352—364

GLOSA

Kybernetická obrana a novela zákona o Vojenském zpravodajství

Jan Svoboda* – Jakub Vostoupal**

Abstrakt: V rámci tohoto článku se autoři soustředí na zhodnocení novely zákona o Vojenském zpravodajství, která legislativně ukotvuje právní úpravu kybernetické obrany a svěřuje ji do působnosti Vojenského zpravodajství. V první řadě se věnují vymezení pojmů kybernetická bezpečnost a kybernetická obrana v českém pojetí a sledují legislativní pouť zmíněné novely včetně neúspěšného prvního návrhu. Následně se zaměřují na vhodnost Vojenského zpravodajství jakožto subjektu odpovědného za materii kybernetické obrany, přičemž provádí porovnání i s dalšími potenciálními subjekty, konkrétně Národním úřadem pro kybernetickou a informační bezpečnost, Armádou ČR a dalšími zpravodajskými službami. V další části se pak zaměřují na analýzu právní úpravy vybraných aspektů zajišťování kybernetické obrany z pohledu proporcionality jednotlivých zásahů a rizik kumulace moci. V první řadě se věnují detekci kybernetických útoků a hrozeb, což představovalo v případě prvního návrhu jeden z nejproblematičtějších aspektů. Poté se věnují institutu inspektora pro kybernetickou obranu jakožto jedné ze záruk proporcionality v rámci nových pravomocí Vojenského zpravodajství. Analýzu zakončují stručným pojednáním o aktivním zásahu.

Klíčová slova: kybernetická bezpečnost, kybernetická obrana, Vojenské zpravodajství, detekční činnost, aktivní zásah, proporcionalita

Úvod

Nestává se příliš často, aby se stát jako Česká republika stal vzorem v regulaci určité oblasti. U právní úpravy kybernetické bezpečnosti se to ovšem povedlo. Když byly v letech 2010–2011 zahájeny přípravné práce na českém zákoně o kybernetické bezpečnosti,[1] byla Česká republika mezi prvními státy, které se touto oblastí na legislativní úrovni začaly zabývat. Při koncepci zákona neměli jeho tvůrci k dispozici žádný zahraniční zdařilý a funkční model, kterým by se mohli inspirovat.[2] Předpis se nakonec rozhodli založit na performativních pravidlech a tzv. chytré regulaci (tedy tlaku na poskytování relevantních informací kompetentním orgánům, které pak mohou situaci ovlivňovat např. skrze reaktivní opatření). I díky tomu nebylo potřeba do zákona extenzivně zasahovat po přijetí směrnice NIS[3] v rámci její implementace.[4]

* Mgr. Jan Svoboda, LL.M., je Cybersecurity Design & Engineering Manager ve skupině SUSE a doktorand na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. E-mail: jan.svoboda@mail.muni.cz. ORCID: https://orcid.org/0000-0001-9086-0415. Vznik tohoto článku byl podpořen projektem MUNI/A/ 1293/2022 (*Právo a technologie XI*).

** Mgr. Jakub Vostoupal je odborným pracovníkem v rámci projektů Národního centra kompetence pro kyberbezpečnost a doktorand na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. E-mail: jakub.vostoupal@law.muni.cz. ORCID: https://orcid.org/0000-0002-1669-9931.

1 Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.

2 Viz POLČÁK, R. et al. *Právo informačních technologií*. Praha: Wolters Kulwer, 2018, s. 587.

3 Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

4 POLČÁK et al. *Právo informačních technologií*, s. 587–589.

Příběh kybernetické obrany je, bohužel, příběhem diametrálně odlišným. V českém právním řádu totiž nebyla až donedávna blíže upravena. Změnit se to povedlo až 31. března 2021, kdy vstoupila v platnost novela zákona č. 289/2005 Sb., o Vojenském zpravodajství, s účinností od 1. července 2021. Nelichotivý kontrast těchto dvou příběhů je pak zvýrazněn skutečností, že NATO již v roce 2016 oficiálně uznalo kyberprostor jako čtvrtou operační doménu. Členské státy tak musí již několik let pracovat na vybudování odpovídajících obranných kapacit v rámci tohoto prostoru (a pro to musí být představen i odpovídající legislativní rámec).[5]

Český zákonodárce se rozhodl pověřit kybernetickou obranou České republiky Vojenské zpravodajství (dále jen jako „VZ“).[6]

Cílem tohoto textu je zhodnotit vybrané aspekty nově zvoleného přístupu ke kybernetické obraně v rámci výše uvedené novely, zejména pak právě výběr VZ jakožto organizace odpovědné za tuto oblast, legislativní ukotvení detekční činnosti, aktivního zásahu a role nově zavedené funkce inspektora pro kybernetickou obranu.

1. Kybernetická bezpečnost a kybernetická obrana

Pojmy „kybernetická bezpečnost“ a „kybernetická obrana“ jsou pro pochopení zmiňované novely klíčové. Naneštěstí však postrádají univerzálně přijímanou definici. Jejich výklad se liší nejen mezi jednotlivými profesemi, ale také napříč mezinárodním společenstvím. Pohled, jakým určitý státní aktér chápe kyberprostor, se pak propisuje i do jeho chápání pojmů kybernetická bezpečnost a kybernetická obrana (např. Ruská federace chápe kyberprostor toliko jako součást informačního prostoru a kybernetickou bezpečnost pak chápe jenom jako součást informační bezpečnosti, nikoliv specifické odvětví).[7] V následující podkapitole stručně popíšeme, jak jsou tyto pojmy obecně vykládány v České republice a jak je pro účely tohoto textu používáme i my.

1.1 Kybernetická bezpečnost

Kybernetickou bezpečnost lze vnímat v širším a užším slova smyslu, což je skutečnost, která zpřehlednění situace příliš nepomáhá.[8] V širším slova smyslu pod kybernetickou bezpečnost spadá mj. i materie kybernetické obrany, která je tím pádem ovlivněna stejnými hodnotami.[9]

České pochopení tohoto pojmu je dle našeho názoru i ve srovnání se zahraničím relativně holistické a detailní. V textu zákona jej však najít nelze (což ostatně není nijak

---

5 Viz MINÁRIK, T. NATO Recognises Cyberspace as a Domain of Operations at Warsaw Summit [online]. In: *CCDCOE*. 2016 [cit. 2022-09-18]. Dostupné z: <https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/>.

