Závěrečná zpráva z hodnocení dopadů regulace

SHRNUTÍ ZÁVĚREČNÉ ZPRÁVY RIA

1. Základní identifikační údaje	
1. Název návrhu: **Zákon, kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony**	
Zpracovatel / zástupce předkladatele: **Ministerstvo obrany**	Předpokládaný termín nabytí účinnosti, v případě dělené účinnosti rozveďte *10. 2020*
Implementace práva EU: Ne	

2. Cíl návrhu zákona
Návrh zákona je zákonným ztvárněním podmínek nezbytných pro realizaci úkolů, které vláda České republiky uložila svým usnesením ze dne 25. května 2015 č. 382, jímž 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. Návrhem zákona je rovněž plněn úkol C. 9.01 uvedeného Akčního plánu, tedy jsou navrhovány zákonné předpoklady pro výkon kybernetické obrany a vybudování Národního centra kybernetických sil (později přejmenovaného na Národní centrum kybernetických operací) v rámci Vojenského zpravodajství.
3. Agregované dopady návrhu zákona
3.1 Dopady na státní rozpočet a ostatní veřejné rozpočty: Ano
Nově stanovené povinnosti Vojenskému zpravodajství, resp. zejména nezbytnost zajistit nové komplexní věcné, organizační a personální podmínky jejich výkonu, nepochybně vyvolají nároky na státní rozpočet, **avšak s předpokladem jejich zajištění v rámci existující rozpočtové kapitoly Ministerstva obrany.** Návrh zákona nepředstavuje vzhledem k předmětu úpravy a nositeli působnosti pro výkon kybernetické obrany žádné nároky na rozpočty krajů a obcí.
3.2 Dopady na mezinárodní konkurenceschopnost ČR: Ne
3.3 Dopady na podnikatelské prostředí: Ano
Návrh zákona vyvolává dopady vůči právnickým a podnikajícím fyzickým osobám, které zajišťují veřejnou komunikační síť nebo poskytují veřejně dostupnou službu elektronických komunikací, a to svými požadavky na zřízení a zabezpečení rozhraní pro připojení nástroje detekce v určených bodech jí zajišťované veřejné komunikační sítě. S tím pak také souvisejí povinnosti strpět provozování těchto nástrojů a jejich zpřístupňování Vojenskému zpravodajství. Za plnění této povinnosti však budou státem hrazeny účelně vynaložené náklady.
3.4 Dopady na územní samosprávné celky (obce, kraje): Ne

3.5 Sociální dopady: Ne
3.6 Dopady na spotřebitele: Ne
3.7 Dopady na životní prostředí: Ne
3.8 Dopady ve vztahu k zákazu diskriminace a ve vztahu k rovnosti žen a mužů: Ne
3.9 Dopady na výkon státní statistické služby: Ne
3.10 Korupční rizika: Ano
Velmi nízká. Podrobnosti jsou popsány v další části tohoto dokumentu.
3.11 Dopady na bezpečnost nebo obranu státu: Ano
Pokud jde o dopady na bezpečnost a obranu státu, návrh se samozřejmě přímo dotýká zabezpečování obrany České republiky, neboť upravuje specifika zajištění obrany České republiky v kybernetickém prostoru. Návrh zákona koncipuje významnou část zajišťování obrany České republiky, nastavuje pravidla jejího plánování, budování a přímého výkonu, čímž ve svém souhrnu významně přispívá k zajišťování obrany České republiky (blíže k tomu viz také popis a vyhodnocení jednotlivých variant, zejména pak dále popsané varianty IV.).

Závěrečná zpráva o zhodnocení dopadů regulace (RIA)

1. Důvod předložení a cíle

1.1 Název

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

1.2 Definice problému

Problematika bezpečnosti je v českém právním řádu již řešena, přičemž jako základ lze považovat ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů. Ustanovení definuje „zajištění svrchovanosti a územní celistvosti České republiky, ochranu jejich demokratických základů a ochranu životů, zdraví a majetkových hodnot“ za základní povinnosti státu.

Kybernetický prostor nabývá v moderním světě stále více na důležitosti. Na informacích a informačních technologiích je založeno velké množství lidských činností, dnes si bez nich není možné představit žádnou podstatnější aktivitu, ať už jde o obchod, zábavu, koníčky, ale především ani výkon státní správy respektive veřejné správy jako takové. Závislost společnosti a jejího fungování na informačních technologiích rapidně narůstá, a to ve všech oblastech (nejedná se pouze o služby informační společnosti jako je internetový obchod, ale i o fungování informačních systémů, na jejichž správné funkci je závislá celá řada základních služeb jako například řízení dopravy, výroba a přenos energií, zdravotnictví, výkon veřejné moci, ale samozřejmě i obrana a bezpečnost státu – tedy občanů apod.). Jak už to ale bývá, tak kromě ryze pozitivních aspektů s sebou moderní technologie přináší i dříve neznámá rizika. V souvislosti s vývojem a využíváním informačních technologií dochází ke vzniku nových etických, právních, ale i bezpečnostních otázek. Nově se tedy musíme zabývat hrozbami, které přichází z na první pohled neviditelného kybernetického prostoru. Se vzrůstající závislostí společnosti na informačních technologiích pak ale na straně druhé vzrůstá i riziko zneužívání těchto technologií a přibývá útoků na tyto technologie, které mají rozsáhlé dopady do činnosti subjektů, které s nimi pracují, a potencionálně mohou vést ke značným škodám.

Kybernetický prostor se stále více stává také prostorem, ve kterém mohou být vedeny konflikty jak mezi státními, tak nestátními aktéry. Kybernetické hrozby již dávno nejsou pouze hypotetické, příkladem lze poukázat jak na útoky z Gruzie, Estonska či Ukrajiny, tak i u nás v České republice. Kybernetické útoky jsou totiž ideálním nástrojem pro poškození politických, obchodních či dalších obdobných cílů a také silným nástrojem pro vynucení vlastní vůle. Zároveň je ve většině případů velmi obtížné rozkrýt původce útoku, a to především v reálném čase. Tím se snižuje pravděpodobnost případné adekvátní reakce. Tyto skutečnosti, v kontextu s relativní absencí geografických a obdobných omezení, představují pro útočníka značnou výhodu. Kybernetický prostor je bez jasného vymezení jeho hranic v rámci jednotlivých států coby tradičních subjektů mezinárodního práva veřejného velmi neurčitý pojem, bez objektivní definice pro jeho uchopení pro účely praktického působení v něm. Přitom vzhledem ke stále se rozšiřujícímu významu elektronických sítí a komunikačních prostředků je určení jednotlivých států za cíl útoku v kybernetickém prostoru stále běžnější, a tím roste i důležitost jejich ochrany v tomto prostoru.

