
**Výroční zpráva
Bezpečnostní informační služby
za rok 2019**





Obsah:

Slovo ředitele Bezpečnostní informační služby	3
1 Náplň a rozsah zpravodajské činnosti	4
2 Zpravodajská činnost a zpravodajské poznatky	5
2.1 Činnosti ohrožující bezpečnost nebo významné ekonomické zájmy ČR.....	5
2.2 Zpravodajské služby a nepřátelské aktivity cizí moci v ČR	8
2.3 Ochrana ústavnosti a demokratických základů státu	11
2.4 Terorismus	13
3 Ochrana utajovaných informací	15
3.1 Administrativní bezpečnost	15
3.2 Bezpečnost informačních a komunikačních systémů, kryptografická ochrana	15
3.3 Fyzická bezpečnost.....	15
3.4 Krizové řízení	15
4 Spolupráce se zpravodajskými službami ČR a ostatními státními orgány	16
4.1 Spolupráce se zpravodajskými službami ČR.....	16
4.2 Spolupráce s Policíí ČR	16
4.3 Spolupráce s dalšími státními orgány a institucemi.....	16
5 Spolupráce se zpravodajskými službami cizí moci	19
6 Kontrola.....	20
6.1 Vnější kontrola	21
6.2 Vnitřní kontrola	22
7 Dodržování kázně, vyřizování žádostí a stížností.....	23
8 Rozpočet.....	24



Slovo ředitele Bezpečnostní informační služby

Vážení čtenáři,

Bezpečnostní informační služba stejně jako během předchozích 24 let zveřejňuje i letos pro širokou veřejnost neutajovanou verzi Výroční zprávy o činnosti BIS, tentokrát za rok 2019.

Stejně jako v letech předchozích očekáváme velký zájem o její obsah i nesčetné diskuse nejen o jednotlivých kapitolách, ale také o smyslu jejího zveřejňování. Už mnohokrát jsem při různých příležitostech říkal, že veřejnou kontrolu naší práce považuji za stejně důležitou jako kontrolu ze strany vlády ČR a Parlamentu. Občané České republiky by měli vědět, jakým tématům v předchozím roce služba věnovala pozornost, jaké priority a proč měla, s kolika dalšími organizacemi a institucemi spolupracovala a jaké informace poskytovala zákonným adresátům, mezi které patří předseda vlády a členové vlády, prezident republiky a orgány činné v trestním řízení.

Pravděpodobně se debaty povedou opět i o části pro média a veřejnost nejatraktivnější, a to o aktivitách cizích zpravodajských služeb. Zde musím jasně říci, že BIS věnuje pozornost skutečně všem zpravodajským službám, které působí na území České republiky. Také proto můžeme jednoznačně konstatovat, že ruské a čínské zpravodajské služby jsou u nás nejaktivnější. Jsou tu ovšem i další zpravodajské služby, například z Íránu či Severní Koreje, jejichž činností se zabýváme.

Velmi důležitou kapitolou je každý rok také část týkající se významných ekonomických zájmů státu. Zde, stejně jako v dalších kapitolách, jsou v obecné rovině naznačena témata a oblasti, které považuje BIS za důležité. Konkrétní informace se všemi detaily dostávají zákonní adresáti v pravidelných zprávách v průběhu roku a jsou shrnuty také v rozsáhlejší utajované verzi Zprávy o činnosti BIS za rok 2019.

Přes velkou míru obecnosti věřím, že předkládáme poměrně plastický obraz činnosti Bezpečnostní informační služby, a doufám, že Vás její obsah stejně jako v předchozích letech zaujme.

plk. Ing. Michal Koudelka
ředitel Bezpečnostní informační služby



1 Náplň a rozsah zpravodajské činnosti

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

Zpravodajské služby jsou podle § 2 zákona č. 153/1994 Sb. státní orgány pro získávání, shromažďování a vyhodnocování informací důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnost a obranu České republiky. BIS 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. BIS plní 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 zpravodajských služeb odpovídá a koordinuje ji vláda. Vláda podle ustanovení § 8 odst. 4 tohoto zákona ukládá BIS úkoly v mezích její působnosti. Oprávnění ukládat úkoly BIS v mezích její působnosti náleží i prezidentu republiky s vědomím vlády.

K plnění svých úkolů je BIS oprávněna spolupracovat s ostatními zpravodajskými službami ČR. Zákon č. 153/1994 Sb. tuto spolupráci podle § 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

V roce 2019 se BIS velmi aktivně věnovala činnostem ohrožujícím bezpečnost nebo významné ekonomické zájmy státu. Tomu také odpovídá nejrozsáhlejší informační produkce týkající se těchto témat.

Velmi vážnou hrozbu pro bezpečnost ČR představovaly i v roce 2019 nepřátelské aktivity cizí moci. BIS se proto ve zvýšené míře zaměřovala mimo jiné na rizikové aktivity týkající se strategických projektů z oblasti energetiky a informačních a komunikačních technologií. Z pohledu bezpečnosti ČR hodnotí BIS jako nežádoucí zejména potenciální závislost na dodavatelských pocházejících ze zemí, které aktivně působí proti ČR, jejím zájmům nebo jejím spojencům z NATO či EU.

S velkou intenzitou se i v roce 2019 věnovala BIS také aktivitám osob majících vazby na teroristické či radikální skupiny a organizace s cílem odhalovat a eliminovat rizika a hrozby pro bezpečnost České republiky. Další skupinu hrozeb představoval fenomén organizovaného zločinu, který se prolínal řadou jiných témat, jako je např. ochrana významných ekonomických zájmů nebo nepřátelské aktivity cizí moci.

Souhrn veškeré zpravodajské činnosti Bezpečnostní informační služby v roce 2019 obsahuje utajovaná Zpráva o činnosti BIS za rok 2019, 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 2019 oprávněné adresáty podle § 8 zákona č. 153/1994 Sb. V tomto období předala BIS prezidentovi a členům vlády více než 200 dokumentů. Další informace zaslala BIS Policii ČR (PČR), Úřadu pro zahraniční styky a informace (ÚZSI), Vojenskému zpravodajství (VZ) a dalším státním orgánům.