6 Viz hlavu II část čtvrtou zákona o Vojenském zpravodajství.

7 Viz FEIX, M. – PROCHÁZKA, D. Aktuální úkoly kybernetické obrany rezortu Ministerstva obrany. *Vojenské rozhledy*. 2017, roč. 26, č. 3, s. 31–50. DOI:10.3849/2336-2995.26.2017.03.031-050.

8 Viz LORENTS, P. – OTTIS, R. *Cyberspace: Definition and Implications*. Dayton, OH, US: Academic Publishing Limited, 2010.

9 Pro lepší vizualizaci tohoto vztahu odkazujeme na obrázek č. 2 ve FEIX, M. – PROCHÁZKA, D. *Aktuální úkoly kybernetické obrany rezortu Ministerstva obrany*; také viz Kybernetická obrana. In: *Vojenské zpravodajství* [online]. 2021 [cit. 2022-09-25]. Dostupné z: <https://www.vzcr.cz/kyberneticka-obrana-46>.

neobvyklé[10]). Definice se místo toho nalézá v Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020: *„Kybernetická bezpečnost představuje souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost. Kybernetická bezpečnost pomáhá identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury. Hlavním smyslem kybernetické bezpečnosti je pak ochrana prostředí k realizaci informačních práv člověka.“*[11]

Pro posuzování vhodnosti nástrojů zakotvených novelou zákona o Vojenském zpravodajství je pak zvláště důležitá poslední věta uvedené definice, která se dotýká hodnotového rozporu mezi Alexym a Dworkinem ohledně legitimity bezpečnostních opatření a zásahů.[12] Český přístup se, pravděpodobně i na základě dědictví minulého režimu,[13] přiklonil k názorům Dworkina a *„co do své teleologie se nespokojuje s konstatováním, že nové regulatorní nástroje jsou potřebné prostě proto, že zvyšují míru bezpečnosti. Každá komponenta našeho systému kyberbezpečnosti musela namísto toho projít obsahovým testem vzhledem ke konkrétnímu přínosu pro distributivní práva člověka“* (tedy např. práva na informační sebeurčení – pozn. autorů).[14] Stejně tak i konkrétní nástroje kybernetické obrany musí projít shodným testem potřebnosti, vhodnosti a proporcionality v kontextu distributivních práv člověka.

1.2 Kybernetická obrana

Ani české pochopení kybernetické obrany není ukotveno v textu zákona. I zde se tak vznášejí nad pojmem určité pochybnosti, např. ohledně zahrnutí prvků aktivní obrany.[15] V mnohém je však možné vycházet z pojmu *„obrany“* ve smyslu § 2 odst. 1 zákona č. 222/ 1999 Sb., o zajišťování obrany České republiky.[16] Feix a Procházka pak obranu zjednodušují jako *„kombinaci defenzivních a ofenzivních činností a opatření, ať už aktivního, či pasivního charakteru,“*[17] přičemž kybernetickou obranu vykládají jako *„obranu v kyberprostoru a skrze (prostřednictvím) něj“*.[18] Rozdíl mezi kybernetickou bezpečností v užším

10 FISCHER, E. A. *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*. New York: Nova Science Publishers, 2009, s. 6. Dostupné z: <http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=281158>.

11 Viz NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020*. Dostupné z: <https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2015-2020.pdf>.

12 Viz POLČÁK et al. *Právo informačních technologií*, s. 587–589.

13 V tomto režimu se nedistributivní práva hojně zneužívala k zásahům do lidských práv a svobod.

14 Viz POLČÁK et al. *Právo informačních technologií*, s. 589.

15 Viz FEIX, M. – PROCHÁZKA, D. *Aktuální úkoly kybernetické obrany rezortu Ministerstva obrany*.

16 *„Obrana státu je 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“* – § 2 odst. 1 zákona č. 222/1999 Sb., o zajišťování obrany České republiky.

17 Viz FEIX, M. – PROCHÁZKA, D. *Aktuální úkoly kybernetické obrany rezortu Ministerstva obrany*.

18 Ibidem.

slova smyslu a kybernetickou obranou je pak (zjednodušeně řečeno) v intenzitě a druhu útoků, které jsou schopné relevantní systémy aktivovat, a v povaze opatření, kterých je možné využít. Kybernetická obrana totiž nenabízí pouze souhrn preventivních a běžných reaktivních opatření, ale také možnost ofenzivní obrany (a budování kapacit pro tuto obranu). Takováto ofenzivní obrana může mít i podobu preventivního zásahu, který povede k odvrácení reálně hrozícího útoku.[19] Je však nutné upozornit, že zvláště ofenzivní kapacity kybernetické obrany je možné využít až jako řešení „poslední instance".

2. Vývoj právní úpravy kybernetické obrany v ČR

Na národní úrovni bylo prvním významným krokem směrem k ukotvení kybernetické obrany přijetí Národní strategie kybernetické bezpečnosti na období let 2015–2020[20] a souvisejícího Akčního plánu, ve kterém bylo zajišťováním kybernetické obrany pověřeno VZ.[21] Akční plán byl následně schválen v rámci usnesení vlády č. 382/2015 a již toto pověření, v kombinaci se zákonem o Vojenském zpravodajství a zákonem o zpravodajských službách[22], nabízelo určité možnosti a pravomoci, kterých bylo ze strany VZ možné využít k zajišťování kybernetické obrany ČR a k budování příslušných kapacit (ve smyslu defenzivní obrany).[23, 24] Akční plán je však pouze koncepčním nástrojem a zakotvit nové pravomoci a nástroje zvláště pro ofenzivní obranu nemůže ani při schválení usnesením vlády. Již při přijímání Akčního plánu se tak počítalo s budoucím zákonným ukotvením, ve kterém budou tyto aspekty upraveny.[25]

K zákonnému ukotvení kybernetické obrany došlo v rámci novely zákona o Vojenském zpravodajství, jejíž první návrh spatřil světlo světa v roce 2016. Ten se ovšem setkal s bouřlivou reakcí. Pravděpodobně nejkontroverznějším bodem návrhu se stala pravomoc monitorovat tok dat na internetu. Návrh pro tyto účely představoval tzv. sondy, zařízení VZ, která měla být umístěná do uzlů sítí pod správou poskytovatelů služeb informační společnosti.[26] Zde je nutné podotknout, že schopnost detekovat anomální chování/situace je jedním z nejdůležitějších procesů efektivního zajištění kybernetické obrany. Schopnost takovéto chování/situace detekovat je ovšem závislá na relativně značném

---

19 Na podobné téma viz HELLER, K. J. The Unlawfulness of a "Bloody Nose Strike" on North Korea. *International Law Studies*. 2020, Vol. 96, s. 1–25.