Jestliže srovnáme řešení kybernetických a fyzických hrozeb, tak například elektrárny, ale i další prvky kritické infrastruktury, mají svá bezpečnostní pravidla, brání se výstavbou fyzických bariér, kamerovými systémy, ostrahou, a pokud toto všechno selže, zavolají Policii ČR, která jako státní autorita přijede a útok odvrátí. Stejně tak mají elektrárny v kybernetické oblasti svá dohledová pracoviště, firewally, tým lidí, kteří situaci monitorují. Nicméně když dojde k opravdu masivnímu útoku a všechny tyto prvky selžou, nenacházejí tyto subjekty žádnou oporu v konkrétně stanovených pravidlech pro řešení takové situace a určených státních orgánech, které by pro takové případy nastoupily do rolí odpovědných osob za řešení, resp. odvrácení zjištěného, popřípadě probíhajícího kybernetického útoku. Sami přitom legálně zasáhnout nemohou.

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

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

Každý stát by proto měl budovat struktury k zajištění ochrany a obrany svých zájmů v kybernetickém prostoru před kybernetickými útoky. Budování obranných schopností v kyberprostoru je pro ČR potřebné i s ohledem na členství v NATO, neboť kyberprostor byl uznán jako plánovací a operační doména s tím, že kybernetický útok je způsobilý aktivovat čl. 5 Severoatlantické smlouvy. Proto v souladu s požadavkem zakotveným v čl. 3 Severoatlantické smlouvy by smluvní strany měly udržovat a rozvíjet jak individuální, tak kolektivní schopnosti odolat i kybernetickým útokům.

K zajišťování národní obrany v kyberprostoru nabádá i Strategie kybernetické bezpečnosti EU (CELEX 52013JC0001), kde je kladen důraz na to, aby se zvýšila odolnost komunikačních a informačních systémů, jež podporují obranné a bezpečnostní zájmy členských států.

V rámci Bezpečnostní strategie České republiky, aktualizované v únoru 2015, jsou mezi identifikovanými hrozbami uvedeny kybernetické útoky, k jejichž povaze je zde uvedeno: „kybernetický prostor je velmi specifický neexistencí geografických hranic a relativizací vzdálenosti mezi zdroji hrozeb a potenciálním cílem. Díky své asymetričnosti pak umožňuje

státním i nestátním aktérům poškodit strategické a významné zájmy České republiky bez využití konvenčních prostředků. Neustále se zvyšuje počet a sofistikovanost kybernetických útoků proti veřejné a soukromé sféře. Tyto útoky mohou způsobit selhání zejména komunikačních, energetických a dopravních sítí či dopravních procesů, průmyslových nebo finančních systémů, mající za následek významné hmotné škody. Závislost ozbrojených sil státu na informačních a komunikačních systémech může mít vliv na obranyschopnost státu. S kybernetickými útoky zároveň úzce souvisí problematika politické a ekonomické špionáže". Česká republika výše uvedené skutečnosti reflektuje a postupně přijímá potřebná opatření. Přístup k řešení kybernetických útoků je však zatížen systémovými nedostatky. S ohledem na významný celospolečenský a technologický vývoj je potřebné změnit zažité formy a způsoby zajišťování obrany. V současné době je totiž na vzestupu forma asymetrického vedení konfliktů, kde významnou roli hraje využívání kyberprostoru.

V návaznosti na kybernetickou bezpečnost České republiky je pak nutné definovat specifické nástroje či opatření, která by měla být aktivována převážně ve chvílích, kdy kybernetické útoky mířené proti České republice budou takové intenzity a budou směřovat proti svrchovanosti, územní celistvosti, principům demokracie a právního státu, ochrany života obyvatel a jejich majetku[19)], že je již nebude možné zvládat běžnými prostředky a opatřeními kybernetické bezpečnosti, jak je v současnosti zná zákon o kybernetické bezpečnosti. Z výše uvedeného je patrné, že Česká republika potřebuje v rámci obranných kapacit prvek schopný provádět široké spektrum operací v kybernetickém prostoru, který by byl schopen aktivního využití prostředků kybernetické obrany a byl by schopen eliminace závažných kybernetických útoků mířených proti České republice a jejím zájmům. V neposlední řadě by měl mít tento prvek schopnost v případě ozbrojeného konfliktu provádět vojenské operace v kybernetickém prostoru na podporu konvenčních vojenských sil. Takový prvek by přispěl ke zvýšení odolnosti informačních a komunikačních systémů obranných složek a navýšily by se tak možnosti a kapacity v oblasti obrany státu.

Jako jeden z inspiračních zdrojů teoretických východisek pro řešení problematiky kybernetické obrany a bezpečnosti lze využít výstupy z Tallinského manuálu[20)], který se zabývá v rámci NATO kybernetickou bezpečností. Jedním ze základních dokumentů je Rámcový manuál k národní kybernetické bezpečnosti, který podává poměrně vyčerpávající teoretický základ k tvorbě národních strategií kybernetické bezpečnosti.

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

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

1. pravidla využívání infrastruktury a její ochrana,

[19)] § 2 odst. 1 zákona č. 222/1999 Sb., o zajišťování obrany České republiky.

[20)] Manuál NATO Cooperative Cyber Defence Centre of Excellence, dostupný online zde: https://ccdcoe.org/tallinn-manual.html.

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

2. ochrana kritické infrastruktury a národní krizový management,
3. boj proti kybernetické kriminalitě a kyberterorismu,
4. rozvědná a kontrarozvědná činnost v kybernetickém prostoru,
5. kybernetická obrana (ve vojenském smyslu).

Jak vyplývá z výše uvedeného, bezpečnost národního kybernetického prostředí závisí na mnoha aktérech s různými rolemi a úkoly, a na mnoha faktorech. Úspěšná ochrana tohoto prostoru se neobejde bez toho, aby úloha všech zainteresovaných subjektů byla jasně identifikována a popsána, aby si všichni tito aktéři uvědomili svoji sféru odpovědnosti a aby všichni měli k dispozici nezbytné prostředky k efektivnímu plnění svých úkolů. K naplnění těchto požadavků slouží mj. základní strategické dokumenty České republiky, Obrannou strategií počínaje (schválená usnesením vlády ze dne 26. září 2012 č. 699), přes Bezpečnostní strategii (schválená usnesením vlády ze dne 4. února 2015 č. 79), Národní strategii kybernetické bezpečnosti (schválená usnesením vlády ze dne 16. února 2015 č. 105) až k Akčnímu plánu k této strategii (schválená usnesením vlády ze dne 25. května 2015 č. 382). Národní centrum kybernetických operací vypracovalo v roce 2018 Strategii kybernetické obrany, která stanovuje koncepční podmínky pro řádné zajišťování obrany státu v kybernetickém prostoru pro období 2018 – 2022. Dokument definuje základní vizi a cíle, které popisují plánovaný vývoj kybernetické obrany v jednotlivých dílčích oblastech. Strategie je rozpracována do úrovně specifických cílů, které jsou popsány s takovou mírou podrobností, aby bylo možné zveřejnění tohoto dokumentu (strategie je dostupná na webu Vojenského zpravodajství).

