Vyhodnocení našich připomínek

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

Legenda semafor

	Nezohledněno
	Nejasné/Sporné/Částečně
	Zohledněno

Naše původní připomínka	Naše původní znění	Nový návrh MO	Komentář
Monitoring kybernetického prostoru			
Monitorování kybernetického prostoru bylo dle původního návrhu změny zákona definováno jako nepřetržité vyhodnocování neadresných dat v kybernetickém prostoru, přičemž chyběla jasná definice termínu neadresná data. Gramatickým výkladem termínu neadresná data by bylo možné dojít k chybné interpretaci, že je tímto termínem myšlen samotný obsah zpráv oproštěn o "adresná data", jako jsou identifikační údaje odesílatelů a příjemců zprávy. V takovém případě by zákon přiznával Vojenskému zpravodajství pravomoc monitorovat a vyhodnocovat samotný obsah zpráv.	**§ 16b odst. 2) a odst. 3)** (2) Monitorováním kybernetického prostoru se rozumí nepřetržité vyhodnocování **metadat** zpráv v kybernetickém prostoru za účelem včasného zjištění bezpečnostních hrozeb pro důležité zájmy státu, posouzení míry jejich intenzity, závažnosti jejich důsledků a možností jejich zastavení nebo odvrácení. Součástí monitorování kybernetického prostoru není zpracovávání osobních údajů nebo provádění odposlechů a záznamů podle zákona o elektronických komunikacích[21)]. **(3) Metadaty zprávy se rozumí takové údaje o zprávě, které jsou nezbytné**	**§ 16c** (2) Nástroj detekce v rozsahu určeném indikátory útoků a hrozeb podle § 16a odst. 2 zaznamenává metadata o a) provozu veřejných komunikačních sítí a veřejně dostupných služeb elektronických komunikací, b) provozu nástroje detekce a c) manipulaci s konfigurací nástroje detekce pro potřeby auditu Vojenským zpravodajstvím vykonávaných činností. (3) Metadaty podle odstavce 2 se rozumí data popisující bez zaznamenávání samotného obsahu dat a informací souvislosti jejich přenosu v čase a jejich	Přestali používat termín "neadresná data" a používají námi navrhovaný termín "metadata". To je obecně pozitivní. Požadovali jsme zde pozitivní i negativní definici toho, co jsou metadata. U tohoto bodu jsme sami nedokázali dostatečně dobře definovat metadata a sami jsme to považovali za otevřené. Jejich pozitivní definice v odstavci 3) je podle mě lepší, ale současně negativní definice trochu pokulhává. Podle mě tento bod a definici metadat by měl zkontrolovat někdo, víc technický a méně právní člověk. Takže zde to je z mého pohledu nejasné. Ani naše a ani

Monitorování a vyhodnocování samotného obsahu zpráv osob považujeme za nepřípustný zásah do soukromí, pokud má být prováděn plošně a necíleně na veškeré zachycené datové komunikaci. Dle vyjádření pracovníků samotného Vojenského zpravodajství není pro dosažení cíle ustanovení této části zákona - zajištění kybernetické bezpečnosti a obrany České republiky - nezbytné znát obsah zpráv přenášených dat, a že termínem neadresná data byla myšlena pouze metadata informačních paketů. Z tohoto důvodu navrhujeme zaměnit termín “neadresná data” v odstavci 2 za termín, který přesněji definuje okruh monitorovaných a vyhodnocovaných dat. Navrhujeme použití termínu "metadata"/“řídící data paketů”, který v oboru informačních a komunikačních technologiích označuje metadata datových zpráv. Současně navrhujeme nový odstavec 3, kde bude tento termín vymezen negativní i pozitivní definicí. Negativní vymezení pojmu “řídící data paketů” je formulováno tím, že “neobsahují datový obsah paketů”, čímž je v informačních a komunikačních technologiích myšleno datové pole neboli *payload*, což je samotný obsah zpráv přenášený při přenosu dat. Pozitivní vymezení “metadata” je následně vymezeno jako “údaje o zprávě, které jsou nezbytné pro její přenos”. Úpravu odstavce 2 a doplnění § 16b o odstavec 3 považujeme za nezbytné z důvodu jasného vymezení	**pro její přenos. Součástí metadat není samotný obsah zprávy.**	strukturu. (4) Nástroje detekce nesmí být využito pro provádění odposlechů a záznamu nebo zpráv podle zákona o elektronických komunikacích. (5) Cílenou detekci a identifikaci a vyhodnocování jevů nasvědčujících existenci útoku nebo hrozby ohrožujících důležité zájmy státu v kybernetickém prostoru Vojenské zpravodajství provádí výlučně způsobem, který zaručuje, že a) je zachována důvěrnost komunikací fyzických a právnických osob při poskytování veřejně dostupné služby elektronických komunikací, integrita veřejných komunikačních sítí a dostupnost veřejných komunikačních sítí a služeb elektronických komunikací a b) není zasahováno nebo ovlivňováno plnění povinností právnické nebo podnikající fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací vůči uživatelům sítě jinak, než v rozsahu přiměřeném veřejnému zájmu na zajišťování obrany státu.	jejich definice v tomto ohledu není dokonalá.

monitorovaných a vyhodnocovaných dat, aby nemohlo dojít k chybné interpretaci ustanovení zákona a následně k jeho zneužití zpracováváním jiných než vymezených dat. Je nezbytné v zákoně jasně vymezit rozsah monitorovaných a vyhodnocovaných dat, protože představuje zásah do základních lidských práv, který vyžaduje jasné zákonné omezení.			
Původní návrh změny zákona uvádí v odstavci 2 § 16b, že "monitorováním kybernetického prostoru nesmí být narušena důvěrnost obsahu zprávy a může být prováděno výlučně způsobem vylučujícím zásahy do soukromého života." Taková formulace jde proti samotnému významu pravomocí udělených Vojenskému zpravodajství tímto paragrafem, proto vyžaduje přeformulovat tak, aby odpovídala záměru navrhovaného zákona. Důvěrnost obsahu zprávy a zásah do soukromého života jsou dotčeny ze samotné podstaty monitoringu a vyhodnocování řídících dat paketů v kybernetickém prostoru. Se zásahem do soukromé sféry občanů v důsledku monitoringu kybernetického prostoru navíc počítá v tomto smyslu také samotná důvodová zpráva k návrhu změny zákona, kde se zvažuje proporcionalita mezi ochranou národní bezpečnosti a základními lidskými právy a svobodami, chráněnými ustanoveními čl. 7 a čl. 10 odst. 2 a 3 Listiny základních práv a svobod, čl. 8 Evropské úmluvy o ochraně lidských práv a	**§ 16b odst. 4)** **(4) Zásahy do soukromí osoby při monitorování kybernetického prostoru jsou přípustné pouze tehdy, pokud jsou nezbytné k dosažení cíle uvedeného v odstavci 2, tohoto cíle nelze efektivně dosáhnout jinak a zásah do soukromí je přiměřený bezpečnostní hrozbě, který má být odvrácena.**	**§ 16f** **Omezení základních lidských práv a svobod** Vyžaduje-li to veřejný zájem na zajišťování obrany státu, lze na základě vyhodnocení jevů nasvědčujících o existenci útoku nebo hrozby ohrožující důležité zájmy státu v kybernetickém prostoru a v souvislosti s opatřeními přijatými k odstranění útoku nebo hrozby nebo omezení jejich důsledků připustit v nezbytně nutném rozsahu také zásahy do základních práv a svobod fyzických osob, je-li to nezbytné ke splnění povinností Vojenského zpravodajství při provádění činností, jimiž se podílí na zajišťování obrany státu a nelze-li splnění těchto povinností dosáhnout jiným způsobem, a to v rozsahu přiměřeném síle útoku nebo hrozby, které mají být odvráceny nebo jejichž důsledky mají být omezeny, a po dobu nezbytně nutnou.	V tomto bodu nám vyšli vstříc. Požadovali jsme zakotvení minimalizace zásahu do práv uživatelů komunikačních sítí při sbírání dat Vojenským zpravodajstvím, ale navíc zakotvili samotný paragraf, který vztahuje tuto záruku na celém zajišťování obrany státu v kybernetickém prostoru. To znamená na všechny jejich činnosti včetně aktivních zásahů. Ovšem nutno podotknout, že se nejedná v podstatě o žádný ústupek, protože to by vyplývalo už ze samotné Ústavy ČR. Je to v podstatě trochu jinak formulovaný test proporcionality. Má to v zákoně jenom deklaratorní význam.

