podle § 2 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, jímž je stanoveno, že zpravodajské služby jsou státní orgány pro „získávání, shromažďování a vyhodnocování informací důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnost a obranu České republiky“. Podle § 5 odst. 4 zákona č. 153/1994 Sb. sice zpravodajské služby mohou plnit také další úkoly, pokud tak stanoví zvláštní zákon nebo mezinárodní smlouva, jíž je Česká republika vázána, je však zřejmé, že i takto ukládané úkoly nemohou překročit zákonný rámec účelu, k němuž jsou zpravodajské služby České republiky zřizovány (viz § 2 zákona č. 153/1994 Sb.). Tento stav však neznamená, že úkol zadaný vládou České republiky je neřešitelný a že – aniž by byly porušeny požadavky na dodržení ústavnosti právního řádu – by bylo nemožné předpokládanou zákonnou úpravu zpracovat a předložit ji k posouzení do legislativního procesu.

K tomu, aby bylo možné při dodržení ústavnosti realizovat vládou České republiky uložené úkoly, je nutné detailně vyhodnotit existující právní rámec zajišťování obrany České republiky jako jedné ze základních funkcí státu a určení subjektů, které jsou k výkonu souvisejících činností zmocněny.

 Základní – a pro řešení zcela rozhodující – je úprava podmínek zajišťování bezpečnosti České republiky, provedená ústavním zákonem č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb. Podle čl. I tohoto ústavního zákona je „zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot základní povinností státu“. Podle čl. 3 odst. 1 citovaného ústavního zákona jsou výkonem této povinnosti státu pověřeny ozbrojené síly, ozbrojené bezpečnostní sbory, záchranné sbory a havarijní služby, čímž je provedena limitace postavení Vojenského zpravodajství pro zajišťování „kybernetické obrany“, neboť ustanovení § 3 odst. 1 a 2 zákona č. 219/1999 Sb., o ozbrojených silách České republiky, stanoví, že „k zajišťování své bezpečnosti vytváří Česká republika ozbrojené síly, které se člení na armádu, Vojenskou kancelář prezidenta republiky a Hradní stráž“.

 Pro předkládanou úpravu pak bylo důležité vyhodnotit také to, že „kybernetická obrana“ v rámci zajišťování obrany (tedy vnější bezpečnosti) státu není specifická, souběžně působící struktura nad standardní obranou státu, ale její nedílná součást, byť vlivem rozvoje moderních komunikačních technologií a služeb součást novější a specificky technologicky vybavená a zejména působící v nestandardním prostředí sítí a služeb elektronických komunikací. I přes tato specifika je však na kybernetickou obranu nutno pohlížet jako na standardní součást obrany státu ve smyslu § 2 odst. 1 zákona č. 222/1999 Sb., o zajišťování obrany České republiky, tedy jako na součást „souhrnu 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 a v tomto smyslu rovněž kybernetická obrana musí podléhat jednotnému koncepčnímu řízení, plánování a strategii, stejně jako platí, že v uvedeném smyslu za její přípravu a zajišťování odpovídá vláda České republiky (§ 4 zákona č. 222/1999 Sb.).

 Současný právní řád však umožňuje, aby se Vojenské zpravodajství na zajišťování „obrany státu v kybernetickém prostoru“ (jak je nově do právního řádu zaváděn název této součásti obrany České republiky) podílelo, navzdory tomu, že není ozbrojenou silou a že rámec účelu zřízení zpravodajských služeb jako státních orgánů pro „získávání, shromažďování a vyhodnocování informací důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnost a obranu České republiky“ by mohl sám o sobě aktivní podíl na zajišťování obrany státu vylučovat. Nositelem této možnosti je ustanovení čl. 3 odst. 2 ústavního zákona č. 110/1998 Sb., který stanoví, že „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.“. Navrhovaná právní úprava tedy není ničím jiným, než provedením zákonné úpravy rozsahu povinností Vojenského zpravodajství, kterými se do budoucna bude podílet na zajišťování obrany státu, a to s konkrétním vymezením tohoto podílu vzhledem k zajišťování obrany státu v kybernetickém prostoru. Stejně tak jsou návrhem zákona stanovovány podrobnosti, jimiž se upřesňují podmínky výkonu takto Vojenskému zpravodajství ukládaných povinností, a to včetně stanovení vnějších vazeb garantujících začlenění kybernetické obrany do celého kontextu zajišťování obrany a bezpečnosti České republiky, stanovení garancí pro ochranu soukromí a osobních údajů pro oblast monitorování oblasti sítí a služeb elektronických komunikací a kontrolních mechanismů poskytujících záruky proti zneužití takto Vojenskému zpravodajství svěřených pravomocí nebo případnému zabránění svévolného jednání tam, kde je nutné důsledně zvažovat proporcionalitu mezi prosazením bytostného zájmu státu a mezi ústavně garantovanými základními právy a svobodami fyzických osob.

I. 2 Zhodnocení současného stavu ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen

Právní úprava podmínek zajišťování jedné ze základních povinností státu při zajištění svrchovanosti a územní celistvosti České republiky, ochrany jejích demokratických základů a ochrany životů, zdraví a majetkových hodnot je v současné době upravena systémem právních předpisů souhrnně označovaných jako tzv. „systém branné legislativy“, který byl pro každou ze svých součástí, ale i jako celek, podroben důkladné analýze, zda jím nastavované instituty a procesy odpovídají zásadám vyloučení diskriminace a zachování principů rovnosti žen a mužů. Proto také tam, kde jsou Vojenskému zpravodajství ukládány nové povinnosti za účelem uvedeným v subkapitole I. 1, jsou tyto zásady zachovávány se stejnou důsledností. Rozšíření působnosti a pravomocí Vojenského zpravodajství a nové povinnosti podnikajících osob jsou stanovovány způsobem, který vylučuje jakoukoliv diskriminaci a který garantuje zachování 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

Ministerstvo obrany zpracovalo a k posouzení předkládá návrh zákona, který je v označení shodný s názvem návrhu neprojednaného zákona, tedy návrh zákona, kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony. Základním zpracovatelským principem pro tento návrh je vytvořit úpravu zcela ústavně slučitelnou, jednoznačnou, předvídatelnou a zajišťující jak potřebné podmínky pro zajišťování kybernetické obrany České republiky, tak současně potřebné vazby na zajišťování kybernetické bezpečnosti České republiky, ale také dostatečné záruky pro stanovení povinností a ochranu práv třetích osob, a to jak provozovatelů sítí a služeb elektronických komunikací, tak ochrany základních práv a svobod fyzických osob pro oblast ochrany soukromí a osobních údajů tak, jak nás zavazuje Úmluva o ochraně lidských práv a základních svobod.

