Název materiálu:	**Novela zákona o Vojenském zpravodajství**
Jméno:	ICT UNIE z.s.
Telefon :	739 316 624
e-mail:	sarka.stulova@ictu.cz

A. SHRNUTÍ HLAVNÍCH DOPADŮ PŘEDLOŽENÉHO MATERIÁLU

Novela zákona o Vojenském zpravodajství zavádí nový termín v rámci kyberprostoru České republiky, a to pojem „kybernetická obrana". V souvislosti s obranou ČR není zřetelná vazba na kybernetickou bezpečnost a úkoly spojené se zajištěním kybernetické bezpečnosti státu v rámci kritické informační infrastruktury. Důvodová zpráva výslovně uvádí, že „obrana státu v kybernetickém prostoru, není prozatím v právním řádu České republiky výslovně řešena." Ani v návrhu novely zákona není obsah činností v rámci kybernetické obrany blíže specifikován, opět je výslovně zmíněno, že „kybernetická obrana není zatím v právním řádu definována a ani předpisy upravující zajišťování obrany státu s ní nepočítají."

Motivem této novely je umožnit Vojenskému zpravodajství vybudovat Národní centrum kybernetických sil, proto má být návrhem zmocněno k oprávnění používat „technické prostředky kybernetické obrany" tedy takové prostředky, které umožňují monitorování a analýzu provozu sítí a služeb elektronických komunikací, s odkazem na novelu zákona o elektronických komunikacích. Nový § 98a zákona o elektronických komunikacích pak definuje povinnost právnické nebo fyzické osoba zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací zřídit a zabezpečit v určených bodech své sítě rozhraní pro připojení technických prostředků kybernetické obrany, přičemž specifikace těchto technických prostředků je i nadále velmi nespecifická a vágní.

Návrh zákona také nestanovuje, zda tyto prostředky budou v síti permanentně aktivní či zda dojde k jejich aktivaci pouze v případě kybernetického ohrožení (např. na základě vyhlášení určitého stavu ze strany Národního bezpečnostního úřadu, Vlády ČR, Ministerstva obrany). Zmocnění Vojenského zpravodajství se má podle důvodové zprávy týkat nikoliv sledování obsahu komunikace konkrétních osob, ale pouze „signalizovat určité přesně definované negativní jevy související s kybernetickým prostorem", k čemuž důvodová zpráva opakovaně uvádí, že nepůjde o zásahy do práv na ochranu soukromí nebo tajemství dopravovaných zpráv - monitoring by neměl být určen k tomu, aby se zaměřoval na obsah konkrétních informací nebo komunikaci konkrétních osob. Údajně jej lze přirovnat např. k úsekovému měření rychlosti na silnicích, kde 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. Není zřejmé, jak se tyto informace budou shromažďovat, vyhodnocovat a uchovávat, přesto se v části VIII. důvodové zprávy tvrdí, že dopad na ochranu osobních údajů návrh nemá. Stanovisko dotčených orgánů, regulátorů, tedy Českého telekomunikačního úřadu a Úřadu na ochranu osobních údajů důvodová zpráva nedokládá a není zřejmé, zda byla s těmito úřady problematika projednána.

Při prováděném monitoringu však údajně nepůjde o sledování komunikace konkrétních osob (k tomuto účelu Vojenské zpravodajství může využívat institutu zpravodajské techniky), 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 – tato aktivita není nijak specifikována. Jelikož ale údajně nepůjde o cílené sledování, nebylo možné do návrhu vložit jakékoliv mechanismy kontroly a nezávislé povolovací procesy. Konkrétní nasazování a používání technických prostředků tak má stanovovat vláda jako kolektivní orgán. Z popsaného mechanismu vypořádání, tedy absence formálního procesu žádosti a jejího schválení nevyplývá možnost přezkumu rozhodnutí o nasazení technických prostředků. Postupem proti žádosti o nasazení technických prostředků je opět velmi vágně stanovený postup – odmítnutí dohody o nasazení, vyjádření se k žádosti, či podání žaloby podle § 82 soudního řádu správního, což není dostatečná ochrana pro zajištění ochrany a integrity sítě a jejího provozu.

Celá problematika je v rámci novel řešena velmi obecně, velmi vágně a vytváří právní nejistotu na straně povinných subjektů, které mají možnost se k problematice vyjádřit až v příběhu připomínkového řízení.