základních svobod. Dle navrhované právní úpravy je vystaven zásahu do svých práv prakticky každý uživatel telekomunikačních sítí. Skutečnost, že se v případě nakládání s metadaty v elektronické komunikaci jedná o zásah do soukromí dle článku 10 (práva na ochranu před neoprávněným zasahováním do soukromého a rodinného života a před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě) a článku 13 Listiny základních práv a svobod (právo na zachování tajemství zpráv podávaných telefonem či jiným podobným zařízením), předpokládá také Ústavní soud České republiky v nedávném nálezu Pl. ÚS 45/17 ze dne 22. května 2019. V tomto řízení Ústavní soud zkoumal střet zmíněných práv mimo jiné také z důvodu ochrany národní bezpečnosti. Soud zkoumal omezení těchto základních lidských práv z důvodu preventivního uchovávání provozních a lokalizačních údajů o elektronické komunikaci u poskytovatelů telekomunikačních služeb, což jsou data svým charakterem podobná těm, která mají být předmětem monitoringu a vyhodnocování Vojenským zpravodajstvím. Navrhujeme, aby znění zákona tento zásah do práv a svobod na deklaratorní úrovni připustilo do nového odstavce 4 § 16b, ale současně aby deklarovalo, že jiným než uvedeným způsobem nebudou základní práva a svobody narušeny, a že k tomu bude docházet jen v nezbytné			

míře v demokratické společnosti, což vyplývá již ze samotného výkladu Listiny a Úmluvy.			
Zásah v kybernetickém prostoru			
Návrh ministerstva je neurčitý a nejasný. Především **chybí upřesnit, jak je definován "aktivní zásah"**. Stejně tak **v celém právním řádě dosud chybí definice pojmu "kybernetický útok"**. Přitom se jedná o dosti zásadní pojmy, na jejichž základě bude možné použít mimořádně silné mocenské nástroje státu, de facto nasazení armády v kyberprostoru. Oprávnění "aktivně zasáhnout" nemůže zůstat s takto nedostatečnou zákonnou definicí. **Požadujeme podrobného přepracování daného ustanovení, aby aktivní zásah měl jasné mantinely a pravidla.** Navrhujeme znění v podobě, že na základě provedeného vyhodnocení rozhodne Vojenské zpravodajství, zda zasáhne v kyberprostoru na území České republiky za účelem zastavení nebo odvrácení kybernetického útoku, případně za účelem odstranění bezpečnostní hrozby. **Prostorové vymezení zásahu na kyberprostor na území České republiky** zajistí, že se nebude v případě zásahu moci jednat o válečnou operaci v kyberprostoru na území cizího státu. Pojem "aktivně zasáhne" lze gramaticky zredukovat na **pouhé "zasáhne",** přičemž pravomoc orgánu provést operaci zůstane nezměněná a sníží to možnosti interpretace rozsáhlejších pravomocí.	**§ 16c odst. 2)** (2) Na základě provedeného vyhodnocení podle odstavce 1 rozhodne Vojenské zpravodajství, zda a) zasáhne **v kybernetickém prostoru na území České republiky** za účelem zastavení nebo odvrácení kybernetického útoku, případně za účelem odstranění bezpečnostní hrozby, nebo b) předá zjištěné informace k provedení dalších opatření k zajištění bezpečnosti České republiky podle jejich povahy: 1. Generálnímu štábu Armády České republiky k provedení opatření k zajištění obrany České republiky ozbrojenými silami České republiky, nebo 2. Národnímu úřadu pro kybernetickou a informační bezpečnost k provedení opatření směřujících k zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru, nebo 3. Ministerstvu vnitra k provedení opatření k zajištění bezpečnosti České republiky ozbrojenými bezpečnostními sbory, a to s přihlédnutím k působnosti uvedených státních orgánů.	**§ 16e** **Oprávnění provést aktivní zásah v kybernetickém prostoru** (1) Vojenské zpravodajství v případě zjištěného útoku nebo hrozby směřující proti důležitým zájmům státu provede za podmínek stanovených tímto zákonem aktivní zásah k jejich neprodlenému odvrácení, hrozí-li nebezpečí z prodlení. (2) Vojenské zpravodajství je oprávněno provést aktivní zásah podle odstavce 1 výlučně v případě, že a) skutečnosti jím zjištěné v kybernetickém prostoru svědčí o existenci ohrožení důležitým zájmům státu ve značném rozsahu, b) útok nebo hrozba směřující proti důležitým zájmům státu trvají nebo bezprostředně hrozí a c) útok nebo hrozbu směřující proti důležitým zájmům státu nelze odvrátit v součinnosti s ozbrojenými silami České republiky a aktivní zásah byl vyhodnocen jako jediný možný účinný způsob jejich odvrácení.	Není ani v nové verzi nikde definováno, co to "aktivní zásah" znamená a jak by měl vypadat. Nevyhověli požadavkům, aby se "aktivní zásah" přejmenoval na "zásah". Slovo "zásah" už aktivitu obsahuje ze své podstaty. Tento zásah není omezen na kybernetický prostor na území ČR, tudíž nevíme zda nebude moci zahrnovat bojové akty na území cizích států.

Navrhovaná úprava dává dle § 16a odst. 1) Vojenskému zpravodajství povinnost odvrátit nebo snížit účinky při ochraně důležitých zájmů státu identifikované v kybernetickém prostoru při dvou alternativních okolnostech. Za prvé má Vojenské zpravodajství tuto povinnost, pokud je odvrácení nebo snížení účinku vzhledem k intenzitě ohrožení nezbytné provést okamžitě po jeho zjištění. Druhou alternativní možností, kdy tato povinnost Vojenskému zpravodajství vzniká je, pokud k zastavení nebo odvrácení ohrožení nedisponují ozbrojené síly nebo ozbrojené bezpečnostní sbory potřebnými silami nebo prostředky. Obě tyto vzájemně se vylučující možnosti (spojka “anebo”) jsou novou pravomocí výkonné moci provádět vojenské operace v kyberprostoru. Prakticky se jedná o situaci analogickou té, o které dnes běžně rozhoduje vláda (§ 4 a § 5 zákona č. 222/1999 Sb., o zajišťování obrany České republiky a čl. 43 odst. 4 Ústavy ČR) a nikoliv pouze ministr obrany. Není žádný důvod, proč by o opatřeních jinak prováděných ozbrojenými silami státu měl rozhodovat sám ministr obrany, pokud se jedná o ohrožení, které není natolik intenzivní, aby bylo nezbytné provést opatření okamžitě po jeho zjištění. Teoreticky by mohla být druhá alternativní povinnost Vojenského zpravodajství dle návrhového § 16a odst. 1) naplňována na základě povinnosti poskytnout součinnost nebo podporu	**§ 16c odst. 4)** (4) K provedení opatření podle odstavce 2 písm. a) je nutný souhlas **a) ministra obrany v případě, že je jeho provedení vzhledem k intenzitě kybernetického útoku nebo bezpečnostní hrozby nezbytné okamžitě po jeho zjištění, anebo** **b) vlády v případě, že k zastavení nebo odvrácení kybernetického útoku nebo bezpečnostní hrozby nedisponují ozbrojené síly nebo ozbrojené bezpečnostní sbory potřebnými silami nebo prostředky.**	**§ 16e** **Oprávnění provést aktivní zásah v kybernetickém prostoru** (1) Vojenské zpravodajství v případě zjištěného útoku nebo hrozby směřující proti důležitým zájmům státu provede za podmínek stanovených tímto zákonem aktivní zásah k jejich neprodlenému odvrácení, hrozí-li nebezpečí z prodlení. (2) Vojenské zpravodajství je oprávněno provést aktivní zásah podle odstavce 1 výlučně v případě, že a) skutečnosti jím zjištěné v kybernetickém prostoru svědčí o existenci ohrožení důležitým zájmům státu ve značném rozsahu, b) útok nebo hrozba směřující proti důležitým zájmům státu trvají nebo bezprostředně hrozí a c) útok nebo hrozbu směřující proti důležitým zájmům státu nelze odvrátit v součinnosti s ozbrojenými silami České republiky a aktivní zásah byl vyhodnocen jako jediný možný účinný způsob jejich odvrácení. (3) K provedení aktivního zásahu je Vojenské zpravodajství oprávněno pouze po předchozím souhlasu ministra obrany.	Tady jsme požadovali to, aby o "aktivním zásahu" v některých případech rozhodovala vláda a v některých, aby rozhodoval ministr. Mělo to být v závislosti na tom, zda je nutné ho provést nezbytně po jeho zjištění. Nevyhověli nám, že by udělali dvě kategorie aktivních zásahů, ale obecně píší o tom, že VZ provede aktivní zásah "hrozí-li nebezpečí z prodlení". Dále pak zmiňuje tři podmínky, které musí být splněny kumulativně, ale právě ta nezbytnost jednat okamžitě tam není. Ideální by bylo, aby právě tu podmínku nezbytnosti jednat okamžitě k jeho odvrácení dali také mezi výlučné podmínky k provedení aktivního zásahu.

