Výroční zpráva
Bezpečnostní informační služby
za rok 2018

Obsah:

Slovo ředitele Bezpečnostní informační služby

Dámy a pánové,

je mi ctí a potěšením, že Vám mohu opět po roce představit novou veřejnou Výroční zprávu o činnosti Bezpečnostní informační služby za rok 2018. Hned na úvod bych rád připomněl veřejný charakter této zprávy. Vy, kteří se o zpravodajské služby zajímáte, víte, že primárním produktem tohoto typu, který BIS každý rok, v souladu se zákonem, připravuje, je utajovaná výroční zpráva určená pouze zákonným adresátům. Ta je přehledným souhrnem nejdůležitějších informací vztahujících se k činnosti služby za dané období. Utajovaná zpráva obsahuje mnohem detailnější a konkrétnější popis některých událostí, jevů a analýz a zároveň připomíná přehled hlavních informací, které BIS v předchozím roce poskytla například prezidentu republiky, předsedovi vlády, ministrům či dalším bezpečnostním složkám.

Neutajovaná a tedy veřejná výroční zpráva není a nemůže být konkrétní. Přesto jsem stejně jako moji předchůdci přesvědčen, že je to dokument důležitý a pro objektivní obraz zpravodajské služby velmi užitečný. Čtenář si ze stručného přehledu udělá velmi jasnou představu o činnosti služby, o oblastech působnosti, o prioritách schválených vládou a také obecně o tématech, na která BIS příjemce zpravodajských informací upozorňovala a před jakými hrozbami varovala.

Výroční zprávy jsou součástí komunikace s veřejností, tedy s Vámi občany, kteří máte nezpochybnitelné právo vědět, proč je důležité, aby stát měl zpravodajské služby, a v obecné rovině, jakou činnost pro stát, a tím pádem pro Vás, vykonávají. Je to nástroj důvěry, bez které v dnešní celosvětové bezpečnostní situaci nemůže žádná zpravodajská služba plnohodnotně fungovat.

Pro zpravodajské služby se stále používá označení tajné. To ovšem už dávno neznamená, že se jedná o organizace, jejichž existence je vládami popírána. Zpravodajské služby mají dnes svoji legislativu, své kontrolní orgány a také kapitolu ve státním rozpočtu, v tom rozpočtu, do kterého všichni přispíváme. Každý člověk chce vědět, kam a na co jdou jeho peníze. Umírněnou komunikaci, do které zahrnujeme i veřejnou výroční zprávu, považujeme za nástroj, kterým občanům můžeme takové informace poskytnout.

Nepochybně se opět objeví kritické hlasy, které budou tuto zprávu označovat za zbytečnou a nic neříkající. Každoroční obrovský zájem o ni nám však říká něco jiného. Nechávám na každém, ať následující stránky posoudí sám.

Přeji zajímavé čtení

plk. Ing. Michal Koudelka
ředitel Bezpečnostní informační služby

1 Náplň a rozsah zpravodajské činnosti

Činnost, postavení a působnost Bezpečnostní informační služby (dále též „BIS“) jako zpravodajské služby demokratického státu jsou upraveny příslušnými zákony, zejména zákonem č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů, a zákonem č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů. Ve své činnosti se BIS řídí rovněž Ústavou ČR, Listinou základních práv a svobod, mezinárodními smlouvami a dalšími právními předpisy České republiky.

Zpravodajské služby jsou podle § 2 zákona č. 153/1994 Sb. státními orgány pro získávání, shromažďování a vyhodnocování informací (dále jen „zabezpečování informací“) důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnost a obranu České republiky. Bezpečnostní informační služba je podle § 3 zákona č. 153/1994 Sb. zpravodajskou službou, která v rámci své působnosti podle § 5 odst. 1 zákona č. 153/1994 Sb. zabezpečuje informace:

- o záměrech a činnostech namířených proti demokratickým základům, svrchovanosti a územní celistvosti České republiky,
- o zpravodajských službách cizí moci,
- o činnostech ohrožujících státní a služební tajemství,
- o činnostech, jejichž důsledky mohou ohrozit bezpečnost nebo významné ekonomické zájmy České republiky,
- týkající se organizovaného zločinu a terorismu.

Podle § 5 odst. 4 zákona č. 153/1994 Sb. plní BIS další úkoly, pokud tak stanoví zvláštní zákon (např. zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů) nebo mezinárodní smlouva, jíž je Česká republika vázána.

Zákon č. 153/1994 Sb. v ustanovení § 7 dále stanoví, že za činnost BIS odpovídá vláda, která zároveň koordinuje její činnost. Vláda podle ustanovení § 8 odst. 4 tohoto zákona ukládá BIS úkoly v mezích její působnosti. Prezident republiky ukládá BIS úkoly v mezích její působnosti a s vědomím vlády.

K plnění svých úkolů je BIS oprávněna spolupracovat s ostatními zpravodajskými službami ČR. Zákon č. 153/1994 Sb. tuto spolupráci v § 9 podmiňuje dohodami uzavíranými mezi zpravodajskými službami se souhlasem vlády.

Spolupráci se zpravodajskými službami cizí moci může BIS podle § 10 zákona č. 153/1994 Sb. uskutečňovat pouze se souhlasem vlády.

2 Zpravodajská činnost a zpravodajské poznatky

Vážnou hrozbu pro bezpečnost ČR představovaly v roce 2018 zejména nepřátelské aktivity cizí moci. Státní i nestátní, cizí i domácí aktéři se snažili zapojením široké škály metod a aktivit oslabit české státní instituce, ovlivnit oficiální mezinárodně-bezpečnostní postoje státu a vydávat přirozené atributy demokratického zřízení za jeho slabiny. Ohrožení těmito tzv. hybridními hrozbami se týkalo řady oblastí napříč působností BIS.

Hybridní hrozby využívají multivektorové nástroje a kombinují koordinovanou i organicky vzniklou činnost. S využitím ekonomických, politických, vojenských a informačních tlaků využívají zdánlivých nedokonalostí (dlouhý legislativní proces, parlamentní diskuse, správní procedury, apod.) státních institucí a demokratických procesů. Cílem je ovlivnit rozhodovací proces na různých úrovních veřejné správy ve svůj strategický prospěch, a to aktivitou, neaktivitou nebo paralýzou subjektu odpovědného za rozhodování.

Vedle toho pokračoval růst významu kyberprostoru. Potvrdilo se, že kybernetická bezpečnost představuje integrální součást bezpečnosti a že ochrana před nežádoucími aktivitami v kyberprostoru představuje důležitý prvek komplexní péče o chráněné zájmy ČR. Dění v kyberprostoru se podstatně promítalo do zpravodajské situace ve všech oblastech působnosti BIS. To dokládá zejména skutečnost, že ČR a její instituce se staly terčem několika kyberšpionážních kampaní řízených nebo podporovaných cizí státní mocí.

Souhrn veškeré zpravodajské činnosti Bezpečnostní informační služby v roce 2018 obsahuje utajovaná Zpráva o činnosti BIS za rok 2018, kterou podle § 8 odst. 1 zákona č. 153/1994 Sb. předkládá BIS každoročně vládě a prezidentovi republiky.

O konkrétních zpravodajských zjištěních a výsledcích analýz, z nichž rámcový přehled o činnosti BIS v této veřejné výroční zprávě vychází, informovala BIS v průběhu roku 2018 oprávněné adresáty podle § 8 zákona č. 153/1994 Sb. V tomto období předala BIS prezidentovi a členům vlády téměř 400 dokumentů. Další stovky informací zaslala BIS Policii ČR (PČR), Úřadu pro zahraniční styky a informace (ÚZSI), Vojenskému zpravodajství (VZ) a dalším státním orgánům.

2.1 Zpravodajské služby a nepřátelské aktivity cizí moci v ČR

Bezpečnostní informační služba se v rámci své zákonné působnosti i v roce 2018 věnovala všem zpravodajským službám působícím na našem území proti zájmům České republiky.

V souladu s vládou stanovenými prioritami, mírou ohrožení zájmů České republiky a kapacitami a možnostmi BIS byly v roce 2018 prioritními cíli zpravodajského rozpracování aktivity ruské a čínské státní moci ohrožující bezpečnost a další klíčové zájmy ČR. Ruské a čínské zpravodajské aktivity zasahovaly do oblastí politiky, diplomacie, špionáže, ekonomiky i informačního boje.

V případě Ruska není hlavní hrozbou některá ze složek zpravodajských či para-zpravodajských aktivit, ale nekonvenční (tzv. hybridní) charakter ruských operací, které jsou cíleny na nepřítele, jehož Rusko chápe jako hlavní vojenskou hrozbu pro svou bezpečnost: NATO a jeho členské státy, tj. i ČR. V ruském podání si zpravodajské a nezpravodajské entity mohou vyměňovat role i funkce, a tedy

jakýkoliv orgán (či jemu podřízená agentura) může být využit pro zpravodajské operace či pro jejich zakrytí. Klíčovým ruským cílem je manipulace s rozhodovacími procesy a jednotlivci zodpovědnými za rozhodování s cílem přimět protistranu k činnostem, kterými se sama oslabí.