Aby bylo možné zásadní požadavky výše zmíněných strategických dokumentů aplikovat, je nutné, aby byly vytvořeny právní podmínky pro jejich naplňování (zabezpečování). Právní řád z uvedených rovin poměrně uspokojivě upravuje podmínky pro zajišťování prvních čtyř rovin kybernetické bezpečnosti. Naopak poslední rovinou, tj. problematikou kybernetické obrany ve smyslu vojensko-zpravodajském, se dosud žádným způsobem nezabývá, resp. doposud byla vnímána jako imanentní součást opatření směřujících k zajištění obrany České republiky ve smyslu zákona č. 222/1999 Sb., a to zcela bez zohlednění významných specifik kybernetického prostoru pro zajišťování obrany České republiky. Vzhledem k tomu pak nelze při přípravě a samotném výkonu této činnosti využívat žádné zvláštní postupy a oprávnění, které ale jsou k této činnosti potřebné. Neexistence takové zvláštní právní úpravy jako části problematiky obrany v kybernetickém prostoru, a to včetně jejího vnímání jako zajišťování obrany České republiky jako součásti plnění základní povinnosti státu při zajišťování své bezpečnosti v širším slova smyslu, je nutné vnímat jako závažný nedostatek, který je navíc zvýrazněn technologickým vývojem především v oblasti sítí a služeb elektronických komunikací, na což právní úprava zajišťování obrany České republiky včas a požadovaným způsobem nezareagovala.

Kybernetická obrana jako taková je komplexní činnost, která v sobě zahrnuje řadu oborů a spojení různých expertních oblastí a činností. Jako samostatná doména vojenského působení je zcela odlišná od tradičních domén, ve kterých se obrana provádí (tedy pozemní, vzdušná, námořní, vesmírná), a to především proto, že je uměle vytvořena, nemá fyzické hranice a umožňuje skryté vedení operací, které je často složité detekovat, natož přisoudit jednoznačnému útočníkovi (jak již bylo výše uvedeno). Z těchto důvodů je kybernetická obrana v mnohem větší míře závislá na schopnosti získat relevantní informace, ať již o hrozbách, útočnících a jejich taktice, nebo o nástrojích potřebných k vedení útoku i obrany, možných zranitelnostech apod.

Zajišťování obrany České republiky v kybernetickém prostoru je velmi složitý, strukturovaný proces, náročný jak co do architektury jeho technického řešení, ale také co do požadavků na odborné znalosti a schopnosti jeho personální složky. Tento proces lze rozdělit do několika základních oblastí:

- zisk informací o hrozbách a zranitelnostech,
- detekce škodlivých aktivit,
- atribuce útočníka,
- detterence.

Samotná první oblast (zisk informací o hrozbách a zranitelnostech) je vlastním, složitým procesem, v rámci kterého dochází k získávání jak technických, tak strategických informací o hrozbách a zranitelnostech v kybernetickém prostoru. Na tuto oblast pak navazují identifikační činnosti, v rámci kterých jsou detekovány „škodlivé aktivity", tedy kybernetické útoky a hrozby směřující proti bráněným systémům. V praxi se nemusí vždy nezbytně nutně jednat o již probíhající kybernetický útok, ale lze například odhalovat již přípravné činnosti, které jsou k provedení útoku nezbytné.

S přihlédnutím k základnímu účelu tohoto dokumentu, tedy vyhodnotit věcný a právní stav regulace dané oblasti, potřeby jejího nového řešení a zejména nalezení optimálního právního řešení, které v praxi umožní a podpoří zabezpečování obrany České republiky v kybernetickém prostoru, je z analytického hlediska mimořádně důležitá také třetí z uvedených oblastí, tedy atribuce útočníka. Obsahem regulace této oblasti musí být nastavení schopností určit pravou totožnost zdroje kybernetického útoku, což je základem pro každou reakci na závažný kybernetický incident. Jedná se o spojení veškerých dostupných informací (nejen z kybernetického prostoru), pro navrhované normativní řešení je důležité posoudit efektivnost existujících zdrojů informací vypovídajících o ohrožení bezpečnosti České republiky a současně stanovit zdroje nové, obsahově jednoznačné a co do podmínek jejich získávání právně bezvadné.

Poslední oblastí celého procesu je detterence, tedy druh obrany, při kterém je snaha odvrátit útok, probíhající i budoucí, prokázáním schopnosti úspěšné atribuce.

Účelem zamýšlené regulace je vzhledem ke shora uvedenému doplnění systému obrany České republiky tak, aby bylo umožněno efektivněji

1. získávat poznatky o kybernetických hrozbách,
2. detekovat, že vůbec dochází, nebo se bezprostředně schyluje ke kybernetickému útoku,
3. určit konkrétní zdroj útoku, případně identifikaci směru odkud útok přichází, a
4. provádět aktivní obranu.

1.3 Popis existujícího právního stavu v dané oblasti

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

Existující právní úprava se věnuje těmto oblastem:

- **Využívání infrastruktury a rovněž zajištění její bezpečnosti** řeší zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů,

především hlava V., § 87 až 104, upravující ochranu údajů, služeb a sítí elektronických komunikací. Provozovatelům této infrastruktury a služeb ukládá řadu úkolů v oblasti zajištění jejich ochrany a bezpečnosti. Působnost v této oblasti má svěřenu Ministerstvo průmyslu a obchodu a Český telekomunikační úřad.

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

- Jednou z dalších rovin zmíněných výše je **boj proti kyberkriminalitě a kyberterorismu**. Ačkoli se jedná o dvě odlišné věci, zejména z hlediska cíle útoků, obecně jde o podobné jevy (navíc postihnutelné nástroji trestního práva). Určitou působnost v této oblasti mají také zpravodajské služby, a to z hlediska získávání informací o záměrech a činnostech směřujících vůči bezpečnosti ČR, základním činitelem je ale zejména Policie České republiky s ostatními orgány činnými v trestním řízení. Řada činností spadajících pod pojem kyberkriminalita nebo kyberterorismus je totiž podle českého trestního práva trestnými činy. V této oblasti je právní úprava poměrně pokročilá, české trestní právo kriminalizuje řadu jednání souvisejících s kybernetickým prostorem, a to zejména v návaznosti na mezinárodní instrumenty, zejména Úmluvu o počítačové kriminalitě z roku 2001 (v platnost vstoupila v roce 2004). Právní úpravu obsahuje trestní zákoník, konkrétně zejména § 230 (neoprávněný přístup k počítačovému systému a nosiči informací), § 231 (opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat), § 232 (poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti), § 182 (porušení tajemství dopravovaných zpráv), ale i další ustanovení odpovídající požadavkům Úmluvy. I některé jiné

skutkové podstaty trestných činů mohou být naplněny jednáním, které se uskuteční v kybernetickém prostoru. Mezi nejzávažnější lze určitě zařadit např. teroristický útok (§ 311) nebo vyzvědačství (§ 316).

