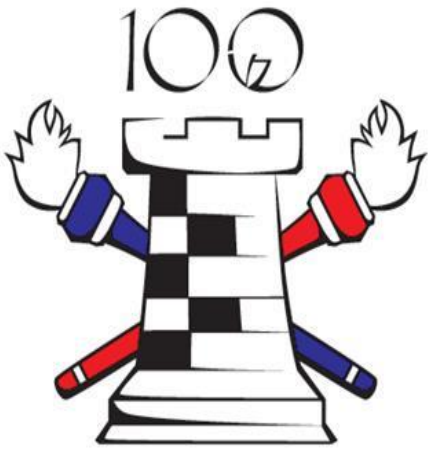
VÝROČNÍ ZPRÁVA O ČINNOSTI VOJENSKÉHO ZPRAVODAJSTVÍ ZA ROK 2018



MINISTERSVO OBRANY
Vojenské zpravodajství
2019

ÚVODNÍ SLOVO ŘEDITELE

Vážení čtenáři,

loňský rok se nesl v duchu oslav 100. výročí od založení samostatného československého státu. I Vojenské zpravodajství, které vzniklo záhy po samotném Československu, se k těmto oslavám připojilo a své výročí si po celý rok připomínalo. Vojenské zpravodajství prošlo za století své existence různými etapami, vždy však bylo důležitým informačním partnerem pro nejvyšší ústavní činitele.

Dnešní Vojenské zpravodajství je etablovanou organizací, která zajišťuje informace klíčové pro obranu České republiky, k čemuž využívá tradiční i moderní zpravodajské disciplíny. V rámci své zákonné působnosti plní úkoly zadané vládou a s jejím vědomím i prezidentem a těmto adresátům také každý rok předkládá výsledky své činnosti v utajované Zprávě o činnosti. V roce 2005 začalo Vojenské zpravodajství publikovat i neutajovanou výroční zprávu, která přibližuje činnost služby široké i odborné veřejnosti.

Od té doby se však díky rozvoji moderních technologií svět několikanásobně zrychlil a současně se také zvýšila rychlost sdílení informací. Ve veřejné výroční zprávě se vždy Vojenské zpravodajství snažilo přinášet informace ze všech oblastí, kterými se v rámci své působnosti zabývalo. Vzhledem k tomu, že se výroční zprávy vydávají zpravidla až ve druhém pololetí následujícího roku, však mohly být uvedené informace již překonané. Proto bylo, symbolicky u 15. veřejné výroční zprávy, rozhodnuto změnit její koncept a nově se soustředit na vybrané problematiky, které Vojenské zpravodajství dlouhodobě hodnotí jako určující pro další světový vývoj.

Vedle toho se Vojenské zpravodajství snaží nacházet stále nové kanály pro komunikaci s veřejností. O své aktuální činnosti informuje na svých internetových stránkách a v oblastech, které lze veřejně prezentovat, se angažuje v odborné veřejnosti i akademické sféře.

Přestože nová obsahová podoba výroční zprávy nemusí splnit očekávání všech, věřím, že čtenářům přinese významné informace o aktuálních tématech.

brigádní generál Ing. Jan BEROUN

OBSAH

ZÁKLADNÍ INFORMACE

Vojenské zpravodajství (VZ) je jednotná ozbrojená zpravodajská služba České republiky (ČR) integrující rozvědnou i kontrarozvědnou činnost, která získává, shromažďuje a vyhodnocuje zpravodajské informace, které jsou zásadní pro zajištění obrany České republiky.

Postavení, působnost, spolupráce a kontrola Vojenského zpravodajství je upravena zákonem č. 153/1994 Sb., *o zpravodajských službách České republiky*, ve znění pozdějších předpisů.

Zákon č. 289/2005 Sb., *o Vojenském zpravodajství*, ve znění pozdějších předpisů upravuje povinnosti a oprávnění příslušníků VZ, používání specifických prostředků získávání informací, využívání osob jednajících v jeho prospěch, vedení evidencí a kontrolu jeho činnosti.

Vnitřní organizaci a činnost vymezuje *Statut Vojenského zpravodajství*, který schválila vláda České republiky.

Úkoly Vojenskému zpravodajství v rámci jeho působnosti ukládá vláda České republiky a současně odpovídá za jeho činnost. S vědomím vlády České republiky je oprávněn ukládat úkoly Vojenskému zpravodajství také prezident České republiky.

Primárním úkolem Vojenského zpravodajství je zabezpečování informační podpory ústavních činitelů, kteří odpovídají za obranu a bezpečnost České republiky. Mimo to poskytuje i informační podporu představitelům Armády České republiky (AČR).

K plnění úkolů Vojenské zpravodajství využívá metody HUMINT[1] (informace získávané a poskytované lidskými zdroji), SIGINT[2] (informace získané z elektromagnetického spektra), OSINT[3] (využívání informací z veřejné dostupných zdrojů) a IMINT[4] (obrazové zpravodajství).

V průběhu loňského roku Vojenské zpravodajství předalo na 1 330 informačních výstupů, které byly určeny zejména předsedovi a členům vlády, prezidentu republiky, nejvyšším představitelům Ministerstva obrany a AČR a dále zpravodajským orgánům NATO a EU a partnerům v rámci bilaterální spolupráce. Souhrn zpravodajské činnosti a zpravodajských poznatků Vojenského zpravodajství za uplynulý rok je obsažen ve Zprávě o činnosti Vojenského zpravodajství za rok 2018. Tato Zpráva byla zpracována ve stupni utajení Tajné a v souladu s § 8 odst. 1 zákona č. 153/1994 Sb. byla předložena prezidentu republiky a vládě ČR. Na základě zákona č. 289/2005 Sb. byla Zpráva zaslána také Stálé komisi

[1] Human Intelligence
[2] Signals Intelligence
[3] Open Source Intelligence
[4] Imagery Intelligence

pro kontrolu činnosti Vojenského zpravodajství Poslanecké sněmovny Parlamentu ČR (PSP ČR).