Čínské aktivity jsou co do komplexity srovnatelné s ruskými. S ohledem na geografické vzdálenosti a absenci historie čínské vojenské angažovanosti v Evropě však BIS pokládá za zásadní bezpečnostní problém uplynulého období zejména nárůst aktivit čínských zpravodajských důstojníků, které lze jednoznačně hodnotit jako vyhledávání a kontaktování potenciálních spolupracovníků a agentů mezi českými občany.

Česká republika byla předmětem zájmu aktérů s vazbou na ruskou a čínskou státní moc i v kyberprostoru. Instituce a občané ČR se stali cílem hned několika kyberšpionážních kampaní, přičemž nejzávažnější z nich byla kompromitace neutajované sítě Ministerstva zahraničních věcí (MZV).

V roce 2018 nebyly na území ČR zjištěny závažné nepřátelské aktivity zpravodajských služeb (ZS) dalších států s výjimkou aktivit íránských ZS, jež jsou popsány níže.

Ruské zpravodajské služby

V roce 2018 byli na území ČR přítomni a vyvíjeli zpravodajskou činnost příslušníci a spolupracovníci všech ruských zpravodajských služeb, tj. civilní rozvědky SVR, vojenské rozvědky GRU a vnitřní bezpečnostní a zpravodajské služby FSB. Dlouhodobým bezpečnostním problémem zůstává personální naddimenzování ruské diplomatické mise v ČR, které pro české občany zvyšuje hrozbu vystavení se kontaktu se zpravodajskou službou cizí moci.

Zpravodajské kapacity RF na území ČR byly částečně oslabeny českou reakcí na útok nervově-paralytickou látkou novičok v britském Salisbury, kterou byl v březnu 2018 otráven Sergej Skripal a jeho dcera. Po britském oznámení podrobností útoku se ruská strana snažila vyvolat na mezinárodní scéně dojem, že použitá toxická látka pocházela z jiných zemí, zejména z ČR. Podle zjištění BIS nervově-paralytickou látku použitou ve Velké Británii žádný subjekt v ČR nevyvíjel, nevyráběl ani neskladoval. S ohledem na skutečnost, že osoby podílející se na útoku se v minulosti mimo jiné pohybovaly i na území ČR, a v návaznosti na britskou žádost o kolektivní solidární postup spojenců zpracovala BIS příslušné podkladové informace, které byly následně využity v rámci procesu vedoucího k vyhoštění tří ruských nedeklarovaných zpravodajských důstojníků.

V souladu s hybridní strategií, kterou se RF snaží ovlivňovat rozhodování politických představitelů jiných zemí, mezitím ruští zpravodajští důstojníci usilovali o vytváření vazeb a kultivaci vlivové báze v blízkém okolí politiků, kteří mají vliv na vývoj v oblastech zájmu RF.

Ruská diplomatická mise a rezidentura jedné z ruských zpravodajských služeb se nadále zajímaly o komunitu ruských krajanů. Pomocí sběru informací a budování vlivových sítí usilovala ruská státní moc zejména o marginalizaci protikremelsky orientovaných krajanských subjektů, resp. posilování vlivu krajanských subjektů sympatizujících se stávající politickou reprezentací RF.

Česká republika byla i v roce 2018 jednou ze scén subverzních aktivit řízených orgány ruské státní moci proti politické svrchovanosti a územní celistvosti Ukrajiny. Inkriminované aktivity nesly znaky aktivních opatření. Snaha utajovaným způsobem v cílových zemích vyvolávat a posilovat společenské tenze na zástupných tématech, jež však v důsledku ovlivňují celou mocenskou rovnováhu, je letitou

ruskou praxí. Její využívání zintenzivnilo v souvislosti s geopolitickým vývojem zarámovaným ruskou anexí Krymu v roce 2014. Řádový nárůst veřejné pozornosti věnované této praxi se pak odrazil do diskuze o tzv. hybridním přístupu RF k vedení války, resp. zahraniční politiky.

BIS v součinnosti s partnerskou ZS získala také informace o aktivitách ruské zpravodajské služby FSB, která na českém území utajeně budovala ICT infrastrukturu. Tato infrastruktura byla součástí rozsáhlejšího systému, který byl využitelný pro utajované kybernetické a informační operace FSB v lokálním i globálním rozsahu. Ve spolupráci s PČR byla tato síť rozbita a bylo tak zabráněno aktivitám FSB proti zájmům ČR či našich spojenců.

Čínské zpravodajské služby

Čínské zpravodajské aktivity se rozrostly jak co do intenzity, tak co do rozsahu a i v roce 2018 představovaly hrozbu pro zájmy a bezpečnost ČR. Na území ČR operovaly všechny nejvýznamnější čínské zpravodajské služby, tj. vojenská rozvědka (MID), Oddělení pro mezinárodní styky Ústředního výboru Komunistické strany Číny (OMSÚV), Ministerstvo státní bezpečnosti (MSS) a Ministerstvo veřejné bezpečnosti (MPS). K nátlakovému prosazování čínských zájmů se uchylovali stejně jako v předcházejícím období také čínští kariérní diplomaté.

V kontextu čínských aktivit cílících na českou akademickou obec, bezpečnostní sbory a státní správu zaznamenala BIS rostoucí počet čínských pozvání adresovaných českým občanům na školení, semináře a poznávací zájezdy. Čínská strana nabízí pozvaným hradit veškeré výdaje (dopravu, ubytování, stravné, zápisné) a nadto ještě přidává kapesné. Organizace takových cest zajišťuje čínské straně řadu výhod – Čína si jimi vytváří kontaktní síť osob, které jí budou nakloněny, resp. si budou vědomy toho, že ČLR „něco dluží“ a budou ochotny jí vycházet vstříc. Ze zpravodajského hlediska je nejrizikovějším aspektem samotná fyzická přítomnost hosta na území Číny. K oslovení pro spolupráci totiž čínské zpravodajské služby obvykle využívají právě pobyt zájmových osob na území Číny, případně ve třetí zemi (tj. zpravidla ne v zemi, odkud zájmová osoba pochází).

K oslovování potenciálních českých zdrojů či spolupracovníků (z řad akademiků, studentů, státních úředníků a jiných osob s přístupem k citlivým informacím) využívají ZS ČLR v ČR mj. profesní sociální síť LinkedIn.

Velmi významnou součástí zpravodajských aktivit Číny v ČR byla trvající čínská snaha narušovat politické i ekonomické česko-tchajwanské vztahy. Zástupci ČLR vyvíjeli v roce 2018 maximální úsilí, aby o vzájemné spolupráci získávali informace a následně mohli rychle reagovat s cílem oslabovat české kontakty s Tchaj-wanem.

Ruské a čínské kyberšpionážní aktivity

Kompromitace sítě MZV

V roce 2018 proběhlo šetření rozsáhlé kompromitace neutajované sítě MZV. Ze získaných informací vyplývá, že se s největší pravděpodobností jedná o ruskou kyberšpionážní kampaň. Vektorem špionážního útoku byl zastupitelský úřad (ZÚ) ČR v zahraničí, k jehož kompromitaci došlo již na konci roku 2017.

V prvotní fázi útoku aktér kompromitoval několik koncových počítačů neutajované sítě ZÚ. Dalším šetřením byly odhaleny pokusy útočníka o použití technik eskalace oprávnění a laterálního pohybu. Útočníci se také snažili o zajištění si trvalého skrytého přístupu do napadeného systému.

BIS také získala informace o jiném, nesouvisejícím, incidentu, a to kompromitaci vybraných počítačových stanic neutajované sítě MZV několika druhy škodlivého softwaru, které bylo možné na základě rozličných indikátorů velmi pravděpodobně spojit s aktivitami čínské kyberšpionážní skupiny. Stopy po pečlivě ukrytých aktivitách bylo možné dohledat několik let zpětně a za tu dobu se útočníkům podařilo exfiltrovat množství dokumentů s tématikou odpovídající zájmům předmětného kyberšpionážního aktéra.

Ministerstvo zahraničních věcí je vzhledem ke své působnosti neustále vystaveno více či méně sofistikovaným kybernetickým útokům nejen státních aktérů, proto je třeba nadále pokračovat ve vylepšování procesů, zabezpečení komunikace a zajištění takových technických opatření, které umožní na útoky efektivně reagovat.

Útoky kyberšpionážní kampaně APT28/Sofacy proti příslušníkům Armády ČR (AČR)

I v roce 2018 BIS informovala své zákonné adresáty o případech kompromitace soukromých e-mailových účtů patřících příslušníkům AČR s tím, že tyto e-mailové účty jsou s největší pravděpodobností kompromitovány ruskou kyberšpionážní kampaní APT28/Sofacy. Ačkoliv útočníci nezískali žádné informace utajované podle zákona č. 412/2005 Sb., získali přístup k řadě osobních a citlivých údajů (bydliště, faktury, místa a termíny dovolených, rodinné zázemí, mnoho kontaktních údajů apod.). Tyto informace mohou v budoucnu zneužít formou sociálního inženýrství pro další útoky, a to nejen na příslušníky AČR.