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

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

  Na tento ústavní zákon pak ovšem navazují další zákony, které spojují a zaměřují institut obrany státu na hrozbu vnějšího napadení, tedy zejména zákon č. 219/1999 Sb., o ozbrojených silách, ve znění pozdějších předpisů, podle něhož „K zajišťování své bezpečnosti vytváří Česká republika ozbrojené síly. Základním úkolem ozbrojených sil je připravovat se k obraně České republiky a bránit ji proti vnějšímu napadení.“. Obdobně je obrana státu zaměřena proti vnějšímu napadení podle § 2 odst. 1 zákona č. 222/1999 Sb., o zajišťování obrany České republiky, který stanoví, že se jedná o „souhrn opatření k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením. Obrana státu zahrnuje výstavbu účinného systému obrany státu, přípravu a použití odpovídajících sil a prostředků a účast v kolektivním obranném systému“.

> Zapomenout ale nelze ani na zákon č. 153/1994 Sb., o zpravodajských službách, podle jehož § 2 zpravodajské služby jsou státní orgány pro získávání, shromažďování a vyhodnocování informací důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnost a obranu České republiky, a tedy se na zajišťování obrany státu také významně podílejí.

Konkrétní zmínka, resp. reflektování specifik kybernetického prostoru a jeho obrany v těchto zákonech zatím absentuje. V rámci uvedených právních předpisů by činnosti obsahově odpovídající kybernetické obraně mohly být prováděny, byť s určitým omezením, vyplývajícím z přece jenom značně odlišného prostředí, v němž by docházelo k aktivitám ohrožujícím bezpečnost České republiky. Pokud by se v oblasti kybernetického prostoru jednalo čistě o obranu státu proti vnějšímu napadení, pak by ozbrojené síly České republiky, resp. Armáda České republiky, mohly vyvíjet činnost i bez novelizace příslušných zákonů, stejně tak i další orgány mající za úkol zajišťovat bezpečnost státu. Bez navrhovaných úprav by však stát často ani nebyl schopen určit, kdo je původcem útoku, jaký je jeho pravý rozsah apod. Navíc vzhledem k povaze kybernetického prostoru není vždy jednoznačně možné okamžitě odlišit vnější a vnitřní napadení, a stejně tak není možné zcela přesně vyhodnotit, zda již jde o ozbrojený útok zakládající právo státu na sebeobranu ve smyslu mezinárodního práva nebo zda se jedná o čin charakteru teroristického, kriminálního nebo např. špionážního. Právní posouzení každé vzniklé situace jako vnějšího napadení opravňujícího ozbrojené síly České republiky k vojenské reakci by tedy bylo značně komplikované, což by se v praxi mohlo reálně projevit i neschopností adekvátně reagovat, resp. nemožností vůbec zasáhnout.

1.4 Identifikace dotčených subjektů

Dotčeným, resp. výkonným subjektem bude Vojenské zpravodajství, spolupráce ve významném rozsahu je předpokládána u Armády České republiky, Bezpečnostní informační služby, Úřadu pro zahraniční styky a informace, Národního úřadu pro kybernetickou a informační bezpečnost, Ministerstva zahraničních věcí, ale v individuálních případech také dalších státních orgánů a jiných právnických nebo také fyzických osob.

V návaznosti na novou roli Vojenského zpravodajství a nová oprávnění pak budou dotčeny právnické nebo podnikající fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací. Pro tyto dotčené subjekty platí, že jejich role je jedinečná, neboť požadovaná data a informace nelze zdrojově získat jiným způsobem, než s využitím jimi zajišťovaných veřejných komunikačních sítí.

1.5 Popis cílového stavu

Cílem navrhované regulace je v základní podobě upravit problematiku chybějících oblastí zajišťování obrany České republiky (a kybernetické bezpečnosti České republiky v širším smyslu), a tím docílit komplexního pojetí právní úpravy obrany České republiky. Jelikož ústavním požadavkem je, aby státní moc byla uplatňována jen v případech, v mezích a způsoby, které stanoví zákon, bude zákonem jednoznačně stanovena nová působnost a pravomoci Vojenského zpravodajství spočívající v podílení se na zajišťování obrany spočívající v povinnosti zasahovat proti těm nejintenzivnějším kybernetickým útokům a hrozbám způsobilým ohrozit základní státem chráněné zájmy, kterými jsou územní celistvost, demokratické základy, životy a zdraví, majetkové hodnoty a životní prostředí. K plnění takto vymezeného cíle je dále třeba mít k dispozici specifické nástroje, jejichž užití vůbec umožní detekovat kybernetické útoky. Narušení územní suverenity může stát vcelku pohodlně

monitorovat i bez zásahů do subjektivních práv nebo součinnosti třetích osob. V případě kybernetického prostoru se však bez této součinnosti a bez zásahů do práv (byť potenciálních) nelze obejít. Druhým neméně podstatným důvodem specifické zákonné úpravy je tedy založení mandatorní spolupráce právnických nebo podnikajících fyzických osob zajišťujících veřejnou komunikační síť nebo poskytujících veřejně dostupnou službu elektronických komunikací s Vojenským zpravodajstvím. Tento moment se od konvenční obranné agendy rovněž výrazně odlišuje. Mandatorní spolupráce s orgány obrany státu (která rovněž omezuje ústavou garantovaná práva – obvykle především právo na vlastnictví nebo právo na práci) je v konvenčních případech omezena na dobu, kdy je ohrožena suverenita státu. V tomto případě však je taková spolupráce nezbytná i mimo mimořádné stavy, a to vzhledem k povaze kybernetického prostoru a v něm nepřetržitě probíhajícím jevům, včetně těch negativních, ohrožujících ústavně chráněné zájmy – v daném případě České republiky; za tímto účelem musí být právnickým nebo podnikajícím fyzickým osobám zajišťujícím veřejnou komunikační síť nebo poskytujícím veřejně dostupnou službu elektronických komunikací uložena povinnost zřídit a zabezpečit na určených bodech těchto sítí rozhraní pro připojení technologií umožňujících získávat poznatky o kybernetických hrozbách.