Základní změnou koncepce zpracovaného návrhu zákona od návrhu neprojednaného zákona je úplný odklon od uměle vytvářeného začleňování Vojenského zpravodajství mezi ozbrojené síly, a tedy nepřípustné nepřímé novelizace zákona č. 219/1999 Sb., o ozbrojených silách České republiky. V této souvislosti bylo nutné se vypořádat s tím, že provádění kybernetické obrany svou povahou přesahuje obecně vymezené úkoly Vojenského zpravodajství jako zpravodajské služby, neboť provádění kybernetické obrany by alespoň v určitém rozsahu bylo aktivní činností přesahující rámec zabezpečování informací. Zákon o zpravodajských službách sice těmto službám umožňuje výkon dalších činností, pokud je ukládá jiný zákon, avšak tyto činnosti nesmí překročit rámec činností zpravodajských obecně vymezených v zákoně o zpravodajských službách, tedy rámec „*získávání, shromažďování a vyhodnocování informací důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnost a obranu České republiky“.* K tomu je využito čl. 3 odst. 2 ústavního zákona č. 110/1998 Sb. tak, jak je uvedeno v kapitole I. Toto řešení postavení Vojenského zpravodajství koresponduje s účelem zadání vyplývajícího z usnesení vlády České republiky 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 současně uložila Ministerstvu obrany úkol předložit návrh normativního řešení vytvoření podmínek kybernetické obrany České republiky. Navrhované právní řešení současně vychází ze skutečnosti, že v mezidobí od přijetí citovaného usnesení vlády České republiky do dnešních dnů Vojenské zpravodajství významně pokročilo ve své připravenosti k převzetí nové role, a tedy z hlediska věcného i odborného nebylo nutné hledat jinou variantu řešení pro stanovení nositele úkolu.

S uvedenou úpravou je pak nedílně spojená úprava začlenění zajišťování obrany státu v kybernetickém prostoru do celkového systému obrany a bezpečnosti České republiky, a to jednak v rámci plánování obrany státu Ministerstvem obrany, jednak v nastavení vazeb vůči dalším nositelům povinností při zajišťování obrany a bezpečnosti státu tak, aby byla zajištěna komplexní ochrana kybernetického prostoru ve všech sledovaných aspektech a za tímto účelem využito synergického účinku společného působení sil a prostředků Armády České republiky, Ministerstva vnitra a Národního úřadu pro kybernetickou a informační bezpečnost.

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 monitorování kybernetického prostoru, pro které – jsou-li užity ve smyslu zpravodajské techniky – platí stejné mantinely
a právní limity, jako je tomu u zpravodajské činnosti.

Navrhovaná úprava s vědomím toho, že se jedná o oblast mimořádně citlivou z hlediska nastavení vztahů mezi státem a provozovateli sítí a služeb elektronických komunikací, ale především z hlediska případných zásahů do soukromí nebo práva na ochranu osobních údajů, řeší jednoznačným, předvídatelným způsobem také pravidla pro ukládání povinností uvedeným podnikatelům i zásady, jimiž musí být zajištěna garance uvedených lidských práv, popřípadě na jejichž základě mohou být tato práva prolomena v zájmu zajištění plnění základních povinností státu s přihlédnutím k proporcionalitě těchto zájmů a ochraně demokratických principů a vyloučení svévole užití prostředků kybernetické obrany nad stanovený zákonný rámec.

## III. Vysvětlení nezbytnosti navrhované právní úpravy v jejím celku

Formálním důvodem zpracování návrhu zákona je – jak je již uvedeno v kapitole I. – usnesení vlády České republiky 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 současně uložila Ministerstvu obrany úkol předložit návrh normativního řešení vytvoření podmínek kybernetické obrany České republiky. Tento úkol i přes neúspěšný legislativní proces k návrhu neprojednaného zákona trvá, a to s akcentací veřejného zájmu na zajištění kompletní bezpečnosti kybernetického prostoru, v němž spolu s dynamickým nárůstem technologií vzrůstá jednak rozsah služeb a nabídek uživatelského prostředí, ale současně také rizika jeho zneužití. Vláda České republiky svým usnesením současně do jisté míry určila jednoho z hlavních nositelů zajišťování kybernetické obrany, i když je jí beze sporu stále nutné vnímat jako součást obrany státu jako takové, včetně uplatnění zásad odpovědnosti za její přípravu a zajišťování (*podle § 4 zákona č. 222/1999 Sb. je jejím nositelem vláda České republiky*) nebo její plánování [*podle § 6 odst. 1 písm. b) a c) zákona č. 222/1999 Sb. je jejím nositelem Ministerstvo obrany, které* *„odpovídá za proces plánování obrany státu a koordinuje jeho přípravu a za plánování a zabezpečení operační přípravy státního území, doplňování ozbrojených sil a mobilizaci ozbrojených sil“*].

Právním důvodem pro zcela nevyhnutelné zajištění účelu sledovaného usnesení vlády České republiky ze dne 25. května 2016 č. 382 formou přijetí zákona je provedená věcná a právní analýza možností řešení dané věci tak, jak je nastíněna v kapitole I., když Vojenské zpravodajství lze jako státní orgán s postavením jednotné ozbrojené zpravodajské služby České republiky pověřit podílením se na zajišťování obrany České republiky výlučně za podmínek stanovených v čl. 3 odst. 2 ústavního zákona č. 110/1998 Sb., tedy uložit související povinnosti včetně stanovení jejich rozsahu zákonem a jím rovněž stanovit další podrobnosti jejich výkonu.

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

Soulad navrhované úpravy s ústavním pořádkem již vyplývá ze skutečností uvedených v kapitole I., když je zřejmé, že návrh zákona je zákonem vydávaným za účelem sledovaným v čl. 3 odst. 2 ústavního zákona č. 110/1998 Sb. a formálně sleduje i zmocnění pro naplnění tohoto účelu stanovené týmž ustanovením. Soulad s právními předpisy souboru tzv. branné legislativy byl zajištěn analýzou vztahu návrhu zákona k zákonu č. 222/1999 Sb. a k zákonu č. 219/1999 Sb.

Při zpracování návrhu byla rovněž důsledně respektována zásada, že státní moc lze uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon.

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 jsou návrhem zákona Vojenskému zpravodajství pro činnosti vykonávané ve prospěch zajišťování kybernetické obrany stanovovány meze, které garantují vyloučení svévole při užití svěřených pravomocí i oddělení výkonu zpravodajské činnosti od zajišťování kybernetické obrany.

V zájmu zajištění předpokladů pro monitorování kybernetického prostoru jsou návrhem zákona stanovena pravidla, která umožní Vojenskému zpravodajství ukládat povinnosti provozovatelům sítí a služeb elektronických komunikací. I v tomto případě je úprava provedena tak, aby respektovala ústavní zásady, v daném případě zásadu, „ že nikdo nesmí být nucen činit, co zákon neukládá“; 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[[1]](#footnote-1). Návrh zákona nepředpokládá zásahy do těchto práv ve větším rozsahu, než tomu je dosud tam, kde budou využity informace získané zpravodajskou činností, při monitorování kybernetického prostoru pak budou vždy vyhodnocována výlučně neadresná data. Cílem monitorování kybernetického prostoru přitom není 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[[2]](#footnote-2). 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[[3]](#footnote-3) práv) České republiky a mezinárodních závazků České republiky.

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
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.

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 sond pro monitorování kybernetického prostoru 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 sond pro monitorování kybernetického prostoru, 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 nebo 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 vyvážená.

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 součástí 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. K zajišťování národní obrany v kyberprostoru však nabádá i výše zmiňovaná Strategie kybernetické bezpečnosti EU.

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[[4]](#footnote-4).

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.