B. **OBECNÁ PŘIPOMÍNKA**

Návrh zákona údajně nepředpokládá zásahy do základních práv a svobod a soukromé sféry osob ve větším rozsahu, než tomu je dosud. Nicméně definice prvků kybernetické obrany je v zákoně velmi vágní a je možné pod ní schovat v podstatě jakékoliv, předem nedefinované zařízení.
Vojenskému zpravodajství se touto novelou dává do rukou možnost monitorovat (popř. uchovávat) plošně veškerý provoz, a to bez soudního příkazu nebo formálně ukotveného procesu. Není nijak definováno a zajištěno, jak s takto získanými daty bude moci Vojenské zpravodajství nakládat, jak bude vyřešena kontrola jejich využívání, zpracování, ad. Není také specifikováno, zda se bude jednat pouze o datový provoz, či půjde i o hlasový provoz či provoz signalizační vrstvě (SMS zprávy). Pro operátory neexistuje žádný opravný prostředek, popřípadě formalizovaná možnost přezkumu využívání těchto prostředků v síti operátora.
V současné podobě návrhu se operátor nebude mít možnost vyjádřit ani k tomu, zda Vojenským zpravodajstvím určený bod, kam budou prostředky umístěny, je optimální, ať již z pohledu technického řešení či z pohledu bezchybného fungování sítě.
Tzv. prostředky kybernetické obrany mohou dle našeho názoru případně i aktivně vstupovat do přenosu dat, pozměňovat jej, ukončovat jej atp., a to vše bez vědomí operátora.
Návrhem novely pak také není specifikováno, zda tyto prostředky budou v síti permanentně aktivní či zda dojde k jejich aktivaci pouze v případě kybernetického ohrožení nebo při plnění konkrétních úkolů tzv. kybernetické obrany. Ta není specifikována jako taková.
Celé řešení nebylo projednáno se zástupci průmyslu a dotčených subjektů. Vyžadované plnění povinnosti není z naší strany blíže identifikovatelné jako aplikovatelné či realizovatelné, což povede paradoxně spíše k možnému ohrožení kybernetické bezpečnosti ČR.

C. ZÁSADNÍ KONKRÉTNÍ PŘIPOMÍNKY

Připomínka k ČÁSTI PRVNÍ, Čl. I., změna zákona o Vojenském zpravodajství
K §§ 16a až 16c navrhujeme zpřesnění termínů „kybernetická obrana" a „technické prostředky kybernetické obrany", včetně možnosti účinného přezkoumání nasazení technických prostředků a specifikace „zřízení a zabezpečení rozhraní pro připojení technických prostředků kybernetické obrany."
Odůvodnění:
Návrh v takto vágním znění vytváří velkou nejistotu spojenou s plněním předpokládaných povinností, včetně časového horizontu, který předpokládá účinnost do 15 dní od vyhlášení novely zákona.

Připomínka k ČÁSTI TŘETÍ, Čl. III., Změna zákona o zajišťování obrany České republiky, bod 3.
V § 2 odst. 9) navrhujeme zpřesnění termínu „kybernetická obrana".
Odůvodnění:
Návrh zákona by měl přesně definovat oblast kybernetické obrany státu a rozdíl a společné úkoly v rámci zajištění kybernetické bezpečnosti.

Připomínka k ČÁSTI ČTVRTÉ, Čl. IV., Změna zákona o elektronických komunikacích a o změně některých souvisejících zákonů, bod 2.
V § 98a odst. 1) navrhujeme zpřesnění povinnosti „zřídit a zabezpečit v určených bodech své sítě rozhraní pro připojení technických prostředků kybernetické obrany".
Odůvodnění:

Touto úpravou má dojít k uložení nové povinnosti osobám zajišťujícím síť elektronických komunikací a osobám poskytujícím službu elektronických komunikací, která spočívá ve „zřízení a zabezpečení v určených bodech sítě rozhraní pro připojení technických prostředků kybernetické obrany." Jedná se o vágní vymezení povinnosti, a ačkoliv je nová povinnost konstruována obdobně jako povinnost dle § 97 zákona o elektronických komunikacích pro odposlechy, liší se tím, že vlastně není jasné o jaký typ sledování či kybernetické obrany se jedná. Zejména v oblasti zabezpečení je specifikace náležitostí takového opatření nezbytná pro zcela jasné vymezení povinnosti a jejího případného budoucího plnění, které by mělo být věcně upřesněno, stejně jako mělo být jasně stanoveno, o jaké body sítě může jít, a na jaké vrstvě sítě má docházet ke sledování.