V souladu s Akčním plánem k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020, který schválila vláda svým usnesením č. 382 ze dne 25. května 2015, pokračovalo Vojenské zpravodajství v plnění úkolů v oblasti kybernetické obrany. V této souvislosti je vhodné uvést, že podle vládního přístupu k dané problematice je kybernetická obrana autonomní a specifickou oblastí širšího konceptu kybernetické bezpečnosti, kterou má v gesci Národní úřad pro kybernetickou a informační bezpečnost. Rozdíl mezi kybernetickou obranou a bezpečností spočívá především v povaze a intenzitě útoků a na to reagujících opatření, aniž by bylo možné vymezit úplně přesná kritéria. Připravenost na kybernetické útoky proto musí být komplexní a nemůže se zaměřit pouze na sféru bezpečnosti, ale je nutné budovat schopnosti i proti útokům, které lze vyhodnotit jako způsobilé aktivovat obranu státu. Aktivace kybernetické obrany tak bude přicházet v úvahu pouze v případě těch nejintenzivnějších útoků. Specifikem kybernetické obrany bude skutečnost, že bude prováděna jak v případě vyhlášení mimořádných stavů, především formou součinnosti s ostatními složkami zajišťujícími obranu České republiky, tak i nepřetržitě mimo tyto stavy.

Na základě přistoupení České republiky k plnění cílů rozvoje schopností NATO v oblasti kosmického obrazového průzkumu pokračovalo Vojenské zpravodajství v plnění úkolů spojených s budováním expertních schopností zpravodajské disciplíny IMINT, včetně vytvoření národního prvku v oblasti obrazového zpravodajství tzv. Satelitní centrum ČR (SATCEN ČR).

V souladu s příslušnými usneseními vlády a usneseními Poslanecké sněmovny Parlamentu ČR (PSP ČR) i v loňském roce VZ zabezpečovalo zpravodajskou podporu a kontrarozvědnou ochranu jednotek AČR v zahraničních misích.

Při plnění zadaných úkolů je důležitá spolupráce s ostatními bezpečnostními složkami a sdílení informací. Vojenské zpravodajství spolupracovalo na národní úrovni se zpravodajskými službami České republiky a dalšími orgány státní správy. Spolupráce probíhala především formou pravidelné, ale i ad-hoc výměny zpravodajských informací a formou expertních jednání.

Zahraniční spolupráce probíhala na multilaterální úrovni v rámci struktur NATO a EU a na bilaterální úrovni se zpravodajskými službami jiných států. Spolupráce se zpravodajskými službami jiných států byla v souladu s § 10 zákona č. 153/1994 Sb. schválena vládou ČR.

AKTUÁLNÍ PROBLEMATIKY

V průběhu roku 2018 se svět posunul dále směrem ke konfrontaci, která by se mohla stát přímým vyústěním politiky předních světových velmocí v rámci uplatňování jejich zájmů. Jedná se o důsledek oslabování světové dominance reprezentované Spojenými státy, jejichž protiváhou se prozatím primárně v ekonomické oblasti a díky své výkonnosti stává Čína a ve vojenské oblasti, díky realizaci nových technologických řešení moderních zbraňových systémů, pak opět Rusko. Svět tak pokročil v přípravách na rozpoutání mocenského konfliktu nového typu, který nebude vybojován tradičními vojenskými prostředky. Člověk se v něm může stát jen hybatelem, který uvede do chodu souboj technologií, jehož výsledek bude záviset na míře jejich vyspělosti, ale i jejich složitosti a zranitelnosti.

Rok 2018 charakterizovalo oslabování a zpochybňování role existujících globálních i regionálních organizací, kontrolních režimů a odzbrojovacích smluv, včetně jejich porušování a vypovídání. S tím narůstala i nedůvěra, špatná komunikace a nepředvídatelnost a s nimi spojené nebezpečí nárůstu neporozumění vedoucí k chybnému výkladu jednání, motivů i cílů druhé strany. Zásadním problémem je, že konání mnoha subjektů je stále více ovlivněno nikoli reálnou představou o stavu věcí, ale jejich mediálním obrazem, který je často účelově manipulován a tendenčně zkreslován. Nástrojem soupeření se stává nikoli souboj klasických ideologií, jako tomu bylo v minulosti, ale střet společenských modelů a konflikt vidění světa s cílem prosazení vlastní vize světa jako všeobecně platné. Jde o soupeření usilující o ovládnutí myslí, formování názorů a z nich vyplývajících postojů lidí.

Lze zaznamenat i trendy, které budou určovat podobu konfliktů mezi předními globálními hráči a případně i bloky vyspělých států. Odrazujícím faktorem bránícím rozpoutání většího konfliktu tradičními vojenskými prostředky nebo dokonce zbraněmi hromadného ničení nadále je a bude vědomí fatálních ztrát na životech a materiálních hodnot na obou stranách a všeobecné devastace životního prostředí, stejně jako i v období studené války. Cena vítězství je, s výjimkou vedení zástupných lokálních konfliktů ve třetím světě, příliš vysoká a jedná se spíše o hypotetickou výhru. Případný velký vojenský konflikt se tak může odehrávat prostřednictvím přesně cílených a předem kalkulovaných (i jaderných) úderů novými vojenskými prostředky, proti nimž protivník nemá obranu a které způsobí vyřazení jeho vojenských operačních schopností.