## 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

Nově stanovené povinnosti Vojenskému zpravodajství, resp. zejména nezbytnost zajistit nové komplexní věcné, organizační a personální podmínky jejich výkonu, nepochybně vyvolají nároky na státní rozpočet, když bude nutné navýšit rozpočet Ministerstva obrany - Vojenského zpravodajství. Konkrétní náklady lze pouze odhadovat, protože budou záviset zejména na rozhodnutích vlády České republiky o tom, v jakém rozsahu bude pracoviště kybernetické obrany budováno a jaké budou ambice pro jeho vybavenost, když je zřejmé, že pracoviště musí umožňovat rychlou reakci na technologický vývoj tak, aby nezaostávalo za uživateli sítí a služeb elektronických komunikací zejména tam, kde jsou (zne)užívány s cílem poškodit bezpečnost tohoto prostředí a působit proti zájmům státu.

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 sítí a služeb elektronických komunikací vznikne povinnost součinnosti
při vytvoření rozhraní na jimi provozovaných síti pro umístění sond umožňujících monitorovat kybernetický prostor.

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

 Návrhem zákona je stanoveno, že Vojenské zpravodajské plní jemu uložené povinnosti v oblasti zajišťování kybernetické obrany jednak na základě využití výsledků analýz prováděných u získaných, shromážděných a vyhodnocovaných informací v rozsahu jemu svěřené působnosti podle 5 odst. 3 zákona č. 153/1994 Sb. (zpravodajská činnost), jednak monitorováním provozu sítí a služeb elektronických komunikací. První z uvedených zdrojů je v oblasti ochrany soukromí a osobních údajů v potřebném rozsahu zajištěn dosavadní právní úpravou zásad činnosti zpravodajských služeb České republiky a v některých specifických aspektech dále ještě specifickými zásadami činnosti Vojenského zpravodajství. Dodržování těchto zásad je podrobeno kontrolním mechanismům, které je však nutné vnímat z úrovně účelu zpracování příslušných osobních údajů nebo prováděných zásahů do soukromí fyzických osob. Účelem získávání a shromažďování osobních údajů zpravodajskými službami je ochrana ústavního zřízení, významných ekonomických zájmů, bezpečnosti a obrany České republiky. Vedle sebe tak stojí dva obdobně silné zájmy státu a jeho obyvatel, pro něž za standardních (tedy předvídatelného a legálního chování všech účastníků) podmínek není problémem, aby nerušeně působily vedle sebe, aniž by se vzájemně ovlivňovaly. V případě, že je tento rovnovážný stav narušen, je však vždy nutné pro každý individuální případ takového narušení provést test proporcionality a určit, který z daných principů je v daném okamžiku hoden větší ochrany, resp. kdy zabránění důsledkům narušení jednoho principu je tak důležité pro zachování funkcí státu, že je možné po omezený čas v omezené míře zasáhnout do principu druhého. Proporcionalita mezi zájmem na zajišťování obrany státu a zájmem na zajišťování práva na soukromí je návrhem zákona zohledněna, a tedy obava, že by útok v kybernetickém prostoru mohl být automaticky vždy obecně kvalifikován jako „menší (nebo naopak větší) hrozba, než obava z neomezeného a nekontrolovaného průniku výkonné moci do soukromé sféry lidí“ není na místě díky jednoznačné, předvídatelné právní úpravě (k*tomu viz také rozsudek ESD ze dne 12. ledna 2016 ve věci 37138/14 – Szabó a Vissy proti Maďarsku, který uvádí:* „Mohu-li být dotčena základní práva a svobody, je však v demokratickém právním státě nepřípustné, aby byla diskrece svěřena orgánům moci výkonné v oblasti národní bezpečnosti bezbřehá. Právo tedy musí stanovit jasné meze pro její výkon tak, aby byli jednotlivci chráněni před svévolnými zásahy do svých práv.“).

Z této oblasti pak stav zůstává zachován a návrhem zákona nevznikají jiné situace nebo důvody, které by mohly být považovány za nové zdroje narušování ochrany soukromí a osobních údajů.

 Nově je Vojenskému zpravodajství v zájmu zajišťování povinností při zajišťování obrany v kybernetickém prostoru svěřena pravomoc tento prostor monitorovat, tedy nepřetržitě vyhodnocovat neadresná data v kybernetickém prostoru tak, aby bylo zaručeno včasné zjištění bezpečnostních hrozeb pro důležité zájmy státu, posouzení míry jejich intenzity, závažnosti jejich důsledků a způsobu jejich zastavení nebo odvrácení v kybernetickém prostoru. Bez takového monitoringu není zajišťování kybernetické obrany v praxi proveditelné; přitom však je stále nutné mít na mysli, že nepůjde o sledování komunikace konkrétních osob, 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.

Návrh zákona pro tyto případy výslovně stanoví, že „součástí monitorování kybernetického prostoru není zpracovávání osobních údajů nebo provádění odposlechů a záznamů podle zákona o elektronických komunikacích. V souvislosti s tím je pak Vojenskému zpravodajství uložena povinnost zajistit, aby monitorováním kybernetického prostoru nebyla narušena důvěrnost obsahu zprávy a aby bylo prováděno pouze způsobem vylučujícím zásahy do soukromého života.

V této souvislosti je pak nutné upozornit, že návrh zákona pro uvedené činnosti nastavuje vícestupňové mechanismy kontroly, a to jak uvnitř Vojenského zpravodajství, resp. Ministerstva obrany jako správního úřadu Vojenské zpravodajství řídící [§ 16 odst. 2 písm. e) kompetenčního zákona], tak kontroly vnější, tedy vládní a parlamentní, a dále také kontroly prováděné orgánem zvláštní kontroly podle zákona o zpravodajských službách České republiky.

V tomto ohledu je pak nově zaváděn v § 24a zákona o Vojenském zpravodajství nový, vnitřní kontrolní orgán této zpravodajské služby.

## 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.

Návrh zákona kompetence Vojenského zpravodajství rozšiřuje jen v nezbytné míře, která mu umožní plnit úkoly nově právně zakotvených činností v rámci kybernetické obrany, přičemž jeho korupční potenciál je velice nízký. Teoreticky je možné si představit snahy některých provozovatelů zajišťujících sítě elektronických komunikací nebo poskytujících službu elektronických komunikací ovlivnit – ať už pozitivně nebo negativně – své zařazení mezi subjekty, jimž bude ukládána povinnost pro zřízení rozhraní, na které bude připojována monitorovací sonda. Vzhledem k tomu, že taková povinnost bude ukládána formou rozhodnutí vydávaného ve správním řízení a že jeho vydání bude nezbytně nutně předcházet vyhodnocení účinnosti umístění sondy, lze toto riziko označit za velmi nízké.

Ryze jako teoretickou úvahu lze posoudit riziko možnosti ovlivnit výši náhrady nákladů spojených se zřízením rozhraní pro připojení sond monitoringu kybernetického prostoru. Pojistka vyloučení vzniku tohoto rizika je totiž obsažena v samotném návrhu zákona, a to ve zmocnění pro stanovení výše a podmínek poskytování náhrad vyhláškou Ministerstva obrany, jež by měls 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, neboť určuje nový subjekt, jemuž se stanovují povinnosti při zajišťování obrany státu, a to obrany v kybernetickém prostoru. Obrana státu je tak posilována v oblasti zcela specifických hrozeb, a to nejenom z pohledu technologického, ale také z pohledu prostorového umístění hrozeb, jejich vzniku, možností likvidace i případných účinků. Současně je tato specifická část obrany České republiky důsledně začleňována do celkové koncepce obrany České republiky, jejího plánování, přípravy a zajišťování.