vykonávaných opatření ozbrojeným silám České republiky nebo ozbrojeným bezpečnostním sborům, pokud o to v individuálních případech výlučně pro účely jimi zajišťování bezpečnosti nebo obrany České republiky v kybernetickém prostoru požádají (dle § 16f odst 4). Tím spíše by byla nutná vyšší míra kontrola těchto opatření. Navrhujeme znění odstavce 4 tak, aby **rozlišoval nutný souhlas k provedení opatření podle odstavce 2 písm. a) tak, že bude zohledněna nutnost časové nezbytnosti. V první variantě, kdy je zásah nutné provést okamžitě po jeho zjištění, by stačil pouhý souhlas ministra obrany, který by tím získal novou pravomoc. V druhé variantě, kdy ozbrojené síly nebo bezpečnostní složky disponují potřebnými silami nebo prostředky by byl potřeba souhlas vlády analogicky situacím, kdy o opatřeních při obraně České republiky rozhoduje vláda dle článku 43 odst. 4 Ústavy a § 5 zákona č. 222/1999 Sb., o zajišťování obrany České republiky.**			
Soudní ochrana provozovatelů sítě			
Navrhované ustanovení obsahuje nesprávné označení opravného prostředku proti rozhodnutí ministerstva jako “odvolání”, které je potřeba zaměnit za “rozklad”. Dle § 152 Správního řádu (zákon č. 500/2004 Sb.) lze proti rozhodnutí, které vydal ústřední správní úřad, ministr nebo vedoucí jiného ústředního správního úřadu v prvním	**§ 16g odst. 3)** (3) K zajištění účelu podle odstavce 1 vydá Ministerstvo obrany rozhodnutí, jímž právnické nebo podnikající fyzické osobě zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací uloží povinnost zabezpečit rozhraní pro připojení sond určených	**§ 16d** **Zajištění podmínek cílené detekce a identifikace** (3) K plnění povinnosti podle odstavce 1 vydá Ministerstvo obrany na základě návrhu Vojenského zpravodajství vypracovaného jako opatření k zajištění závěrů jím plněných povinností stanovených v § 16a odst. 1 a 2	Zde jsme požadovali ať: Za prvé odstraní faktickou chybu a neoznačují opravný prostředek jako "odvolání", ale správně jako "rozklad". To vyplývá ze samotného správního řádu a pokud by tam zůstala chyba, tak by to na praktickou aplikaci nemělo význam. Bylo by to jenom terminologicky blbě v zákoně. to opravili.

stupni, podat jako opravný prostředek rozklad. Navrhujeme do návrhu doplnit, aby Ministerstvo obrany při ukládání povinnosti rozhodlo také o časovém období, po které má být sonda připojena. Časově neomezené rozhodnutí by vytvořilo trvalou povinnost provozovatelů sítí strpět umístění sondy a to bez ohledu na aktuální potřebnost. Časové omezení může zajistit opětovnou kontrolu potřebnosti ze strany ministerstva.	k monitorování kybernetického prostoru a povinnost strpět umístění a provozování tohoto zařízení, **včetně časového období, po kterou má být toto zařízení umístěno.** Rozhodnutí podle věty první obsahuje výrokovou část a poučení účastníků; **rozklad** proti rozhodnutí nemá odkladný účinek.	rozhodnutí, jímž právnické nebo podnikající fyzické osobě zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací uloží povinnost zřídit a zabezpečit rozhraní pro připojení nástrojů detekce v určeném bodě veřejné komunikační sítě a povinnost strpět umístění a provozování těchto nástrojů. (4) Rozhodnutí podle odstavce 3 musí vedle náležitostí stanovených správním řádem obsahovat také a) určení doby, po kterou má být nástroj detekce v určeném bodě provozován, a b) lhůtu, ve které je právnická nebo podnikající fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinna v určených bodech jí zajišťované veřejné komunikační sítě zřídit rozhraní pro připojení nástroje detekce. (5) Doba podle odstavce 4 písm. a) nesmí být delší než 6 měsíců, Ministerstvo obrany ji však může na návrh Vojenského zpravodajství prodloužit. (6) Rozklad proti rozhodnutí nemá odkladný účinek.	Za druhé jsme chtěli, aby bylo v rozhodnutí Ministerstva obrany o umístění detekčního zařízení/sondy uvedeno také časové období na jak dlouho uvedené povolení je. Tomu vyhověli a navíc stanovili to, že uvedené povolení může být nejdéle na měsíců s tím, že může být prodlužováno. Tohle si myslím, že zásadně zvýšilo nějaké záruky provozovatelů sítě, protože Ministerstvo obrany nemůže rozhodnout o umístění sondy na neomezeně dlouhou dobu, ale musí opakovaně rozhodovat, že je to zařízení tam stále potřeba.
Spolupráce Vojenského zpravodajství s tuzemskými a zahraničními orgány			
Navrhujeme z navrhovaného ustanovení **vyjmout možnost, aby mohly ozbrojené bezpečnostní sbory (Policie ČR a případně další) po Vojenském**	**§ 16f odst. 4)** (4) Vojenské zpravodajství je při plnění úkolů podle § 16a odst. 1 povinno	**§ 16e Oprávnění provést aktivní zásah v kybernetickém prostoru** (7) Vojenské zpravodajství může	V tomto bodu jsme požadovali, že bezpečnostní sbory (mj. Policie ČR) nemůže požádat Vojenské zpravodajství o součinnost, protože není jasné, při