2.1 Činnosti ohrožující bezpečnost nebo významné ekonomické zájmy ČR

Ochrana významných ekonomických zájmů

V roce 2019 se BIS zaměřovala ve zvýšené míře na rizikové aktivity týkající se několika strategických projektů, jejichž význam pro bezpečnost ČR svojí šíří přesahoval rámec ochrany významných ekonomických zájmů. Patřily mezi ně zejména projekty z oblasti energetiky a informačních a komunikačních technologií. V podobném rozsahu jako v předchozích letech popisovala BIS rizika v oblasti zásahů do činnosti regulatorních a dohledových orgánů státu, které směřovaly proti nezávislému výkonu jejich funkce. BIS zaznamenala také řadu dalších případů nelegitimního lobbingu, klientelismu a korupce, které měly charakter srovnatelný s minulým obdobím.

V roce 2019 stát a jím ovládané společnosti zahájily nebo pokračovaly v realizaci několika ekonomicky významných projektů, které zároveň měly silný vztah k bezpečnostním zájmům ČR. Jejich příprava, uskutečnění i samotné dokončení přímo souviselo zejména s některými strategickými bezpečnostními zájmy, mezi které patří např. zajištění energetické bezpečnosti, kybernetické bezpečnosti či posilování konkurenceschopnosti ekonomiky¹. Nepřímo však s ohledem na svůj



ekonomický rozsah a míru, s jakou ovlivňovaly strategické bezpečnostní zájmy, měly vliv i na zajištění životních bezpečnostních zájmů¹, jako jsou politická nezávislost a suverenita ČR.

Nejvýraznějším rizikem, které bylo společné všem monitorovaným případům, byla možná účast problematických subjektů majících schopnost i motivaci zneužít svého postavení v projektu k dosažení vlastních partikulárních zájmů nebo uskutečnění cílů třetí strany, např. cizí moci, a to v rozporu se zájmy ČR. K naplnění těchto rizik by v závislosti na charakteru projektu mohlo dojít zejména zneužitím přístupu k velkému objemu citlivých informací (osobních, ekonomických, bezpečnostních) či vytvořením závislosti na dodávkách od rizikového dodavatele a následným podmiňováním dokončení projektu ekonomickými, politickými nebo bezpečnostními požadavky. Hrozby mohou v těchto případech vznikat rovněž pokračováním závislosti na dodavateli i po dokončení projektu se všemi typickými důsledky (vendor lock in).

Za problematické lze ve smyslu popsaných rizik považovat především subjekty pocházející ze zemí, kde má státní administrativa možnost prosazovat své zahraničně-politické cíle bez ohledu na ekonomické zájmy tamních společností, a to i soukromých. S popsaným problémem pak úzce souvisí také téma rizikových zahraničních investic a mechanismu na vyhledávání s nimi souvisejících bezpečnostních hrozeb. Právě původ investora v zemi s autoritářskými rysy je totiž podobně jako u výše zmíněných projektů jedním z důležitých faktorů ovlivňujících hodnocení rizikovosti konkrétní investice.

V obecnější rovině je možné obdobný pohled uplatnit i na nedůvěryhodné české subjekty usilující o obchodní vztahy se státem. BIS zaznamenala případy, kdy společnosti s rizikovým profilem (krátká historie, chybějící reference, kriminální historie osob v pozadí apod.) stavěly své obchodní a investiční plány především na nepravdivé nebo zveličené prezentaci údajné podpory státu nebo jeho zástupců. Představitelé těchto společností dokázali obratným způsobem využít každého, byť zcela marginálního setkání k získání podkladů pro další manipulativní a zkreslené vylepšení své reputace. Takové jednání pak v důsledku ohrožovalo dobrou pověst zúčastněných osob a zprostředkovaně i ČR.

V některých odvětvích, zejména v energetice, zdravotnictví nebo telekomunikacích, BIS sledovala intenzivní snahu významných účastníků trhu nelegitimními metodami ovlivnit ve svůj prospěch legislativní proces a personální obsazení či fungování regulatorních orgánů. Typicky nedocházelo v těchto případech k nelegálním aktivitám, avšak použité způsoby prosazování zájmů v mnoha případech flagrantně překračovaly hranice běžného lobbingu. Mezi nejčastěji používané postupy patřilo zkreslování původu podkladů s cílem vytvořit zdání jejich objektivitu, vyvolávání nedůvodných obav z negativních důsledků pro rozhodující osoby nebo snaha promlouvat do personálního obsazení klíčových úřadů.

Trvajícím jevem, který dlouhodobě závažným způsobem ohrožuje ekonomické zájmy státu, byly v některých oblastech kartelové dohody mezi dodavateli při zadávání zakázek státními institucemi nebo státem ovládanými společnostmi. Zadavatel měl přitom často jen omezené možnosti jak i při povědomí o těchto dohodách negativní důsledky eliminovat. Jako problematická se v této souvislosti jevila především obtížná dokazatelnost kartelových dohod nebo závažné důsledky v případě vyřazení

¹ Srov. Bezpečnostní strategie České republiky 2015.



klíčových dodavatelů, neboť kartelové dohody se často vztahovaly ke klíčovými státními aktivům, např. strategické infrastruktury.

BIS informovala také o negativních důsledcích plynoucích ze starších zátěží v podobě nevýhodných obchodních vztahů státu se soukromými partnery. V souladu s trendem z předchozích období se tyto problémy týkaly především některých ICT projektů a pohledávek souvisejících se státní podporou exportu.