Návrh zákona nemá dopady na aktiva zpravodajských služeb ani bezpečnostních sborů ani na jejich příslušníky. Podrobnosti obsahuje závěrečná zpráva RIA.

## Zvláštní část

**K části první – novela zákona o Vojenském zpravodajství**

###### **K čl. I**

**K bodu 1**

Obecně:

 Bodem 1 je do zákona č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, začleňována nová část čtvrtá, která má pro účely identifikace Vojenského zpravodajství jako jednoho z nositelů povinnosti podílet se na zajišťování obrany České republiky v informačních systémech a službách a sítích elektronických komunikacích (kybernetickém prostoru) povahu provedení čl. 3 odst. 2 věty druhé ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, tedy stanovení nezbytného rozsahu povinností a dalších podrobností pro výkon činností, jimiž se státní orgán – Vojenské zpravodajství – má podílet na zjišťování obrany státu.

Částí čtvrtou jsou nově upravovány povinnosti Vojenského zpravodajství, jimiž se podílí na zajišťování obrany v kybernetickém prostoru; vzhledem k specifické povaze tohoto prostoru i aktivitám, které v něm probíhají, včetně nemožnosti určit jeho hranice a předpokládané možné lokalizaci zdrojů jednotlivých hrozeb a rizik také mimo území České republiky, je Vojenskému zpravodajství přiznána možnost využívat výsledků analýzy jeho zpravodajské činnosti nikoliv pouze pro určení hrozby, ale také k přímému výkonu jejího odvrácení tam, kde by jinak příslušné byly ozbrojené síly České republiky.

K plnění úkolů Vojenského zpravodajství při zajišťování obrany státu v kybernetickém prostoru jsou návrhem zákona vytvářeny specifické podmínky, ale vždy s přihlédnutím k tomu, že k obraně státu jsou určeny ozbrojené síly a obrana státu je zajišťována jako celek, tedy bez ohledu na místo jejího provádění, typu využívaných sil a prostředků apod. Kybernetická obrana je tedy pojata jako nedílná součást obrany České republiky, tedy včetně využívání všech jejich aspektů přípravy, organizace a strukturálních vazeb.

Stejně je důraz kladen na to, že obrana státu v kybernetickém prostoru má velmi proměnlivé hranice ve vztahu k zajišťování vnitřní bezpečnosti státu v kybernetickém prostoru a že by bylo mimořádně kontraproduktivní obě tyto úrovně zajišťování bezpečnosti státu jako celku vnímat jako dvě důsledně oddělované aktivity.

K § 16a:

V navrhovaném znění § 16a odst. 1 je tak, jak je uvedeno výše, stanovena Vojenskému zpravodajství povinnost podílet se na zajišťování obrany státu v kybernetickém prostoru; situace, kdy má být tato povinnost naplňována je blíže vymezena identifikováním hrozby pro důležité zájmy státu, kterými jsou skutečnosti, jejichž ochranu svěřil zákonodárce v ústavní rovině do působnosti státu, tedy identifikováním hrozby pro svrchovanost, územní celistvost, demokratické základy České republiky nebo ve značném rozsahu pro ohrožení životů a zdraví, majetkových hodnot nebo životního prostředí. Limitace aktivní činnosti Vojenského zpravodajství při zajišťování obrany státu v kybernetickém prostoru je stanovena jednak časem a intenzitou identifikované hrozby, jednak aktuální absencí předpokladů pro její odvrácení ozbrojenými silami České republiky.

V odstavci 2 jsou ve prospěch Vojenského zpravodajství stanovovány informační zdroje, na jejichž základě identifikuje hrozby a rizika pro důležité zájmy státu. Těmito zdroji jsou jednak informace (data) získaná jeho standardní zpravodajskou činností (viz § 2 zákona č. 153/1994 Sb. – „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 dále provádění nepřetržitého monitorování kybernetického prostoru, tedy informačních systémů a sítí a služeb elektronických komunikací.

V odstavci 3 je provedeno důsledné oddělení monitorování kybernetického prostoru od standardní zpravodajské činnosti Vojenského zpravodajství; informace vyhodnocované Vojenským zpravodajstvím při monitorování kybernetického prostoru mu mohou sloužit výlučně pro aktivní zajišťování obrany státu v kybernetickém prostoru, nikoliv pro výkon jemu svěřené působnosti podle § 5 odst. 3 zákona č. 153/1994 Sb.

K § 16b:

S odkazem na znění § 16a odst. 2 písm. b) návrhu zákona, v němž je jako jeden ze zdrojů informací sloužících Vojenskému zpravodajství pro plnění povinností při zajišťování obrany v kybernetickém prostoru stanoveno také monitorování kybernetického prostoru, je ustanovením § 16b odst. 1 Vojenskému zpravodajství svěřováno oprávnění nepřetržitě monitorovat kybernetický prostor, když v odstavci 2 je současně jednoznačně stanoveno, co se tímto monitorováním rozumí a jaký je jeho konkrétní účel pro plnění povinnosti Vojenského zpravodajství podílet se na zajišťování obrany státu v kybernetickém prostoru. Monitorování kybernetického prostoru je definováno jako nepřetržité vyhodnocování neadresných dat v kybernetickém prostoru zaručující včasné zjištění bezpečnostních hrozeb pro důležité zájmy státu, posouzení míry jejich intenzity, závažnosti jejich důsledků a způsobu jejich zastavení nebo odvrácení v kybernetickém prostoru. Tato definice umožňuje využití více kritérií při posuzování identifikovaných hrozeb, a tedy přesně vyhovuje účelu prolínání zajišťování vnitřní bezpečnosti a obrany státu v tomto prostoru, předávání zjištěných skutečností podle jejich vyhodnocení např. Národnímu úřadu pro kybernetickou a informační bezpečnost tak, aby byla zajištěna okamžitá, správná a maximálně efektivní reakce na zjištěné hrozby vzhledem k souvisejícím rizikům jejich dopadů.

V zájmu zachování ústavně garantovaných práv na ochranu soukromí a osobních údajů je (na základě oddělení monitoringu od výkonu zpravodajské činnosti) návrhem zákona současně výslovně upravena výluka pro zpracovávání osobních údajů nebo provádění odposlechů a záznamů podle zákona o elektronických komunikacích. Vojenskému zpravodajství je pak v souvislosti s uvedeným ukládána povinnost provádět monitorováníkybernetického prostoru výlučně způsobem, kterým zaručuje, že nebude narušována důvěrnost obsahu zprávy a zásahy do soukromého nebo rodinného života.

V odstavci 3 jsou stanoveny prostředky používané k provádění monitorování kybernetického prostoru, tedy v zásadě oprávnění Vojenského zpravodajství využívat pro tyto účely sondy umísťované na sítích elektronických komunikací.

K § 16c

 V zájmu vytvoření potřebných vazeb pro komplexní zajišťování vnitřní bezpečnosti a obrany České republiky v kybernetickém prostoru a současně s přihlédnutím k nezbytnosti zajistit potřebný, tedy účelný a pro výkon stanovených povinností efektivní „rozsah povinností a podrobnosti“ pro jejich provádění, je v § 16c návrhu zákona Vojenskému zpravodajství stanoveno, že informace (údaje), které Vojenské zpravodajství shromáždí při plnění úkolů zajišťování kybernetické obrany nebo při jiné své činnosti (tedy zpravodajské činnosti), a na základě jejich analýzy identifikuje v kybernetickém prostoru hrozbu pro „důležité zájmy státu“ ve smyslu návrhu zákona, je nutné podrobit vyhodnocení podle navržených kritérií.