Při šetření zaměřeném na aktivity kyberšpionážní kampaně APT28/Sofacy na území ČR odhalila BIS i případ kompromitace, při kterém byla e-mailová schránka příslušníka AČR automatizovaně vytěžována prostřednictvím svého propojení protokolem IMAP nebo POP3 s další e-mailovou schránkou ovládanou útočníky. Tento postup propojení e-mailových schránek je vysoce efektivní a u řady českých e-mailových služeb pro oběť neodhalitelný, protože poskytovatelé neumožňují uživatelům kontrolovat, z jakých IP adres bylo do jejich schránky přistupováno.

Mimo případy kompromitace osobních účtů příslušníků AČR šetřila BIS v průběhu roku 2018 ještě několik dalších obdobných případů e-mailových účtů, u kterých panovalo podezření z jejich kompromitace ruskou kyberšpionážní kampaní APT28/Sofacy.

2.2 Ochrana ústavnosti a demokratických základů státu

Nejzávažnější hrozbu pro ústavnost ČR představovalo v roce 2018 působení spektra proruských aktivistů, kteří se podíleli na šíření dezinformací. Termínem „proruští aktivisté“ v tomto kontextu BIS neoznačuje všechny prorusky smýšlející osoby, ale primárně ty, které svými aktivitami vědomě či nevědomě přímo napomáhají cizí moci.

BIS se nadále věnovala monitorování aktivit paramilitárních a domobraneckých uskupení, která svou samotnou existencí zpochybňovala monopol státu na legitimní užití násilí na vlastním území. Domobranecké skupiny v roce 2018 stagnovaly, což souviselo jednak s celospolečenským vývojem, zejména nenaplněním obav z příchodu většího množství migrantů do ČR, jednak s vnitřním stavem jednotlivých uskupení. Jako skutečně funkční se vyprofilovaly především skupiny působící na lokální

úrovni, a to jen v některých regionech ČR. Spíše než radikály s jasným ideologickým ukotvením i tyto skupiny přitahovaly především osoby, které bojový výcvik a činnost v rámci domobran vnímaly jako volnočasovou aktivitu a hobby. Působení paramilitárních a domobraneckých uskupení proto nepředstavovalo reálnou bezprostřední hrozbu pro demokratické základy a bezpečnost ČR.

Stejně tak rok 2018 potvrdil, že v současnosti bezpečnostní hrozbu nepředstavují ani tradiční pravicově a levicově extremistická uskupení. Pravicově extremistická scéna se již několik let potýká s vnitřní krizí a nelze očekávat, že by v nejbližších letech došlo k výrazné změně. Popularita a podpora politicky angažovaných pravicových extremistů byla zcela minimální. Rovněž členská základna levicových antiautoritářských platforem je dlouhodobě početně slabá a stagnuje. Militantní anarchisté se v ČR neprojevovali. Současný stav obou scén ilustruje i fakt, že násilné pouliční střety levicových a pravicových extremistů téměř vymizely.

Proruští aktivisté

Proruští aktivisté v posledních letech stále intenzivněji, koncepčněji a systematičtěji brojí proti politickému uspořádání v ČR a členství v EU a NATO. Při svém působení se podílejí na nastolování témat konstruovaných nebo podporovaných cizí mocí. V rámci těchto agend často dochází ke zveličování významu existujících hrozeb a vytváření imaginárních problémů. Nezřídka rovněž obsahují podněty k jednání proti zájmům spojenců. Za využití zavádějících, manipulativních či lživých tvrzení proruští aktivisté působí na veřejné mínění a vyvolávají a udržují strach a napětí ve společnosti, což přispívá k její polarizaci a radikalizaci a podkopávání důvěry obyvatel v principy svobodného demokratického státu. Témata sloužící zájmům cizí moci mohou vytvářet tlak na politické představitele a rozhodovací systémy či procesy.

Proruští aktivisté tak, ať již vědomě či nevědomě, podporovali vlivové operace RF a prosazovali ruské zájmy na úkor zájmů ČR. Značný počet proruských aktivistů je motivován ideologickým spřízněním, obdivem k režimu prezidenta Putina či adorací Ruska obecně. U některých osob nicméně existují indicie o jejich přímé provázanosti s ruskou státní mocí či řízení zpravodajskými službami RF.

Spektrum proruských aktivistů tvoří široký okruh subjektů bez ohledu na pravo-levé dělení a formální postavení. Zahrnuje členy nejrůznějších nacionalistických a populistických hnutí, některých politických stran, zapsaných spolků, neformálních iniciativ a sdružení osob i nezařazené jednotlivce, včetně osob a skupin vzešlých z dříve působícího protiimigračního hnutí. Do spektra dále spadají média, která se prezentují jako nezávislá či alternativní, osoby usilující o územní dezintegraci Ukrajiny a kozácká uskupení. Všechny tyto subjekty byly vzájemně provázané a jejich představitelé dokázali díky společným sympatiím k Rusku spolupracovat bez ohledu na různá ideologická východiska.

Proruští aktivisté ovlivňovali veřejné mínění mimo jiné rozšiřováním různých konspiračních teorií a proruské propagandy, k čemuž jako média využívali zejména internet, sociální sítě, vlastní internetové videokanály či tzv. nezávislá/alternativní média, která jsou v dnešní době hlavními producenty dezinformací ve prospěch RF.

Část spektra proruských aktivistů se soustředila na veřejná shromáždění, debaty, besedy a petiční akce zaměřené proti EU, NATO a proti rozhodnutím těchto mezinárodních struktur souvisejícím s problémem imigrace do Evropy.

Paramilitární a domobranecká uskupení

Navzdory tomu, že celková rizika plynoucí z činnosti domobran hodnotí BIS jako nepříliš významná, dílčí aspekty aktivit uskupení a jejich členů měly rizikový potenciál. Mezi členy uskupení se nacházeli i jednotlivci tíhnoucí ke konspiračním teoriím či s radikálnějšími sklony. Ve spojení s kladným vztahem a přístupem ke zbraním šlo o potenciálně rizikové jedince, jejichž chování nelze předvídat.

Členové paramilitárních uskupení kvůli své výrazné protizápadní orientaci také přispívali k šíření proruské propagandy a na ni navázaných konspiračních narativů. Poté, co ve společnosti pozvolna utichlo téma migrace a souvisejícího nebezpečí ze strany uprchlíků, se mnozí paramilitáři (přestože téma migrace nadále hojně využívali) zaměřili také na vytváření dojmu hrozícího ozbrojeného konfliktu mezi Západem a RF.

Za účelem získání legitimity se paramilitární uskupení dále pokoušela pořádat různé osvětové akce pro veřejnost a navazovat kontakty a spolupráci se zástupci obcí a bezpečnostních složek na regionální úrovni v oblasti zajištění bezpečnosti v ulicích obcí a měst. Významným cílem představitelů domobraneckých uskupení bylo i v roce 2018 dosáhnout legalizace domobran jejich zakotvením v právním řádu ČR.

Tradiční politický extremismus

Mezi dominantní témata pravicových extremistů stejně jako v předchozích letech patřila kritika migrační politiky, výrazné protiunijní postoje, kritická vyjádření na adresu muslimů, vymezování se vůči lidskoprávním aktivistům či nevládním organizacím atp. Docházelo i k reaktivaci protiromské rétoriky, která byla několik posledních let na okraji jejich zájmu.

V roce 2018 se více než kdykoliv předtím ukázalo, že rétorika a témata dříve vyhrazená „ortodoxním“ pravicovým extremistům postupně využívá stále se rozšiřující spektrum subjektů. Tolerance veřejnosti k těmto projevům se výrazně zvýšila a významně se posunulo vnímání hranice, jaká xenofobní či rasistická vyjádření mohou být součástí politického mainstreamu. Tento posun je jedním z důvodů úpadku tradičních extremistických uskupení, která ztrácí prostor, v němž se mohla profilovat jako jedinečný nositel radikálních idejí.

Veřejné aktivity anarchoautonomních kolektivů stagnovaly, pořádaly především interní akce menšího rozsahu zaměřené dovnitř hnutí jako přednášky, aktivistická setkání, solidární a vzpomínkové akce, koncerty či happeningy. Většina anarchoautonomní scény odmítala násilí i ideový proud tzv. povstaleckého anarchismu.

Militantně orientovaní anarchisté byli prakticky neaktivní, nedošlo k žádné přímé akci, k níž by se přihlásili. Minimální aktivita byla patrná i na internetu, omezovali se především na vyjadřování podpory zadrženým anarchistům v zahraničí. Výjimkou bylo zveřejnění návodu, jak anonymizovat svou činnost na internetu.

Radikálně komunistická část levicově extremistické scény je fragmentovaná, názorově nesourodá a dlouhodobě stagnuje. Její představitelé si toho byli vědomi a v roce 2018 došlo k několika (ve výsledku neúspěšným) pokusům o zvrácení tohoto stavu a aktivizaci scény. Někteří radikální komunisté považovali za východisko užší kooperaci napříč celou „pokrokově“ levicovou scénou a zvažovali vytvoření širší levicové fronty. Jednotlivé subjekty nepořádaly akce většího rozsahu, ale často spolupracovaly na organizaci menších akcí.