Současně lze předpokládat vedení útoku i tzv. nevojenskými prostředky, tedy v digitálním světě, a to díky světovému datovému propojení a závislosti moderní společnosti na bezchybném fungování digitálních sítí. Míra zranitelnosti konkrétních a z technologického hlediska klíčových bodů a soustředění řídících prvků v rámci vyspělých a komplikovaných systémů je výzvou pro potenciálního protivníka. Jeho cílem je nikoli nejistá a plná eliminace soupeře klasickými vojenskými prostředky, ale zejména oslabení jeho vojenských schopností a obranných možností, včetně zasazení celkově destabilizujícího cíleného úderu s dopadem do

oblasti bezpečnosti a veřejného pořádku – za účelem narušení fungování společenských mechanismů a norem.

Soustředění informačního úsilí na nové a dosud ne zcela přesně definované hrozby (a z nich přímo plynoucí rizika) a na nové informační priority se proto stává nutností. To vede i k vědomí nezbytné změny dosavadních přístupů a postupů a k přehodnocení informačních zájmů. Vybrané části dosavadních priorit jsou proto prostorem intenzivního rozboru získaných poznatků a jejich analýzy. Její nedílnou součástí je i schopnost rozboru aktuální situace a současně odhad jejího budoucího vývoje.

Právě s ohledem na výše uvedené vývojové trendy a nutnost změny chápání aktuálních hrozeb se pozornost Vojenského zpravodajství, a to zcela v souladu se zadávanými úkoly, obrací do oblasti nejmodernějších strategických zbraňových systémů a k problematice kybernetických hrozeb, jejich specifikace a odhadů dalšího vývoje. Jde zde i o stanovení míry vlastní i cizí závislosti na technologických možnostech resp. konkrétních cílech, které budou při ofenzivních útocích stanoveny.

VÝVOJ RAKETOVÝCH PROSTŘEDKŮ VYBRANÝCH STÁTŮ

Pro hodnocení potenciálních hrozeb použití raketových prostředků vůči ČR vychází VZ z reálného, či v blízké budoucnosti dosažitelného vojenského, resp. raketového potenciálu, a záměrů možného protivníka tyto raketové prostředky použít. Z globálního hlediska mají nezanedbatelný podíl na zhoršujícím se bezpečnostním prostředí například probíhající programy vývoje a modernizace raketových zbraňových prostředků.

Rusko lze v otázkách hodnocení dosaženého stavu modernizace jeho raketo-jaderného potenciálu považovat za stabilní a předvídatelný subjekt. Raketovým prostředkům strategického určení, jež mají zajišťovat národní bezpečnost a účinnou odstrašující politiku, je ruskou administrativou věnována trvale vysoká pozornost. Podle stávajících předpokladů bude RF udržovat svůj raketo-jaderný potenciál v množství odvíjejícím se od ekonomických možností a stavu ruského vojenskoprůmyslového komplexu (VPK). Přes současnou omezenou produkční schopnost svého VPK zůstane Rusko i do budoucna státem disponujícím robustním a ničivým potenciálem, který bude určovat jeho postavení v regionálním i celosvětovém významu.

Probíhající modernizace raketo-jaderných kapacit orientuje RF zejména na zvýšení odolnosti raketových nosičů strategického určení vůči působení systémů protiraketové obrany

(PRO). Vývoj je zaměřen na nové typy vícenásobných jaderných bojových hlavic (MIRV[5]) nebo manévrujících bojových hlavic (MaRV[6]) se schopností měnit programově průběh trajektorie jejich letu.

Rusko zamýšlí posílit svůj raketo-jaderný odstrašující potenciál rovněž prostřednictvím obnoveného vývoje a zavedením „těžké“ mezikontinentální balistické řízené střely s pohonem na kapalné raketové palivo SS-X-30 Sarmat. Vedle záměru postupného nahrazení zastaralých řízených střel SS-18 Satan a SS-19 Stiletto je hlavní motivací RF pro vývoj této kategorie střel jejich velká nosnost umožňující vyzbrojit tyto raketové nosiče novými typy manévrujících bojových hlavic. S jejich pomocí má Rusko dosahovat vyšších schopností při eliminaci působení jak stávajících, tak plánovaných systémů PRO.

Za manévrující typ bojové hlavice lze v této souvislosti považovat také Ruskem vyvíjený hypersonický návratový bojový prostředek. Ten plánuje RF používat i jako součást výzbroje vybraných typů raketových prostředků strategického určení. V první fázi jeho zavedení, tedy do doby dokončení vývoje řízené střely SS-X-30 Sarmat, plánuje Rusko v roce 2019 vyzbrojit tímto prostředkem raketový nosič řízené střely SS-19 Stiletto.