1.6 Zhodnocení rizika

Riziko spojené s nepřijetím navržené úpravy spočívá zejména v tom, že činnosti, které dosud nejsou výslovně právními předpisy upraveny, tj. kybernetickou obranu, nelze plnohodnotně provádět bez součinnosti s některými soukromými subjekty, přičemž tuto součinnost a její pravidla lze nastavit jedině zákonnou cestou. Při nepřijetí úpravy by tak činnosti kybernetické obrany mohly sice být prováděny, ale ve značně omezeném, a tedy poměrně neúčinném režimu. Kromě toho by nebyl výslovně určen žádný orgán odpovědný za tuto oblast obrany státu, což by mohlo vést k tomu, že by se této činnosti řádně nevěnoval žádný státní orgán, anebo naopak by si tuto činnost osvojilo orgánů více. Ochrana kybernetického prostoru v České republice před narušením jak špionážními aktivitami, tak i dalšími útoky, by tak byla značně omezená, nesourodá a nesystémová (viz zákon č. 222/1999 Sb.).

2. Návrh variant řešení

Varianta I. (nulová)

Znamená zachování současného stavu. Zajištění kybernetické obrany zůstane v obecné rovině na Ministerstvu obrany a Armádě České republiky, jelikož jejím úkolem je bránit Českou republiku před vnějším napadením. Tato činnost však nebude mít žádná zákonná pravidla, Armádě České republiky nebude k provádění této činnosti svěřeno žádné speciální oprávnění. Kontrašpionáž, a tedy i kontrašpionáž v kybernetickém prostoru, zůstane úkolem BIS a Vojenského zpravodajství. Tyto zpravodajské služby však prozatím mají za úkol jen zabezpečování informací, tj. budou pouze zjišťovat kdo, jak a proč se pokouší nelegálně v kybernetickém prostoru získávat informace nebo vyvíjet aktivity proti ústavně chráněným zájmům České republiky vyvolávající potřebu využití konkrétních opatření systému obrany České republiky; o těchto zjištěních jsou zpravodajské služby povinny informovat oprávněné adresáty. Oproti současnému stavu nebudou mít svěřena rovněž žádná oprávnění, což vzhledem ke skutečnosti, že znění zákonů upravujících jejich činnost má původ v první polovině devadesátých let minulého století a jejich ustanovení o zpravodajské technice současný stav kybernetického prostoru nereflektují, znamená, že jejich schopnost reagovat na hrozby v kybernetickém prostoru zůstane značně omezená. Kybernetická bezpečnost v podobě, která je popsána v zákoně o kybernetické bezpečnosti, pochopitelně zůstane v působnosti Národního

úřadu pro kybernetickou a informační bezpečnost; současný stav regulace však upravuje zajišťování kybernetické bezpečnosti zásadně v pasivním módu, nepočítá tedy s žádnými prvky obrany aktivní, bez níž se v případě závažnějších útoků obejít nelze.

Realizace této varianty však nepřichází v úvahu, neboť jeho zpracování vychází ze zadaného úkolu vlády České republiky, která rozhodla o tom, že podmínky výkonu kybernetické obrany budou v konkrétní části řešeny samostatnou právní úpravou. Návrh zákona je tak zákonným promítnutím podmínek nezbytných pro realizaci úkolů, které vláda České republiky uložila svým usnesením ze dne 25. května 2015 č. 382, jímž 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. Návrhem zákona je rovněž plněn úkol C. 9.01 uvedeného Akčního plánu, tedy jsou navrhovány zákonné předpoklady pro výkon kybernetické obrany a vybudování Národního centra kybernetických sil (později přejmenovaného na Národní centrum kybernetických operací) v rámci Vojenského zpravodajství.

Dílčí závěr: *Tato varianta vylučuje dosažení vládou České republiky zadaného úkolu a navíc se stává překážkou pro provedení „aktualizace" opatření tvořících strukturu obrany České republiky z hlediska zohledněné specifik kybernetického prostoru.*

Varianta II.

Další ze zvažovaných variant bylo možné „pověření" Vojenského zpravodajství jako státního orgánu, který přímo zajišťuje obranu státu v kybernetickém prostoru.

Zákonem by se tak určilo, že kybernetická obrana není součástí obrany České republiky, ale jedná se o specifickou oblast vyžadující jiné pravomoci výkonu veřejné moci. Pro zajištění komplexnosti tohoto úkoly by bylo přiznáno Vojenskému zpravodajství oprávnění plošně monitorovat kybernetický prostor a přiznat pravomoc aktivně zasáhnout proti útokům.

Vojenské zpravodajství by bylo jak zpravodajskou službou, tak v oblasti kybernetického prostoru i „další, specifickou ozbrojenou" silou stanovenou mimo zákon o ozbrojených silách České republiky. V rámci kybernetického prostoru by mohlo provádět monitoring, který by bylo možné zákonně limitovat.

Dílčí závěr: *Tato varianta, byť je možné ji technicky popsat, v sobě skrývá tak mimořádné problémy právní, že je v zásadě ústavně neuchopitelná; z hlediska jednoznačných nepřímých novelizací jiných zákonů je nesystémová a zejména ústavně nekonformní.*

Varianta III.

Jednou z variant by mohlo být také rozšíření pravomocí Národního úřadu pro kybernetickou a informační bezpečnost i na sféru „aktivní" kybernetické obrany. Výhodou by bylo využití stejné vědomostní i technické základny, nicméně nevýhodou by bylo nežádoucí prolínání různých rovin a úrovní zajišťování kybernetické vnitřní a vnější bezpečnosti (obrany) v České republice. Institucionální specifikace jednotlivých výkonných kompetencí je v našem ústavním systému velmi důležitá. K přirozené konkurenci různých silových složek výkonné moci je u nás o to větší důvod, že máme na rozdíl např. od USA nebo západoevropských států důkladnou historickou zkušenost s koncentrací moci nad těmito složkami. Zakotvení nových oprávnění a nástrojů veřejné moci s sebou totiž nese potřebu adaptovat současné specifikační mechanismy tak, aby nedošlo na jedné straně k nějaké fatální institucionální nekoherenci, ale aby na straně druhé nevzniklo riziko stejně fatální koncentrace reálných silových pravomocí.