20 Viz NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020*.

21 Konkrétně úkoly C. 9.01 ad. Viz NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI. *Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020*. 2015. Dostupné z: <https://nukib.cz/download/publikace/strategie_akcni_plany/akcni_plan_2015-2020.pdf>.

22 Zákon č. 153/1994 Sb., o zpravodajských službách České republiky.

23 Viz MAGDOŇOVÁ, J. Šéf Vojenského zpravodajství: Čas je v kyberobraně klíčový, novela zákona všechna bílá místa nesmaže. In: *iROZHLAS* [online]. 8. 7. 2020 [cit. 2022-09-29]. Dostupné z: <https://www.irozhlas.cz/veda-technologie/technologie/jan-beroun-vojenske-zpravodajstvi-kyberutok-kyberbezpecnost-hackeri_2007080705_gak>.

24 Informace, která se často šířila v rámci debat o novele zákona o Vojenském zpravodajství, tedy že Česká republika je v rámci kyberprostoru bezbranná a VZ nemá příslušné nástroje a pravomoci k zajištění kybernetické obrany, tudíž nebyla úplně pravdivá.

25 Viz MAGDOŇOVÁ, J. *Šéf Vojenského zpravodajství: Čas je v kyberobraně klíčový, novela zákona všechna bílá místa nesmaže*.

26 Viz NOVÁK, J. Příběh novely zákona o Vojenském zpravodajství: od černých krabiček ke spolupráci. In: *Root.cz* [online]. 18. 11. 2020 [cit. 2022-09-26]. Dostupné z: <https://www.root.cz/clanky/pribeh-novely-zakona-o-vojenskem-zpravodajstvi-od-cernych-krabicek-ke-spolupraci/>.

zásahu do soukromí uživatelů a problémem sond se stala jednak obava z toho, že skrze ně bude možné číst obsah komunikace, jednak i to, že byly i pro zapojené poskytovatele služeb informační společnosti netransparentní.[27]

Návrh byl i v jiných aspektech nešťastně formulován (i prezentován). Nebyl dostatečně diskutován s odbornou veřejností a zúčastněnými osobami a ani přínosy, které by představoval, nepřevažovaly nad zásahy do distributivních práv. Nakonec se ani nestihlo projednání pozměňovacích návrhů či plnohodnotná debata se zástupci Ministerstva obrany když, i kvůli volbám, nebylo v legislativním procesu pokračováno.[28]

Neúspěch prvního návrhu pak vedl k zásadnímu přepracování ze strany Ministerstva obrany, ke kterému byli tentokrát přizváni i zástupci soukromého sektoru, i ke změně jeho prezentace.[29] I to pravděpodobně vedlo k tomu, že legislativní proces novely zákona o Vojenském zpravodajství dne 31. 3. 2021 zdárně skončil.[30]

3. Zapojení VZ do kybernetické obrany

Jednou z klíčových otázek již v roce 2015 bylo, komu agendu kybernetické obrany vůbec svěřit. Před tím, než došlo k vydání zmíněného Akčního plánu a svěření materie VZ, byla ze strany NBÚ vypracována analýza požadavků spojených se zabezpečováním kybernetické obrany.[31] Mimo jiné se v ní uvádí, že zajišťování kybernetické obrany v sobě zahrnuje prvky *„utajení, mezinárodní spolupráce, výměny zpravodajských informací i nutnosti operativního nákupu techniky“*.[32, 33] Jedná se tak v zásadě o činnost, která kombinuje aspekty vojenských a zpravodajských aktivit, kvůli čemuž došlo k vybrání VZ.[34] Ale protože v minulosti byla volba VZ pro zajišťování kybernetické obrany označena za koncepčně zcela odtrženou od dosavadní ochrany kybernetického prostoru,[35] zaměříme se v následujících řádcích na zhodnocení této volby v kontextu dalších možných kandidátů a právě představených prvků zajišťování kybernetické obrany.

---

27 Ibidem.

28 Ibidem.

29 Ibidem.

30 I přestože došlo ke značnému přepracování návrhu a odstranění mnoha kontroverzí, z finálního návrhu rozhodně nepanovalo všeobecné nadšení. Svaz průmyslu a dopravy ČR dokonce ve svém stanovisku z 27. dubna 2020 uvádí, že se Ministerstvo obrany rozhodlo *„nevyslyšet zásadní připomínky civilního sektoru a nabídky možných alternativ k realizaci zamýšlených nástrojů“* a dále kritizovalo schvalovací proces, který probíhal v rámci vyhlášeného nouzového stavu kvůli pandemii covidu-19, což značně snižovalo transparentnost celého procesu. Viz SVAZ PRŮMYSLU A DOPRAVY ČESKÉ REPUBLIKY. *Stanovisko Svazu průmyslu a dopravy České republiky k návrhu zákona, kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství*. 2020. Dostupné z: <https://www.spcr.cz/images/SPCR-stanovisko_novela_VOZ-2020-04-27.pdf>.

31 MAGDOŇOVÁ, J. *Šéf Vojenského zpravodajství: Čas je v kyberobraně klíčový, novela zákona všechna bílá místa nesmaže*.

32 Ibidem.

33 Problematické aspekty poslední zmíněné kategorie rozebírají jak Polčák a ostatní, tak brigádní generál Miroslav Feix v rozhovoru pro Lupa.cz. Viz POLČÁK et al. *Právo informačních technologií*, s. 623; SEDLÁK, J. Miroslav Feix (Armáda ČR): Kyberzbraně si musíme vždycky kupovat „od kamarádů“. In: *Lupa.cz* [online]. 30. 9. 2021 [cit. 2022-09-25]. Dostupné z: <https://www.lupa.cz/clanky/miroslav-feix-armada-cr-kyberzbrane-si-musime-vzdycky-kupovat-od-kamaradu/>.

34 Viz MAGDOŇOVÁ, J. *Šéf Vojenského zpravodajství: Čas je v kyberobraně klíčový, novela zákona všechna bílá místa nesmaže*.

35 ČESKÁ ADVOKÁTNÍ KOMORA. Stanovisko ČAK k návrhu zákona o kybernetické obraně. In: *CAK.cz* [online]. 2020 [cit. 2022-09-29]. Dostupné z: <https://www.cak.cz/scripts/detail.php?id=16787>.