Stanovená kritéria v podstatě určují hlavní roli Vojenského zpravodajství při zajišťování kybernetické obrany poté, kdy identifikují hrozbu pro důležité zájmy státu v kybernetickém prostoru; touto rolí je posoudit intenzitu ohrožení důležitých zájmů státu, časovou naléhavost provedení zastavení nebo odvrácení kybernetického útoku anebo odstranění nebo omezení důsledků vyhodnocených bezpečnostních rizik pro důležité zájmy státu v kybernetickém prostoru a aktuální schopnosti a technické možnosti ozbrojených sil České republiky nebo ozbrojených bezpečnostních sborů zastavit nebo odvrátit kybernetický útok anebo odstranit nebo omezit důsledky vyhodnocených bezpečnostních rizik pro důležité zájmy státu v kybernetickém prostoru v potřebném čase; poslední z uvedených kritérií bude vyhodnocováno na základě informací sdílených mezi Ministerstvem obrany a Ministerstvem vnitra na základě § 27 kompetenčního zákona *(„Ministerstva si navzájem vyměňují potřebné informace a podklady.“*), resp. konkrétněji na základě § 6 odst. 1 písm. a) a b) zákona č. 222/1999 Sb., o zajišťování obrany České republiky (*Ministerstvo obrany k zajišťování obrany státu „navrhuje vládě základní opatření k přípravě a organizování obrany státu; k tomu zejména zpracovává obranné koncepce a požadavky na zabezpečení obrany státu“ a „odpovídá za proces plánování obrany státu a koordinuje jeho přípravu; k tomu může vyžadovat od příslušných ministerstev, jiných správních úřadů a územních samosprávných celků podkladové materiály“).*

Dalším kritériem, jehož vyhodnocení musí být identifikovaná hrozba podrobena, je stanovení účelného a účinného řešení identifikované bezpečnostní hrozby a zastavení nebo odvrácení kybernetického útoku; toto kritérium je mimořádně důležité, neboť identifikovanou hrozbu podrobuje testu jejího nejúčelnějšího řešení z hlediska veškerých souvislostí, tedy času, intenzity, důsledků, možností provedených aktivit, doby působení a její povahy z hlediska ohrožení zájmů vnitřní bezpečnosti státu nebo jeho obrany. Tento kontext prolíná zajišťováním obrany státu v kybernetickém prostoru, neboť každá hrozba musí být vyhodnocována z hlediska zajišťování vnitřní bezpečnosti a obrany České republiky jako celku aktivně podporovanému všemi státními subjekty, jimž byly svěřeny úkoly v této oblasti. Dané kritérium tedy obecně nastoluje zásadu „brání ten, kdo je v dané chvíli a pro danou hrozbu nejlépe připraven a vybaven, ale síly mohou být i spojeny, a to dokonce i pro různé časové fáze odstranění a vyhodnocení důsledků identifikované hrozby“.

Posledním stanoveným kritériem, jímž je identifikovaná hrozba posuzována, je stanovení míry tolerance vůči bezpečnostním rizikům vyvolaným kybernetickým útokem vzhledem k jeho předpokládaným důsledkům vůči důležitým zájmům státu a nezbytnosti zajistit podmínky pro plnění jiných povinností České republiky. Toto kritérium vychází z praktických zásad řízení rizik, když v některých případech je pro dosažení sledovaného účelu vhodné ponechat působení hrozby až do míry akceptovatelného rizika (tedy akceptovatelných důsledků pro důležité zájmy státu), což například umožní shromáždit kvalitnější soubor informací o zdroji hrozby nebo soustředit síly proti hrozbě působící tak, že odvrátí hrozbu společně s likvidací jejího zdroje.

Vyhodnocení identifikované hrozby podle stanovených kritérií je pro Vojenské zpravodajství spojeno s jemu stanovenou povinností (a odpovědností) rozhodnout, který ze subjektů zřízených za účelem zajišťování vnitřní bezpečnosti a obrany České republiky bude „nejlepší“ k provedení zásahu proti identifikované hrozbě; na základě svého rozhodnutí pak Vojenské zpravodajství samo aktivně proti hrozbě zasáhne, nebo řešení situace předá určenému, nejvýhodnějšímu subjektu, a to s přihlédnutím k jeho působnosti.

Postup Vojenského zpravodajství při identifikování, vyhodnocování a zvládání hrozeb v kybernetickém prostoru je pak zarámován evidenčními a informačními povinnostmi Vojenského zpravodajství, které jsou zárukou jednak zpětného hodnocení všech skutečností souvisejících s identifikovanou hrozbou a jejím odstraněním, popřípadě zmírněním jejích důsledků, jednak posilováním vnitřní bezpečnosti a obrany České republiky sdílením informací o identifikovaných hrozbách tak, aby bylo možné reagovat i na s nimi související jevy nebo nastavovat společné postupy, popřípadě rozvíjet využívané technologie.

Pro tyto plnění informační povinnosti Vojenským zpravodajstvím je návrhem zákona stanovována jediná výjimka, vycházející z respektování primárního účelu zřízení Vojenského zpravodajství jako jednotné ozbrojené zpravodajské služby České republiky; povinnost poskytnout informace o vyhodnocení a řešení identifikované hrozby v kybernetickém prostoru nemusí být realizována, pokud by poskytnutí informací ohrozilo důležitý zájem sledovaný Vojenským zpravodajstvím.

K § 16d

Navrhovaným ustanovením § 16d je plnění úkolů Vojenského zpravodajství při zajišťování kybernetické obrany začleňováno do obrany státu jako celku, tedy vnímání kybernetické obrany jako součásti souhrnu opatření k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením. Proto také kybernetická obrana musí být plánována v rámci celého souboru opatření, který je označován jako plánování obrany státu (§ 2 odst. 8 zákona č. 222/1999 Sb.) a Vojenské zpravodajství se při jejím zajišťování musí důsledně podřizovat příslušnými plány nastaveným parametrům, zásadám a vazbám s ozbrojenými silami.

Navrhovaným ustanovením je současně vláda České republiky zmocňována k vydání nařízení, jímž bude stanovena strukturu předávaných informací podle § 16c odst. 2 písm. b) návrhu zákona, a to v zájmu zajištění jednotného a předvídatelného postupu a zejména v zájmu zajištění jednotné informační úrovně (hodnoty) předávaných skutečností.

K § 16e:

Návrhem zákona je v souvislosti s plněním úkolů při zajišťování obrany v kybernetickém prostoru ukládána Vojenskému zpravodajství povinnost vést o každém provedeném zásahu nebo jiném opatření vážícím se k řešení identifikované hrozby v kybernetickém prostoru záznam, a to v přesně stanovené struktuře, tedy opět se stejnou informační hodnotou každého záznamu. Vedení těchto záznamů má velký význam pro vyhodnocování správnosti a účinnosti zvolených postupů, účelné plánování obrany v této oblasti, ale také pro zajišťování potřebného technického a personálního vybavení Vojenského zpravodajství pro plnění jemu svěřených úkolů.

Zpracované záznamy je Vojenské zpravodajství povinno vést 10 let od data jejich zpracování, a to v zájmu možnosti zpětného vyhodnocování prováděných činností nebo jejich porovnání s obdobnými aktivními zásahy v kybernetickém prostoru.