BIS dále na konkrétních případech popsala řadu negativních jevů, které zaznamenávala již v předchozích letech, a to zejména selhání způsobená nedbalostí, korupcí a klientelismem. V jejich důsledku pak stát nebo jím ovládané společnosti čelily únikům citlivých interních informací, nákupu nepotřebných nebo předražených služeb a zboží, vysokým nákladům z pozastavené ekonomické činnosti a nevýhodným prodejům či pronájmům majetku. BIS např. informovala o několika případech dlouhodobě budovaných vztahů mezi soukromým dodavatelem a veřejným zadavatelem, který byl založen především na osobních přátelských vazbách rozhodujících osob. Jejich důsledkem pak bylo např. přehlížení chyb dodavatele, neuplatňování sankcí nebo zvýhodňování poskytnutím neveřejných informací. Obvyklé přitom bylo, že motivací zástupců státu nebyla zjevná korupce, ale snaha zjednodušit si pracovní situaci a nevystavovat se například riziku potíží s novým, neosvědčeným dodavatelem. Pokud pak ze strany zástupců státu docházelo k přijetí korupčního plnění, byly přijímané materiální výhody často poměrně nevýznamné a zcela nesrovnatelné s objemem obchodního plnění, příjemcům však poskytovaly určitý pocit výlučnosti.

Proliferace zbraní hromadného ničení a obchod s vojenským materiálem

BIS se svou činností podílí na dodržování mezinárodních závazků, k nimž se Česká republika zavázala v oblasti proliferace zbraní hromadného ničení (ZHN) a jejich nosičů, tj. chemických, biologických a radiologických prostředků podle mezinárodních kontrolních režimů (MKR)² a požadavků rezolucí Rady bezpečnosti (RB OSN), nařízení, směrnic a společných postojů Rady EU nebo Organizace pro spolupráci a bezpečnost v Evropě (OBSE). Zbraně hromadného ničení jsou v ČR z obchodu zcela vyloučeny a obchod s položkami dvojího užití je v zájmu snížení rizika jejich zneužití ve vojenských programech proliferačně rizikových zemí regulován evropskou³ i národní⁴ legislativou.

Mimo výše uvedené závazky je činnost BIS v této oblasti směřována i k zabránění proliferace položek vymezených dalšími mezinárodními smlouvami a závazky. Jedná se o Smlouvu o obchodu se zbraněmi (Arms Trade Treaty, ATT) nebo Smlouvu o konvenčních ozbrojených silách v Evropě. Další spojenecké závazky ČR v NATO vedle toho vyžadují nedodávat vojenský materiál, zbraně, střelivo

² ČR je členem mezinárodních kontrolních režimů Australská skupina (*Australia Group, AG*), Kontrolní režim raketových technologií (*Missile Technology Control Regime, MTCR*) posílený o Haagský kodex (*The Hague Code of Conduct, HCoC*), Skupina jaderných dodavatelů (*Nuclear Suppliers Group, NSG*), Zanggerův výbor (*Zangger Committee, ZC*), Wassenaarské ujednání (*Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, WA*) a rezoluce RB OSN č. 1540 (2004).

³ Nařízení Rady (ES) 428/2009, režim ES pro kontrolu vývozu, zprostředkování a tranzitu zboží dvojího užití.

⁴ Zejména zákon č. 594/2004 Sb., jímž se provádí režim ES pro kontrolu vývozu, přepravy, zprostředkování a tranzitu zboží dvojího užití, a zákon č. 38/1994 Sb., o zahraničním obchodu s vojenským materiálem.



a výbušniny do zemí pod zbrojnými embargy, do zemí, které neposkytují záruky ohledně jejich možného reexportu, či nestátním aktérům spojeným s teroristickými skupinami. Nedodržení mezinárodních závazků by poškodilo ekonomické a bezpečnostní zájmy i dobré jméno ČR a oslabilo by její postavení na mezinárodní úrovni. Cílem BIS v této oblasti je rovněž eliminovat proliferační aktivity vedoucí k sekundárním problémům s přímým dopadem na bezpečnostní situaci v ČR.

Proliferačně rizikové státy, mezi něž patří například KLR, Sýrie, Írán nebo Pákistán, pokračovaly v roce 2019 ve svých snahách o skryté obstarávání mezinárodně kontrolovaných položek. Za tím účelem využívaly méně známé nebo účelově založené obchodní společnosti a reexportní trasy přes třetí země, přičemž platby strukturovaly tak, aby maximálně ztížily jejich identifikaci.

Na rizika spojená s reexporty a využitím reverzního inženýrství poukázaly v září 2019 útoky proti civilní infrastruktuře Saúdské Arábie, mj. i proti ropným zařízením v Abkajk a Churajs. Z analýzy trosek střel použitých k útokům bylo zjištěno, že k útokům byly použity kopie českých motorů sestavené reverzním inženýrstvím, které využívaly některé komponenty originálních motorů. Šetření případu nebylo v roce 2019 uzavřeno.

Konkrétním příkladem využívání komplikovaných reexportních tras pak může být v roce 2019 zveřejněný případ staršího pokusu o vývoz motorů pro tanky a bojová vozidla z ČR do KLR. BIS zjistila, že severokorejská strana si k vývozu připravila dodavatelskou cestu přes Moldavsko, kde byly v celních deklaracích tankové motory označeny za rybářské motory. V další části transportní cesty se pak deklarovaný obsah zásilky opět měnil a na Ukrajině měly být označeny za motory pro generátory. Obchod zajišťovaly bankovní instituce z několika zemí. Na základě poznatků BIS k vývozu motorů do KLR nedošlo.

BIS získala dále řadu poznatků o snahách obcházet mezinárodní sankční opatření uplatňovaná vůči Íránu, Rusku, státům Blízkého a Středního východu, jihovýchodní Asie a kavkazským nebo africkým zemím. V dalších případech BIS informovala o zájmu o vojenský materiál, zbraně a výbušniny nebo o speciální komponenty využitelné k vývoji a výrobě např. bezpilotních systémů (dronů) ze strany Číny, Ruska a dalších zemí s nestabilním a represivním režimem nebo zemí, ve kterých probíhají ozbrojené konflikty.