Dalším významným směrem rozvoje ruského raketo-jaderného zbraňového arzenálu je modernizace samotných raketových nosičů strategického určení. Té má být dosaženo nahrazením mezikontinentálních řízených střel typové řady SS-25 Topol nebo SS-27 Topol-M, a to novými řízenými střelami raketových kompletů SS-29 Jars. Konečného stavu modernizace však RF plánuje docílit plnou technologickou nezávislostí na dodávkách klíčových raketových technologií ze zahraničí, například z Ukrajiny nebo Běloruska. Výsledkem této nezávislosti má být úspěšná realizace tzv. projektu Avangard, v rámci něhož Rusko vyvíjí nový raketový komplet SS-X-31 Rubež. V roce 2018 pokračovala RF i v modernizaci výzbroje vojenského námořnictva, a to výstavbou a zaváděním ponorek na jaderný pohon třídy Projekt 955 Borej/Kosatka. Tato plavidla Rusko používá jako nosiče námořních balistických řízených střel SS-N-32 Bulava.

Kromě nasazení již zavedených plavidel Jurij Dolgorukij, Alexandr Něvský a Vladimír Monomach pokračovaly i testy čtvrté ponorky této třídy Kníže Vladimír. Celkový plán, původně počítající s výrobou osmi ponorek Borej, zahrnuje do budoucna výstavbu dalších až šesti kusů plavidel, průběžně modernizovaných na modifikaci Projekt 955A Borej-A. Za renesanci celkového ruského raketo-jaderného odstrašujícího potenciálu lze považovat i modernizaci útočných ponorek na jaderný pohon třídy Projekt 885 Jaseň. Tato plavidla, vyzbrojená řízenými střelami s plochou dráhou letu s jadernou hlavicí, mohou být použita i proti pozemním cílům, a to na vzdálenost až 2 500 km. Pro dosažení výsledného odstrašujícího

[5] Multiple Independently targetable Reentry Vehicle
[6] Maneuvering Reentry Vehicle

efektu plánuje RF výstavbu až sedmi ponorek této třídy. Vedle zavedené ponorky Projekt 885/08850 Severodvinsk postoupila v hodnoceném období do fáze série plavebních testů druhá, modernizovaná obměna ponorky Projekt 885M/08851 Kazaň.

Paralelně s posilováním technologické úrovně raketových prostředků strategického určení RF modernizuje vlastní systémy protiraketové a protidružicové obrany. S cílem dosáhnout generační obměny výzbroje těchto systémů souvisí i letové testy nového typu protiraketového interceptoru, který má být součástí nové, modernizované PRO Moskvy. Funkcí nového palebného prostředku má být odvrácení útoku mezikontinentálními balistickými řízenými střelami jejich ničením na vzdálenost až 350 km. Za druhý typ palebného prostředku této kategorie lze rovněž považovat Ruskem vyvíjený systém protidružicové obrany Nudol. U obou uvedených typů protiraketové a protidružicové obrany se předpokládá jejich schopnost ničit předurčené cíle kinetickou energií, tedy jejich zasažením bojovou částí interceptoru.

Nad rámec vývoje výše zmiňovaných typů zbraňových systémů zahájila RF testy zaměřené na ověření technologií nového protivzdušného a protiraketového systému S-500 schopného ničit balistické řízené střely kategorií středního a dalekého dosahu na vzdálenost 400 až 600 km. Balistické řízené střely má systém S-500 ničit ve střední fázi trajektorie jejich letu probíhající mimo atmosféru a rovněž v závěrečné fázi letu, tedy v atmosféře Země.

Dalším subjektem, jehož raketo-jaderný potenciál může vyústit v ohrožení ČR i států NATO, je Čínská lidová republika (ČLR). Raketová vojska, vyzbrojená jak mezikontinentálními, tak námořními balistickými řízenými střelami, jsou považována za nezbytný prostředek nejen k udržení odstrašující síly země, ale i k posílení její politické prestiže na mezinárodním poli. V předchozím období, obzvláště v důsledku enormního rozvoje informačních technologií a aplikované elektroniky, dosáhla Čína výrazných úspěchů v modernizaci převážné většiny svých raketových prostředků. To se týká jak raketových prostředků strategického určení, tak zejména vývoje nových typů balistických řízených střel krátkého, středního i dalekého dosahu a vývoje a zavádění manévrujících hypersonických návratových prostředků i systémů protiraketové nebo protidružicové obrany.

Zvyšující se technologická úroveň Číny, pokrývající celou škálu typů raketových zbraňových prostředků, znepokojuje řadu zemí mezinárodního společenství. Důvodem obavy těchto států je zejména možnost následné proliferace čínských raketových technologií do z bezpečnostního hlediska problémových států, například do Íránu.

Získané raketové technologie sehrávají obzvláště v případě Íránu významnou roli. Výrazný technologický posun je zaznamenáván především v případě balistických řízených střel. Rozvojem raketového programu a vývojem těchto zbraní demonstruje Írán schopnost a záměr vyvinout limitované množství více či méně sofistikovaných raketových prostředků

kategorie středního až dalekého dosahu, s jejichž pomocí může ohrozit většinu evropských států NATO, tedy i ČR.

Raketové zbraňové prostředky, a zejména v jejich konstrukci aplikované technologie, jakými jsou manévrující bojové hlavice nebo hypersonické návratové prostředky, přináší v otázce zhoršujícího se bezpečnostního prostředí řadu explicitně negativních konsekvencí.

Tento z bezpečnostního hlediska nežádoucí stav lze dokumentovat nejen na příkladech vývoje nových typů raketových technologií v RF, ale především progresivně se vyvíjejícího čínského raketového zbraňového arzenálu, jehož skladba ani objem nejsou limitovány či svázány s některými z mezinárodních kontrolních režimů. Raketové zbraňové prostředky nabývají na významu zejména v případech nedostačující působnosti stávajících regulačních mechanismů schopných omezit nejen jejich vývoj a držení, ale rovněž zabránit jejich následné proliferaci.