2.3 Terorismus a organizovaný zločin

Terorismus

Situace v oblasti terorismu a islamistické radikalizace byla na území ČR i v roce 2018 klidná. Kromě běžného monitoringu vývoje situace v muslimské populaci prověřovala BIS v minulém roce signály o možném výskytu islamistických radikálů na území ČR. Konkrétní přímá rizika ve vztahu k ČR nebyla v žádném z případů potvrzena. Několika dalším podezřením se BIS věnovala v rámci boje proti financování terorismu. Ani v této oblasti nebyly získány poznatky nasvědčující tomu, že by území ČR sloužilo jako logistická či jiná základna mezinárodního terorismu.

BIS věnovala pozornost radikálním muslimům, kteří v předchozích letech opustili ČR, aby se připojili k teroristickým organizacím v Sýrii a Iráku. BIS potvrdila úmrtí jednoho z těchto zahraničních bojovníků. BIS stejně jako v předchozích letech zabezpečovala a předávala zákonným adresátům zpravodajské informace o radikálním imámovi Sameru Shehadehovi, který byl do ČR vydán na základě mezinárodního zatykače pro obvinění z podpory terorismu, protože radikálními názory ovlivnil svého bratra a jeho muslimskou manželku, oba občany ČR, kterým následně pomohl v organizaci cesty a připojení se k syrské odnoži al Qá'idy v Sýrii.

Pokračovalo také získávání informací o rizikových Maghrebanech, projevech islamistické radikalizace v části kazašské komunity, libyjských pacientech s vazbami na islamistické sítě a o radikalizačním potenciálu části muslimské komunity v Praze.

Maghrebská komunita je decentralizovaná a postrádá autority, které by bránily projevům radikalizace. Za indikátory rizikovosti u Maghrebanů považuje BIS nezájem o integraci do většinové společnosti, kriminální činnost, snahu legalizovat svůj pobyt v ČR účelovým sňatkem (či vztahem) a finanční tíseň. V okruhu osob vykazujících tyto znaky zaznamenala BIS několik jedinců s radikálními projevy a jejich aktivitám věnovala odpovídající zpravodajskou pozornost.

Bezpečnostní riziko představovala stejně jako v předchozích letech část kazašské komunity, jejíž členové nadále odmítají integraci do české společnosti a vyznávají specifickou formu islamismu. Potenciál šíření islamistické radikalizace těchto muslimů byl v ČR omezený.

V problematice tzv. libyjských pacientů, kteří se přijíždějí do ČR léčit v rámci Libyí hrazeného léčebného programu pro zraněné veterány, přispěla BIS ve spolupráci s ostatními bezpečnostními složkami ČR k odhalení řady osob s vazbami na islamistické struktury v Libyi. Vůči těmto osobám z řad léčených libyjských pacientů, jejich doprovodů a zprostředkovatelů léčby byla iniciována opatření k zamezení jejich dalšího vstupu na území ČR.

Dění v jednotlivých organizacích sdružujících muslimy na území ČR bylo ovlivněno jejich dynamickým interním vývojem, přičemž nejvýznamnější proměnou prošla Muslimská obec v Praze. Muslimské organizace se stejně jako v předchozích letech potýkaly s personálními a finančními problémy. I přes snahy různých skupin o získání vlivu nad těmito organizacemi byl zachován dlouhodobě umírněný charakter muslimské komunity.

Vzhledem k poznatkům z minulých let o státní podpoře terorismu ze strany Íránu věnovala BIS nadále svou pozornost činnosti íránských zpravodajských služeb v ČR. Ty byly aktivní na území ČR i v roce 2018. V rámci rozvoje vztahů ČR s Íránem pokračovala spolupráce na různých podnikatelských projektech. Tato spolupráce má nicméně i bezpečnostní aspekty, protože mezi běžnými íránskými

obchodníky se mohou nacházet jedinci, kteří jsou různou měrou spjati s bezpečnostními složkami Íránu.

Počátkem roku BIS úspěšně zakončila operaci monitorující infrastrukturu kyberšpionážní kampaně hnutí Hizballáh umístěnou na území ČR. Tato kyberšpionážní kampaň necílila na české občany, ale především na oběti z oblasti Blízkého východu.

Útočníci operovali z Libanonu a na území ČR v letech 2017 a 2018 využívali několik serverů, jejichž primární funkcí byla distribuce škodlivé špionážní aplikace pro mobilní operační systém Android. Využívali při tom metod sociálního inženýrství a pokoušeli se skrze falešné profily atraktivních žen na sociálních sítích přesvědčit své cíle k nainstalování upravené aplikace, vydávající se za legitimní komunikační program. Po instalaci začala aplikace odesílat citlivá data z telefonu na servery útočníků.

Na začátku roku 2018 došlo na základě získaných zpravodajských informací k eliminaci útočné infrastruktury určené pro šíření škodlivého kódu.

BIS se dále zabývala vlivem blízkovýchodního napětí na bezpečnostní situaci v ČR. V tomto ohledu nebyly získány poznatky nasvědčující tomu, že došlo k přenosu tohoto napětí na území ČR a že by v jeho důsledku hrozilo spáchání teroristického útoku na území ČR.

Organizovaný zločin

Stejně jako v minulých letech monitorovala BIS situaci kolem informačního systému Visapoint (IS Visapoint) provozovaného Ministerstvem zahraničních věcí. Ten měl zefektivnit zápis žadatelů o vízum na volné termíny pro pohovor na ZÚ ČR a eliminovat machinace s místy ve frontách. Spuštěn byl v roce 2009, jeho zavedení ale nesplnilo očekávání, protože problém s machinacemi jen přenesl z fyzického světa do kybernetického prostředí.

Zprostředkovatelé, kteří za úplatu prováděli v IS Visapoint zápisy na termíny pohovorů, se snažili u vybraných typů víz zaplňovat veškeré volné termíny fiktivními osobami a znemožnit tak zápis reálným žadatelům mimo svůj dosah. Za místo v elektronické frontě pak požadovali až několik tisíc eur za osobu. Dominantní zprostředkovatel zápisů nakonec za využití automatizovaných nástrojů takřka zcela kontroloval přístupy k vízovým pohovorům na několika ZÚ ČR. Tento zprostředkovatel svým jednáním bránil legitimním zájemcům podat žádost o vízum a tito zájemci byli následně nuceni nakupovat volná místa na pohovory za stovky až tisíce eur za osobu. Za využití svých IT znalostí tak zprostředkovatel dlouhodobě a systematicky ovlivňoval vízový proces ČR za účelem vlastního obohacení, což mu přinášelo zisky v řádu milionů korun ročně.

Ukončení provozu IS Visapoint a změna způsobu získávání volných termínů pohovorů zkomplikovaly tomuto zprostředkovateli cestu za vlastním obohacením, přesto se dále pokoušel najít způsob, jak blokovat termíny pohovorů na ZÚ ČR.

V září 2018 kriminalisté sekce organizovaného zločinu Národní centrály proti organizovanému zločinu služby kriminální policie a vyšetřování zadrželi osm cizích státních příslušníků původem z Ruské federace a Vietnamské socialistické republiky, kteří jsou důvodně podezřelí z organizování trestné činnosti, která souvisí s podáváním žádostí o udělení pobytových oprávnění na území České republiky ze strany občanů Vietnamské socialistické republiky. BIS na tomto případu úzce spolupracovala s policií.

2.4 Činnosti ohrožující bezpečnost nebo významné ekonomické zájmy ČR

Proliferace zbraní hromadného ničení a obchod s vojenským materiálem

Česká republika se na mezinárodním poli zavázala nepodílet se na šíření (proliferaci) zbraní hromadného ničení (ZHN) a jejich nosičů a minimalizovat rizika spojená s mezinárodním obchodem s konvenčními zbraněmi, vojenským materiálem, výbušninami a zbožím dvojího použití. ČR je členem všech Mezinárodních kontrolních režimů (MKR)[1], které se zabývají jadernými, chemickými a biologickými (bakteriologickými a toxinovými) ZHN a jejich nosiči a dalšími mezinárodně kontrolovanými položkami.

V této oblasti je úkolem BIS získávat a vyhodnocovat informace a včasně informovat o konkrétních událostech, jevech nebo trendech spojených se zahraničním obchodem s kontrolovanými položkami, včetně obcházení nebo nedodržování závazků ČR vycházejících ze sankčních opatření proti konkrétním zemím, subjektům nebo entitám[2].

Zbraně hromadného ničení jsou v ČR z obchodu zcela vyloučeny a další kontrolované položky podléhají v ČR zákonným předpisům[3]. Mezi proliferačně rizikovými zeměmi je nicméně ČR vnímána jako tradiční strojírenská země s kvalitními výrobky, materiály a technologiemi v cenově přístupných relacích. I v roce 2018 proto BIS zaznamenala množství případů, kdy proliferačně rizikové země v ČR usilovaly o nákup strojírenských zařízení, speciálních materiálů, technologií a know-how využitelných k výzkumu a vývoji vlastních ZHN. Mezi proliferačně rizikové země patří zejména KLDR, Sýrie, Írán a Pákistán.

Účinným opatřením proti obchodu se ZHN a kontrolovanými položkami jsou mezinárodní sankční opatření, která jsou nadále platná proti KLDR, Sýrii a přes uvolnění sankcí proti Íránu v jaderné oblasti platí nadále i zákaz dodávek konvenčních zbraní a zboží pro íránský raketový program. Mezinárodní sankční zbrojní opatření se týkala také řady zemí Blízkého a Středního východu, jihovýchodní Asie a kavkazských nebo afrických zemí. Sankce EU se od srpna 2014 týkají také dodávek ruským zbrojovkám i subjektům zabývajícím se zbrojními programy.