2.2 Zpravodajské služby a nepřátelské aktivity cizí moci v ČR

Bezpečnostní informační služba se v rámci své zákonné působnosti i v roce 2019 věnovala všem zpravodajským službám (dále též „ZS“) působícím na našem území proti zájmům České republiky. V souladu se stanovenými prioritami, mírou ohrožení zájmů České republiky a vlastními kapacitami a možnostmi BIS byly v roce 2019 prioritními cíli zpravodajského rozpracování aktivity ruské a čínské státní moci ohrožující bezpečnost a další klíčové zájmy státu.

Navzdory častějšímu uplatňování nekonvenčních konceptů v prosazování ruských zájmů zastávají zpravodajské služby v ruských operacích a aktivitách nadále důležitou roli. Dohled a kontrolu ruských zpravodajských důstojníků lze totiž vysledovat nebo dovozovat i v případech, kdy nepřátelskou činnost samotnou vykonávají nestátní entity.

Intenzita čínských zpravodajských a vlivových aktivit nikterak nezaostává za ruskými. Klíčový rozdíl je však v tom, že Rusko usiluje o destabilizaci a rozklad svých protihráčů, zatímco čínským cílem



je vybudovat sinocentrickou globální komunitu, kde ostatní národy uznají legitimitu čínských zájmů a přiznají Číně respekt, který jí (dle čínského mínění) náleží.

Česká republika byla předmětem zájmu pro aktéry s vazbou na ruskou a čínskou státní moc i v kyberprostoru. V tomto kontextu zaznamenala BIS i v roce 2019 další bezpečnostní incidenty spojené s aktivitami státních či státem podporovaných kyberšpionážních skupin jako jsou Turla, Zebrocy, APT28 nebo APT15.

Vedle výše uvedeného věnovala BIS okrajově pozornost i některým rizikovým aspektům činnosti vietnamské státní moci a jejím zájmům v ČR. Aktivity iránských zpravodajských služeb byly sledovány po linii boje proti terorismu.

Ruské zpravodajské služby

V roce 2019 byli na území Česka přítomni a vyvíjeli zpravodajskou činnost příslušníci a spolupracovníci všech ruských zpravodajských služeb: civilní rozvědky SVR, vojenské rozvědky GRU, vnitřní bezpečnostní služby FSB a Federální služby ochrany.

Aktivity ruských zpravodajských důstojníků pracujících pod diplomatickým krytím v rámci ruské diplomatické mise se v ČR přirozeně zaměřovaly především na prosazování ruských zahraničně-politických zájmů, na zajišťování pozitivního obrazu Ruska v ČR a na propagaci názorů a postojů Kremlu. Počty příslušníků ruských zpravodajských služeb s diplomatickým krytím zůstávají v ČR již několik let relativně stabilní. Účinné omezení jejich činnosti bylo ale nadále mimořádně obtížné z důvodu dlouhodobé disproporce ve velikosti diplomatických misí ČR a Ruska.

V předchozích letech BIS dlouhodobě registrovala zájem ruského ministerstva zahraničních věcí a důstojníků ruské civilní rozvědky SVR o ovládnutí dění v ruskojazyčné komunitě v Česku, a to zejména skrze podporu prokemelské části diaspory. V roce 2019 ruská státní moc na tomto poli utlumila činnost a podle dostupných poznatků neřídila ani medializovanou agresivní kampaň prokemelské části ruské komunity proti zástupkyni ruské menšiny v Radě vlády pro národnostní menšiny.

Přechod od státem kontrolovaných či řízených aktivit k živelné nátlakové činnosti zapadá do vzorců ruských nekonvenčních praktik: představitel ruské státní moci dá najevo, co si přeje (což může být posíleno souběžnými manipulativními akcemi v informačním prostoru) a proxy aktéři mimo struktury ruské státní moci následně z vlastní iniciativy vykonají aktivity v souladu s předpokládanou vůlí či přáním ruské státní moci. Zásadním psychologickým prvkem je v těchto situacích kolektivní přesvědčení proxy aktérů, že je třeba „něco dělat“.

Scénář, kdy státní moc neprovádí vlastní činnost, zůstává v pozadí a různými cestami (PR, návodná prohlášení, propaganda atp.) volně inspiruje samostatné aktéry k možné akci, považuje BIS za rizikový, a to zvláště pokud by se počet takových iniciativních aktérů, jak z řad ruskojazyčné komunity, tak z řad českých občanů, v budoucnosti zvyšoval.



Čínské zpravodajské služby

Na území ČR byli v roce 2019 aktivní zejména příslušníci civilní rozvědky Ministerstva státní bezpečnosti (MSS) a vojenské rozvědky (MID). Stranická organizace Oddělení pro mezinárodní styky Ústředního výboru Komunistické strany Číny (OMSÚV) v českém prostředí na jedné straně navazovala oficiální styky, na straně druhé k plnění svých cílů využívala metod zpravodajské práce.

Čínské zpravodajské služby při své činnosti využívaly tradiční krytí (diplomaté, novináři, akademici) i moderní metody zpravodajské práce (např. sociální sítě), zajímaly se o rozličné obory a využívaly otevřenosti českého prostředí k nabídce čínských investic. Jejich zájem cílil na široké spektrum oborů, ať se jednalo o technologická témata, vojenství, bezpečnost, infrastrukturní projekty, zdravotnictví, ekonomiku, životní prostředí, nebo témata mezinárodní i domácí politiky.

Čínští aktéři – zpravodajci, diplomaté, členové stranických organizací a další – hledali v ČR způsoby, jak ovlivňovat veřejné mínění, šířit čínskou propagandu a budovat pozitivní obraz ČLR prostřednictvím otevřeného i skrytého ovlivňování mediálního obsahu.

Šíření pozitivních článků o ČLR mělo za cíl nejen budovat čínským aktivitám nakloněné prostředí a otevírat dveře pro čínskou expanzi, současně ale mělo působit i na čínské čtenáře, jelikož texty bývaly otiskovány v čínských periodikách a prezentovány jako názor českých zavedených médií, potažmo jako stanovisko celé ČR. Spolupráci mezi českými a čínskými médii často zajišťovali příslušníci ZS ČLR. Česká média se tak stávala nástrojem ZS ČLR k šíření čínského vlivu.