zpravodajství požadovat povinnost poskytnout součinnost nebo podporu jimi vykonávaných opatření. Z důvodové zprávy není zřejmé, k jakému účelu by mohla policie a případně další bezpečnostní sbory požadovat od Vojenské rozvědky povinnost součinnosti při jimi vykonávaných úkolech. Možnost spolupráce mezi bezpečnostními sbory a Vojenskou rozvědkou přitom umožňuje již odstavec 1 stejného paragrafu. Formulace v původním návrhu § 16f odst. 4 neobsahuje záruky, že informace získané v rámci monitoringu provozu (§ 16b) nebudou moci být díky tomuto ustanovení použity pro účely trestního řízení jako operativní poznatky. Původní návrh bez vysvětlení případů, při kterých může policie nebo jiné bezpečnostní sbory úkolovat Vojenskou rozvědku, považujeme z uvedených důvodů za problematický. Případně požadujeme doplnění možných případů, při kterých by bezpečnostní sbory požadovali povinnost součinnosti při plnění jejich úkolů.	poskytnout součinnost nebo podporu vykonávaných opatření ozbrojeným silám České republiky, pokud o to v individuálních případech výlučně pro účely jimi zajišťování bezpečnosti nebo obrany České republiky v kybernetickém prostoru požádají; tím není dotčena povinnost Vojenského zpravodajství podle odstavce 1.	v souvislosti s jím prováděnými činnostmi a opatřeními, jimiž se podílí na zajišťování obrany státu České republiky v kybernetickém prostoru, poskytnout součinnost nebo podporu úkolů plněných Národním úřadem pro kybernetickou a informační bezpečnost nebo bezpečnostními sbory, pokud o to v individuálních případech výlučně pro účely jimi zajišťované bezpečnosti České republiky v kybernetickém prostoru požádají; tím není dotčena součinnost výkonu veškerých činností Vojenského zpravodajství prováděných podle této části zákona vůči ozbrojeným silám České republiky při zajišťování obrany státu.	jakých úkolech policie by mělo Vojenské zpravodajství tuto součinnost poskytovat. Nevyhověli nám a Vojenské zpravodajství může dělat aktivní zásahy na žádost policie. Podezřelé jsou zde dvě věci: 1) Podle jejich původního návrhu mělo Vojenské zpravodajství **povinnost!** poskytnout součinnost na žádost bezpečnostních sborů. Nový návrh zavádí diskreci ("Vojenské zpravodajství může"). Jinými slovy najednou je na libovůli Vojenského zpravodajství zda policii součinnost poskytne nebo ne. 2) Původně bylo toto ustanovení zařazeno pod neutrální paragraf 16f o obecných podmínkách činnosti VZ. Nově je toto ustanovení zařazeno pod paragraf 16e týkající se oprávnění provádět "aktivní zásah" v kyberprostoru. To znamená, že součinnost s policií pravděpodobně nebude o předávání informací, ale provádění "aktivních zásahů". Pokud má skutečně provádět VZ aktivní zásahy na požádání PČR, tak by to měli vysvětlit.
Ministerstvem navrhovaný § 16f odst. 1 připouští, že Vojenské zpravodajství při plnění úkolů na kybernetické obraně České republiky spolupracuje s orgány jiných států, přičemž neobsahuje bližší spolupráci, na základě jakých principů by měla tato spolupráce probíhat. Účelem zahraniční spolupráce nesmí být plošné	**§ 16f odst. 5)** **(5) Vojenské zpravodajství není oprávněno zpřístupnit sondy nebo plošný obsah dat získaných při monitoringu kybernetického prostoru prováděný dle § 16b spolupracujícím orgánům jiných států. V**	**§ 16b** **Spolupráce Vojenského zpravodajství při provádění činností, jimiž se podílí na zajišťování obrany státu** (3) Informace podle odstavce 2 může Vojenské zpravodajství předat také Ministerstvu zahraničních věcí, je-li	Není jasné za jakých podmínek probíhá spolupráce se zahraničními orgány. V zákoně je pouze uvedeno, že VZ spolupracuje s "dalšími státními orgány", ale není jasné zda jsou to orgány ČR nebo jiných států. Prakticky nám nevyhověli a stále není jasné, jak bude mezinárodní spolupráce probíhat. Na

předávání dat nebo zpřístupnění sond samotných. Navrhujeme proto v novém odstavci 5 zakotvení ochrany osobních údajů obyvatel s ohledem na předávání informací od zahraničí. Podle námi navrhovaného ustanovení by Vojenské zpravodajství nemělo oprávněno zpřístupnit sondy nebo plošný obsah dat získaných při monitoringu kybernetického prostoru spolupracujícím orgánům jiných států, přičemž by mohlo na dožádání orgánů jiných států předávat informace získané při monitoringu pouze v individuálních odůvodněných případech. V této souvislosti je potřeba doplnit, že obecným problémem zpravodajských služeb v České republice je nedostatečné zákonné ošetření zásad zahraniční zpravodajské spolupráce. Agentura Evropské unie pro základní práva (*European Union Agency for Fundamental Rights*) vydala v roce 2017 srovnávací analýzu právních předpisů Sledování zpravodajskými službami: záruky ochrany základních práv a prostředky nápravy v Evropské unii – díl II. Podle agentury mají téměř všechny členské státy zákony o mezinárodní zpravodajské spolupráci. Třetina z nich ukládá zpravodajským službám, aby stanovily vnitřní předpisy pro postupy a metody mezinárodní spolupráce, včetně ochranných opatření při sdílení údajů. Několik členských států pak umožňuje vnější posouzení dohod o mezinárodní zpravodajské spolupráci. Dle stanoviska agentury: “*Členské státy EU by měly*	**individuálních odůvodněných případech může na žádost orgánů jiných států předávat informace získané při monitoringu.**	z povahy identifikovaného útoku nebo hrozby směřující proti důležitým zájmům státu zřejmé, že přijímaná opatření mohou být významně podpořena jeho aktivitami, jimiž zajišťuje ochranu práv a zájmů České republiky v zahraničí.	druhou stranu píší, že mohou předávat jednotlivé informace Ministerstvu zahraničí § 16b odst. 3), čím možná reagují na naší připomínku. Návrh zákona vlastně k nějaké přímé spolupráci se zahraničními státy mlčí.

stanovit pravidla pro způsob mezinárodní výměny zpravodajských informací.” V České republice samostatný zákon o mezinárodní zpravodajské spolupráci neexistuje a není tato spolupráce dostatečně ošetřena ani v zákoně o zpravodajských službách či v zákoně o Vojenském zpravodajství. Nedostatek zákonného ošetření mezinárodní spolupráce zpravodajských služeb je proto zásadním deficitem současné právní úpravy v České republice.			
Náhrada škody			
Navrhované ustanovení o náhradě škody považujeme za nedostatečné. Z toho důvodu navrhujeme rozšířit dané ustanovení tak, aby byly zohledněny všechny formy škody, které mohou v důsledku nových pravomocí a povinností Vojenského zpravodajství občanům vzniknout, a aby mohly být řádně nahrazeny. Obecná právní úprava o náhradách škody (zákona č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem) poskytuje náhrady v případě, že škoda vznikla v důsledku nezákonného rozhodnutí či nesprávného úředního postupu. V obecné rovině musí být dle uvedeného zákona pro vznik odpovědnosti státu splněny tři kumulativní podmínky (nesprávný úřední postup, vznik škody a existence příčinné souvislosti mezi nimi). **V případě, že je státní orgán zmocněn k novým**	**§ 16k** **Náhrada škody** **(1) Ministerstvo obrany je povinno nahradit škodu způsobenou právnické nebo podnikající fyzické osobě zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací** **a) v souvislosti s monitoringem kybernetického prostoru, pokud dojde k ovlivnění plnění povinností této osoby vůči uživatelům sítě;** **b) pokud dojde k cílenému kybernetickému útoku na infrastrukturu této osoby v souvislosti s umístěním sondy zřízené za účelem monitoringu kybernetického prostoru.** **(2) Povinnost státu podle odstavce 1) písmene b) nevznikne, pokud se jedná o škodu způsobenou osobě, která vyvolala kybernetický útok proti sobě v souvislosti porušením povinnosti zachovávat mlčenlivost dle § 98a**	**§ 16m** **Náhrada škody nebo nemajetkové újmy** (1) Každý, komu vznikla škoda nebo nemajetková újma v souvislosti s činnostmi Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu, má právo na jejich náhradu. (2) Fyzické nebo právnické osobě se nahrazuje také škoda nebo nemajetková újma, která jí vznikla v důsledku realizace opatření přijatých Vojenským zpravodajstvím v zájmu provedení aktivního zásahu směřujícího k odstranění kybernetického útoku nebo hrozby v rámci zajišťování obrany státu v kybernetickém prostoru. (3) Povinnost státu k náhradě škody nebo nemajetkové újmy podle odstavců 1 a 2 nevznikne, pokud se jedná o škodu nebo nemajetkovou újmu způsobenou fyzické nebo právnické osobě, která	Tady došlo k zásadnímu posunu k větší zodpovědnosti státu za způsobené škody, ale námi vyjmenovaným případům nevyhověli. Nárok na náhradu bude mít nejen provozovatel sítě. Podle nového návrhu má nárok kdokoliv, komu vnikne škoda v souvislosti s celou činností vojenského zpravodajství. V tom jdou dále než jsme sami navrhovali. Stejně tak nové znění presumuje zodpovědnost VZ za škodu pří výkonu jejich oprávnění, takže by poškozený nemusel dokládat, že VZ provedlo nějaký nesprávný postup, jako to je při odškodnění obecnými právními předpisy. Jakákoliv způsobená škoda bez ohledu na oprávněnost postupu by měla být zaplacena. Tím vlastně řeší nepředvídatelné situace, které bychom jinak složitě vyjmenovávali. Není domyšleno, co se stane v případě, že provozovatel sítě bude mít napadenou infrastrukturu v souvislosti s