HROZBY V KYBERNETICKÉM PROSTORU

Bezpečnostní rizika spojená s hrozbami v kybernetickém prostoru zaznamenávají neustálý dynamický růst. K tomuto stavu přispívá mimo jiné i masivní rozvoj informačních a komunikačních technologií, které přinášejí vedle pozitivních dopadů i řadu nových zranitelností. Tato skutečnost generuje rostoucí požadavky na schopnost ČR efektivně reagovat na nové bezpečnostní hrozby.

STÁTNÍ AKTÉŘI

Přes široce rozšířenou kybernetickou kriminalitu zůstávají nadále nejnebezpečnějšími aktéry v oblasti kybernetické bezpečnosti státní a státem podporované skupiny podnikající útoky známé jako tzv. Advanced Persistent Threats (APTs)[7]. Ačkoliv aktivity těchto uskupení představují jen malý zlomek z množiny globálních kybernetických útoků, sofistikovanost a vytrvalost jejich provádění spolu s cílením na nejvýznamnější systémy a sítě předmětných organizací je od běžné kybernetické kriminality odlišují.

Zatímco běžní kybernetičtí zločinci útočí na komparativně vysoký počet slabě zabezpečených systémů bez ohledu na jejich provozovatele, uskupení typu APT selektivně cílí na významné systémy a sítě specificky zvolených organizací, o nichž lze předpokládat, že

[7] Advanced Persistent Threat (APT) – též pokročilá a trvalá hrozba. Typickým účelem APT je dlouhodobé a vytrvalé infiltrování a zneužívání cílového systému za pomoci pokročilých a adaptivních technik (na rozdíl od běžných jednorázových útoků)

budou dobře chráněny. V případě úspěchu jsou však schopna zcizit na nich uložená data a informace vysoké hodnoty, napadnout existující procesy nebo je jinak poškodit či zneužít.

Nebezpečným fenoménem v tomto kontextu zůstanou potenciální kyberfyzické či na kritickou infrastrukturu zaměřené útoky, které mohou cíleně či neplánovaně způsobit významné škody nebo spustit kaskádový efekt s neočekávanými důsledky. Ofenzivní výzkumné kybernetické programy již zavedla celá řada zemí, je však pravděpodobné, že v oblasti ničivých kybernetických útoků budou nadále zdrženlivé, a tyto budou nasazeny pouze v období probíhajících konfliktů, geopolitického napětí či ostrých diplomatických rozepří. Naopak u některých nestátních aktérů, typicky extremistických či teroristických organizací, bude tato zdrženlivost absentovat. Motivaci především teroristických organizací způsobit závažné škody prostřednictvím kybernetických útoků bude ve střednědobé budoucnosti vyvažovat prozatím nízká míra sofistikovanosti jejich schopností. V případě úspěšného rekrutování odborníků na kybernetickou bezpečnost a průmyslové ovládací systémy však nelze vyloučit zdárné vyvinutí ofenzivních schopností, které by měly významný ničivý potenciál.

Kvůli tzv. věrohodnému popření (plausible deniability) [8] budou pro prosazování zahraničněpolitických cílů některých mocností i nadále využíváni zástupní aktéři. Kromě možnosti popřít zapojení veřejných institucí v ofenzivních kybernetických kampaních, které mohou mít zásadní důsledky, je zde motivací také efektivní využití sofistikovaných schopností soukromých firem a nestátních organizací (včetně služeb entit na černém trhu či politicky motivovaných hacktivistů), možnost dočasného doplnění nedostatečných personálních kapacit nebo jednodušší manévrovatelnost mimo sféru vlastní jurisdikce či suverenity. Tyto inklinace jsou potvrzením trendu významné privatizace v oblasti kybernetické bezpečnosti, kde soukromé společnosti často nabízejí nejen konzultace a asistenci při defenzivní činnosti, ale i ofenzivní schopnosti, informace o existujících zranitelnostech, či dokonce služby ofenzivního charakteru.

Státy provozované či podporované APT skupiny si nadále udrží vysokou míru adaptability vůči obranným opatřením jejich cílů. Tato schopnost kontinuální proměny postupů a metod infiltrace do určité míry kontrastuje se standardizací oblíbených nástrojů užívaných jednotlivými skupinami, která v některých případech indikuje možnou existenci oddělených týmů, z nichž jedny vyvíjejí dané nástroje, které následně předávají druhým pro jejich operativní nasazení.

---

[8] Jedná se stav, kdy mohou představitelé či veřejné instituce daného státu věrohodně popírat, že jejich státní instituce, ozbrojené síly, bezpečnostní sbory či jejich příslušníci participovali či odpovídají za čin, který je v rozporu se zákony státu, v němž se tento čin odehrál, či s mezinárodním právem. V kontextu kybernetické bezpečnosti se typicky jedná o kybernetické útoky, které jsou v řadě států včetně ČR klasifikovány jako trestné činy

Rozvíjet se bude nadále také trh se zranitelnostmi a ofenzivními nástroji, který je zdrojem komerčních produktů, jež se spolu s proprietárním malwarem[9] vyprodukovaným nejsofistikovanějšími aktéry stanou významnou proměnnou proliferace ofenzivních kybernetických schopností.