Zájem o vojenský materiál, zbraně a výbušniny nebo o speciální komponenty využitelné k vývoji a výrobě např. bezpilotních systémů (dronů) pro vojenské účely projevovaly subjekty z Ruska, Číny i dalších zemí s nestabilním a represivním režimem a ze zemí, ve kterých probíhají ozbrojené konflikty. V případech vývozů komponent k bezpilotním prostředkům existuje také riziko reexportu do dalších proliferačně rizikových zemí.

---

[1] Wassenaarské ujednání *(Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, WA),* Australská skupina *(Australia Group, AG)*, Kontrolní režim raketových technologií *(Missile Technology Control Regime, MTCR)* posílený o Haagský kodex *(The Haague Code of Conduct, HCOC),* Skupina jaderných dodavatelů *(Nuclear Suppliers Group, NSG),* Zanggerův výbor *(Zangger Committee, ZC)* a rezoluce RB OSN č. 1540 (2004).

[2] § 5 odst. 4 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů.

[3] Např. zákon č. 38/1994 Sb., o zahraničním obchodu s vojenským materiálem, zákon č. 594/2004 Sb., jímž se provádí režim Evropských společenství pro kontrolu vývozu zboží a technologií dvojího užití, nebo zákon č. 61/1988 Sb., o hornické činnosti, výbušninách a o státní báňské správě, ve znění pozdějších předpisů.

Společnosti z proliferačně rizikových zemí jsou schopné při obstarávání zboží s potřebnými technickými parametry připravit složité obchodní cesty přes třetí země a reexportům zboží přizpůsobit platby za zboží s cílem znemožnit identifikaci takových obchodních tras a všech zapojených firem. Porušení nebo obcházení mezinárodních závazků by poškodilo bezpečnost, ekonomické zájmy i dobré jméno ČR a oslabilo by její postavení na mezinárodní úrovni.

Ochrana významných ekonomických zájmů

V roce 2018 se BIS zaměřovala ve zvýšené míře na negativní jevy směřující proti nezávislému a řádnému výkonu regulatorních a dohledových funkcí centrálních orgánů státu. Důležitým tématem se stala také rizika plynoucí z ekonomických aktivit subjektů napojených na cizí moc prosazující skrze ně své zahraničně politické a strategické cíle.

V ostatních oblastech byla struktura sledovaných jevů ohrožujících významné ekonomické zájmy ČR podobná jako v předchozích letech. BIS popsala řadu případů klientelismu, nelegitimního lobbingu či snah obcházet zákon, které měly obdobný charakter jako případy zaznamenané v minulosti. BIS také věnovala pozornost důsledkům takových aktivit a schopnostem státu či státem ovládaných společností se s těmito důsledky vyrovnat.

BIS identifikovala několik závažných zásahů do činnosti regulatorních a dohledových orgánů. Některé subjekty se z části úspěšně pokoušely ovlivňovat klíčová rozhodnutí úřadů ve prospěch svých partikulárních zájmů. K tomu využívaly široké spektrum metod sahající od zcela legálního lobbingu přes skryté ovlivňování mediálního prostoru až po pokusy přímo řídit rozhodování úřadů skrze vysoce postavené insidery v jejich struktuře. Obvyklou součástí strategie těchto subjektů byla i snaha se různými cestami dostat ke klíčovým informacím zevnitř úřadů, jako jsou chystaná rozhodnutí nebo plánované analýzy sloužící úřadům ke stanovení dalšího postupu.

Uvedené zásahy považuje BIS za závažné ohrožení významných ekonomických zájmů ČR. Zmíněné regulatorní a dohledové úřady mají významný vliv na podmínky v celých odvětvích a manipulace s jejich rozhodováním se výrazně negativně podepisují na důvěře znevýhodněných subjektů ve schopnost státu zajistit spravedlivé ekonomické prostředí. Znevýhodněny přitom mohou být jak podnikatelské subjekty, tak i široké vrstvy spotřebitelů. Takový stav pak může mít negativní dopad na investiční klima a může snižovat atraktivitu ČR pro renomované zahraniční investory.

Schopnost některých z těchto úřadů řádně vykonávat svoji činnost byla snížena také v důsledku personální nestability a sporů mezi jednotlivými představiteli. Spory v několika případech vedly až ke zpochybnění legitimity rozhodování celého úřadu. Vzájemná animozita a z ní plynoucí snahy poškodit protivníky vytvářely i terén pro nelegitimní lobbistické aktivity. Součástí sporů byly totiž mj. snahy o získání vlivného zastání, což bylo spojeno s rizikem, že vyjádření podpory bude nebo již bylo směněno za poskytování výhod při rozhodování úřadu.

BIS zaznamenala také snahy regulovaných a dohlížených subjektů obcházet zákonná pravidla. V jednom z regulovaných odvětví docházelo k uzavírání dohod týkajících se cen a přístupu k zakázkám. V jiném strategickém odvětví docházelo k obcházení důležitých norem tak, aby zúčastněné subjekty mohly pod clonou legální ekonomické činnosti zneužívat přítomnost na českém trhu k realizaci pro ČR nežádoucích cílů. V tomto ohledu se jako rizikové ukázaly zejména subjekty financované kapitálem pocházejícím ze zemí, kde státní administrativa prosazuje své zájmy v zahraničí skrze silný vliv na rozhodování obchodních společností.

Důležitým tématem se proto stala identifikace a hodnocení rizik, která mohou vyvstávat z napojení ekonomických subjektů působících v ČR na cizí moc. Potvrdilo se, že čím méně demokratický je režim v zemi, ze které kapitál pochází, tím vyšší je riziko zneužívání ekonomických prostředků k zahraničně-politickým cílům. Autoritářské země dokáží ze své podstaty prosadit svůj vliv v soukromých společnostech účinněji. Řadou formálních i neformálních nástrojů jsou schopny přinutit tyto společnosti v případě potřeby potlačit vlastní ekonomické zájmy a upřednostnit před nimi politické, vojenské nebo zpravodajské cíle státu. Tyto cíle mohou být přitom v závažném rozporu se zájmy ČR např. v oblasti ochrany klíčových technologií nebo informační a energetické bezpečnosti.

Zneužití ekonomické aktivity zahraniční společnosti v ČR se může týkat jakéhokoliv ekonomického vztahu. Rizika mohou být spojena s dodávkami citlivého zboží nebo služeb, investicemi do bezpečnostně relevantních aktiv i s kapitálovým vstupem do strategických společností. V některých těchto případech měla ČR k dispozici nedostatečné nástroje, jak uvedeným hrozbám čelit, případně dostupných prostředků využívala jen omezeně. Při aplikaci jakýchkoliv regulací je však zároveň potřeba vzít v úvahu, že ČR je velmi otevřenou ekonomikou, ve které je působení zahraničních společností a přítomnost zahraničního kapitálu důležitým faktorem rozvoje. Při hodnocení rizik je proto třeba posuzovat nejen vůli a schopnost zahraničního aktéra působit proti ČR, ale také to, zda konkrétní aktivita může skutečně vytvořit prostor pro zneužití těchto schopností proti zájmům ČR.

Stát dále čelil přetrvávajícím problémům v oblasti správy a budování ICT systémů. Zdrojem rizik byla především závislost mnoha státních zadavatelů na dlouholetých dodavatelích technologií, která značně omezovala možnosti vyjednávání o lepších podmínkách nebo náhradu stávajících systémů jinými.

BIS rovněž identifikovala rizika, jež mohla ohrožovat kybernetickou bezpečnost v instituci zajišťující provoz několika informačních systémů, které spadají do kategorie kritické informační infrastruktury. Tyto bezpečnostní nedostatky nebyly dlouhodobě a systematicky řešeny a některé z nich přetrvávaly po delší dobu, přičemž se objevovaly další nové problémy. Oddělení odpovídající za informační technologie v instituci postupně opouštěli zkušení zaměstnanci mající znalosti a dovednosti pro správu systémů úřadu a na jejich místa se nedařilo získat vhodnou náhradu. Vedoucí pracovníci klíčových oddělení navíc neměli potřebné znalosti a problematiku kybernetické bezpečnosti povětšinou ignorovali.

Během roku 2018 se v několika případech stále nedařilo vyřešit mnoho let staré zátěže způsobené nekvalitními obchodními vztahy, které nepříznivě zasahovaly činnost orgánu státu nebo některých státem ovládaných společností. Obvyklou překážkou nalezení přijatelného východiska byla právní, technologická nebo i zahraničně politická složitost daných okolností. V některých případech se však na průtazích podílela i pasivita, nedokonalá spolupráce či rivalita mezi jednotlivými odpovědnými aktéry na straně státu.

BIS zaznamenala i několik případů klientelismu nebo závažného střetu zájmů. V těchto případech se často jednalo o aktivity, které dle mnoha znaků měly i charakter trestné činnosti. Průvodním jevem bylo v některých popsaných případech přesvědčení hlavních aktérů o jejich domnělé nedotknutelnosti plynoucí z kontaktů s lobbisty a různými poradci, kteří jim prodávali svůj často záměrně nadhodnocovaný vliv na státní aparát. Poznatky s trestněprávním přesahem BIS předávala orgánům činným v trestním řízení.