K § 16f:

Navrhovaným ustanovením § 16f odst. 1 je Vojenskému zpravodajství v souvislosti s plněním povinností při zajišťování obrany v kybernetickém prostoru ukládána obecná součinnostní povinnost, a to v zájmu naplnění obecné povinnosti státu zajistit obranu státu ve všech jejích úrovních jako celek; pokud si stát k obraně státu zřizuje ozbrojené síly, ale současně je mu umožněno využít povinnosti státních orgánů, orgánů územních samosprávných celků a právnických nebo fyzických osob podílet se na zajišťování vnitřní bezpečnosti a obrany České republiky, je zřejmé, že všechny povinné osoby musí postupovat koordinovaně, s jednotně řízeným cílem a pravidly. Proto tam, kde jsou Vojenskému zpravodajství nad rámec jeho obvyklé působnosti svěřovány zvláštní úkoly při obraně České republiky, musí být zajištěna jejich koordinace (součinnost) s dalšími subjekty podílejícími se na zajišťování obrany České republiky, tedy s dalšími státními orgány, ozbrojenými silami České republiky, ozbrojenými bezpečnostními sbory, právnickými a fyzickými osobami a s orgány jiných států, a to zejména pokud působí v oblasti zajišťování kybernetické bezpečnosti a obrany České republiky.

Podmínky součinnosti tak, jak jsou upraveny pro účely části čtvrté zákona o Vojenském zpravodajství, je však nutné vnímat skutečně v rámci plnění úkolů svěřených Vojenskému zpravodajství v oblasti jeho podílu na zajišťování obrany státu v rámci kybernetické obrany. V žádném případě pak v rámci této součinnosti není možné poskytovat nebo vyžadovat spolupráci v oblasti trestního řízení apod.

K § 16g:

Navrhovaným ustanovením § 16g je upraveno právo Vojenského zpravodajství požadovat od právnické nebo fyzické osoby zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací zřízení rozhraní pro připojení technických prostředků kybernetické obrany a podmínky jeho výkonu. 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 § 16g upravuje obdobné oprávnění k součinnosti pro účely kybernetické obrany.

Uvedené povinnosti budou právnickým nebo fyzickým osobám zajišťujícím sítě elektronických komunikací nebo poskytujícím službu elektronických komunikací ukládány rozhodnutím vydávaným Ministerstvem obrany; forma rozhodnutí, jimž je pro ten který konkrétní případ rozhodováno o nezbytnosti umístit sondu, je nejvhodnějším řešením, neboť umožňuje zohlednit individuální podmínky jak na straně provozovatele sítě elektronických komunikací, tak potřeb Vojenského zpravodajství na umístění a užívání sondy pro monitorování. Související finanční nároky provozovatele sítí elektronických komunikací pak budou řešeny na základě jednotné úpravy provedené vyhláškou Ministerstva obrany. Odvolání proti rozhodnutí, jímž se provozovateli sítí elektronických komunikací ukládá povinnost zřídit na těchto sítích rozhraní pro umístění sondy, nebude mít odkladný účinek. Rozhodnutí nebude možné vydat bez předběžného stanoviska Vojenského zpravodajství, ve kterém toto bude povinné posoudit, zda připojení sond samo o sobě není bezpečnostním rizikem, popřípadě zda je možné důsledky takového bezpečnostního rizika přijmout jako akceptovatelné vzhledem k účelu připojení konkrétní sondy.

Ustanovení § 16g je klíčovým ustanovením návrhu zákona pro zajištění ochrany soukromí fyzických osob a ochrany jejich osobních údajů tak, jak je podrobněji popsáno v kapitole VIII. Obecné části důvodové zprávy, a to s přihlédnutím k nezbytnosti poměřování síly ochrany zájmu (práva) vzhledem k aktuální situaci, ze které vyplývá převažující hodnota pro ochranu „vyššího“ zájmu státu. Jak je již uvedeno výše, účelem získávání a shromažďování osobních údajů zpravodajskými službami je ochrana ústavního zřízení, významných ekonomických zájmů, bezpečnosti a obrany České republiky. Vedle sebe tak stojí dva obdobně silné zájmy státu a jeho obyvatel, pro něž za standardních (tedy předvídatelného a legálního chování všech účastníků) podmínek není problémem, aby nerušeně působily vedle sebe, aniž by se vzájemně ovlivňovaly. V případě, že je tento rovnovážný stav narušen, je však vždy nutné pro každý individuální případ takového narušení provést test proporcionality a určit, který z daných principů je v daném okamžiku hoden větší ochrany, resp. kdy zabránění důsledkům narušení jednoho principu je tak důležité pro zachování funkcí státu, že je možné po omezený čas v omezené míře zasáhnout do principu druhého. V zájmu zabránění svévole při uplatňování veřejného zájmu je proto návrhem zákona stanoveno, že při plnění úkolů při zajišťování kybernetické obrany zasahuje Vojenské zpravodajství do základních práv a svobod jen v rozsahu přiměřeném nezbytnosti zajištění důležitých zájmů státu a po dobu nezbytně nutnou, a to jen v případě, kdy k zajištění bezpečnosti České republiky v kybernetickém prostoru nepostačují prostředky ozbrojených sil České republiky nebo ozbrojených bezpečnostních sborů, popřípadě kdy intenzita kybernetického útoku nesnese pro jeho zastavení nebo odvrácení časového odkladu.

Obdobné limity jsou pak ještě doplňkově nastaveny pro monitorování kybernetického prostoru, a to jednak ve vztahu k dodržení pravidel pro zachování neutrality a integrity sítí elektronických komunikací a veřejných komunikačních sítí, jednak ve vztahu ke znemožnění zásahů do plnění povinností právnických nebo podnikajících fyzických osob zajišťujících sítě elektronických komunikací nebo poskytující službu elektronických komunikací vůči uživatelům sítě. V této souvislosti se předpokládá, že v rámci vydávání rozhodnutí, jímž bude ukládána povinnost pro vytvoření rozhraní v síti elektronických komunikací, budou individuálně posouzeny podmínky pro umístění sondy, a to tak, aby byly chráněny zájmy Vojenského zpravodajství při monitorování kybernetického prostoru, ale současně ve stejné váze zájmy provozovatele těchto sítí. Pro zachování neutrality provozu sítí elektronických komunikací se předpokládá také nezávislé testování jak samotných sond, tak podmínek jejich umísťování.

 K § 16h:

Dosavadní znění zákona o Vojenském zpravodajství stanoví pravidla pro nakládání s daty (údaji), které Vojenské zpravodajství shromáždilo, uchovává a vyhodnocuje při své standardní zpravodajské činnosti (§ 17 a 18 zákona o Vojenském zpravodajství). Nově je však nutné stanovit také pravidla pro zpracovávání dat získaných monitorováním kybernetického prostoru s tím, že je třeba mít na paměti, že zákon - avšak výlučně pro oblast zajišťování kybernetické obrany – umožňuje obě formy získaných dat (informací) sdružovat.