3.1 Kdo, když ne my?

Přistoupíme-li ke kybernetické obraně jako k (zejména adresné) složce kybernetické bezpečnosti, mohlo by se jevit účelným kybernetickou obranu svěřit některému z těles již nyní působících v bezpečnostní oblasti na základě zákona o kybernetické bezpečnosti. V úvahu tedy připadá zejména Národní úřad pro kybernetickou a informační bezpečnost (dále jen jako „NÚKIB") a vládní CERT, které již mají svou zkušenost jak s utajením, tak i mezinárodní spoluprací. A přestože je NÚKIB garantem kybernetické bezpečnosti v ČR (zejména neadresné), postrádá zmíněný zpravodajský a vojenský mandát i odpovídající kapacity. Pokud by tudíž NÚKIB byl vybrán, bylo by nutné tuto volbu široce systémově zakotvit, poskytnout nezanedbatelné prostředky na vytvoření kapacit, a i poté by byl buď ve veškerém fungování v rámci kybernetické obrany odkázán na sdílení informací od zpravodajských služeb či by se *de facto* sám stal čtvrtou zpravodajskou službou. I při ignorování malé politické popularity obdobných kroků se tato volba ve výsledku jeví jako podstatně méně vhodná varianta.

Druhým kandidátem pak je, s ohledem na vojenskou povahu provozovaných aktivit, Armáda ČR. Její působení a případné nasazování je ovšem striktně limitováno zákonem, což by vedlo k tomu, že zajišťování kybernetické obrany by bylo ve výsledku velmi neefektivní a spíše sporadické. Je nutné zdůraznit, že oproti tomu VZ není složkou ozbrojených sil podle zákona č. 219/1999 Sb., o ozbrojených silách České republiky, ale ozbrojenou zpravodajskou službou. Zabezpečování kybernetické obrany tak není závislé na vyhlašování mimořádných stavů.[36, 37] Navíc, i v případě Armády ČR zůstává argument absentujícího zpravodajského mandátu, kapacit a nástrojů.

Poslední množinou relevantních kandidátů, nabízejících odpověď na nedostatky těch zbývajících, pak logicky jsou zpravodajské služby – Bezpečnostní informační služba a Úřad pro zahraniční styky a informace. Obě mají zpravodajský mandát, obě mají zkušenosti s utajením i mezinárodní spoluprací, ale pokud pomineme očividné postrádání vojenského aspektu (obě jsou civilní zpravodajské služby), je zde ještě jeden problém: působnost. Bezpečnostní informační služba a Úřad pro zahraniční styky by při zajišťování kybernetické obrany musely velice úzce spolupracovat dle toho, zda by se cíl aktivit nacházel v rámci ČR nebo zahraničí, což dle našeho soudu není na efektivní úrovni proveditelné. Oproti tomu VZ je zpravodajskou službou s vnitřní i vnější působností najednou.

3.2 Koncepčně vhodné?

Na základě výše uvedeného se zdá, že jiný již existující subjekt není vhodnějším pro zajišťování kybernetické obrany než VZ. Je tedy pověření VZ koncepčním úkrokem stranou, či nikoliv?

Pokud se zaměříme na schopnost působení v informační rovině, zpravodajské služby jsou dle definice v § 2 odst. 1 zákona č. 153/1994 Sb., o zpravodajských službách *„státní*

[36] Viz Kybernetická obrana. In: *Vojenské zpravodajství* [online]. 2021 [cit. 25. 9. 2022]. Dostupné z: <https://www.vzcr.cz/kyberneticka-obrana-46>.

[37] I Armáda ČR má své vlastní kyberjednotky, konkrétně Velitelství kybernetických sil a informačních operací. Jejich nasazení je však limitované válečným stavem a mezinárodním humanitárním právem. Více viz SEDLÁK, J. *Miroslav Feix (Armáda ČR): Kyberzbraně si musíme vždycky kupovat „od kamarádů"*.

orgány pro získávání, shromažďování a vyhodnocování informací důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnost a obranu České republiky“. Je tedy logické, že zpravodajské služby vyvíjely činnost v oblasti kybernetického prostoru již před danou novelou. Tyto činnosti se přitom mohou týkat jak získávání informací o hrozbách majících původ v tomto prostoru, tak v získávání informací prostřednictvím kyberprostoru. V informační rovině tak není důvod pro to, aby zpravodajské služby nevyvíjely svou činnost v kyberprostoru i bez přijetí zde rozebírané novely.

Co se dalších pravomocí v rámci úpravy kybernetické obrany týká, ani zde není důvod pro to uzavřít, že se jedná – z legislativního pohledu – o nekoncepční řešení. Důvodem je, že § 5 odst. 4 zákona o zpravodajských službách výslovně zakotvuje, že zpravodajským službám mohou být na základě zákona (tedy tak, jak se právě stalo) uloženy i další úkoly. A proto, i když se zpravodajská služba na poli kybernetické obrany možná na první pohled jeví poněkud nezvykle, není možné její zákonné pověření považovat za nekoncepční ani z věcné, ani z legislativní roviny. Např. Polčák v publikaci *Právo informačních technologií* z roku 2018, konkrétně v podkapitole 12.9, již VZ s obranou státu výslovně spojuje.

Co však lze považovat za legislativně nekoncepční, je dopad předmětné novely, která neupravuje jen zákon o Vojenském zpravodajství, ale i zákon o zpravodajských službách. Konkrétně lze problém spatřovat v zařazení § 2 odst. 2, který uvádí: „*Vojenské zpravodajství se v rozsahu a způsobem stanoveným zákonem o Vojenském zpravodajství podílí na zajišťování obrany České republiky v kybernetickém prostoru.*“ Toto ustanovení je nadbytečné, neboť upravená skutečnost by automaticky vyplývala z novelizovaného znění zákona o Vojenském zpravodajství ve spojení s do té doby účinnou verzí zákona o zpravodajských službách. Hlavně ale může být chybně vykládáno, za použití argumentu *a contrario*, že se ostatní zpravodajské služby na této činnosti nemohou jakkoli spolupodílet, což, jak pevně věříme, není cílem. S podivem přitom je, že zákonodárce toto ustanovení zařadil i přesto, že byl na jeho problematičnost upozorněn v rámci připomínkového řízení.[38]

Otázkou by však nemělo být pouze, zda je výběr VZ jakožto hlavní složky zajišťující kybernetickou obranu ospravedlnitelný, např. z koncepčního hlediska, ale zda je i vhodný. Při kybernetické obraně je rozhodující právě dostatek informací. Ze své podstaty by tak zpravodajská služba měla být vhodným subjektem pro výkon předmětné agendy. Co se týče personálního obsazení, ani v této oblasti není důvod se domnívat, že zde bylo Vojenské zpravodajství v nevýhodě oproti jinému subjektu taktéž závislému na veřejných rozpočtech. Zisk potřebných odborníků tak v tomto ohledu není nikterak ztížen oproti jiným variantám.[39] I z pohledu věcné způsobilosti se tak Vojenské zpravodajství jeví jako vhodná volba.