Zpravodajské služby ČLR se v roce 2019 intenzivně angažovaly v akademické sféře. V rámci rozvoje spolupráce s ČLR byly vytvářeny projekty na výměnu studentů a vědeckých pracovníků, otevírání společných výzkumných center, na vzájemnou pomoc při vlastním vědeckém bádání apod. Čeští akademici dostávali četné pozvánky na školení, konference a setkání pořádaná v ČLR, která byla hrazena čínskou stranou. Vzhledem k faktu, že ČLR preferuje uskutečnění zpravodajského kontaktu na svém území, případně ve třetí zemi (tj. nikdy ne v zemi, odkud zájmová osoba pochází), mohou být tyto akce využity k oslovení zájmové osoby ze strany ZS ČLR. Pokud nedojde přímo ke zpravodajskému oslovení, může ČLR zahrnout účast na rozličných platformách spolupráce do svého propagandistického narativu, anebo alespoň využít závazků, které za čínské pohostinství vzniknou.

Akademická sféra je obecně citlivým prostorem, který může být pro svou otevřenost předmětem zájmu zpravodajských služeb, stejně jako jiných vlivových aktérů. Vzhledem k politickému uspořádání ČLR a čínským zákonům je hranice svobodného akademického prostředí a státních zájmů značně rozostřená. Odhalit příslušníka ZS ČLR či osoby jednající ve prospěch ZS ČLR pod akademickým krytím je proto velmi obtížné, a to i s přihlédnutím ke skutečnosti, že osoby s vazbou na ZS ČLR obvykle bývají zkušenými badateli zaštitěnými významnými institucemi. Obecně lze konstatovat, že akademici, u nichž existuje podezření z vazeb na ZS ČLR, anebo byly tyto vazby potvrzeny, rozšiřují svoji vědeckou práci o sběr informací v oblastech zájmu ZS ČLR, čili o témata domácí i zahraniční politiky, obranných a silových sborů, technologií, průmyslu, infrastrukturních a energetických projektů aj.

Ruské a čínské kyberšpionážní aktivity

V roce 2019 navázala BIS na dřívější šetření kompromitace neutajované sítě Ministerstva zahraničních věcí (MZV) kyberšpionážní kampaní, za níž stála skupina pracujících ve prospěch cizí moci, s vysokou pravděpodobností Ruské federace.



V průběhu roku byla odhalena pokračující kompromitace zmíněné sítě i malwarem připisovaným kyberšpionážní skupině jiného státního aktéra.

Kybernetické útoky státních aktérů se nevyhnuly ani zastupitelským úřadům ČR v zahraničí. V roce 2019 byly odhaleny dva případy jejich kompromitace.

Kromě výše uvedeného se ve druhé polovině roku BIS podílela také na prověřování napadení ICT infrastruktury jedné z českých diplomatických misí při mezinárodní organizaci. Nejméně jedno zařízení bylo na konci roku 2018 kompromitováno v rámci intenzivní celosvětové vlny útoků kyberšpionážní kampaně cizího státního aktéra, s vysokou pravděpodobností opět Ruské federace. K nakažení došlo otevřením textového dokumentu v příloze útočného phishingového e-mailu. Podrobná analýza ukázala, že kompromitované zařízení bylo již v předchozích letech napadeno i malwarem spojovaným s kyberšpionážní skupinou jiného státního aktéra.

V září 2019 získala BIS informaci o průniku pravděpodobně čínské kyberšpionážní skupiny do infrastruktury antivirové společnosti Avast. Na základě podnětu BIS začala firma extenzivně auditovat celou svou vnitřní síť a odhalila závažnou kompromitaci. Spolupráce s BIS umožnila společnosti Avast přijmout rozsáhlá bezpečnostní opatření a v konečném důsledku přispěla k ochraně dat uživatelů.

Nejčastějším způsobem útoků ze strany státních aktérů útočících nejen na české cíle byly jednoznačně phishingové/spear-phishingové e-maily obsahující kompromitovanou přílohu (např. dokument obsahující makro). Tímto způsobem se útočníci snažili o doručení škodlivého kódu do zařízení uživatele bez jeho významného přičinění. V jednom případě bylo zaznamenáno také využití skrytého prvku přímo v samotném těle phishingového e-mailu, jehož cílem bylo stažení škodlivého kódu z odkazu, který nebyl pro uživatele viditelný.

2.3 Ochrana ústavnosti a demokratických základů státu

V roce 2019 pokračovalo šíření manipulativního zpravodajství a dezinformací, jehož důsledkem byla polarizace společnosti, podryvání důvěry v demokratický právní stát a jeho instituce a podpora zájmů cizí moci. Poté, co se v ČR v posledních několika letech vytvořila a etablovala poměrně stabilní dezinformační scéna složená z médií, která se prezentují jako nezávislá či alternativní, jsou stále častěji patrné pokusy jejich protagonistů o očištění od přívlastku „dezinformační“ a legitimizaci jejich názorů skrze tradiční a zavedená média. Tyto aktivity lze interpretovat jako přirozenou součást širšího trendu, který lze popsat jako snahu posunout konspirační teorie, proruské narativy a protizápadní postoje z okraje mediálního spektra do jeho středu.

V souvislosti s volbami do Evropského parlamentu v květnu 2019 monitorovala BIS možné snahy o nelegitimní ovlivňování výsledků voleb. Přestože v předvolebním období došlo k patrnému nárůstu zpravodajství obsahujícího tendenční narativy (zejména protiunijní, protimigrační či proruské), BIS nezískala žádné informace, které by svědčily o ohrožení integrity volebního procesu domácími aktéry ani ze strany cizí moci.

Tradiční extremistická uskupení ani v roce 2019 nenašla žádná témata, kolem kterých by mobilizovala své příznivce a veřejnost. Pravicoví a levicoví extremisté proto vzhledem ke své nevýznamnosti nepředstavovali hrozbu ústavnosti ČR. Se stejným závěrem lze hodnotit i působení existujících paramilitárních skupin.