Navrhované ustanovení proto nastavuje pravidla pro nakládání s daty, které Vojenské zpravodajství shromáždilo při zajišťování kybernetické obrany České republiky v rámci monitorování kybernetického prostoru, tedy jak neadresných dat monitoringu, tak dat o provozu sítě. Vojenskému zpravodajství jsou ustanovením ukládány povinnosti data zabezpečit před vyzrazením, poškozením, zničením, odcizením nebo jiným způsobem jejich zneužití a současně data uchovávat výlučně po dobu trvání účelu jejich shromáždění, tedy výlučně po dobu, kdy lze jejich informační hodnotu využít pro účely zajištění kybernetické obrany v daném čase (tedy v rámci úkonů podle § 16c až 16e). Po uplynutí doby trvání účelu shromáždění předmětných dat je Vojenské zpravodajství data věrohodným způsobem zlikvidovat. Data získaná standardní zpravodajskou činností využitá pro úkoly zajišťování kybernetické obrany si ponechávají režim své dosavadní úpravy stanovený v § 17 zákona o Vojenském zpravodajství.

Povinnost likvidování dat také neznamená, že by Vojenské zpravodajství muselo likvidovat např. analýzy vytvořené na základě získaných dat či monitoringu provozu.

K § 16i:

Podle § 4 zákona č. 222/1999 Sb. „za přípravu a zajišťování obrany státu odpovídá vláda“, která také vyhodnocuje rizika ohrožení státu, která mohou být příčinou ozbrojeného konfliktu, a činí nezbytná opatření ke snížení, popřípadě vyloučení těchto rizik, a  vyhodnocuje úroveň připravenosti státu k zajišťování jeho obrany a v souvislosti s tím předkládá prezidentu republiky a komorám Parlamentu zprávu o zjištěných skutečnostech a navržených opatřeních k posílení obranyschopnosti státu. Je tedy zřejmé, že pokud jsou státnímu orgánu svěřovány úkoly při zajišťování obrany České republiky mimo obecnou koncepci jejich zajišťování ozbrojenými silami, je nezbytné, aby vláda České republiky měla možnost plnit své úkoly a nést odpovědnost za přípravu a zajišťování obrany státu také v oblasti výkonu svěřených úkolů. Návrhem zákona je proto Vojenskému zpravodajství ukládána povinnost informovat vládu České republiky prostřednictvím ministra obrany o plnění svěřených úkolů, a to včetně provedení analýzy účinnosti aktivních zásahů, předání zjištěných skutečností dalším subjektům nebo spolupráci při odstraňování zjištěných hrozeb v kybernetickém prostoru s Ministerstvem vnitra, popřípadě Národním úřadem pro kybernetickou a informační bezpečnost.

Stejně jako první z uvedených povinností, také povinnost nově ukládaná Vojenskému zpravodajství v § 16i odst. 2 navazuje na ustanovení jiného zákona, konkrétně na § 16 odst. 2 písm. e) kompetenčního zákona, jímž je stanoveno, že Ministerstvo obrany řídí Vojenské zpravodajství. Proto je Vojenskému zpravodajství ukládána informační povinnost rovněž vůči ministru obrany, a to jednak v rámci jeho řídící pravomoci vůči Vojenskému zpravodajství jako celku, jednak v rámci zajištění podmínek pro plnění úkolů Ministerstva obrany stanovených v § 6 odst. 1 zákona č. 222/1999 Sb., z nichž lze v souvislosti s plněním povinností Vojenského zpravodajství při zajišťování kybernetické obrany zdůraznit především odpovědnost Ministerstva obrany za proces plánování obrany státu a koordinaci jeho přípravy [§ 6 odst. 1 písm. b) zákona č. 222/1999 Sb.] (k tomu viz § 16d odst. 1 návrhu zákona). Ministr obrany je oprávněn vyžádat kdykoliv jakékoliv informace o zajišťování kybernetické obrany Vojenským zpravodajstvím, pokud jsou nezbytné pro plnění povinností Ministerstva obrany podle § 6 odst. 1 zákona č. 222/1999 Sb., a tedy provázaně k již uvedenému také k nastavení koordinačních vazeb mezi činnostmi Vojenského zpravodajství při zajišťování kybernetické obrany k zajišťování obrany jako celku (a to i pro další činnosti ozbrojených sil České republiky v kybernetickém prostoru).

K § 16j:

Pro činnosti Vojenského zpravodajství vykonávané podle nově vkládané části čtvrté zákona o Vojenském zpravodajství nelze využít nastavení kontrolních mechanismů pro zpravodajskou činnost prováděnou Vojenským zpravodajstvím. Proto je návrhem zákona stanovována kontrola Vojenského zpravodajství pro činnosti představující jeho účast na zajišťování obrany České republiky, a to  s přihlédnutím k povaze prováděných činností a jejich významu pro zajišťování funkcí státu, v několika úrovních. Základní kontrola je svěřena vládě České republiky (která odpovídá za přípravu zajišťování obrany státu), v další úrovni pak Poslanecké sněmovně a také Orgánu nezávislé kontroly zpravodajských služeb České republiky.

Návrhem zákona je stanoven rozsah dokumentů, které je Vojenské zpravodajství povinno v zájmu účelného provedení kontroly předložit, přičemž je současně umožněno, aby si kontrolující vyžádal zpracování dalších souvisejících, avšak účelem kontroly odůvodněných zpráv, nebo poskytnutí dalších informací. Poskytnutí těchto „podkladů ke kontrole“ je navrhováno omezit o sdělování informací nebo zpřístupňování dokumentů, které se týkají dosud neukončených situací zajišťování kybernetické obrany, a to v zájmu jejich nerušeného provedení (dokončení).

Ministru obrany je pak vzhledem ke skutečnostem uvedeným v odůvodnění k § 16i svěřena pravomoc prověřovat stav přípravy a zajišťování obrany státu v kybernetickém prostoru, na němž se podílí Vojenské zpravodajství.

Navrhovaným ustanovením je pak z provádění kontroly Vojenského zpravodajství při provádění činností v zájmu zajišťování kybernetické obrany vyloučen kontrolní řád, neboť vzhledem k povaze prováděných činností, jejich struktuře a času, ve kterém jsou v jednotlivých segmentech vykonávány, je jeho užití nevhodné.

K § 16k:

 Z povahy činností naplňujících povinnosti při zajišťování kybernetické obrany, například pak také z kritérií pro vyhodnocování identifikovaných hrozeb a rizik v kybernetickém prostoru je zřejmé, že při odvracení nebo zastavení kybernetického útoku nebo odstranění kybernetického rizika nelze vyloučit případy, kdy je nutné přijmout v zájmu ochrany důležitých zájmů státu jako převažující hodnoty skutečnost, že v ojedinělých situacích může vzniknout fyzickým nebo právnickým osobám škoda; návrh zákona pro tyto případy nestanoví žádné specifické postupy, ale odkazuje se na obecnou úpravu náhrady škody.

**K bodu 3**

Na základě názoru výborů Poslanecké sněmovny vzneseného při posuzování neprojednaného návrhu zákona v roce 2017 je doplněna úprava vnitřního kontrolního orgánu Vojenského zpravodajství a jeho vztahu k ministru obrany.