Problémem by však mohla být kumulace moci. To nejen v rukou zpravodajských služeb vůči zbytku veřejných orgánů, ale v rukou VZ vůči zbylým dvěma službám (za připomínku stojí i např. výše nastíněný problém s možným omezujícím výkladem dosavadní

38 ÚŘAD PRO ZAHRANIČNÍ STYKY A INFORMACE. Připomínky Úřadu pro zahraniční styky a informace k návrhu zákona, kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony. In: *Aplikace ODok* [online]. 2019 [cit. 2021-12-10]. Dostupné z: <https://apps.odok.cz/veklep-detail?p_p_id=material_WAR_odokkpl&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=3&_material_WAR_odokkpl_pid=ALBSB9BGVY8D&tab=remarks>.

39 Byť úspěšný nábor odborníků kvůli konkurenci soukromého sektoru v oblasti bezpečnosti určitě nepředstavuje jednoduchou výzvu.

působnosti zbylých zpravodajských služeb). Vyhodnocení tohoto problému je však možné až po představení a analýze hlavních kompetencí založených zde rozebíranou novelou.

4. Klíčové aspekty novely

Novela představuje řadu novinek v rámci kompetencí (pravomocí a povinností) VZ, přičemž jsme vybrali tři oblasti, které vnímáme jako klíčové pro posouzení vhodnosti a proporcionality návrhu a potenciální kumulace moci v rukou VZ: detekce kybernetických útoků a hrozeb, ofenzivní obrana (respektive aktivní zásah) a institut inspektora pro kybernetickou obranu.

4.1 Detekce kybernetických útoků a hrozeb

VZ je nově pověřeno *„cílenou detekcí kybernetických útoků a hrozeb majících původ v zahraničí a směřujících proti důležitým zájmům státu, jejich identifikací a vyhodnocováním a prováděním odpovídajících opatření k odvracení detekovaných kybernetických útoků a hrozeb“*.[40] I v tomto případě budou k realizaci sloužit sondy, přestože došlo k jejich legislativnímu přejmenování na „neškodnější“ nástroje detekce. Je přitom nasnadě, že tak široká pravomoc zpravodajské služby jako je schopnost detekovat probíhající kybernetický útok v reálném čase musí být omezena, a to nejen proto, aby nedocházelo ke koncentraci moci a neproporcionálním zásahům do soukromí a vlastnictví (což byl ostatně problém v případě prvního návrhu), ale i proto, aby činnost VZ byla ekonomická a personálně proveditelná. Právě z těchto důvodů zákonodárce povinnost detekce omezil na útoky a hrozby ze zahraničí, které zároveň směřují proti důležitým zájmům státu a jsou také předmětem obrany České republiky dle ústavního zákona č. 110/1198 Sb., o bezpečnosti ČR.

Je však třeba poukázat na skutečnost, že např. i Bezpečnostní informační služba, která byla v připomínkovém řízení opravdu činná (uplatnila 19 zásadních a 6 doporučujících připomínek, mimo jiné i k tomu, že v návrhu chybí odhad dopadů na státní rozpočet[41]), upozornila na možnou kumulaci moci. Konkrétně poznamenala, že monitoring kybernetického prostoru (který je pro detekční činnost nezbytnou podmínkou) může nejen umožnit reagovat na kybernetický útok, ale rovněž získat informace, jejichž získávání náleží do působnosti právě Bezpečnostní informační služby.

Tato připomínka navazuje na řadu pochybností ohledně rozsahu detekce, a to nejen ze strany veřejného sektoru, ale také veřejnosti. Je sice validní co do striktně obsahové, respektive kompetenční části, již méně však (zejména s ohledem na nakonec přijaté znění zákona) v případě praktického pohledu na věc. Novela se v tomto ohledu navíc (alespoň částečně) poučila od svého předchůdce a limituje detekční možnosti hned v několika aspektech.

---

40 Viz § 16a odst. 1 zákona o Vojenském zpravodajství.

41 BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA. Připomínky k materiálu s názvem: Návrh zákona, kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony. In: *Aplikace ODok* [online]. 2019 [cit. 2021-12-15]. Dostupné z: <https://apps.odok.cz/veklep-detail?p_p_id=material_WAR_odokkpl&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=3&_material_WAR_odokkpl_pid=ALBSB9BGVY8D&tab=remarks>.

Prvním, spíše „slabším“ (vycházejícím primárně z „dobrozdání“ VZ), je preference dobrovolné spolupráce s poskytovateli služeb informační společnosti před mocenskými zásahy při nasazování nástrojů detekce, která by měla probíhat na základě písemných dohod o spolupráci (ty ovšem nejsou v zákoně příliš specifikovány a není např. jasné, jak moc má být spolupráce mezi poskytovateli služeb informační společnosti a VZ utajena či jaké informace o zařízeních budou mít poskytovatelé k dispozici). VZ navíc chce s poskytovateli spolupracovat do určité míry i v rámci testování nástrojů detekce.[42]

Detekce je pak limitována i funkčně, neboť nástroje detekce nesmí být využívány pro provádění odposlechů nebo pro záznam zpráv podle zákona o elektronických komunikacích[43] nebo k aktivnímu zásahu.[44] Nástroje detekce také nesmí zasáhnout do CIA triády v rámci nasazených systémů,[45] přičemž poskytovatelé služeb informační společnosti mají nárok na náhradu škod či nemajetkové újmy, která vznikla v souvislosti s činnostmi VZ.[46]

Na základě této úpravy nemá docházet k plošnému sledování, ani k plošnému ukládání metadat. Detekce má probíhat pouze na základě zákonem stanovených ukazatelů kybernetických útoků.[47] Zákon se tak snaží vymezit proti obavám veřejnosti a stanovit explicitně, že povaha nástrojů detekce je čistě pasivní. Na tomto výkladu se ostatně shoduje i většina vybraných odborníků, které oslovil časopis *Data Security Management* v polovině legislativního procesu.[48]

Pokud se tedy vrátíme k připomínce bezpečnostní informační služby – ano, VZ se bezesporu může dostat k informacím, které nespadají do jeho působnosti. Toto však není specifikum kybernetického prostoru, ale zpravodajské činnosti obecně a prakticky není možné zisku těchto informací zabránit, ať už by kybernetickou obranou byl pověřen jakýkoli orgán. Stěžejní tedy je, že tyto informace i nadále nemůže VZ dále využít, nespadají-li do jeho působnosti.[49] Tato připomínka tak v případě, kdy panuje široká shoda na potřebnosti kybernetické obrany, není efektivně řešitelná. Nastavené limity detekce pak představují v kombinaci s odpovědným výkonem práce inspektora pro kybernetickou obranu dostatečně proporcionální řešení, které balancuje potřebu sběru informací se zásahy do práv jednotlivců.