V posledních letech byly detekovány početné kybernetické útoky, kdy útočníci prováděli kybernetické útoky v bezprostřední blízkosti svých cílů tzv. close access operations. Možné pokračování tohoto trendu bude klást vyšší nároky na kombinaci vhodných přístupů k zajištění kybernetické a zároveň fyzické bezpečnosti významných objektů kritické infrastruktury, domácích i zahraničních pracovišť veřejných institucí i vojenských základen.

KYBERNETICKÁ KRIMINALITA, ŠPIONÁŽ A SUBVERZE

Pro některé izolované státy, na něž jsou uvaleny mezinárodní sankce, bude kybernetická kriminalita prostředkem i pro zisk zahraničních měn. Pro praní špinavých peněz, financování zpravodajských operací nebo z důvodu snah o zakrytí plátců či příjemců finančních transakcí mohou být využity i kryptoměny. Průmyslová a na akademickou sféru trvale zaměřená špionáž pak bude nadále jedním ze zdrojů vědeckého a průmyslového pokroku těchto zemí.

Pokračovat budou útoky na nejhodnotnější cíle, jež v českém prostředí, podobně jako jinde v Evropě a zemích NATO, představují ústřední orgány státní správy a diplomatická pracoviště, podniky a společnosti s globálně konkurenceschopným know-how, korporace i střední a malé podniky či přední české univerzity pyšnící se kvalitními výzkumnými projekty.

V neposlední řadě je možné očekávat pokusy o zisk kompromitujících informací s potenciálem ovlivnit demokratické procesy či polarizovat společnost po liniích třecích ploch v kontextu vnitropolitického dění i zahraničněpolitického směřování země.

ÚTOKY NA DODAVATELSKÉ ŘETĚZCE

Ač se nejedná o nový fenomén, začíná být často skloňována hrozba cílených útoků na dodavatelské řetězce, a to v oblasti softwaru i hardwaru. V softwarové oblasti kvůli svému nedostatečnému zabezpečení hrozbu představují některé produktové doplňky či celé stavební platformy, na nichž jsou komplexní softwarové produkty často modulárně vystavěny. V oblasti vývoje webu pak vytváří riziko například nedostatečně auditované skripty (kupř. reklam) vložené do řady webových stránek či některé softwarové platformy a součásti.

[9] Zde chápáno jako malware vyvíjený specializovanými týmy na míru pro vlastní použití ve specifických ofenzivních kybernetických operacích bez záměru jej dále šířit. Riziko horizontální proliferace těchto schopností představuje možnost, že budou odchyceny či objeveny a následně upraveny a/nebo použity dalšími aktéry

V oblasti hardwaru a fyzických komponent se pak jedná především o klíčové prvky kritické a informační infrastruktury, na níž budou do budoucna ještě více závislé národní ekonomiky vyspělých i rozvíjejících se států. Nedostatečně zabezpečené komponenty kritické informační infrastruktury mohou být zneužity ke způsobení efektů negativně ovlivňujících vojenskou, ekonomickou, politickou, societální i environmentální bezpečnost ČR.

Nejsilněji lze tuto problematiku vnímat v oblasti výstavby sítí páté generace (5G) a datových center, které mají mimo jiné potenciál zásadně proměnit podobu, jakou budou spravovány moderní průmyslové podniky, a jejich efekt se s vysokou pravděpodobností projeví i na fungování moderní společnosti jako takové. Komplexní řešení v tomto kontextu totiž dokáží poskytovat pouze společnosti pocházející z nečlenských zemí NATO. Národní úřad pro kybernetickou a informační bezpečnost dokonce před některými z nich vydal varování.

Z hlediska ekonomické bezpečnosti je dále nežádoucí, aby se ČR stala závislou na jediném dodavateli uvedených komponent, a to především v případě, kdy by tento ovládl celý trh s těmito technologiemi.

PŘISOUZENÍ KYBERNETICKÝCH ÚTOKŮ

V kontextu procesu přisuzování (atribuce) kybernetických útoků lze očekávat sílící mezinárodní snahy o definici a aplikaci nejprve národních, později možná i mezinárodních standardů přisouzení. Cílem bude postihovat, a případně i odstrašovat kybernetické útočníky, což bez dostatečně průkazné analýzy uskutečněných útoků nebude možné.

Kroky v této oblasti již podnikají někteří spojenci ČR, kteří definují národní standardy, či dokonce vydávají zatykače na ztotožněné útočníky provádějící ekonomicky či politicky motivované kybernetické útoky ve prospěch třetích zemí. V případě, že se bude kontinuálně dařit přisoudit konkrétním osobám či organizacím odpovědnost za ofenzivní kybernetické kampaně, lze očekávat změny v modu operandi útočníků. Vytvořené standardy a pro přisuzování použité indikátory bude třeba na jednu stranu dostatečně komunikovat směrem k veřejnosti a odborné komunitě, na stranu druhou by odhalení metod vedoucích k přisouzení kybernetických útoků mohlo útočníkům poskytnout návod, jak se mu vyhnout či jak provést tzv. operaci pod falešnou vlajkou (false flag operation).

Pro pokrok v této oblasti bude klíčová mezirezortní a mezinárodní spolupráce, výměna informací a zpravodajských poznatků a koordinace diplomatických snah na úrovni nadnárodních či mezinárodních organizací (EU, NATO).

DALŠÍ VÝZNAMNÉ TRENDY

Významné změny v oblasti kybernetické bezpečnosti a obrany přinesou nové technologie a vývoj těch stávajících, ať už se jedná o umělou inteligenci, či sítě 5G. Implikace pro bezpečnost budou mít také nové trendy v řadě odvětví, např. dopravě (autonomní a na internet napojená vozidla), v oblasti ukládání a zpracování dat (pokračující přechod na cloudová řešení, přírodní zpracování jazyka), v informačních technologiích obecně (např. kvantové počítače) i jinde.