3 Ochrana utajovaných informací

3.1 Administrativní bezpečnost

V oblasti ochrany utajovaných informací nedošlo během roku 2018 k zásadním změnám. Stejně jako v předchozím roce byla vyhotovována odborná vyjádření v rámci BIS, dokumenty byly posuzovány z hlediska stanovení stupně utajení podle zákona č. 412/2005 Sb., byl podáván výklad seznamu utajovaných informací v působnosti BIS a příslušných vnitřních předpisů a poskytována metodická pomoc organizačním útvarům.

3.2 Bezpečnost informačních a komunikačních systémů, kryptografická ochrana

Při řízení bezpečnosti IS BIS je kladen důraz na neustálé zlepšování zabezpečení ICT systémů a poskytovaných služeb, a to jak v systémech zpracovávajících utajované informace, tak v neutajovaných systémech. Všechny informační systémy BIS zpracovávající utajované informace mají platný certifikát Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

V roce 2018 byla provedena aktualizace bezpečnostní dokumentace a zároveň úspěšná recertifikace informačního systému zpracovávající utajované informace stupně utajení „Tajné“. V informačním systému jsou stále zdokonalovány technologie zajišťující sledování přístupu jednotlivých uživatelů k datům.

Všichni uživatelé certifikovaných informačních systémů jsou v souladu se zákonem č. 412/2005 Sb. proškoleni před jejich prvním přístupem do systému a následně prochází jednou ročně pravidelným proškolením.

V průběhu roku 2018 v BIS nebyl zaznamenán žádný závažný incident nebo kompromitace v provozu informačních a komunikačních systémů nebo kryptografických prostředků. Pravidelné inventury kryptografického materiálu nezjistily žádné nedostatky ve správě a manipulaci s kryptografickým materiálem.

3.3 Fyzická bezpečnost

V oblasti fyzické bezpečnosti pokračovalo zkvalitňování systémů režimových opatření, technické ochrany a fyzické ostrahy objektů BIS za účelem zajištění ochrany utajovaných informací v souladu s požadavky zákona č. 412/2005 Sb. a s vyhláškou č. 528/2005 Sb., ve znění pozdějších předpisů.

Pokračovala tvorba nových povinných složek objektové dokumentace pro pracoviště a objekty BIS, v důsledku redislokací některých pracovišť byly novelizovány příslušné objektové dokumentace tak, aby odpovídaly aktuálnímu stavu.

3.4 Krizové řízení

V oblasti ochrany utajovaných informací při krizových situacích byly aktualizovány Plány zabezpečení objektů či oblastí, které jsou součástí Bezpečnostních projektů.

4 Spolupráce se zpravodajskými službami ČR a ostatními státními orgány

4.1 Spolupráce se zpravodajskými službami ČR

Vojenské zpravodajství a Úřad pro zahraniční styky a informace jsou pravidelnými adresáty zpravodajských informací a analytických materiálů. Další spolupráce s oběma službami probíhá i v ostatních činnostech operativního, analytického či servisního charakteru.

Intenzivní spolupráce s oběma službami probíhala v problematikách boje proti špionáži, kybernetické bezpečnosti, proliferace zbraní hromadného ničení a jejich nosičů a v problematice nelegálního obchodu s vojenským materiálem.

4.2 Spolupráce s Policií ČR

PČR je po prezidentovi republiky, předsedovi vlády a ministrech dalším adresátem některých zpravodajských informací BIS na základě § 8 odst. 3 zákona č. 153/1994 Sb. Informace, které náležejí do její působnosti, jsou PČR předávány v případech, kdy předání neohrozí důležitý zájem BIS. Spolupráce mezi jednotlivými útvary BIS a PČR pak přirozeně v mnoha případech navazuje na obsah takto poskytnutých informací. K výměně informací dochází také cestou odpovědí na dožádání PČR, popř. příslušného státního zastupitelství, ke konkrétnímu trestnímu řízení.

Jednou z forem spolupráce BIS s PČR je posuzování důvěryhodnosti fyzických osob v souvislosti s novelou zákona č. 49/1997 Sb., o civilním letectví, z roku 2015, obsahující ustanovení o ověřování spolehlivosti fyzické osoby pro účely vydání osvědčení, které vydává Úřad pro civilní letectví (ÚCL). Jeho nedílnou součástí je posouzení důvěryhodnosti fyzické osoby, které provádí PČR. Na základě žádostí PČR o součinnost při posuzování důvěryhodnosti se BIS vyjadřovala k jednotlivým žadatelům o vydání osvědčení ÚCL. V souvislosti s touto agendou zpracovala BIS žádosti, které se týkaly více než 7 000 osob.

Spolupráce s Národní centrálou proti organizovanému zločinu (NCOZ) v průběhu roku 2018 spočívala ve výměně poznatků týkajících se prověřování zájmových subjektů, dále byly předávány poznatky v oblasti ekonomické kriminality a kybernetické bezpečnosti.

Pokračovala spolupráce s PČR v problematikách nelegálního obchodu a nakládání s vojenským materiálem, bezpečnostním materiálem, střelnými zbraněmi, municí, výbušninami, nebezpečnými látkami a v boji proti šíření ZHN a jejich nosičů.

V oblasti fyzické bezpečnosti probíhá spolupráce s PČR při fyzické ostraze objektů BIS.

4.3 Spolupráce s dalšími státními orgány a institucemi

BIS nadále úzce spolupracovala s Národním bezpečnostním úřadem (NBÚ) v oblasti ochrany utajovaných informací. Šlo zejména o šetření na žádost NBÚ v rámci řízení v oblasti personální a průmyslové bezpečnosti a bezpečnostní způsobilosti a šetření v rámci prověřování, zda fyzické osoby a podnikatelé i nadále splňují podmínky stanovené pro držitele osvědčení nebo dokladu. V průběhu celého roku docházelo zejména k jednáním týkajícím se spolupráce na konkrétních případech.

V rámci plnění svých zákonných povinností podle zákona č. 412/2005 Sb. provedla BIS na žádost NBÚ téměř 20 tisíc šetření v rámci bezpečnostního řízení pro vydání osvědčení pro fyzické nebo právnické osoby.

Kromě úkonů prováděných na žádost NBÚ postupuje BIS v souladu se svou zákonnou oznamovací povinností informace nasvědčující tomu, že držitel osvědčení fyzické osoby nebo podnikatele anebo držitel dokladu přestal splňovat podmínky pro jejich vydání. Takové informace postupuje BIS v souladu s ustanovením § 8 odst. 3 zákona č. 153/1994 Sb. a podle ustanovení § 140 odst. 3 zákona č. 412/2005 Sb. NBÚ, případně jiným zpravodajským službám, jestliže se jedná o jejich příslušníky nebo zaměstnance. V této souvislosti BIS standardně postupuje informace také v reakcích na četné a opakované dotazy NBÚ, zda o subjektech, které jsou držiteli osvědčení nebo dokladu, má informace (dotazy podle § 107 odst. 1, § 108 odst. 1 a § 109 odst. 1 zákona č. 412/2005 Sb.).

V rámci boje proti terorismu se BIS i v průběhu roku 2018 aktivně podílela na jednáních pracovní platformy určené pro shromažďování, zpracovávání a sdílení informací o rizikových osobách důvodně podezřelých z aktivit souvisejících s terorismem s názvem Národní kontaktní bod pro terorismus (NKBT), která působí v rámci NCOZ. Partnery v rámci NKBT jsou NCOZ, BIS, ÚZSI a VZ. Aktivní účast probíhala i v rámci Společné zpravodajské skupiny, stálého pracovního orgánu Výboru pro zpravodajskou činnost (VZČ), jejíž náplní je výměna zpravodajských informací a koordinace mezi zpravodajskými službami ČR, PČR, MV a MZV. Cílem skupiny je odhalování bezpečnostních hrozeb pro ČR, zejména v oblasti terorismu.

BIS spolupracovala i na projektech jiných orgánů státu (např. Ministerstvo vnitra, Ministerstvo zahraničních věcí) s cílem přispět k ochraně zájmů ČR a jejích občanů a přispět k omezování bezpečnostních rizik či k jejich úplnému odstranění. Na žádost jiných státních orgánů a jejich součástí BIS přijala a zpracovala žádosti, které se v souhrnu týkaly téměř 140 000 fyzických a více než 800 právnických osob.

V roce 2015 vstoupila v platnost novela zákona č. 49/1997 Sb., o civilním letectví, obsahující ustanovení týkající se ověření spolehlivosti fyzické osoby, které vydává Úřad pro civilní letectví (ÚCL). Jeho nedílnou součástí je posouzení důvěryhodnosti fyzické osoby. V souvislosti s touto agendou zpracovala BIS žádosti, které se týkaly více než 7 000 osob.

Na základě článku 9 Schengenské prováděcí úmluvy poskytuje BIS jako garant za zpravodajské služby ČR stanoviska k žádostem o schengenská víza. V roce 2018 provedla BIS bezpečnostní prověrku více než 1 800 000 takových žádostí.