Co se týká systémového ukotvení, novela skrze explicitně určenou povinnost VZ doplňuje kybernetickou bezpečnost zajišťovanou v tomto ohledu NÚKIB, který do určité míry provádí analýzu a monitoring kybernetických hrozeb a rizik,[50] o kybernetickou obranu. Dále pak doplňuje aktivity orgánů činných v trestním řízení v kontextu kyberkriminality (např. podle § 230 zákona č. 40/2009 Sb., trestní zákoník, je neoprávněný přístup k počítačovému systému trestným činem). Do již existujícího rámce detekční činnosti tak díky zde představované novelizaci vstupuje nový aktér, který může v kyberprostoru na základě

42 MAGDOŇOVÁ, J. *Šéf Vojenského zpravodajství: Čas je v kyberobraně klíčový, novela zákona všechna bílá místa nesmaže*.

43 Zákon č. 127/2005, o elektronických komunikacích.

44 Viz § 16d odst. 3 zákona o Vojenském zpravodajství.

45 Viz § 16d odst. 4 zákona o Vojenském zpravodajství.

46 Viz § 16n zákona o Vojenském zpravodajství.

47 Viz NOVÁK, J. *Příběh novely zákona o Vojenském zpravodajství: od černých krabiček ke spolupráci*.

48 Viz Odpovědi na otázky k novele zákona o Vojenském zpravodajství. *Data Security Management* [online]. 19. 8. 2020 [cit. 2022-09-26]. Dostupné z: <https://dsm.tate.cz/cs/2020/dsm-2-2020/zdarma-2-2020/odpovedi-na-otazky-k-novele-zakona-o-vojenskem-zpravodajstvi>.

49 Viz § 16j zákona o Vojenském zpravodajství.

50 Viz § 22 písm. u) zákona o kybernetické bezpečnosti.

svých relativně rozsáhlých kompetencí poměrně efektivně působit. Česká republika tak disponuje všemi třemi prvky, které např. Fischer uvádí ve vztahu k řízení rizik – prevence (zajišťovaná zejména na základě zákona o kybernetické bezpečnosti), detekce a protiopatření (společně zajištěna na základě zákona o kybernetické bezpečnosti, trestního zákoníku a nově zákona o Vojenském zpravodajství), přičemž právě provádění posledních dvou opatření bylo značně usnadněno.[51]

Na závěr této podkapitoly je ještě vhodné se alespoň krátce vyjádřit k výkladu pojmu metadata, se kterým se v rámci detekce operuje. Samotný zákon tento pojem nedefinuje, jenom v § 16d odst. 2 specifikuje, jaká metadata budou sbírána a že součástí záznamu nebude obsah přenášených dat.[52] Nicméně, dle našeho názoru i nadále zůstává reálnou možnost, že v rámci metadat budou zpracovávány „citlivé" údaje (nikoli nutně údaje zvláštní kategorie ve smyslu čl. 9 GDPR). Samotný údaj o tom, že komunikace vůbec probíhá, totiž může být v určitých situacích informační aktivum hodné ochrany.[53] Avšak obdobně jako je tomu u výše uvedené připomínky Bezpečnostní informační služby, ani tato obava není efektivně řešitelná jinak než kvalitním výkonem dohledu a kontroly, zejména z pozice inspektora pro kybernetickou obranu.

4.2 Inspektor pro kybernetickou obranu

Inspektor pro kybernetickou obranu je pravděpodobně jedním z nejzásadnějších aspektů celé novely, který může výrazně ovlivňovat výsledné posouzení, zda je návrh a zajišťování kybernetické obrany koncipován proporcionálně a nedochází k nadměrné kumulaci moci. Inspektor je součástí VZ a podřízeným ministra obrany, na jehož návrh a po projednání sněmovním výborem pro bezpečnost je vládou ČR jmenován (či odvolán), a to s funkčním obdobím pěti let.[54] Mezi úkoly inspektora patří např. prověřování správnosti postupů VZ, poskytování poradenské podpory příslušníkům VZ a skrze spolupráci se subjekty, u nich byly umístěny nástroje detekce, se inspektor také podílí na dodržování práv potenciálně dotčených osob.[55]

U funkce inspektora pro kybernetickou obranu je možné spatřovat značnou podobnost s funkcí pověřence pro ochranu osobních údajů dle GDPR. I pověřenec monitoruje soulad postupů s předpisy konkrétní oblasti (ochrany osobních údajů), poskytuje poradenství a skrze svou činnost dohlíží na dodržování práv subjektů údajů.[56] Inspektor pro kybernetickou obranu musí být, stejně jako pověřenec pro ochranu osobních údajů, nezávislý.[57]

---

51 FISCHER, E. A. *Creating a national framework for cybersecurity*, s. 7.

52 Explicitní vyjádření považujeme za zvláště přínosné v reakci na připomínky v průběhu legislativního procesu, mj. z dílny Pirátů. Ti mimo jiné poukazovali na to, že za absence definice metadat může být toto ustanovení zneužito např. odkazem na definici metadat v zákoně č. 106/1999 Sb., o svobodném přístupu k informacím, podle kterého (§ 3 odst. 10) metadata zahrnují i obsah zaznamenávaných informací. Více viz *Odpovědi na otázky k novele zákona o Vojenském zpravodajství*.

53 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Text s významem pro EHP).