Značný nárůst zaznamenává segment zařízení tzv. internetu věcí (Internet of Things – IoT)[10], které se nacházejí jak v domácnostech, tak v privátních a veřejných organizacích, i jako součást průmyslových systémů a řídících prvků kritické infrastruktury. Producenti IoT přitom přinášejí na trh neustále nové a nové produkty, jež často obsahují zneužitelné zranitelnosti a jejich následná podpora je mnohdy nedostatečná, poskytování aktualizací zanedbávané a časově omezené. Již nyní jsme svědky masivních kybernetických útoků typu tzv. distribuovaného odmítnutí služby (Distributed Denial of Service – DDoS)[11], ke kterým jsou zneužívány zotročené sítě (botnety) [12] IoT. Počet IoT se bude v nadcházejícím období s příchodem rychlých sítí 5G navíc násobit. Kombinace rychlých sítí a množství zranitelných IoT zařízení pak mohou otevřít prostor pro ničivější kybernetické útoky, které je budou využívat jako násobitel efektu útoků DDoS či jako vstupní bránu pro další útočné vektory. Rovněž budou narůstat kybernetické útoky zaměřené na samotná IoT zařízení využívaná v rámci průmyslových systémů a řídících prvků kritické infrastruktury.

Významným trendem je hrozba použití ransomwaru [13] ze strany kybernetických útočníků, zejména kybernetického organizovaného zločinu, která se v poslední dekádě významně zvyšovala. Kybernetický organizovaný zločin však v posledním roce přesunul své úsilí spíše na více lukrativní oblast nelegální těžby digitálních měn prostřednictvím kompromitace počítačových systémů různých organizací, a četnost ransomware kyberútoků tak poklesla. Nicméně hrozba aplikace ransomwaru nezmizí a lze předpokládat další nárůst

---

[10] Internet věcí (Internet of Things, IoT) – síť fyzických zařízení, vozidel, domácích spotřebičů a dalších zařízení, která jsou vybavena elektronikou, softwarem, senzory, pohyblivými částmi a síťovou konektivitou umožňující těmto zařízením se propojit a vyměňovat si data

[11] Distribuované odmítnutí služby (DDoS) – typ síťového útoku na servery, internetové služby nebo celé sítě, který způsobuje přehlcování serverů, přetěžování sítě a blokování služeb. Výsledkem bývá nefunkčnost a nedostupnost služby pro internetové uživatele. U DDoS je do útoku zapojeno více počítačů s vědomím nebo bez vědomí jejich uživatelů

[12] Botnet (síť botů) – síť infikovaných počítačů ovládaných jediným hackerem/crackerem, který tak má přístup k výpočetnímu výkonu mnoha tisíců strojů současně. Umožňuje provádět nezákonnou činnost ve velkém měřítku – zejména útoky DDoS a distribuci spamu

[13] Ransomware – druh malware, pomocí kterého vzdálený útočník zašifruje data na počítači oběti a následně požaduje výkupné za sdělení hesla k těmto datům

jeho sofistikovanosti a přesné cílení na velké a bohaté organizace s úmyslem je vydírat. Ransomware se rovněž stal zajímavým nástrojem APT aktérů, kteří jeho prostřednictvím mohou financovat své operace, zametat digitální stopy či vytvořit zmatek k odvrácení pozornosti, nebo také provádět kybernetickou sabotáž.

Přes rostoucí sofistikovanost kybernetických útoků, metod infekce (včetně sociálního inženýrství) i způsobů, jak se proti těmto bránit, zůstane nejdůležitější proměnnou lidský aspekt – uživatel. Nedostatečné povědomí o hrozbách a rizicích i absentující důraz na dodržování bezpečnostních praktik jsou příčinou mnoha úspěšných kybernetických útoků. Pokračující hrozbu budou představovat také insideři, a to především z řad nespokojených, nespolehlivých či bezpečnostně nezpůsobilých zaměstnanců organizací.

Pokračující výzvou bude nábor a zaměstnávání vhodných uchazečů na pozice související s kybernetickou bezpečností a obranou, neboť odborníků s touto specializací je na pracovním trhu dlouhodobý nedostatek. S rostoucí potřebou rozšíření počtu pozic na úseku kybernetické bezpečnosti a obrany bude tento deficit pouze narůstat.

KONTROLA ČINNOSTI VOJENSKÉHO ZPRAVODAJSTVÍ

Kontrola zpravodajských služeb České republiky je upravena v § 12 až 13a zákona č. 153/1994 Sb. Z těchto ustanovení vyplývá právo výkonu kontroly činnosti zpravodajských služeb z úrovně vlády České republiky a Parlamentu České republiky.

Podle ustanovení § 13 zákona č. 153/1994 Sb. není ustanoveními tohoto zákona dotčena působnost státních orgánů ke kontrole plnění úkolů hospodaření se státním majetkem a plnění státního rozpočtu podle zvláštních právních předpisů. Těmito jsou zejména zákon č. 166/1993 Sb., o Nejvyšším kontrolním úřadu, ve znění pozdějších předpisů, a zákon č. 320/2001 Sb., o finanční kontrole, ve znění pozdějších předpisů.

V loňském roce proběhly kontroly z úrovně Stálé komise pro kontrolu VZ PSP ČR.