Zástupci BIS se účastnili jednání pracovních orgánů Bezpečnostní rady státu - Výboru pro zpravodajskou činnost, Výboru pro kybernetickou bezpečnost, Výboru pro vnitřní bezpečnost, Výboru pro koordinaci zahraniční bezpečnostní politiky, Výboru pro obranné plánování a Výboru pro civilní nouzové plánování. Odborné útvary BIS připravovaly stanoviska a připomínky BIS k materiálům všech výborů, jakož i Bezpečnostní rady státu.

Aktivní spolupráce dále probíhala i v rámci Mezirezortního orgánu pro potírání nelegálního zaměstnávání cizinců či pracovní skupiny Stálého výboru pro jadernou energetiku pro otázky týkající se bezpečnostních zájmů státu v oblasti jaderné energetiky.

Mimo výše uvedené spolupracovala BIS v roce 2018 intenzivně také s NÚKIB, Generální inspekcí bezpečnostních sborů, Finančně analytickým úřadem, Celní správou ČR, Generálním ředitelstvím cel

(GŘC), Vězeňskou službou ČR, Generálním finančním ředitelstvím a se soudy a státními zastupitelstvími.

Předmětem spolupráce s dalšími orgány státní správy bylo také řešení konkrétních případů v problematice proliferace ZHN a jejich nosičů a obchodů s vojenským materiálem. Probíhala spolupráce zejména s orgány celní správy, a to jak na úrovni GŘC, tak na úrovni jednotlivých celních ředitelství. Pokračovala i spolupráce s orgány celní správy týkající se rizik možných transportů kontrolovaných položek, především vojenského materiálu a položek dvojího použití do sankcionované země. V konkrétních případech probíhala spolupráce také s MZV, Licenční správou MPO, Státním úřadem pro jadernou bezpečnost a na ně navázanými organizacemi, a to i v probíhajících povolovacích a licenčních řízeních a při informování o dodržování licenčních podmínek a mezinárodních kontrolních režimů. BIS se dále zabývala problematikou vývozů zboží limitně se blížícího položkám podléhajícím mezinárodním kontrolním režimům z ČR do rizikových zemí.

Kromě standardní spolupráce formou poskytování či výměny informací předává BIS dalším státním orgánům zobecněné poznatky a doporučení formou připomínek a podkladů pro různé legislativní i nelegislativní dokumenty, poskytuje různé konzultace a školení apod.

5 Spolupráce se zpravodajskými službami cizí moci

BIS spolupracuje se zpravodajskými službami cizí moci na základě § 10 zákona č. 153/1994 Sb. Se souhlasem vlády je BIS oprávněna bilaterálně spolupracovat s více než stovkou zpravodajských služeb z celého světa. Na multilaterální úrovni se BIS aktivně zapojovala v několika uskupeních (např. Counter-Terrorist Group nebo NATO Civilian Intelligence Committee).

V rámci mezinárodní spolupráce přijala BIS přes 10 000 zpráv a postoupila téměř 2 000 dokumentů. Na strategické a expertní úrovni proběhlo více než 700 mezinárodních jednání.

Informační výměna v mezinárodní spolupráci byla srovnatelná s předchozím rokem. Hlavními tématy spolupráce BIS se zahraničními zpravodajskými službami zůstávají boj proti terorismu, kontrašpionáž, proliferace a kybernetická bezpečnost. Hlavními partnery v mezinárodní spolupráci jsou pro BIS především zpravodajské služby zemí EU a NATO a některých dalších zemí.

6 Kontrola

Základ právní úpravy kontroly činnosti BIS je zakotven v § 12 odst. 1 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, z něhož vyplývá, že činnost BIS podléhá kontrole vlády, Poslanecké sněmovny a Orgánu nezávislé kontroly zpravodajských služeb České republiky. Citovaný zákon sám obsahuje úpravu vztahu Poslanecké sněmovny k vládě ohledně zpravodajských služeb (§ 14 až 16), zatímco s přímou parlamentní kontrolou zpravodajských služeb odkazuje především na tento nebo zvláštní zákon (§ 12) a upravuje zvláštní kontrolní režim ve vztahu ke kontrolnímu řádu (§ 13a), který je upraven v zákoně č. 255/2012 Sb. o kontrole (kontrolní řád).

Zákon č. 153/1994 Sb. nestanoví konkrétní rozsah ani způsob provádění kontrolní činnosti vládou. Kontrolní činnost vlády vůči BIS se však odvíjí od oprávnění vlády ukládat BIS úkoly v mezích její zákonné působnosti a hodnotit jejich plnění. Kontrolní činnost vlády vůči BIS rovněž úzce souvisí s tím, že vláda odpovídá za činnost BIS, koordinuje ji a jmenuje a odvolává jejího ředitele. Ve smyslu § 8 odst. 1 zákona č. 153/1994 Sb. je BIS povinna podávat prezidentovi republiky a vládě jednou za rok a kdykoliv o to požádají zprávy o své činnosti. Z této úpravy je zřejmé, že kontrolní činnost vlády se zaměřuje na všechny oblasti činnosti BIS.

V ustanoveních § 14 až 16 obsahuje zákon č. 153/1994 Sb. úpravu poskytování informací vládou Poslanecké sněmovně. Na základě § 14 je Poslanecká sněmovna o činnosti zpravodajských služeb informována vládou prostřednictvím svého příslušného orgánu pro zpravodajské služby. Současná právní úprava tedy tento institut systematicky odděluje od přímé parlamentní kontroly zpravodajských služeb, s níž odkazuje na zvláštní zákon (§ 12), jde tudíž o způsob parlamentní kontroly vůči vládě. Působnost příslušného orgánu připadla s účinností od 1. 1. 2018 zvláštním kontrolním orgánům zpravodajských služeb; ve vztahu k BIS jde o zvláštní kontrolní orgán zřízený podle zákona 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů (viz níže).

Zvláštním zákonem podle § 12 odst. 1 zákona č. 153/1994 Sb. je zákon č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů. Podle § 18 tohoto speciálního zákona vykonává kontrolu činnosti BIS Poslanecká sněmovna, která k tomuto účelu zřizuje zvláštní kontrolní orgán – Stálou komisi pro kontrolu činnosti Bezpečnostní informační služby. Konkrétní rozsah oprávnění tohoto kontrolního orgánu je v ustanoveních § 19 a 20 zákona č. 154/1994 Sb., a to např. oprávnění členů kontrolního orgánu vstupovat v doprovodu ředitele BIS nebo jím pověřeného příslušníka do objektů BIS či oprávnění kontrolního orgánu požadovat od ředitele BIS potřebné vysvětlení v případě, že má kontrolní orgán za to, že činnost BIS nezákonně omezuje nebo poškozuje práva a svobody občanů. Na druhé straně je ředitel BIS povinen předkládat kontrolnímu orgánu zákonem určené informace a písemnosti.

V právní úpravě kontroly zpravodajských služeb došlo k zásadní změně přijetím zákona č. 325/2017 Sb., kterým se mění zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů, a další související zákony, který vstoupil v účinnost dnem 1. ledna 2018.

Podle této nové právní úpravy by měl být nově zřízen pětičlenný expertní kontrolní orgán, nazvaný Orgán nezávislé kontroly zpravodajských služeb České republiky, volený Poslaneckou sněmovnou na dobu 5 let na návrh vlády, který by měl vykonávat kontrolu na základě podnětu některého ze zvláštních kontrolních orgánů (touto novelou má být zvláštní kontrolní orgán nově zřízen

také pro ÚZSI). Orgán nezávislé kontroly by měl být oprávněn požadovat od zpravodajské služby všechny potřebné informace o její činnosti, které souvisejí s prováděnou kontrolou. Výjimku tvoří informace, které by mohly zmařit účel probíhající akce, odhalit totožnost příslušníků zpravodajské služby vykonávajících zpravodajskou činnost, totožnost osob jednajících ve prospěch zpravodajské služby, ohrozit jiné osoby, jejichž bezpečnost je v důležitém zájmu zpravodajské služby nebo porušit požadavky zpravodajské služby cizí moci na nepředání utajované informace třetí straně. Tento orgán nebyl dosud zřízen.

Kontrolu plnění úkolů BIS v oblasti hospodaření se státním majetkem a plnění státního rozpočtu vykonávají příslušné státní orgány např. podle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, vyhlášky č. 416/2004 Sb., kterou se tento zákon provádí, a zákona č. 166/1993 Sb., o Nejvyšším kontrolním úřadu, ve znění pozdějších předpisů.

Zvláštní způsob provádění kontroly stanoví § 13a zákona č. 153/1994 Sb. a má za cíl ochranu utajení činnosti zpravodajských služeb. Kontrola v zařízeních zpravodajské služby tak může být vykonána jen se souhlasem jejího ředitele. Nebude-li souhlas udělen, zajistí zpravodajská služba výkon kontroly ve své působnosti a podá do 60 dnů ode dne odmítnutí udělení souhlasu zprávu o výsledku vykonané kontroly kontrolnímu orgánu, který o souhlas požádal, nestanoví-li tento kontrolní orgán lhůtu delší. Dále zákon stanoví, že není-li zpravodajská služba schopna zajistit výkon kontroly ve své působnosti, je povinna umožnit výkon kontroly kontrolnímu orgánu. Může si však vyhradit zvláštní podmínky způsobu výkonu takové kontroly.