54 Viz § 16k odst. 1, 2 a 3 zákona o Vojenském zpravodajství.

55 Viz § 16l odst. 1 zákona o Vojenském zpravodajství.

56 Viz článek 39 GDPR.

57 Srov. § 16k odst. 5 zákona o Vojenském zpravodajství a článek 38 odst. 3 a 4 GDPR.

Jak inspektor, tak pověřenec jsou součástí organizace, ve které působí. Inspektor je součástí VZ, a tedy i Ministerstva obrany. I když se na jmenování tohoto inspektora spolupodílí vláda České republiky, je třeba připomenout, že je to stále ta stejná vláda, jejíž součástí je i Ministr obrany, kterému je inspektor odpovědný. Byť pověřencem pro ochranu osobních údajů může být i externí kontraktor, stále je to správce nebo zpracovatel, který jej jmenoval, a může jej tedy i odvolat. Bez ohledu na smluvní vztah mezi správcem/zpracovatelem a pověřencem zde tak vždy budou určité prvky závislé práce a tedy závislosti.

Díky podobnostem mezi těmito dvěma instituty je tedy možné se podívat na fungování pověřenců pro ochranu osobních údajů a identifikovat tak určitá rizika/nedostatky ve vztahu k zajištění nezávislosti podobného institutu – inspektora pro kybernetickou obranu.

Opomeňme teď problém některých pověřenců, kteří byli do funkce jmenováni přes nesplnění potřebných kvalifikačních požadavků. Opomeňme také „formální" pověřence, jejichž pracovní zařazení vzniklo tak, že jednomu ze zaměstnanců byly kvůli „bruselskému diktátu" vyměněny vizitky, přičemž na nových se teď objevují tři písmenka – DPO – a nic dalšího se v náplni jejich práce nezměnilo. Stranou nechme i to, že někteří pověřenci systém ochrany osobních údajů ve společnosti reálně zavádějí, a tak vlastně dozorují svou vlastní práci a u revize nepřekvapivě docházejí k závěru, že je podle nich vše v pořádku. To, na co bychom zde ze své praxe rádi poukázali, je, že pověřenci se někdy vžívají do rolí obhájců správce či zpracovatele. Namísto toho, aby působili jako opravdová protiváha právního oddělení, externích advokátních kanceláří nebo GRC pracovníků, a reálně přispívali ke zvýšení ochrany osobních údajů v organizaci, respektive práv, povinností a zájmů subjektů údajů, vymýšlejí, jak zredukovat zásadu transparentnosti či dokonce zákonnosti, nebo jak kvalifikovat porušení zabezpečení osobních údajů jako běžnou událost a nikoli jako incident, tak aby nemuselo docházet k ohlašování Úřadu pro ochranu osobních údajů nebo informování subjektů údajů. A přestože nemůžeme tyto problémy ilustrovat na žádné vědecké studii či empirických datech, očividnou obavu z obdobného scénáře ukazují i připomínky k zařazení inspektora pro kybernetickou obranu pod VZ. V prvním návrhu musel být inspektor vybrán toliko z členů VZ. Po odmítavé reakci byla tato podmínka rozšířena a novela umožňuje, aby inspektor vzešel i z řad vojáků z povolání.[58] Ředitel VZ Jan Beroun vysvětlil původní pojetí nutné příslušnosti následovně: *„[…] abychom měli alespoň nějakou kontrolu nad tím, jak se ten člověk chová, nad jeho bezpečnostní prověrkou, že nám nevynáší nějaké informace […], když tohoto člověka nebudeme mít pod nějakou kontrolou, tak v podstatě máme špiona uprostřed organizace"*.[59] A přestože plně chápeme tyto důvody, není dle našeho názoru jediným (a možná ani nejvhodnějším) řešením nutná příslušnost k VZ či její následné rozšíření na vojáky z povolání.

Zatímco normotvůrce v případě ochrany osobních údajů neměl prakticky jinou možnost než učinit pověřence součástí organizací správců a zpracovatelů, neboť je potřeba jejich velké množství (protože velké množství je i entit, u kterých pověřenci musí působit),

58 Viz PRUCKOVÁ, M. Česko na prahu přijetí novely o Vojenském zpravodajství. Co je kybernetická obrana a kam zemi posune? In: *Právo21 – Právo srozumitelně a pro všechny* [online]. 21. 3. 2021 [cit. 2022-09-23]. Dostupné z: <https://pravo21.cz/pravo/cesko-na-prahu-prijeti-novely-o-vojenskem-zpravodajstvi-co-je-kyberneticka-obrana-a-kam-zemi-posune>.

59 Viz MAGDOŇOVÁ, J. *Šéf Vojenského zpravodajství: Čas je v kyberobraně klíčový, novela zákona všechna bílá místa nesmaže*.

v případě inspektora pro kybernetickou obranu tomu tak není. Inspektor je totiž jeden, pro jednu jedinou organizaci. Požadavky na bezpečnostní prověrku, nevynášení informací a určitou znalost fungování VZ vnímáme jako relevantní, potřebu kontroly inspektora pak již méně. Jednou z variant je možnost, aby byl inspektor po vzoru finančního arbitra nebo ombudsmana samostatným orgánem. K tomuto uvádí důvodová zpráva, že *„inspektor pro kybernetickou obranu v rámci stanovování opatření a poskytování poradenské podpory nemůže mít postavení ‚vnějšího subjektu' stojícího mimo Vojenské zpravodajství, neboť by to vedlo k vysoké míře neúčinnosti jeho aktivit a nemožnosti zamýšlené komunikace, aniž by nemusely být odstraňovány administrativní bariéry přístupu k utajovaným informacím apod."*. Jsme ovšem přesvědčeni, že zvažujeme-li riziko snížení míry nezávislosti osoby, jejíž hlavní devizou má být právě tato nezávislost, a problematičnost odstranitelných administrativních bariér, prim by měla hrát právě nezávislost. Navíc se nabízí řešení, které administrativní bariéry i bezpečnostní rizika snižuje – výběr inspektora pro kybernetickou obranu z řad jiných zpravodajských služeb. Tento postup společně s pravomocemi inspektora má značný potenciál nejen zastavit jakoukoliv nežádoucí kumulaci moci, ale také efektivně dohlížet na proporcionalitu zásahů prováděných v rámci kybernetické obrany (a to mj. pro určitou rivalitu, která panuje mezi zpravodajskými službami). Oproti výše zmíněným zkušenostem s institutem pověřence pro ochranu osobních údajů by v zájmu samotného inspektora bylo, aby VZ nepřekračovalo s touto novou mocí zákonné mantinely, protože by to znevýhodňovalo zbývající zpravodajské služby. Navíc by nebyl v přímém podřízení, přesto by se i nadále jednalo o důvěryhodnou a prověřenou osobu. I s ohledem na povinnosti, které zákon inspektorovi pro kybernetickou obranu ukládá, je možné, že by zde představená varianta poskytovala jistější zázemí ohledně nezávislosti a motivace inspektora, které jsou tak zanechány na personálních kapacitách a kvalitách konkrétních inspektorů pro kybernetickou obranu.