Proruský aktivismus

Spektrum činnosti proruských aktivistů, tedy prorusky smýšlejících osob, které svými aktivitami vědomě či nevědomě přímo napomáhají cizí moci, se oproti roku 2018 nijak zásadně nezměnilo. Proruští aktivisté stále intenzivně a systematicky vystupovali proti politickému uspořádání ČR a členství v EU a NATO. Témata, která ve veřejném prostoru nastolovali a šířili, se i nadále významně překrývala s agendou prosazovanou Ruskem.

Ve druhé polovině roku 2019 se dominantním tématem prokremelského spektra stal boj proti záměru vedení Prahy 6 odstranit sochu sovětského maršála I. S. Koněva. Do akcí, které následovaly po zakrytí sochy plachtou a kritice vedení Prahy 6 ze strany ruského velvyslanectví, se zapojilo široké spektrum aktivistů, kteří události využili k vlastní propagaci.

Obdobně jako v předchozích letech probíhaly i v roce 2019 v ČR subverzní aktivity proti Ukrajině řízené orgány ruské státní moci.

Paramilitární a domobranecká uskupení

Charakter aktivit paramilitárních a domobraneckých uskupení se oproti předchozímu období výrazněji nezměnil, a proto v roce 2019 nepředstavovaly reálnou bezprostřední hrozbu. Tento stav souvisel především s neutěšenou situací uvnitř jednotlivých uskupení, která opustili někteří jejich vedoucí představitelé.

Nejvýznamnějším mobilizačním tématem se pro jinak pasivní domobraneckou scénu stalo zveřejnění záměru Ministerstva vnitra (MV) navrhnout právní úpravu, která by zakázala vytváření a organizování ozbrojených paramilitárních skupin. Návrh zamýšlené legislativy zaktivizoval vedení hlavních celostátně působících uskupení a přiměl je koncem roku k prohloubení vzájemné spolupráce. V této souvislosti lze očekávat, že se domobranecké skupiny budou transformovat, aby se vyhnuly případným finančním či jiným postihům. Jednou z variant je například zintenzivnění jejich aktivit na poli branné výchovy.

Tradiční politický extremismus

Tradiční pravicově i levicově extremistická scéna se již několik let nachází v krizi. Existující skupiny štěpí a oslabuje vnitřní názorová roztříštěnost i řada osobních animozit a v důsledku nejsou schopny získávat nové členy ani podporovatele. Aktivity extremistických uskupení stagnují nebo upadají i proto, že extremistům dlouhodobě chybí témata, která by scénu aktivizovala a mobilizovala její příznivce.

Tento stav je mimo jiné důsledkem postupné proměny veřejné debaty a zvýšené tolerance veřejnosti k projevům nenávisti, která umožnila dalším politickým subjektům opanovat prostor, v němž se dříve realizovali extremisté.

Jediným výraznějším mobilizačním tématem tradiční extremistické scény se tak stala kauza možného odstranění sochy sovětského maršála Koněva v Praze 6. Na demonstracích za její zachování

participovali stoupenci marxisticko-leninského spektra spolu s dalšími aktivisty proruské a dezinformační scény.

2.4 Terorismus

Situace v oblasti terorismu a islamistické radikalizace byla na území ČR i v roce 2019 klidná a BIS nezískala poznatky o tom, že by se území ČR stalo logistickou či ideologickou základnou mezinárodního islamistického terorismu. V souvislosti s vývojem v zahraničí a stále intenzivněji vnímanou potřebou včasné identifikovat osamělé, samostatně radikalizované aktéry však BIS prověřovala zvýšený počet osob, které byly hodnoceny jako potenciální nositelé teroristického rizika.

Hlavní faktory, které mohly podněcovat radikalizaci muslimské komunity v ČR, zůstaly stejné jako v letech předchozích. Byly jimi zejména ideologická propaganda ze zahraničí (a v ojedinělých případech i z místní komunity), trvající islamofobní tendence v části české společnosti a také zahraniční události spojené s islámským světem.

Příkladem události s radikalizačním potenciálem byl v roce 2019 útok na mešitu v novozélandském Christchurch, po kterém předseda pražské muslimské obce Leonid Kushnarenko vyzval muslimy k ozbrojování. V důsledku negativní pozornosti, kterou na sebe a na české muslimy upoutal, byl ale Kushnarenko pod tlakem ze strany vedení muslimských organizací donucen svou pozici opustit.

BIS monitorovala rovněž dopady dění na Blízkém východě a v dalších krizových oblastech na situaci v ČR. Zásadní událostí s významným mezinárodním přesahem byla v tomto ohledu zejména turecká ofenziva v severní Sýrii. V souvislosti s ofenzivou nicméně nezaznamenala BIS v komunitě žádné nepokoje či konflikty. Konflikt nebyl zaznamenán ani mezi místní tureckou a kurdskou komunitou, jejichž vztah je dlouhodobě založen na společných podnikatelských aktivitách.

Bezpečnostní informační služba získala během roku 2019 informace o smrti dalšího z dobrovolníků, kteří mezi lety 2012 – 2017 opustili ČR a vydali se bojovat do válečných oblastí na Blízkém východě. Je-li tato informace pravdivá, jedná se již o pátého zabitého bojovníka, který vycestoval z ČR. Další dva stále na území konfliktu v Sýrii zůstávali, o několika zbylých nezískala BIS aktuální informace. Riziko ve vztahu k radikalizaci muslimské komunity dlouhodobě představuje možnost návratu dobrovolníků z bojových zón zpět do ČR. V roce 2019 však BIS nezískala žádné informace o návratech bojovníků na území ČR a zároveň podle dostupných informací nikdo další z ČR do válečných zón neodcestoval.