oprávněním či povinnostem, při kterých by občanům nebo provozovatelům sítě mohla vzniknout škoda, může být pro vymahatele škody problematické prokázat nesprávný úřední postup. Z toho důvodu navrhujeme vyjmenovat možné situace, při kterých mohou vzniknout škody při výkonu oprávnění a povinností Vojenského zpravodajství a určit povinnost státu vzniklou škodu nahradit. Navrhujeme, aby měl stát vůči provozovatelům sítě povinnost nahradit škody vzniklé v souvislosti s monitoringem kybernetického prostoru, pokud dojde k ovlivnění plnění povinností této osoby vůči uživatelům sítě. Tuto možnost škody provozovatelů sítí připouští také ustanovení § 16f odst. 3 písm. c), které tvrdí, že monitorování kybernetického prostoru může ovlivňovat plnění povinností právnické nebo podnikající fyzické osoby zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací vůči uživatelům sítě. Na takto vzniklé škody by se totiž ve všech případech nemusel vztahovat navrhovaný § 98a odstavec 3) zákona o elektronických komunikacích, který stanoví úhrada nákladů za zřízení a zabezpečení sondy umožňující monitorování kybernetického prostoru. Dále navrhujeme, aby měl stát vůči provozovatelům sítě povinnost nahradit škody vzniklé v důsledku cíleného kybernetického útoku na infrastrukturu této osoby v souvislosti s umístěním	**odst. 4 zákona o elektronických komunikacích.** **(3) Ministerstvo obrany je povinno nahradit škodu způsobenou Vojenským zpravodajstvím v souvislosti s aktivním zásahem dle § 16c odstavce 2 písm. a).** (4) V případě, že při vykonávání oprávnění a povinností Vojenského zpravodajství při zajišťování bezpečnosti České republiky v kybernetickém prostoru vznikne **jiná škoda než uvedená v odst. 1 až 3,** postupuje Ministerstvo obrany podle obecných právních předpisů upravujících náhradu škody.	vyvolala útok nebo hrozbu. (4) Náhradu škody nebo nemajetkové újmy podle odstavců 1 a 2 poskytuje a rozhoduje o ní Ministerstvo obrany. (5) Právo na náhradu škody podle odstavců 1 a 2 je třeba uplatnit do tří měsíců ode dne, kdy se poškozený dozvěděl o škodě, nejpozději však do tří let od vzniku škody, jinak toto právo zanikne.	umístěním sondy. Ač se jedná o hypotetickou situaci, je otázka zda by se na to ustanovení použilo. Současně se zde trochu zhoršilo postavení poškozených tím, že byla stanovená tříměsíční subjektivní lhůta k uplatnění nároku, protože podle obecných právních předpisů by měli mnohem více.

sondy zřízené za účelem monitoringu kybernetického prostoru. Povinnost státu by v tomto případě nevznikla, pokud by provozovatel sítě vyvolala kybernetický útok proti sobě v souvislosti porušením povinnosti zachovávat mlčenlivost o umístění sondy. V dalších dvou odstavcích daného paragrafu navrhujeme uvést, že stát je povinen nahradit škodu způsobenou Vojenským zpravodajstvím v souvislosti s aktivním zásahem v kybernetickém prostoru, a že ve zbytku se postupuje podle obecných právních předpisů upravujících náhradu škody.			
Kontrola Vojenského zpravodajství			
Vytvoření silného mechanismu dohledu je zásadní součástí systému odpovědnosti zpravodajských služeb obecně. Rámec dohledu kontrolních orgánů by proto měl odpovídat pravomocem, které jsou Vojenskému zpravodajství svěřeny. Vyplývá to z výsledků výzkumu, který Agentura Evropské unie pro základní práva (*European Union Agency for Fundamental Rights*) vydala v roce 2017 v publikaci Sledování zpravodajskými službami: záruky ochrany základních práv a prostředky nápravy v Evropské unii – díl II. Zmíněná zpráva porovnává činnost a zákonné ukotvení zpravodajských služeb ve všech státech EU. Část stanoviska 3 z tohoto reportu uvádí: "*Členské státy EU by měly zřídit spolehlivý rámec dohledu odpovídající pravomocem a kapacitám zpravodajských služeb. Členské státy by*	**§ 22 odst. 3)** (3) Ředitel Vojenského zpravodajství předkládá kontrolnímu orgánu na jeho požádání **zejména** a) zprávu o činnosti Vojenského zpravodajství[11)], b) zprávu o použití zpravodajských prostředků, vyjma zpravodajských prostředků použitých při zabezpečování informací majících původ v zahraničí[12)], a to pouze ve věcech a v případech, ve kterých Vojenské zpravodajství svou činnost již ukončilo, c) souhrnnou informaci obsahující zaměření a počet případů a věcí, v nichž je Vojenské zpravodajství činné, vyjma případů a věcí při zabezpečování informací majících původ v zahraničí[12)]; v informaci odliší případy a věci podle zvláštního právního předpisu[13)],	**§ 16l** **Kontrola činností, jimiž se Vojenské zpravodajství podílí na zajišťování obrany státu v kybernetickém prostoru, a prověřování souvisejících opatření** (1) Provádí-li vláda, Poslanecká sněmovna nebo orgán nezávislé kontroly kontrolu činností a opatření Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, je Vojenské zpravodajství povinno kontrolujícímu předložit zejména a) záznamy podle § 16h a b) další zprávy, které jsou nezbytné pro zjištění skutečného stavu v rozsahu nezbytném pro dosažení účelu kontroly. (2) Kontrolující podle odstavce 1 jsou oprávněni kdykoliv požádat o	Tady vyhověli částečně. 1) Požadovali jsme zahrnout tři informace, které by mělo VZ povinnost poskytnout kontrolním orgánům. a) zpracovávané zprávy o činnosti VZ na úseku kybernetické obrany. Tomu vyhověli. b) záznamy, které VZ zpracovává o opatřeních při kybernetickém útoku. To tam výslovně nezahrnuly. c) rozhodnutí Ministerstva obrany o umístění sondy. To zahrnuly mezi informace, o které může kontrolní orgán požádat, ale nestanovili povinnost VZ je poskytnout. Takže to je nejasné. 2) Dále jsme chtěli, aby z § 22 odst. 3) udělali demonstrativní výčet. To by