Na „pasivní“ zajišťování kybernetické bezpečnosti musí navazovat systém, který bude tzv. ultima ratio, tzn. ve chvílích, kdy běžný systém zajištění kybernetické bezpečnosti, jak jej zná současný zákon o kybernetické bezpečnosti, již nepostačuje, respektive již není na tento typ nebezpečí zaměřen, tedy ve všech případech, kdy je bezprostředně ohrožena svrchovanost, územní celistvost, demokratické základy České republiky nebo ve značném rozsahu vnitřní pořádek a bezpečnost, životy a zdraví, majetkové hodnoty nebo životní prostředí anebo je-li třeba plnit mezinárodní závazky o společné obraně, přičemž nelze vyloučit ani působení v rámci jednoho ze základních principů mezinárodního práva, tj. povinnost bdělosti (due diligence). Jde o podobný vztah, jako je při zajišťování bezpečnosti mezi Policií České republiky a Armádou České republiky. Obrana kybernetického prostoru bude aplikována při takových útocích, které již spadají do kategorie kyberterorismus nebo kybernetická válka (viz výše dělení kybernetických útoků), naopak by její aplikace a uplatnění pravomocí s kybernetickou obranou spojených v žádném případě neměla zasahovat do oblasti vymezené zákonem o kybernetické bezpečnosti, což navrhovaná právní úprava naopak plně respektuje.

Dílčí závěr: *Tato varianta III. proto není vhodná zejména právě z hlediska rozdělení kompetencí.*

Varianta IV.

Další zvažovaná varianta znamená doplnění stávajícího systému zajišťování bezpečnosti státu o právní nástroje v souvislosti se specifiky kybernetického prostoru a stávajícího právního stavu. Jedná se o doplnění systému zajišťování obrany České republiky ve fázi, kdy již není možné odolávat kybernetickým útokům pouze opatřeními kybernetické bezpečnosti v dikci zákona o kybernetické bezpečnosti (nebo dokonce jen běžnou činností soukromých subjektů, aniž by byl potřebný zásah veřejné moci).

Varianta počítá s umožněním detekovat ty nejzávažnější kybernetické útoky, aniž by muselo docházet k plošnému monitoringu komunikace. Možnost obrany proti útoku by byla zákonem jasně vymezena konkrétními pravidly a procesními postupy, aniž by bylo nutné vyhlašovat mimořádné stavy. Vojenské zpravodajství by mohlo zasáhnout pouze v případě naplnění zákonem stanovených podmínek a pouze v krajních případech, při zachování principu subsidiarity, tedy pouze v případě, že to nepůjde jinak a bude nutné zasáhnout bezprostředně. V ostatních případech by Vojenské zpravodajství zjištění, že dochází k útoku, předalo v rámci spolupráce kompetentnímu orgánu k přijetí nutných opatření, nejtypičtěji NÚKIB.

V této variantě jsou hodnoceny výše uvedené cíle z pohledu možného, ryze ústavního hlediska jejich dosažení. 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 „zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot je 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.“.

Tato varianta se proto zabývá řešením, formálně vycházejícím z provedení 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. Tato varianta vyhodnocuje podrobnosti, jimiž je nutné upřesnit 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 základních lidských práv a svobod 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.

Důvodem pro preferenci této varianty je, že kybernetický prostor není typické „kinetické“ válčiště, ale spíše prostor informační, kde velkou roli tradičně mají zpravodajské služby. Kromě toho vzhledem k povaze kybernetického prostoru není vždy jednoznačně možné odlišit vnější a vnitřní napadení, a stejně tak není možné zcela přesně vyhodnotit, zda již jde o ozbrojený útok zakládající právo na sebeobranu ve smyslu mezinárodního práva nebo zda se jedná o čin charakteru teroristického, kriminálního nebo např. špionážního. Z těchto hledisek se jeví jako nejvhodnější svěřit tento úkol zpravodajským službám, které jsou určeny k tomu, aby se podílely na zajišťování bezpečnosti státu v celém spektru hrozeb. Z ekonomických a praktických důvodů se pak jeví jako vhodné, aby to byla jen jedna ze služeb. Vzhledem k povaze kybernetické obrany z principu jako souhrnu opatření, prováděných v kybernetickém

prostoru, směřujících k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením[22)] pak konkrétně Vojenské zpravodajství jakožto vojenská zpravodajská služba, integrální součást Ministerstva obrany, podílející se na systému zabezpečování obrany státu[23)], což nabízí i další výhody, a sice jednodušší spolupráci s Armádou České republiky a z toho vyplývající snadné pokračování v činnosti v případě přechodu státu do mimořádných stavů. Podstatným argumentem pro tuto variantu je dále skutečnost, že zpravodajské služby jsou zvyklé své činnosti vykonávat v utajeném režimu, k čemuž jim právní řád již nyní dává i mnohé nástroje, které tak nebude nutné nově zavádět nebo měnit. Vojenské zpravodajství je navíc jedinou zpravodajskou službou České republiky s vnitřní i vnější působností, což je při činnostech v kybernetickém prostoru rovněž velmi významnou výhodou. Vojenské zpravodajství tak může při kybernetické obraně využít informací, které má k dispozici z jiných zdrojů.

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

Současný právní řád České republiky pojem „kybernetická obrana“ dosud nezná. Z toho vyplývá, že ji také žádný státní orgán nemůže provádět, zejména mohlo-li by přitom dojít k zásahům do základních lidských práv a svobod. Pokud bychom se dovolávali existující definice pojmu „obrana České republiky“, pak by i obranu kybernetického prostoru mohly zabezpečovat ozbrojené síly České republiky. Ve chvíli, kdy si ale uvědomíme, že kybernetická obrana je obsahově odlišná aktivita oproti standardní obraně proti vnějšímu útoku v tradičním smyslu tohoto pojmu, pak nutně musíme dojít k závěru, že zákonné vymezení výkonu oblasti kybernetické obrany, určení státního orgánu, který za ni bude odpovědný, a vymezení alespoň základních prostředků sloužících k této činnosti, je nezbytné. Nezbytnost provedení regulace pro oblast zajišťování kybernetické obrany totiž vychází z analýzy skutečností souvisejících s tím, že sledované aktivity mají několik podob a dimenzí, z nichž čistě vojenská (sebeobrana na základě ozbrojeného útoku podle mezinárodního práva) je pouze jedna z nich.

Vojenské zpravodajství má zákonem vymezenou působnost k zabezpečování informací, kromě jiného také ve prospěch zajišťování obrany České republiky, ne však k aktivní obraně České republiky. Provádění kybernetické obrany by alespoň v určitém rozsahu aktivní činností přesahující rámec zabezpečování informací nezbytně nutně bylo.

Státní moc lze uplatňovat jen na základě zákona a v jeho mezích. V okamžiku, kdy v rámci zajišťování kybernetické obrany bude nutné vyžadovat od právnických nebo

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

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

podnikajících fyzických osob zajišťujících veřejnou komunikační síť nebo poskytujících veřejně dostupnou službu elektronických komunikací jakoukoli součinnost nebo bylo-li by touto činností jakkoli zasahováno do základních práv a svobod osob, je nutné také tuto činnost stanovit zákonem.