Ve srovnání s rokem 2018 zaznamenala BIS úbytek otevřeného sympatizování s tzv. Islámským státem mezi sunnitskými muslimy. Hlavní příčinou byla územní porážka islamistického chalífátu a s tím spojená ztráta jeho atraktivity. Některé rizikové osoby nicméně nadále vyjadřovaly negativní postoje vůči české společnosti. Mezi faktory, které přispívaly k přijímání radikálních postojů, patřily zejména nedostatečná integrace, ztráta rodinného zázemí, finanční tíseň, kriminální činnost nebo užívání omamných a psychotropních látek. BIS se zaměřila především na vyhledávání osob, u nichž došlo v posledním období k příklonu k víře a zároveň se u nich objevily i výše zmíněné rizikové faktory. V roce 2019 nebyly identifikovány osoby představující bezprostřední hrozbu pro bezpečnost ČR.



Stejně jako v předchozích letech se BIS i nadále zabývala prověřováním možných projevů islamistické radikalizace, přičemž výskyt těchto projevů sledovala i v internetovém prostředí, především pak na sociálních sítích. Uživatelé internetu a sociálních sítí, kteří v rámci diskusí prezentovali názory ovlivněné radikální náboženskou ideologií, až na výjimky nepředstavovali bezpečnostní riziko. Jejich radikální projevy byly obvykle motivovány snahou o upoutání pozornosti ve virtuální komunitě, případně byly manifestací určité psychické poruchy. Na identifikaci a vyhodnocení rizikovosti autorů radikálních e-mailů a příspěvků na sociálních sítích BIS pravidelně spolupracovala s Národní centrálou proti organizovanému zločinu PČR (NCOZ).

V roce 2019 pokračoval program léčby libyjských pacientů, v rámci kterého do českých lázeňských či rehabilitačních zdravotnických zařízení každoročně přijíždějí desítky až stovky Libyjců. Většina z nich přijíždí v rámci tzv. programu pro libyjské veterány, který je plně hrazen libyjskou vládou. S ohledem na rizika, která tento program přinášel, byla v rámci mezirezortní spolupráce přijata preventivní opatření k včasné detekci rizikových osob mezi potenciálními pacienty a jejich doprovodem. I navzdory těmto opatřením však do určité míry přetrvávalo riziko zneužití léčebného programu k jiným účelům, popřípadě riziko vstupu islamistických radikálů na území ČR.

BIS pokračovala v monitorování dění v kazašské sektě tzv. čistého islámu, jejíž členové se nadále izolovali od většinové společnosti a vytvářeli uzavřené komunity odmítající integraci. Tuto specifickou lokální formu islamismu v ČR vyznává několik desítek rodin s různými formami pobytového statusu a s vazbami na podobné komunity v zahraničí.

Vzhledem k existující státní podpoře terorismu ze strany Íránu věnovala BIS nadále pozornost činnosti íránských zpravodajských služeb v ČR, jejichž agresivita v Evropě v posledních letech vzrůstá. V roce 2018 připravovala íránská zpravodajská služba MOIS pumový útok na konferenci opoziční organizace Mudžáhedín e-Khalq ve Francii. Útok organizoval íránský diplomat působící v Rakousku. BIS v roce 2019 prověřovala dřívější cesty tohoto Íránce do ČR.

BIS v rámci své působnosti prověřovala také teroristické incidenty, k nimž v průběhu roku 2019 došlo v Evropě. Získané informace poté neprodleně předávala dotčeným partnerským službám.



3 Ochrana utajovaných informací

3.1 Administrativní bezpečnost

V oblasti ochrany utajovaných informací nedošlo během roku 2019 ke 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

Řízení bezpečnosti informačních a komunikačních systémů BIS vychází z Bezpečnostní politiky ICT BIS. Cílem je zajištění vysoké úrovně bezpečnosti informací a budování důvěry v oblasti informační bezpečnosti. BIS klade důraz na neustálé zlepšování zabezpečení ICT systémů a poskytovaných služeb, a to jak v systémech zpracovávajících utajované informace, tak v neutajovaných systémech. Informační systémy jsou chráněny jak před zneužitím zvenku, tak i zevnitř organizace.

Všechny informační systémy BIS zpracovávající utajované informace mají platný certifikát NÚKIB. V roce 2019 byla provedena aktualizace bezpečnostní dokumentace a zároveň úspěšná recertifikace informačního systému zpracovávajícího utajované informace stupně utajení „Přísně tajné“.

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. Obsahem školení je i kybernetická bezpečnost.

V průběhu roku 2019 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., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.

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

3.4 Krizové řízení

Za účelem ochrany utajovaných informací při krizových situacích byly aktualizovány Plány zabezpečení objektů či oblastí, které jsou součástí Bezpečnostních projektů, a dále Havarijní plány objektů BIS.



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 probíhala i v ostatních činnostech operativního, analytického či servisního charakteru.

Z pohledu problematik se intenzivní spolupráce s oběma službami zejména týkala boje proti nepřátelským aktivitám cizí moci, kybernetické bezpečnosti, terorismu, proliferace zbraní hromadného ničení a jejich nosičů a problematiky 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.

V rámci jednotlivých útvarů PČR v uplynulém roce pokračovala spolupráce s Ředitelstvím služby cizinecké policie (ŘSCP) při hodnocení bezpečnostních rizik spojených s udělováním víz, na kterém se BIS, jako garant za jednotné stanovisko zpravodajských služeb ČR, od roku 2000 podílí. V roce 2019 se BIS vyjádřila k téměř dvěma miliónům žádostí o krátkodobá schengenská víza, které byly podány na ZÚ ČR anebo ke kterým se ČR vyjadřuje v rámci konzultací prováděných při udělování víz ostatními státy schengenského prostoru.

Další formou 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 se BIS vyjádřila k více než osmi tisícům žadatelům o ověření spolehlivosti.

Spolupráce s NCOZ v průběhu roku 2019 spočívala ve výměně poznatků zejména po linii problematik významných ekonomických zájmů, terorismu a ochrany ústavnosti a demokratických základů státu. Předmětem spolupráce bylo prověřování zájmových subjektů, dále byly předávány poznatky v oblasti ekonomické kriminality a kybernetické bezpečnosti.