Jako první zaujal pozici inspektora pro kybernetickou obranu Jan Vacek, a to v první polovině tohoto roku (tj. 2022). Post byl tak téměř rok neobsazen a na reálné vyhodnocení fungování tohoto institutu je v době psaní článku ještě příliš brzy a autoři si toto ani nekladou za cíl, neboť se v textu zaměřují na normativní rovinu předmětné novely.

4.3 Aktivní zásah

Posledním vybraným klíčovým aspektem je problematika aktivního zásahu. Jedná se fakticky o možnost provést protiopatření vysoké intenzity, které má sloužit k odrazení protivníka od útoku (tedy mj. protiútok na infrastrukturu, ze které útok vychází). Je pak relativně snadno představitelné, že takové protiopatření může vést k eskalaci, neboť naplní kvalifikační práh použití síly a situace může přerůst v ozbrojený konflikt. I z toho důvodu se tak samozřejmě jedná o nástroj *ultima ratio* kontrolovaný politickou mocí. Překvapivé ovšem je, že se jedná o kontrolu značně odlišnou od „konvenčních" protiopatření, které mohou dosáhnout intenzity použití síly v kontextu mezinárodního práva.

Kritika nezůstala jen u tohoto bodu, problematickým se stalo i abstraktní vymezení aktivního zásahu, respektive víceméně kompletní absence dané specifikace. U tak invazivního institutu je samozřejmě pochopitelné, že vyvolává otázky i obavy, zvláště když není jasné, jakých konkrétních nástrojů může VZ v jeho rámci využít. Avšak na rozdíl od ideálního světa, kde i tuto materii lze vyčerpávajícím způsobem „vydefinovat", vylučuje dle našeho názoru samotná povaha tohoto institutu v kombinaci s potřebou flexibilní reakce na jednotlivé krize komplexní a do určité míry i nutně obecné legislativní řešení.

Zákon se pak pochopitelně drží flexibilnějšího a abstraktnějšího pojetí aktivního zásahu, přičemž regulace se obecně nesoustředí na nástroj samotný, ale spíše na podmínky, za kterých jej lze využít, což považujeme za podstatnější, a tím pádem vhodnější. Též absentující uvedení preferované intenzity zásahu dle našeho názoru není problematickým.[60] Stejně jako v případě nutné obrany v trestním právu i v rámci mezinárodního práva je totiž přípustná pouze taková minimální intenzita, která je s to odradit útočníka od útoku (a to včetně užití preventivního útoku), což je v rámci mezinárodního práva reprezentováno principem proporcionality.

Za palčivější problém pak považujeme spíše absenci transparentního národního rámce pro přičitatelnost kyberútoků, který by vyřešil otázku zacílení aktivního zásahu. Nesprávné vyřešení problému přičitatelnosti totiž může vyústit mj. v mezinárodněprávní odpovědnost České republiky či eskalovat danou krizi. Tato problematika však již přesahuje limity tohoto článku.

Závěr

Na základě výše zmíněného docházíme k závěru, že zákon o Vojenském zpravodajství ve zde analyzovaných oblastech kybernetické obrany nastavuje většinu limitů odpovídajícím a vhodným způsobem, který zajišťuje proporcionalitu a zároveň předchází kumulaci moci v rukou VZ. Detekční pravomoc, primárně postavená na pasivním principu, sice může vést k získání nadbytečných informací, ale zákon obsahuje adekvátní záruky proti jejich dalšímu užití. I aktivní zásah, potenciálně nejinvazivnější nová pravomoc VZ, přestože postrádá konkrétní vymezení potenciálních nástrojů, je vhodně regulován, zejména pak co se týká možností jeho užití. Jediným aspektem, u kterého jsme tak nabyli určité pochybnosti ohledně vhodnosti použitého řešení, je institut inspektora pro kybernetickou obranu, a to zvláště s ohledem na záruky jeho nezávislosti a motivace dohlížet na dodržování zákonných limitů a proporcionality. Posílení této oblasti by pak posloužilo i jako jistější pojistka proti kumulaci moci než prosté spolehnutí se na kvality konkrétních inspektorů.

Můžeme tedy shrnout, že považujeme zapojení VZ jakožto garanta kybernetické obrany za nejen opodstatněné, ale také koncepčně vhodné. Za legislativně nekoncepční, až nešťastné, lze však označit možný dopad zde rozebírané novely do zákona o zpravodajských službách ČR, neboť kvůli nevhodnému (a nadbytečnému) znění § 2 odst. 2 může docházet k představě, že se ostatní zpravodajské služby nesmějí na zajišťování kybernetické obrany jakkoli podílet.

60 Srov. např. PRUCKOVÁ, M. *Česko na prahu přijetí novely o Vojenském zpravodajství. Co je kybernetická obrana a kam zemi posune?*

Cyber Defence and the Amendment to the Military Intelligence Act

Jan Svoboda (https://orcid.org/0000-0001-9086-0415) –
Jakub Vostoupal (https://orcid.org/0000-0002-1669-9931)

Abstract: In this article, the authors focus on evaluating the amendment to the Military Intelligence Act, which legislatively anchors the regulation of cyber defence and entrusts it to Military Intelligence. First of all, they define the terms cyber security and cyber defence in accordance with the Czech understanding and follow the legislative journey of the amendment (especially the fate of the unsuccessful first bill). Subsequently, they focus on the suitability of the Military Intelligence as the entity responsible for cyber defence while comparing it with other potential entities, namely the National Cyber and Information Security Agency, the Czech Army and other intelligence services. In the next section, the authors then focus on analysing the legal regulation of selected aspects of cyber defence in terms of the proportionality of individual interventions and the risks of power accumulation. As a first of those, they focus on the detection of cyber-attacks and threats, which was one of the most problematic aspects of the first draft. They then discuss the position of the Cyber Defense Inspector as one of the guarantees of proportionality of the new Military Intelligence powers and conclude the analysis with a brief discussion on the power of active intervention.

Keywords: cybersecurity, cyber defence, military intelligence, detection activity, active intervention, proportionality