**K části druhé – změna zákona o zpravodajských službách**

**K čl. 2**

**K bodu 1**

 Ustanovením § 2 zákona č. 153/1994 Sb. je v současné době stanovena působnost zpravodajských služeb České republiky, která je pak následně v § 5 odst. 1 až 3 pro jednotlivé zpravodajské služby upřesňována podle účelu jejich zřízení; v § 5 odst. 4 zákona č. 153/1994 Sb. je pak upravena možnost rozšířit spektrum úkolů plněných zpravodajskými službami nad rámec stanovený v citovaných odstavcích 1 až 3, a to za předpokladu, že tak stanoví „zvláštní zákon nebo mezinárodní smlouva, jíž je Česká republika vázána“. Toto ustanovení však umožňuje rozšířit spektrum úkolů zpravodajských služeb výlučně v mantinelech jejich působnosti tak, jak je stanovena v § 2 zákona č. 153/1994 Sb., tedy v mezích činností charakterizovaných účelem „získávání, shromažďování a vyhodnocování informací důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnost a obranu České republiky“.

V zájmu vytvoření právních podmínek pro realizaci úkolů uložených usnesením vlády České republiky ze dne 25. května 2016 č. 382, kterým schválila Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 a současně uložila Ministerstvu obrany úkol předložit návrh normativního řešení vytvoření podmínek kybernetické obrany České republiky, je pak nutné uvedenou působnost zpravodajských služeb pro Vojenské zpravodajství doplnit o činnosti náležející obecně do působnosti ozbrojených sil České republiky, a to v rozsahu možnosti podílet se na zajišťování obrany České republiky, konkrétně pak se specifickým zaměřením na kybernetickou obranu. Díky navrhované úpravě pak bude možné využít čl. 3 odst. 2 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, a vytvořit právní základ pro využití Vojenského zpravodajství v oblasti jeho podílu na zajišťování obrany České republiky v kybernetickém prostoru. Citovaným ustanovením je totiž stanoveno, že „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.“, přičemž z této citace je zřejmé, že uvedená povinnost je opět vázána k působnosti příslušného státního orgánu (blíže viz I. kapitola obecné části odůvodnění k návrhu zákona).

Navrhovaná úprava tedy rozšiřuje účel zřízení Vojenského zpravodajství vedle výkonu zpravodajské činnosti také o provádění úkolů, jimiž je zajištována obrana státu v kybernetickém prostoru.

**K bodu 2**

 V souvislosti s úpravou provedenou v bodě 1 (§ 2 zákona č. 153/1994 Sb.) je dále doplňována specifická působnost Vojenského zpravodajství o činnosti související s monitorováním sítí a služeb elektronických komunikací za účelem identifikace hrozeb a rizik v kybernetickém prostoru a jejich řešením.

**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 Český telekomunikační úřad zmocněn k tomu, aby všeobecným oprávněním stanovil konkrétní podmínky týkající se 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 § 98a:**

K odstavci 1:

Nově vkládaný § 98a odst. 1 je provázán k rovněž nově navrhovanému znění § 16g  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 § 16g zákona o Vojenském zpravodajství zřídit a zabezpečit v určených bodech své sítě na základě rozhodnutí Ministerstva obrany rozhraní pro připojení sondy určené pro provádění monitorování kybernetického prostoru za účelem identifikování bezpečnostních hrozeb. 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:

Právnickým nebo podnikajícím fyzickým osobám, které zajišťují síť elektronických komunikací nebo poskytují službu elektronických komunikací, jsou v případech, kdy jim byla uložena povinnost zřídit rozhraní pro umístění sondy monitorující kybernetický prostor, povinny respektovat jim stanovené povinnosti nezbytně související s provozováním sondy a zajišťováním její bezpečnosti. Vzhledem k tomu, že se jedná o povinnosti obecně se vážící ke každé umísťované sondě, bylo by neúčelné je začleňovat do každého jednotlivého rozhodnutí o zřízení rozhraní pro umísťování sondy, ale je správné tyto povinnost stanovit přímo zákonem.

V zájmu nerušených podmínek monitorování kybernetického prostoru a jejich bezpečného provozování jsou právnickým nebo podnikajícím fyzickým osobám, které zajišťují síť elektronických komunikací nebo poskytují službu elektronických komunikací, ukládány povinnosti nezasahovat do umístěných sond nebo omezovat jejich funkčnost tak, aby byly vyloučeny situace, kdy není identifikována hrozba v kybernetickém prostoru vinou takového zásahu, když současně Vojenské zpravodajství předpokládá jeho nerušené monitorování. Vojenskému zpravodajství musí být také za stejným účelem umožněn přístup k sondě; tato povinnost je však limitována ochranou zájmů právnické nebo podnikající fyzické osoby, která zajišťuje síť elektronických komunikací nebo poskytuje službu elektronických komunikací, tedy současně ukládanou povinností Vojenskému zpravodajství nenarušovat činnost těchto provozovatelů sítí elektronických komunikací.

K odstavci 3:

V navrhovaném znění § 98a odst. 3 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 sond pro monitorování kybernetického prostoru, a to k tíži Vojenského zpravodajství (k tomu viz odůvodnění k § 16b části první návrhu zákona). Součástí tohoto ustanovení je zmocnění k vydání prováděcího předpisu – vyhlášky Ministerstva obrany, který následně stanoví výši a způsob určení úhrady za takto vynaložené náklady.

K odstavci 4:

Navrhovaná úprava § 98a odst. 4 stanoví povinnost mlčenlivosti právnických nebo podnikajících 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 skutečností. 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**

 V souvislosti s umísťováním sond na rozhraní sítí elektronických komunikací je Českému telekomunikačnímu úřadu rozšiřována působnost, a to v oblasti ověřování technických a provozních podmínek sond pro monitorování kybernetického prostoru, a to v zájmu zachování integrity a neutrality sítí.

 Český telekomunikační úřad již v současné době vykonává kontrolu elektronických komunikací, vyhledává a odstraňuje zdroje rušení, přičemž umístění předmětných sond je případně možným rizikem pro provozování sítí a jejich uživatele. Je proto nezbytné, aby veškeré parametry stanovené pro provozování sond byly nezávislým subjektem prověřovány tak, aby monitorování kybernetického prostoru nebylo současně přínosem pro provozování a užívání sítí elektronických komunikací z hlediska bezpečnosti státu a současně hrozbou pro uživatele i provozovatele sítí z hlediska jejich práv, neutrality sítí apod.

**K bodu 4**

Navrhovaná úprava doplňuje do zákona o elektronických komunikacích nové skutkové podstaty přestupku spočívající v nezřízení rozhraní pro umístěny sondy, neumožnění přístupu k ní, zasahování do sondy nebo její funkčnosti a v porušení mlčenlivosti.

O sankcích za tyto přestupky bude rozhodovat Český telekomunikační úřad, který je garantem nezávislého posouzení naplnění uvedených skutkových podstat a míry nebezpečnosti naplněné jejich naplněním.

**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. Jelikož zákon samotný neukládá žádné povinnosti, které by bylo nutné plnit okamžitě po nabytí účinnosti zákona, není nutné stanovit delší legisvakanční lhůtu. Naopak žádoucí je tato lhůta co nejkratší, aby Vojenské zpravodajství mohlo co nejdříve začít činit kroky směrem k započetí faktického výkonu obrany státu v kybernetickém prostoru.

1. § 8 a § 15 zákona č. 289/2005 Sb., o Vojenském zpravodajství. [↑](#footnote-ref-1)
2. § 9 odst. 5 zákona č. 289/2005 Sb., o Vojenském zpravodajství. [↑](#footnote-ref-2)
3. 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 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.“ [↑](#footnote-ref-3)
4. Dostupný on-line na adrese: <http://eur-lex.europa.eu/legal-content/CS/TXT/uri>=

 CELEX%A52013PC0048 [↑](#footnote-ref-4)