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

4.3 Spolupráce s dalšími státními orgány a institucemi

V rámci součinnosti s dalšími státními orgány a institucemi BIS 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 k jednáním týkajícím se zejména spolupráce na konkrétních případech.

V rámci plnění svých zákonných povinností podle zákona č. 412/2005 Sb. provedla BIS na žádost NBÚ více než 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 2019 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 BIS v rámci NKBT jsou NCOZ, ÚZSI a VZ. V první polovině roku 2019 se stal součástí NKBT také Finanční analytický úřad (FAÚ), který se podílí na výměně informací z hlediska boje proti financování terorismu. 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. MV, MZV) s cílem přispět k ochraně zájmů ČR a jejich 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 více než 160 000 fyzických a více než 700 právnických osob. Rozsáhlá v tomto ohledu byla zejména spolupráce s MV při posuzování cizinců - žadatelů o mezinárodní ochranu, žadatelů o pobytová oprávnění a žadatelů o udělení státního občanství ČR. Další formou spolupráce byla i součinnost při prověřování právnických nebo fyzických osob žádajících o povolení ke zprostředkování zaměstnání. V rámci mezirezortní spolupráce s MZV pak BIS poskytovala stanoviska k osobám žádajícím MZV o stáže, zaměstnání na ZÚ ČR, novinářskou akreditaci, ke kandidátům na honorární konzuly nebo jinou formu spolupráce s MZV.

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 2019 také s NÚKIB, Generální inspekcí bezpečnostních sborů, Finančním 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. V tomto ohledu probíhala spolupráce zejména s orgány celní správy, a to jak na úrovni GŘC, tak na úrovni jednotlivých celních úřadů. 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 MV, MO, 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.

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, 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 v roce 2019 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 800 mezinárodních jednání.

Informační výměna v mezinárodní spolupráci byla srovnatelná s předchozím rokem. Hlavními tématy spolupráce BIS se zahraničními zpravodajskými službami v roce 2019 byly i nadále boj proti terorismu, kontrašpionáž, proliferace a kybernetická bezpečnost. Stěžejními 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 č. 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 následujících ustanovení citovaného zákona rozhoduje o povolení k použití zpravodajské techniky a provádí kontrolu průběhu jejího použití 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 2019 byly provedeny celkem tři vnější kontroly. V prvním případě se jednalo o kontrolu plateb pojistného na veřejné zdravotní pojištění a dodržování ostatních povinností plátce pojistného, kterou provedla Všeobecná zdravotní pojišťovna ČR. Druhý případ se týkal kontroly hygieny výživy – zjištění stavu plnění požadavků a opatření v oblasti ochrany veřejného zdraví vyplývající zejména 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. Kontrolu provedl odbor zdravotnického zabezpečení MV. Ve třetím případě šlo o kontrolu provádění důchodového pojištění příslušníků, kterou provedl odbor sociálního zabezpečení MV.

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 2019 byly na základě plánu interního auditu realizovány čtyři auditní zakázky.

Ostatní odborné útvary BIS provedly celkem 32 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 10 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, meritorně prošetřované příslušnými orgány PČR a dopravní nehody příslušníků BIS. 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, šetření odcizení služebních průkazů, 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 podle ustanovení hlavy IV (§ 186 – 189) zákona č. 361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů, ve znění pozdějších předpisů.

Stížnosti, oznámení a podněty, ke kterým prováděl odbor inspekce BIS šetření v roce 2019, pocházely obvykle ze strany subjektů mimo BIS. Od roku 2017 počet vyřízených oznámení a podnětů postupně narůstá. Obsahově jsou oznámení od občanů odrazem celospolečenského dění v České republice, ale i v zahraničí.

Spolupráce odboru inspekce BIS s ostatními orgány státní správy spočívá zejména 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 2019 byl stanoven zákonem č. 336/2018 Sb., o státním rozpočtu České republiky na rok 2019.

Stejně jako v minulých letech tvořily největší podíl na čerpání rozpočtu výdaje na služební příjmy, platy a příslušenství. V oblasti osobních výdajů se pak jednalo i o výsluhové nároky, což jsou mandatorní výdaje vyplácené příslušníkům po skončení služebního poměru, a náborový příspěvek, který je poskytován nově přijímaným příslušníkům.

V rámci ostatních běžných výdajů byly zahrnuty zejména výdaje na komunikační a speciální techniku specifickou pro činnost zpravodajské služby a zvláštní finanční prostředky určené pro přímou zpravodajskou činnost. Podstatnou část běžných výdajů dále tvořily výdaje na nákup služeb, paliv a energií sloužících k zajištění běžného chodu BIS. Výdaje na opravy a údržbu primárně směřovaly k zabezpečení provozuschopnosti a udržení odpovídajícího technického stavu majetku a objektů BIS.

V kapitálových výdajích největší část směřovala do stavební oblasti. Další podstatnou část kapitálových výdajů představovaly výdaje informačních a komunikačních technologií. Cílem těchto výdajů bylo zajištění potřebného výkonu serverových a komunikačních technologií, rozvoj softwarových řešení pro podporu zpracování a uchování zpravodajských informací a pro podporu analytické činnosti. Další výdaje směřovaly na opatření posilující bezpečnost zpravodajské činnosti a zpravodajských informací. Nezanedbatelný objem kapitálových výdajů byl určen i na pravidelnou obměnu dopravní techniky.

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. Rozpočtem bylo v dodatečné výši zajištěno financování rozvojových aktivit v oblasti zpravodajské techniky, informačních a komunikačních technologií a zdrojově bylo zabezpečeno i financování stavebních a rekonstrukčních aktivit.

Podrobná zpráva o výsledku hospodaření BIS v roce 2019 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 2019 (v tis. Kč)

	Schválený rozpočet	Upravený rozpočet	Skutečnost
Příjmy celkem	160 000	160 000	247 773
Výdaje celkem	2 076 974	2 071 232	2 029 211