Navrhovaná úprava pak při zajištění věcných aspektů kybernetické obrany současně vychází z nezbytnosti zajistit proporcionalitu mezi svěřenými nástroji a opatřeními jejího výkonu a dostatečnými zárukami proti jejich zneužití (pro jiné účely nebo proti nežádoucímu osobnímu nebo časovému rozsahu jejich účinků). Připravovaný právní rámec proto poskytuje záruky bránící jejímu zneužití, a to jednak v rámci jejího začlenění do podmínek a systému zajišťování obrany České republiky, jednak jednoznačným a předvídatelným nastavením rozsahu a podmínek užití nástrojů, pro které navrhovaná úprava vymezuje jednoznačné mantinely a právní limity užití.

Pravidla výkonu kybernetické obrany, stejně jako limity užití nástrojů detekce ve vztahu k ochraně demokratických principů a vyloučení svévole jejich užití nad stanovený zákonný rámec jsou jednoznačně a předvídatelně nastaveny zákonem, což poskytuje záruky nezneužití výkonu kybernetické obrany k jiným, než stanoveným účelům a zajišťování v rámci ní prováděných činností výlučně za nastavených pravidel.

Úmluva o ochraně lidských práv a svobod (vyhlášená sdělením MZV pod č. 209/1992 Sb.) v čl. 8 odst. 2 předvídá zásahy státní moci do práva na ochranu soukromí, jinak řečeno umožňuje takové zásahy 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.“. Z uvedené citace je zřejmé, že pro dosažení cílů Úmluvy je rozhodující kvalita zákonné úpravy.

Zásah do soukromí Úmluva povoluje za splnění tří kumulativních podmínek, a to

- naplnění účelu (tedy „v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných“). Účel bude patrně splněn vždy – ledaže by se jednalo o zneužití z nějakých zájmů osobních nebo komerčních; tímto rizikem se v zákoně netřeba zabývat, takové riziko je vždy a žádná norma mu zabránit nemůže.
- zachování přiměřenosti (tedy stavu, který Úmluva vyjadřuje slovem „nezbytné“). Nezbytnost se žádným způsobem normovat nedá, tak jako tak bude posuzována v každém individuálním případě, a bylo by zbytečné tento pojem v zákoně opakovat, Úmluva je vnitrostátně aplikovatelným právem.
- zajištění souladem se zákonem. Nemůže obstát argument typu „soulad se zákonem tu je, protože zákon máme takový, že umožňuje cokoliv“. Veřejná moc může postupovat jen způsobem zákonem stanoveným, musí obsahovat pozitivní normu.

Smyslem navrhovaných změn v žádném případě není snaha o omezení svobody fyzických osob, ale naopak jejich ochrana. Bude se jednat o cílenou detekci kybernetických útoků za pomocí nástrojů (detekce) umožňujících detekci jevů nasvědčujících existenci kybernetického útoku nebo hrozby za pomocí stanovených ukazatelů. Tyto nástroje detekce tedy nebudou plošně vyhodnocovat komunikaci a monitorovat prostředí kybernetického prostoru. Budou mít dopředu nadefinované ukazatele, které budou cíleně „zachytávat“ jevy, jejichž charakteristiky budou vypovídat o tom, že jsou hrozbou pro chráněné zájmy České

republiky. Bude se tedy jednat o záležitost principiálně obdobnou jako v případě vojenských radarů.

Daná varianta obsahuje záruky nezneužití svěřené působnosti, a to včetně začlenění oblasti kybernetické obrany do existujících systémů, pro něž uvedená ochrana platí obdobně. Varianta jednoznačně stanoví zákonné limity pro nakládání s daty, kdy mimo jiné také plně reflektuje požadavky vyřčené Ústavním soudem v rámci Nálezu Pl. ÚS 24/10, ve kterém byla posouzena zákonnost právní úpravy související s tzv. „data retention", tedy se shromažďováním a využíváním důvěrných dat. Navrhovaná úprava nepočítá s plošným uchováváním dat.

Obsahem této varianty je i zavedení důsledných specifických kontrolních mechanizmů. Počítá se se zavedením povinnosti auditovat činnosti nástrojů detekce a tyto údaje poskytovat pro potřeby kontroly. V návrhu se zavádí i nová funkce inspektora pro kybernetickou obranu, jakožto systémového doplnění kontrolních mechanizmů o nezávislou osobu, která bude zárukou zákonnosti výkonu svěřených oprávnění.

Dílčí závěr: *Tato varianta poskytuje záruky vysoké efektivity ve vztahu k zajišťování obrany České republiky a současně skýtá potřebné jistoty jejího začlenění do právního řádu jako zcela jednoznačného, předvídatelného a ústavně konformního řešení.*

3. Vyhodnocení nákladů a přínosů

3.1 Identifikace nákladů a přínosů

Přínosem varianty II., III. i IV. je legislativní zakotvení nositele specifických úkolů kybernetické obrany a nastavení jednoznačných, předvídatelných a kontrolovatelných podmínek jejího výkonu s přihlédnutím ke všem specifikům jejího zajišťování a začlenění do plného komplexu vnitřní bezpečnosti a obrany státu, včetně přiřazení odpovídající působnosti subjektům kybernetickou obranu vykonávajícím, čímž dojde ke zvýšení bezpečnosti České republiky. Tato činnost s sebou samozřejmě nese náklady, které mohou být jak na personál, tak na využívané technologie. Přímý přínos varianty I. není žádný, nicméně také kybernetická obrana prováděná bez konkrétních zákonem zakotvených instrumentů by určitý přínos k zabezpečení obrany České republiky měla, ale rovněž by nesla i určité finanční i jiné náklady, které by vzhledem k neregulativnímu zázemí byly náročnější jak co do organizace, tak co do vynakládaných finančních prostředků; otázkou by pak samozřejmě bylo, jak by byl takový stav časově udržitelný vzhledem k jeho nejednoznačnosti nesoucí s sebou riziko snížené efektivity.

3.2 Náklady

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

Varianta II. je – jak je již uvedeno v dílčím závěru – variantou ústavně problematickou, a tedy neudržitelnou. Z tohoto hlediska je jasné, že náklady na její realizaci by byly ze všech variant nejvyšší, protože marně vynaložené.

Varianta III. by znamenala rozšíření oprávnění Národního úřadu pro kybernetickou a informační bezpečnost o činnosti „aktivní" kybernetické obrany. Je pravděpodobné, že tato varianta by byla levnější než varianta IV., jelikož by bylo možné využít část personálních i technických aktiv, jež má NÚKIB k dispozici. S ohledem na postupné budování Národního centra kybernetických operací v rámci Vojenského zpravodajství se však tato skutečnost stává marginální. Navíc vzhledem k rozšíření úkolů o další, odlišný směr činnosti by bylo nutné i v této variantě personální stavy posílit a nákupu technických prostředků by se Česká republika také nevyhnula. Nevýhody této varianty z hlediska praktického byly popsány výše.