orgánům dohledu měly rovněž poskytnout pravomoc zahajovat vlastní vyšetřování jakož i trvalý, úplný a přímý přístup k informacím a dokumentům nezbytným k plnění jejich role." Z důvodu naplnění lepší funkce parlamentní kontroly Vojenského zpravodajství **navrhujeme doplnit seznam informací, které by ředitel Vojenského zpravodajství poskytoval na požádání orgánu parlamentní kontroly.** Konkrétně se jedná o tři typy informací: **1) roční a pololetní zprávu o plnění úkolů na zajišťování kybernetické obrany a bezpečnosti České republiky a vyhodnocení jejich účinnosti (vypracovává Vojenské zpravodajství dle § 16i), 2) záznamy o řešení kybernetických útoků (vypracovává Vojenské zpravodajství dle § 16e), a 3) rozhodnutí Ministerstva obrany vydaná k umístění sondy u provozovatelů sítě (vypracovává Ministerstvo obrany základě § 16g odst. 3. a zmocňuje Vojenské zpravodajství k umístění sond).** Považujeme za nezbytné oprávnění k předání uvedených informací kontrolnímu orgánu od Vojenského zpravodajství uvést výslovně v zákoně. Praxe při kontrolách zpravodajských služeb výslovné uvedení konkrétních dokumentů vyžadují. Bez jejich uvedení by ředitel Vojenského zpravodajství mohl argumentovat, že nemá pravomoc tyto informace předávat. Pokud by nebylo výslovné zmocnění ředitele Vojenského	d) počet případů, ve kterých byla podána žádost o poskytnutí zprávy bankou nebo pobočkou zahraniční banky o záležitostech týkajících se klienta, které jsou předmětem bankovního tajemství[18)], e) zprávu o využívání žádostí o poskytnutí zprávy bankou nebo pobočkou zahraniční banky o záležitostech týkajících se klienta, které jsou předmětem bankovního tajemství18), a to pouze ve věcech a případech, ve kterých Vojenské zpravodajství svou činnost již ukončilo, **f) roční a pololetní zprávu o plnění úkolů podle § 16a odst. 1 a vyhodnocení jejich účinnosti, zpracovávané Vojenským zpravodajstvím dle § 16i,** **g) záznamy provedených opatřeních vedených podle § 16e, nebo** **h) rozhodnutí Ministerstva obrany vydaná na základě § 16g odst. 3.**	a) přístup k auditním záznamům provozu nástroje detekce, b) přístup ke spisové dokumentaci vedené ve věci rozhodování o umístění nástroje detekce, nebo c) poskytnutí dalších informací a dat souvisejících s předmětem kontroly. (3) Kontrolující je při provádění kontroly povinen šetřit práva a oprávněné zájmy Vojenského zpravodajství, stejně jako třetích osob, kterým byly v souvislosti s prováděním činností Vojenského zpravodajství podle této části zákona uloženy povinnosti. (4) Orgán nezávislé kontroly může vykonávat kontrolní činnost podle odstavce 1 také na základě podnětu právnické nebo podnikající fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací, jíž byla uložena povinnost zřídit a zabezpečit rozhraní pro připojení nástroje detekce v určeném bodě veřejné komunikační sítě a povinnost strpět umístění a provozování tohoto nástroje, nebo Českého telekomunikačního úřadu, a to včetně kontroly dodržování základních práv a svobod. V případě, že orgán nezávislé kontroly na základě kontroly provedené z podnětu právnické nebo podnikající fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací podle věty první zjistí, že činností Vojenského zpravodajství, jíž se podílí na zajišťování obrany státu, došlo k protiprávnímu	znamenalo, že by mohly kontrolní orgány obecně chtít pro celou kontrolu VZ (nejen kybernetické obrany) mít nárok vidět i jiné než vyjmenované dokumenty. Pokud tam zůstává taxativní výčet, tak nic jiného VZ poskytnout ani nemůže. Oni to udělali tak, že kontrolu týkající se kybernetické obrany vyňali z uvedeného paragrafu a vytvořili nový paragraf 16l týkající se kontroly kybernetické obrany. Tím pádem původní výčet zůstává uzavřený a udělali otevřené výčty jen z těch dokumentů, které musí VZ poskytnout nebo těch, o které může kontrolní orgán požádat v rámci kontroly kybernetické obrany.

zpravodajství uvedené informace parlamentnímu kontrolnímu orgánu předat, byla by kontrola uvedených dokumentů ze strany orgánů nezávislých na vládě zásadně ztížena. Toto ustanovení tak napomáhá správnému nastavení principu brzd a protiváh v demokratickém systému. Zákonodárná moc tím lépe kontroluje moc výkonou. Taxativní **výčet dokumentů, které ředitel Vojenského zpravodajství předkládá kontrolnímu orgánu na jeho požádání, navrhujeme změnit na demonstrativní výčet přidáním slova "zejména".** Taxativní výčet dokumentů předkládaných ředitelem Vojenského zpravodajství, omezuje výkon parlamentní kontroly pouze na dokumenty uvedené v tomto seznamu. Považujeme za žádoucí, aby kontrolní orgán měl potenciální možnost přístupu také k dalším dokumentům Vojenského zpravodajství.		zásahu do základních práv a svobod, obdrží jím vypracovanou písemnou zprávu[24)] rovněž tato osoba. (5) Kontrolní řád se na kontrolu činnosti Vojenského zpravodajství podle této části zákona nepoužije. (6) Na prověřování opatření přijímaných Vojenským zpravodajstvím v zájmu zabezpečování činností, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, Ministerstvem obrany se použije ustanovení § 41 zákona o zajišťování obrany České republiky obdobně.	
Navrhujeme do zákona doplnit ustanovení, že **kontrolní orgán** dle § 21 a dále Orgán nezávislé kontroly zpravodajských služeb České republiky (dle zákona č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů) **je oprávněn od poskytovatele sítě požadovat informace o monitorování kybernetického prostoru**. Toto poskytování informací kontrolním orgánům od poskytovatelů sítě navrhujeme současně vyjmout z povinnosti mlčenlivosti (v zákoně o elektronických komunikacích).	**§ 23a** **Kontrolní orgán dle § 21 a Orgán nezávislé kontroly zpravodajských služeb České republiky je oprávněn požadovat od právnické nebo podnikající fyzické osoby zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací informace o monitorování kybernetického prostoru Vojenským zpravodajstvím prostřednictvím sítí a služeb elektronických komunikací.**	**§ 16l** (3) Kontrolující je při provádění kontroly povinen šetřit práva a oprávněné zájmy Vojenského zpravodajství, stejně jako třetích osob, kterým byly v souvislosti s prováděním činností Vojenského zpravodajství podle této části zákona uloženy povinnosti. (4) Orgán nezávislé kontroly může vykonávat kontrolní činnost podle odstavce 1 také na základě podnětu právnické nebo podnikající fyzické osoby zajišťující veřejnou komunikační síť nebo	Zde jsme chtěli, aby mohly kontrolní orgány (jak specializovaný "orgán nezávislé kontroly", tak orgán zřízený Poslaneckou sněmovnou) požadovat informace od provozovatele sítě, který zřídil rozhraní pro detekční zařízení. Trochu to otočili a rozdělili: 1) Otočení: v jejich znění nemá kontrolní orgán nezávislé kontroly právo požadovat od provozovatele sítě informace, ale naopak provozovatel sítě se může na kontrolní orgán obrátit. Vhledem k tomu, že tam je nový institut

Navrhované ustanovení je nezbytné pro řádný výkon činnosti kontrolních orgánů. V situaci, kdyby bylo monitoringu zneužito, neměl by bez tohoto ustanovení poskytovatel sítě možnost na tuto skutečnost upozornit kontrolní orgány, které jsou nezávislé na výkonné moci.		poskytující veřejně dostupnou službu elektronických komunikací, jíž byla uložena povinnost zřídit a zabezpečit rozhraní pro připojení nástroje detekce v určeném bodě veřejné komunikační sítě a povinnost strpět umístění a provozování tohoto nástroje, nebo Českého telekomunikačního úřadu, a to včetně kontroly dodržování základních práv a svobod. V případě, že orgán nezávislé kontroly na základě kontroly provedené z podnětu právnické nebo podnikající fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací podle věty první zjistí, že činností Vojenského zpravodajství, jíž se podílí na zajišťování obrany státu, došlo k protiprávnímu zásahu do základních práv a svobod, obdrží jím vypracovanou písemnou zprávu[24)] rovněž tato osoba.	"inspektor kybernetické obrany", který je zaměstnanec VZ, tak to pro provozovatele sítě bude matoucí. Provozovatel sítě asi bude předně kontaktovat "inspektora kybernetické obrany" jehož role bude pravděpodobně, jak už to tak bývá, pokrývat případné přešlapy jako první kontaktovaný. Naopak by měl mít kontrolující orgán možnost kontaktovat toho provozovatele sítě jako první. 2) Rozdělení: kontrolní orgány jsou v zásadě dva (pomineme-li vládu, ministerstvo a "inspektora kybernetické obrany" - vše v podstatě exekutiva). Těmi orgány je kontrolní orgán poslanecké sněmovny (dle zákona o VZ) a specializovaný "orgán nezávislé kontroly". Podle jejich znění by tuto pravomoc měl jen jeden z nich a to "orgán nezávislé kontroly", ale neměl by ho orgán poslanecké sněmovny. Navíc je nutné dodat, že zřídili nový odstavec 3), který se vztahuje na oba orgány (poslance i specializovaný), že práva VZ a třetích osob mají být šetřena. To v podstatě omezuje oba orgány jednat samostatně a iniciativně. Přesně opak toho, co jsme chtěli.