Vnitřní kontrola Vojenského zpravodajství byla zajišťována vlastními odbornými prvky. Kontrolní činnost byla zaměřena zejména na oblast vnitřní bezpečnosti, ochrany utajovaných informací, hospodaření s majetkem státu a výkon jednotlivých odborných činností. V oblasti operativní činnosti byly prováděny kontroly ve vztahu k výkonu této činnosti a ve vztahu k vedení odpovídajících evidencí.

Kromě prověřování dodržování ustanovení právních předpisů České republiky bylo dohlíženo i na dodržování vnitřních řídících aktů Vojenského zpravodajství, které upravují vyšší právní normy pro specifické prostředí Vojenského zpravodajství.

Tak jako v předchozích letech byla kontrolní činnost v uplynulém roce prováděna na základě plánu činnosti Vojenského zpravodajství a ročního plánu kontrol nebo operativně na základě rozhodnutí ředitele VZ. V některých případech byly naplánované kontroly operativně přizpůsobeny aktuálním potřebám a poznatkům.

DŮLEŽITÉ UDÁLOSTI MIMO HLAVNÍ ČINNOST

Vojenské zpravodajství je službou, která zabezpečuje informace, nicméně jako organizace se angažuje i v jiných důležitých činnostech, kterými jsou například charitativní projekty nebo přispívání k osvětě společnosti.

OSLAVY 100. VÝROČÍ ZALOŽENÍ VOJENSKÉHO ZPRAVODAJSTVÍ

V listopadu 2018 uběhlo přesně 100 let od založení profesionálního vojenského zpravodajství v Československé respektive České republice. Toto výročí si jeho příslušníci připomněli slavnostním nástupem v Národním památníku na Vítkově, kterého se vedle ředitele Vojenského zpravodajství brigádního generála Jana Berouna účastnili také ministr obrany Lubomír Metnar, náčelník Generálního štábu armádní generál Aleš Opata, bývalí ředitelé Vojenského zpravodajství a další hosté.

Ředitel Vojenského zpravodajství Jan Beroun při této příležitosti připomenul začátky vojenského zpravodajství i jeho budoucí vizi: *„Dnešní Vojenské zpravodajství navazuje na prvorepublikové hodnoty. Klademe důraz jak na tradiční zpravodajské disciplíny, tak na neustále se rozvíjející technické obory. Naším zájmem je se i do budoucna rozvíjet, reagovat na potencionální hrozby a přizpůsobovat se novému bezpečnostnímu prostředí.“*

U příležitosti 100. výročí založení vojenského zpravodajství vydal Vojenský historický ústav ve spolupráci s Vojenským zpravodajstvím publikaci Ve službách republiky – 100 let od

založení československého vojenského zpravodajství. Knihu sepsali historikové Karel Straka, Prokop Tomek a Tomáš Bandžuch. Jedná se o první ucelenou publikaci mapující československé respektive české vojenské zpravodajství od jeho počátků až po současnost. Dvojjazyčná kniha přibližuje historii vojenského zpravodajství nejen slovem, ale také obrazovým materiálem, z něhož značná část nebyla dosud publikována.

Na přelomu listopadu a prosince se před Generálním štábem AČR na Vítězném náměstí v Praze uskutečnila výstava mapující uplynulých 100 let vojenského zpravodajství. Celkem 22 výstavních panelů přiblížilo historii vojenského zpravodajství od jeho počátků v legiích za první světové války až po současnost. Expozice připomněla založení profesionálního vojenského zpravodajství v roce 1918, roli vojenských zpravodajců za druhé světové války včetně operace Anthropoid, vývoj vojenských zpravodajských služeb za totalitního režimu i jejich transformaci po roce 1989 a současnou činnost Vojenského zpravodajství.

CHARITATIVNÍ ČINNOST

Také v loňském roce pokračovalo Vojenské zpravodajství v charitativní činnosti a aktivně se zapojovalo do stálých i mimořádných sbírek v rámci rezortu Ministerstva obrany. V listopadu se Vojenské zpravodajství zúčastnilo tradiční sbírky u příležitosti Dne válečných veteránů ve prospěch Vojenského fondu solidarity. Příslušníci Vojenského zpravodajství vybrali celkem 117 377 Kč a stejně jako v minulých letech přispěli nejvíce ze všech zainteresovaných složek rezortu.

ZÁŠTITA NAD STŘEDOŠKOLSKOU KYBERNETICKOU SOUTĚŽÍ A WORKSHOP PRO JEHO VÍTĚZE

Ředitel VZ Jan Beroun udělil v roce 2018 záštitu druhému ročníku středoškolské kybernetické soutěže pořádané sdružením AFCEA. Vojenské zpravodajství se na kybernetické soutěži dlouhodobě podílí jak v organizační, tak expertní rovině. Pro finalisty soutěže zároveň v létě uspořádalo odborný workshop ve svém Národním centru kybernetických operací, kde se studenti seznámili s jeho činností, rozšířili si vědomosti v oblasti kybernetické obrany a vyzkoušeli si i praktická cvičení.

PREZENTACE VOJENSKÉHO ZPRAVODAJSTVÍ NA VEŘEJNOSTI

Vojenské zpravodajství se v rámci své působnosti účastní veřejných akcí, diskutuje s odbornou veřejností a snaží se přibližovat svou činnost veřejnosti. Vůbec poprvé se VZ v listopadu prezentovalo na veletrhu Future Forces Forum, kde představilo své nově vzniklé prvky - Národní centrum kybernetických operací a Satelitní centrum ČR.