Činnost BIS podléhá i soudní kontrole, a to v případech používání zpravodajské techniky podle zákona č. 154/1994 Sb. Podle § 9 a násl. ustanovení citovaného zákona rozhoduje o povolení k použití zpravodajské techniky a kontrolu průběhu jejího použití provádí předseda senátu Vrchního soudu v Praze. Dále podle ustanovení § 11a zákona č. 153/1994 Sb. rozhoduje předseda senátu Vrchního soudu v Praze o žádostech BIS o poskytování zpráv o záležitostech týkajících se klienta, které jsou předmětem bankovního tajemství od bank, včetně zahraničních bank, a od spořitelních a úvěrních družstev, které jsou předmětem bankovního tajemství.

Soud tedy nejen vydává předchozí povolení k písemné žádosti BIS, ale také kontroluje, zda důvody žádosti trvají. V opačném případě povolení odejme, resp. odebere.

Veřejnost nemá žádná specifická kontrolní oprávnění, přesto však je tento způsob kontroly důležitým prvkem obecné kontroly činnosti BIS. Veřejnost kontroluje činnost BIS většinou zprostředkovaně – prostřednictvím hromadných sdělovacích prostředků, nebo přes internetové stránky BIS. Na nich jsou volně přístupné např. výroční zprávy či různá aktuální sdělení.

6.1 Vnější kontrola

Vnější kontroly v BIS jsou prováděny orgány a institucemi, které mají podle příslušných zákonů právo provádět kontroly jednotlivých dílčích činností. V roce 2018 byly provedeny celkem dvě vnější kontroly. V prvním případě se jednalo o kontrolní akci Nejvyššího kontrolního úřadu zaměřenou na majetek a peněžní prostředky určené na zajištění činnosti Bezpečnostní informační služby. Ve druhém případě šlo o kontrolu stavu plnění požadavků a opatření vyplývajících ze zákona č. 258/2000 Sb., o ochraně veřejného zdraví, nařízení vlády č. 361/2007 Sb., kterým se stanoví podmínky ochrany zdraví při práci, a souvisejících právních předpisů v této oblasti.

6.2 Vnitřní kontrola

V souladu se zákonem č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, je v BIS zřízena služba interního auditu. Rozsah působnosti stanoví organizační řád a interní předpis ředitele BIS. V roce 2018 byly ukončeny tři auditní zakázky zaměřené na zadávání veřejných zakázek, nakládání s majetkem, se kterým je příslušná hospodařit BIS, a monitoring plnění opatření, která vyplynula z doporučení interního auditu a byla schválena ředitelem BIS.

Ostatní odborné útvary BIS provedly celkem 45 kontrol. Cílem kontrolní činnosti bylo metodicky a věcně usměrňovat činnost organizačních útvarů ve finanční a materiálové oblasti, kontrolovat dodržování principu 3E a rovněž předcházet možnosti vzniku nežádoucích jevů. Součástí kontrol byla odborná a konzultační pomoc.

Orgán nemocenského pojištění podle § 76 zákona č. 187/2006 Sb., o nemocenském pojištění, provedl u příslušníků ve služebním poměru 12 kontrol práce neschopných pojištěnců.

Pracovníci archivní služby a kontrolní skupiny provedli celkem 45 archivních prohlídek spojených s kontrolami spisové služby. Kontroly byly zaměřeny především na fyzickou úplnost utajovaných dokumentů, správnost jejich náležitostí a na přesnost vedení evidenčních záznamů v administrativních pomůckách.

Průběžně probíhaly kontroly svazků zpravodajských dokumentů u organizačních útvarů a kontroly svazků ukládaných do spisovny.

7 Dodržování kázně, vyřizování žádostí a stížností

Činnost odboru inspekce BIS vychází ze znění zákonů týkajících se zpravodajských služeb, z trestního řádu a je dále upravena vnitřními předpisy BIS.

Činnost odboru inspekce BIS lze rozdělit do čtyř hlavních oblastí:

- činnost v postavení policejního orgánu BIS ve smyslu § 12 odst. 2 trestního řádu, a to v případech podezření ze spáchání trestného činu příslušníkem BIS,
- činnost při prošetřování případů podezření ze spáchání jednání majících znaky přestupku a kázeňských přestupků příslušníky BIS, včetně prošetřování mimořádných událostí,
- činnost v rámci prověřování stížností, oznámení a podnětů příslušníků BIS a subjektů mimo BIS,
- činnost v rámci vyřizování dožádání jiných orgánů činných v trestním řízení podle ustanovení trestního řádu a dožádání ostatních orgánů státní správy.

Do kategorie šetření podezření z jednání majících znaky přestupků a z kázeňských přestupků spadají zejména porušení předpisů v oblasti provozu na pozemních komunikacích. Odbor inspekce BIS tato šetření doplňuje o zjištění podstatná pro rozhodnutí služebních funkcionářů ve věci, která policejní útvary nemohou obstarat. Další součástí této kategorie je šetření případů na úseku ochrany utajovaných informací, prošetřování okolností poškození zdraví příslušníků BIS a další podezření ze spáchání kázeňského přestupku nebo jednání majícího znaky přestupku.

Případy, u nichž bylo zjištěno podezření ze spáchání kázeňského přestupku nebo jednání majícího znaky přestupku ze strany příslušníka BIS, byly postoupeny ke kázeňskému řízení.

Stížnosti, oznámení a podněty, ke kterým prováděl odbor inspekce BIS šetření v roce 2018, pocházely obvykle ze strany subjektů mimo BIS. Oproti roku 2017 počet vyřízených oznámení a podnětů výrazně narostl o 89,7 %. Obsahově jsou oznámení od občanů odrazem celospolečenského dění v České republice, ale i v zahraničí.

Odbor inspekce BIS spolupracuje s ostatními orgány státní správy především ve formě dožádání, jež zasílají nejčastěji orgány PČR, které jsou činné v trestním nebo přestupkovém řízení. Počty vyřízených dožádání korespondují s dlouhodobým stavem.

8 Rozpočet

Rozpočet BIS pro rok 2018 byl stanoven zákonem č. 474/2017 Sb., o státním rozpočtu České republiky na rok 2018.

Největší podíl na čerpání výdajů tradičně tvořily výdaje na platy a příslušenství. Na jejich růst měla vliv úprava základních tarifů z listopadu 2017 i změna způsobu proplácení služby přesčas od roku 2018. Do oblasti osobních výdajů lze zařadit i výsluhové nároky, což jsou mandatorní výdaje vyplácené příslušníkům po skončení služebního poměru. Od roku 2018 je nově přijímaným příslušníkům poskytován náborový příspěvek.

V ostatních běžných výdajích tvořily podstatnou část standardní výdaje na nákup služeb, běžného materiálu, paliv a energií sloužících k zajištění běžného chodu BIS. Výdaje na opravy a udržování směřovaly k zabezpečení provozuschopnosti a udržení odpovídajícího technického stavu majetku a objektů BIS. Dále zde byly zahrnuty také výdaje na speciální techniku specifickou pro činnost zpravodajské služby a zvláštní finanční prostředky určené pro přímou zpravodajskou činnost.

V kapitálových výdajích největší část směřovala do informačních a komunikačních technologií. Jejich cílem bylo zajištění potřebného výkonu serverových a komunikačních technologií, diskových kapacit a rozvoj softwarových řešení pro podporu zpracování zpravodajských informací. Významná část kapitálových výdajů směřovala i do stavební oblasti. Zbývající kapitálové výdaje byly realizovány v oblasti zpravodajských technologií. Další výdaje byly vynaloženy i na nezbytnou obměnu dopravních prostředků.

Do výdajových opatření se každoročně promítá plnění požadavků na ochranu utajovaných informací vyplývajících ze zákona č. 412/2005 Sb. a prováděcích předpisů, které tyto požadavky upřesňují pro fyzickou, administrativní a personální bezpečnost i bezpečnost informačních a komunikačních systémů. Zohlednění těchto skutečností v celém průřezu činností BIS vyžaduje řadu výdajů, které se u jiných organizačních složek státu nevyskytují vůbec nebo jen v omezené míře.

Základní provozní i rozvojové potřeby BIS byly vzhledem k dostupným kapacitním možnostem plně pokryty. Zlepšení bylo dosaženo u rozpočtového zabezpečení lidských zdrojů, kde bylo pro rok 2018 možno rozpočtově pokrýt o 4,8 % služebních míst více než v předchozím roce. Rozpočtem bylo také zajištěno financování rozvojových aktivit v oblasti zpravodajské techniky a informačních a komunikačních technologií.

Podrobná zpráva o výsledku hospodaření BIS v roce 2018 ve struktuře dle příslušné vyhlášky Ministerstva financí je jako závěrečný účet kapitoly předkládána ve stanoveném režimu Ministerstvu financí a k projednání ve Výboru pro bezpečnost Poslanecké sněmovny Parlamentu České republiky.

Ukazatele rozpočtu kapitoly 305 – Bezpečnostní informační služba v roce 2018 (v tis. Kč)

	Schválený rozpočet	Upravený rozpočet	Skutečnost
Příjmy celkem	150 000	150 000	202 265
Výdaje celkem	2 007 592	2 005 415	1 649 973