Změna zákona o elektronických komunikacích

Naše připomínka	Naše znění	Nový návrh MO	Komentář
Připojení sondy u provozovatele sítě			
Navrhované ustanovení o připojení sondy do sítě je z hlediska zajištění	**§ 98a**	**§ 98a**	Nevyhověli naším připomínkám.

dobré praxe nedostatečně formulované. Především chybí bližší specifikace sondy - např. **zda se jedná o software či hardware. Navrhujeme do návrhu doplnit, že sonda je pasivním hardwarovým zařízením, které je do zřízeného rozhraní připojeno odbočně.** Nezbytnost použití pasivních typů sond je především v možnosti zneužití sond aktivních. Pasivní sondu je možné plně využít k mapování komunikačních toků. Taková sonda plně dostačuje k monitoringu kybernetického prostoru a současně zajišťuje ochranu dat občanů před možným zneužitím. Aktivní sonda je zapojena tzv. in-line, přímo v cestě, zatímco pasivní sonda je zapojena na odbočce, proto **požadujeme také doplnit, že sonda je na zřízeném rozhraní připojena odbočně.** Aktivní sonda by mohla do komunikace také přímo vstupovat. Mohla by selektivně blokovat některé komunikační toky (například blokovat vybrané weby) nebo se vydávat za některého z účastníků komunikace. Rizikem je u aktivních sond také podvržení kanálu s aktualizacemi operačního systému nebo mobilního telefonu, v důsledku kterého by došlo k úplnému ovládnutí koncového zařízení. Tyto funkce nejsou k účelu monitoringu kybernetického prostoru potřeba, ale je u nich riziko zneužití. Jako další pojistku před zneužitím do ustanovení navrhujeme, aby rozhraní pro připojení sondy muselo být technicky	(1) Právnická nebo podnikající fyzická osoba zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací je povinna na základě rozhodnutí vydaného Ministerstvem obrany podle zákona o Vojenském zpravodajství[70] zřídit a zabezpečit ve vhodných bodech jí provozované sítě rozhraní pro připojení **zařízení** umožňujícího za účelem zajišťování obrany a bezpečnosti České republiky v kybernetickém prostoru nepřetržité monitorování kybernetického prostoru podle zákona o Vojenském zpravodajství[71] (dále jen „sonda“). **Zřízené rozhraní pro připojení sondy musí být technicky uzpůsobeno tak, že do sondy předává pouze metadata zpráv, definovaná v § 16b odst. 3 zákona o Vojenském zpravodajství, a zároveň neumožňuje sondě komunikovat v opačném směru. Bližší technické požadavky na připojení sondy k rozhraní stanoví prováděcí právní předpis.**	(1) Právnická nebo podnikající fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna na základě rozhodnutí vydaného Ministerstvem obrany podle zákona o Vojenském zpravodajství[70] zřídit a zabezpečit v určených bodech jí zajišťované veřejné komunikační sítě rozhraní pro připojení nástroje detekce umožňujícího provádět cílenou detekci jevů nasvědčujících existenci kybernetického útoku nebo hrozby a jejich identifikaci podle zákona o Vojenském zpravodajství[71]. (2) Rozhraní pro připojení nástroje detekce musí být technicky uzpůsobeno tak, že neumožňuje předávat obsah detekovaných jevů provozu veřejné komunikační sítě ani komunikaci nástroje detekce s veřejnou komunikační sítí v opačném směru.	Za prvé jejich nové označení "nástroj detekce" je stejně matoucí jako původní "sonda". Není z toho zřejmé zda jde o hardware nebo software. Za druhé z jejich znění neplyne to, že by bylo zařízení připojeno odbočně a jednalo by se tudíž o pasivní sondu. Za třetí není stanoveno to, že by byly do "detekčního zařízení" předávány jen informace definované v zákoně o Vojenském zpravodajství. Za čtvrté z nového znění plyne, že: rozhraní musí být uzpůsobeno tak, že neumožňuje komunikaci nástroje detekce s veřejnou komunikační sítí v opačném směru. V tom jediném našemu požadavku vyhověli.

uzpůsobené tak, že **do sondy předává pouze ta data, která jsou pro monitoring kybernetického prostoru nezbytná.** Pokud bude provozovatel sítě předávat do sondy jen řídící data paketů, jak jsou definována v zákoně o Vojenském zpravodajství, zamezí se tím, aby mělo Vojenské zpravodajství přímý přístup k obsahu komunikace mezi uživateli sítě. Tato data pak nebudou moci být zneužita a přitom Vojenské zpravodajství od provozovatelů sítí dostane data potřebná k monitoringu kybernetického prostoru. Dále v původním návrhu chybí určení, kde je stanovena specifikace toho, jaké rozhraní mají poskytovatelé sítí zajistit. Z toho důvodu navrhujeme **do návrhu zákona doplnit, že rozhraní pro připojení sondy a technické požadavky na provozovatele sítí stanoví prováděcí právní předpis.** Odpovídajícím způsobem by měl být návrh vyhlášky doplněn. V souvislosti s nedávným varováním Národního úřadu pro kybernetickou a informační bezpečnost, doporučujeme v návrhu vyhlášky zohlednit bezpečnostní požadavky na sondy samotné.			
V návrhu vyhlášky se píše, že se "do výše nákladů se zahrnují pouze ty náklady, které byly zachyceny v účetnictví subjektem". V praxi se však může ukázat jako problematické určit přesný počet odpracovaných hodin zaměstnance subjektu, které strávil při řešení závad v síti, u kterých se například až zpětně zjistí, že vznikly v	**§ 98a odst. 3)** (3) Za plnění povinností podle odstavce 1 náleží právnické nebo podnikající fyzické osobě od Vojenského zpravodajství úhrada efektivně vynaložených nákladů **zaznamenaných v účetnictví nebo jinak**. Způsob určení výše efektivně vynaložených nákladů a	**§ 98a odst. 5)** (5) 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	Zde ponechaly jejich původní znění. Naší připomínku nebrali v potaz. Pokud to chceme skutečně prosadit, tak nelze spoléhat na vyhlášku, kterou si můžou upravit jak chtějí bez vlivu zákonodárné moci.