Varianta IV. znamená využití již budovaného pracoviště pro kybernetickou obranu v rámci Vojenského zpravodajství. Náklady spočívají jednak v prostředcích na kvalifikované pracovníky a jednak v nákupu sofistikovaných technických prostředků. Konkrétní výši nákladů nelze přesně určit, jelikož pracoviště bude budováno postupně a vždy v závislosti na dostupných rozpočtových prostředcích. Náklady tedy budou vždy výhradně záviset na ochotě vlády podporovat kybernetickou obranu České republiky. Zákon samotný proto žádné přímé náklady nepřináší, jelikož pouze otevírá možnost aktivně reagovat na kybernetické hrozby. Až teprve samotný faktický výkon této činnosti a budování schopností bude vyžadovat finanční prostředky, ale lze říci, že jejich výše bude flexibilní a bude záviset jedině na možnostech státních financí, obdobně jako je tomu u jiných oblastí zabezpečování obrany. V současné době se jedná zejména o nákup technických prostředků a platové prostředky na zaměstnance. V pozdějším období budou pravděpodobně klesat nutné výdaje na technické prostředky a vzhledem ke zvyšujícímu se počtu zaměstnanců budou růst platové výdaje. Odhady učiněné v rámci Vojenského zpravodajství počítají z počátku s náklady přibližně 300 milionů korun ročně s tím, že konkrétní údaje nelze s ohledem na svoji povahu ochrany národní bezpečnosti ventilovat. Bude tedy záležet zásadně na navazujících rozhodnutích o podobě a rozsahu tohoto pracoviště, přičemž vzhledem k citlivému charakteru této činnosti nelze v neutajované důvodové zprávě uvádět bližší údaje o jeho předpokládané podobě.

Veškeré finanční prostředky nezbytné pro zajištění výkonu kybernetické obrany podle navrhované regulace budou hrazeny z rozpočtové kapitoly Ministerstva obrany, a to bez požadavku na jakékoliv její navýšení.

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

3.3 Přínosy

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

3.4 Vyhodnocení nákladů a přínosů variant

	I.	II.	III.	IV.
Finanční náklady	2	1	3	3
Přínos pro obranu	2	5	4	4
Využití technických kapacit	1	2	4	5
Využití personálních zdrojů	1	2	5	4
Využití dosavadních schopností daného subjektu	1	1	3	5
Celkem	7	11	19	21

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

Klady a zápory možných variant řešení byly popsány výše. Návrh vychází v souladu s úkolem uloženým vládou v Akčním plánu k Národní strategii kybernetické bezpečnosti z varianty IV. Úkol aktivně se podílet na zajišťování kybernetické obrany a bezpečnosti v České republice bude zákonem svěřen Vojenskému zpravodajství, které k tomuto účelu buduje Národní centrum kybernetických operací. Vojenskému zpravodajství tak přibude nový úkol, který bude mít charakter podílení se na obraně státu nejen zabezpečováním informací, ale i možností aktivně reagovat na kybernetické útoky.

Novela zákona č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů, rozšíří působnost Vojenského zpravodajství s tím, že teprve zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, upraví konkrétní podmínky provádění „kybernetické obrany“, schvalovací proces u opatření majících charakter zásahu do práv třetích osob, a dále stanoví oprávnění požadovat po podnikatelích v oblasti elektronických komunikací součinnost spočívající v umožnění nasazení nástrojů detekce.

Novela zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, pak stanoví povinnosti odpovídající oprávněním Vojenského zpravodajství.

Hospodářský dopad předkládaného návrhu lze očekávat pouze u úzké skupiny osob, které jsou subjekty zajišťujícími sítě nebo služby elektronických komunikací a které budou osloveny s žádostí o součinnost. Tyto osoby budou pravděpodobně částečně ovlivněny právě nutností tuto součinnost poskytnout, nicméně návrh předpokládá úhradu účelně vynaložených nákladů těmto osobám vzniklých. Na druhou stranu je možné očekávat pozitivní hospodářský dopad v případech, kdy činností Národního centra kybernetických operací dojde k odvrácení nebo minimalizování kybernetického útoku, který by jinak měl na hospodářství škodlivé následky. Finanční dopad bude návrh mít pouze na rozpočet Ministerstva obrany (bez požadavku na jeho navýšení).

Z pragmatického pohledu bude značnou výhodou i skutečnost, že výdaje na činnost Národního centra kybernetických operací mají charakter výdaje na obranu v kontextu závazku České republiky vůči NATO.

4. Stanovení pořadí variant a výběr nejvhodnějšího řešení

Na základě vyhodnocení nákladů a přínosů v jednotlivých variantách tak, jak je provedeno v kapitole 3, byla zvolena k realizaci normativního řešení varianta IV, a to pro její systémovost, postižení všech realizačních vazeb a ústavní konformnost.

5. Implementace doporučené varianty a vynucování

Za implementaci řešení bude odpovědné Ministerstvo obrany a jeho součást Vojenské zpravodajství. Implementace doporučeného řešení si v rámci tohoto orgánu nevyžádá žádné zvláštní postupy. Po některých vybraných podnikatelích a dalších osobách v oblasti elektronických komunikací bude do budoucna vyžadována součinnost ohledně připojení nástrojů detekce kybernetických útoků. K nasazení těchto nástrojů bude docházet postupně, a to pouze v místech nutných pro zajištění obrany státu, ve spolupráci s dotčenými subjekty a za jejich součinnosti. Návrh nenařizuje přijetí žádných okamžitých opatření, pouze umožňuje do budoucna tato opatření přijmout.

Vynucování by přicházelo v úvahu jedině u předpokládané součinnosti podnikatelů a dalších osob v oblasti elektronických komunikací. Návrh předpokládá správní řízení o nasazování nástrojů detekce, je teda garantován i případný soudní přezkum. Pouze v případě, že by praxe ukázala problémy s ochotou poskytovat Vojenskému zpravodajství součinnost při plnění úkolů spojených se zajišťováním kybernetické obrany, zákon obsahuje i donucovací mechanismy ve formě nové skutkové podstaty přestupku. Dále může být cestou přestupků vynucována povinnost mlčenlivosti zúčastněných osob. Jedná se o nástroje, které v obdobném provedení již nyní obsahuje zákon o elektronických komunikacích pro vynucení celé řady povinností. O těchto přestupcích bude rozhodovat Český telekomunikační úřad.

6. Přezkum účinnosti regulace

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

7. Konzultace a zdroje dat

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

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

8. Kontakt na zpracovatele RIA

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