důsledku připojení zpravodajské sondy. Navíc není úplně jasné, proč je povinnost navázaná na účetnictví, když tento typ nákladů nebude zpravidla účtován jako samostatná položka. Z toho důvodu navrhujeme upravit navrhované znění zákona tak, že **provozovateli sítí náleží náhrada jakýchkoliv efektivně vynaložených nákladů bez ohledu na to zda jsou zaznamenány v účetnictví nebo jiným prokazatelným způsobem.**	způsob jejich úhrady stanoví prováděcí právní předpis.	právní předpis.	
Navrhujeme doplnit navrhovaný odstavec 4 o **výjimku z povinnosti mlčenlivosti pro provozovatele sítí na komunikaci se členy kontrolních orgánů, které jsou nezávislé na výkonné moci.** Jednalo by se o kontrolní orgán Poslanecké sněmovny (dle § 21 zákona č. 289/2005 Sb., o Vojenském zpravodajství) a dále Orgán nezávislé kontroly zpravodajských služeb České republiky (dle § 12e zákona č. 153/1994 Sb., o zpravodajských službách České republiky). Navrhované ustanovení je nezbytné pro řádný výkon činnosti kontrolních orgánů. V situaci, kdyby bylo monitoringu zneužito a provozovatel sítě by nebyl zproštěn mlčenlivosti vůči kontrolním orgánům, zbývala by provozovateli sítě pouze ochrana prostřednictvím správního soudnictví.	**§ 98a odst. 4)** (4) Osoba uvedená v odstavci 1, jakož i jiné osoby podílející se na plnění povinnosti podle odstavce 1, jsou povinny zachovávat mlčenlivost o všech skutečnostech souvisejících s připojením a užíváním sond. Tato povinnost trvá i poté, kdy tato osoba přestane být osobou podle odstavce 1 nebo osobou podílející se na plnění povinnosti podle věty první. **Povinnost mlčenlivosti se nevztahuje na komunikaci s kontrolním orgánem Poslanecké sněmovny dle § 21 zákona o Vojenském zpravodajství a Orgánem nezávislé kontroly zpravodajských služeb České republiky dle § 12e zákona o zpravodajských službách České republiky.**	(6) Osoba uvedená v odstavci 1, jakož i jiné osoby podílející se na plnění povinnosti podle odstavce 1, jsou povinny zachovávat mlčenlivost o všech skutečnostech souvisejících s připojením a užíváním nástroje detekce. Tato povinnost trvá i poté, kdy tato osoba přestane být osobou podle odstavce 1 nebo osobou podílející se na plnění povinnosti podle věty první. (7) Povinnost zachovávat mlčenlivost podle odstavce 5 se nevztahuje na podávání informací kontrolujícím, kteří provádějí kontrolu činností Vojenského zpravodajství podle části čtvrté zákona o Vojenském zpravodajství.	Zde je podle části čtvrté tohoto zákona pověřen kontrolou u provozovatele sítí pouze "orgán nezávislé kontroly", ale již jím není pověřen kontrolní orgán Poslanecké sněmovny. Výjimka z mlčenlivosti se tudíž netýká kontrolního orgánu Poslanecké sněmovny.
Přestupky			
Navrhujeme **určit výjimku z přestupku** neoprávněného zásahu do sondy nebo omezení její funkčnost ze strany provozovatele sítě za situace, kdy osoba odpojí sondu za stavu kybernetického	**§ 118 odst. 23)** (23) Právnická nebo podnikající fyzická osoba se jako osoba zajišťující síť elektronických komunikací nebo	**§ 118 odst. 23)** (23) Právnická nebo podnikající fyzická osoba se jako osoba zajišťující veřejnou komunikační síť nebo veřejně dostupnou službu elektronických komunikací	Zde ponechaly jejich původní znění. Naší připomínku o výjimku z přestupku nebrali v potaz.

útoku na svou vlastní telekomunikační infrastrukturu z důvodu umístění sondy.	poskytující službu elektronických komunikací dopustí přestupku tím, že a) v rozporu s § 98a odst. 1 nezřídí nebo nezabezpečí v určených bodech své sítě rozhraní pro připojení sondy podle rozhodnutí vydaného Ministerstvem obrany; b) neumožní Vojenskému zpravodajství přístup k sondě; c) neoprávněně zasáhne do sondy nebo omezí její funkčnost, **s výjimkou situace, kdy osoba odpojí sondu za stavu kybernetického útoku na svou vlastní telekomunikační infrastrukturu z důvodu umístění sondy v jí provozované síti; nebo** d) poruší povinnost zachovávat mlčenlivost podle § 98a odst. 4.	dopustí přestupku tím, že a) v rozporu s § 98a odst. 1 nezřídí nebo nezabezpečí v určených bodech jí zajišťované veřejné komunikační sítě rozhraní pro připojení nástroje detekce podle rozhodnutí vydaného Ministerstvem obrany, b) neumožní Vojenskému zpravodajství přístup k nástroji detekce, c) neoprávněně zasáhne do nástroje detekce nebo omezí jeho funkčnost, nebo d) poruší povinnost zachovávat mlčenlivost podle § 98a odst. 6.	
Navržená podoba sankcí za uvedené přestupky je nepřiměřená. Navrhovaná výše pokuty 50 000 000 Kč se svou výší rovná například výši pokuty stanovené pro provozovatele jaderné elektrárny za porušení povinností týkajících se provozu jaderného reaktoru (§ 178 odst. 5 písm. b) atomového zákona). Z tohoto důvodu **navrhujeme zmírnění sankcí podle míry závažnosti jednání.** Sankci za přestupky, kdy provozovatel sítě nezřídí a nezabezpečí připojení sondy podle rozhodnutí Ministerstva obrany (dle § 98a odst. 1), neumožní Vojenskému zpravodajství přístup k sondě, nebo neoprávněně zasáhne do sondy nebo omezí její funkčnost, navrhujeme ve výši 15 000 000 Kč,	**§ 118 odst. 24)** **(24)** Za přestupek podle § 118 lze uložit pokutu do a) 5 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. n) až r), odstavce 2 písm. f), odstavce 3 písm. b), odstavce 5, odstavce 6 písm. g), odstavce 14 písm. ae), **nebo odstavce 23 písm. d),** b) 15 000 000 Kč nebo do výše 5 % z čistého obratu pachatele přestupku dosaženého za poslední ukončené účetní období, podle toho, která z těchto hodnot je vyšší, jde-li o přestupek podle odstavce 1 písm. m), odstavce 2 písm. c) až e), odstavce 3 písm. a), odstavce 8 písm. d) až m), odstavce 10 písm. j) až r), odstavce 12 písm. f) až p), odstavce 13 písm. i) až n), odstavce 14 písm. k) až	Dosavadní odstavec 23 se označuje jako odstavec 24. **3.** V § 118 odst. 24 písm. a) se slova „nebo odstavce 14 písm. ae)“ nahrazují slovy „, odstavce 14 písm. ae) nebo odstavce 23 písm. d)“. **4.** V § 118 odst. 24 písm. b) se slova „nebo odstavce 15“ nahrazují slovy „, odstavce 15 nebo odstavce 23 písm. b) anebo c)“. **5.** V § 118 odst. 24 písm. c) se slova „nebo 22“ nahrazují slovy „, 22 nebo 23 písm. a) “.	Tady našim připomínkám vyhověli částečně. Co se týče přestupků pod body b), c) a d), tak snížili sankce dle našeho návrhu. Trvají na tom, aby přestupek dle § 118 odst. 23) písmene a) byl sankcionován v nejvyšší možné míře, tzn. 50 000 000 Kč. Sporný přestupek je (viz bod výše): Osoba zajišťující veřejnou komunikační síť nebo veřejně dostupnou službu elektronických komunikací dopustí přestupku tím, že nezřídí nebo nezabezpečí v určených bodech jí zajišťované veřejné komunikační sítě rozhraní pro připojení nástroje detekce podle rozhodnutí vydaného

protože již tato výše je dostatečně odrazující sankcí. Sankce za přestupek, kdy provozovatel sítě poruší povinnost zachovávat mlčenlivost (podle § 98a odst. 4.), je dostatečně odstrašující již ve výši 5 000 000 Kč. K podobné výši sankce lze dospět i srovnáním se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, dle kterého je podnikatelům možné uložit sankci za přestupky, při kterých vyzradí informace v různém stupni utajení v maximální výši 5 000 000 Kč. Přitom tato nejvyšší možná sankce je za dva přestupky: 1) když podnikatel poskytne utajovanou informaci stupně utajení Přísně tajné, Tajné nebo Důvěrné zahraničnímu partneru, anebo 2) když vyveze z území České republiky certifikovaný kryptografický prostředek bez povolení Národního bezpečnostního úřadu.	ad), odstavce 15, **odstavce 23 písm. a) až c),** c) 50 000 000 Kč nebo do výše 10 % z čistého obratu pachatele přestupku dosaženého za poslední ukončené účetní období, podle toho, která z těchto hodnot je vyšší, jde-li o přestupek podle odstavce 1 písm. a) až l), odstavce 2 písm. a), b), odstavce 4, odstavce 6 písm. a) až f), odstavce 7, odstavce 8 písm. a) až c), odstavce 9, odstavce 10 písm. a) až i), odstavce 11, odstavce 12 písm. a) až e), odstavce 13 písm. a) až h), odstavce 14 písm. a) až j), odstavce 16, 17, 18, 19, 20, **21 nebo 22.**		Ministerstvem obrany.