BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA

VÝROČNÍ ZPRÁVA 2021

Bezpečnostní informační služba
Výroční zpráva
2021

Obsah

Slovo ředitele Bezpečnostní informační služby 5

Náplň a rozsah zpravodajské činnosti 6

Zpravodajská činnost a zpravodajské poznatky 8

Zpravodajské a subverzní aktivity proti zájmům ČR

- Rusko 10
- Čína 11
- Írán 12
- Kybernetické útoky 13
- Činnosti ohrožující demokratické základy státu 15

Ekonomické zájmy státu 17

Násilné aktivity, extremismus a radikalizace 18

Ochrana utajovaných informací, bezpečnost a krizové řízení 21

Spolupráce se zpravodajskými službami ČR a ostatními státními orgány

- Spolupráce se zpravodajskými službami ČR 22
- Spolupráce s Policií ČR 22
- Spolupráce s dalšími státními orgány a institucemi 23

Spolupráce se zpravodajskými službami cizí moci 26

Kontrola 28

- Vnitřní kontrola a interní audit 29

Dodržování kázně, vyřizování žádostí a stížností 30

Rozpočet 31

Vážení čtenáři,

opět po roce Vám předkládám veřejnou výroční zprávu o činnosti Bezpečnostní informační služby, tentokrát za rok 2021. Před Vámi je na dalších stranách obecný přehled o tom, jakým tématům se Služba věnovala v roce, který si dovolím označit v mnoha ohledech za zlomový. V roce 2021 se odehrála celá řada zásadních událostí, které ovlivnily bezpečnost České republiky a jejích obyvatel na další roky.

V první řadě byl rok 2021 rokem, kdy byla po několika letech intenzivního vyšetřování ze strany Policie ČR v úzké spolupráci s BIS zveřejněna informace, že za výbuchy muničních skladů ve Vrběticích v roce 2014 stála ruská vojenská zpravodajská služba GRU. Tato zásadní zpráva odstartovala celou řadu kroků, které zásadně ovlivnily vztahy s Ruskou federací. Významně se také změnilo dosavadní vnímání Ruska a zejména bezpečnostních rizik s tímto státem spojených.

Operace zpravodajské služby cizí mocnosti na území suverénního státu, která stála dva životy nevinných lidí a způsobila miliardové škody na majetku státu i soukromých osob, byla tragickým potvrzením informací, na které Bezpečnostní informační služba dlouhé roky upozorňovala. Naše varování, že je Ruská federace zásadní bezpečnostní hrozbou pro Českou republiku i celou Evropu, dostala v roce 2022 ještě tragičtější vyústění v podobě ruské agrese na Ukrajině.

Vláda i drtivá většina politické reprezentace země se v roce 2021 ve velmi krátkém čase shodly na dosud bezprecedentních opatřeních, kdy bylo postupně téměř vyprázdněno desítky let personálně předimenzované ruské diplomatické zastoupení v České republice, poprvé od vzniku České republiky byla s Ruskou federací v této oblasti nastavena parita a Rusko bylo vyřazeno z tendru na dostavbu jaderné elektrárny Dukovany.

Přes všechny zmíněné události se BIS věnovala i dalším úkolům vycházejícím z její zákonné působnosti. V roce 2021 předala Služba zákonným adresátům zdaleka největší počet zpráv týkajících se významných ekonomických zájmů státu, nadále jsme věnovali pozornost působení cizích zpravodajských služeb, zejména z Ruské federace a z Čínské lidové republiky. Pozornost jsme věnovali také oblastem terorismu a organizovaného zločinu.

Výroční zprávu vydáváme v roce, ve kterém se po vpádu ruských vojsk na Ukrajinu zcela zásadně změnila bezpečnostní situace nejen v Evropě. Následující období bude pro nás všechny mimořádnou zatěžkávací zkouškou. Dopady ruské agrese pociťujeme již nyní a naši ekonomickou a bezpečnostní situaci ovlivní na řadu dalších let. Jsem si jistý, že Česká republika v této historické zkoušce obstojí.

Doufám, že Vás, i přes logickou míru obecnosti, naše veřejná výroční zpráva zaujme.

Přeji Vám zdraví, odvahu a vše dobré

plk. Ing. Michal Koudelka

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.

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

Zpravodajská činnost a zpravodajské poznatky

Z bezpečnostního hlediska bylo zásadní událostí loňského roku zveřejnění výsledků vyšetřování výbuchů vrbětických muničních skladů, které zasadilo vztahy s Ruskem do nového rámce. Ten symbolizovalo i hromadné vyhoštění příslušníků ruských zpravodajských služeb působících v ČR v rámci ruské diplomatické mise. Vyšetřování vrbětického případu je nadále zcela v kompetenci orgánů činných v trestním řízení, kterým BIS v dané věci poskytuje veškerou možnou součinnost.

Vzhledem k úspěšnému nastolení česko-ruské diplomatické parity BIS v následujícím období předpokládá větší ruské působení na území ČR z ambasád a konzulátů v zahraničí.

V případě čínských zájmů nedošlo k výraznějším změnám hlavních trendů. Tradiční orientace zpravodajské činnosti směřovala na potírání tzv. pěti jedů – aktivit, které Komunistická strana Číny vnímá jako hrozbu pro svůj režim. Tyto aktivity zahrnují podporu nezávislosti Tchaj-wanu, Tibetu a Sin-ťiangu, prodemokratická hnutí v Číně a hnutí Falun Gong. Vedle nich byla důležitým čínským zájmem v ČR politická rozvědka. BIS v této souvislosti identifikovala signály o rostoucím významu čínské krajanské komunity pro čínské zpravodajské aktivity a čínskou ochotu investovat finanční prostředky na legitimní akademickou publikační činnost, která však v konečném důsledku má potenciál transformace do vědomé či nevědomé spolupráce se zpravodajskými službami Číny.

V roce 2021 se ČR stala terčem několika kyberšpionážních útoků, jejichž původci byli s nejvyšší pravděpodobností státní/státem podporovaní aktéři spojovaní s Ruskem a Čínou. Cílem se staly jak státní subjekty, tak subjekty z nevládního sektoru. V ČR se však nenacházely pouze cíle útoků, ale na jejím území se vyskytovala rovněž část infrastruktury útočníků, která byla využívána pro kyberšpionážní útoky proti jiným státům.

BIS se v roce 2021 věnovala detekci případného nelegitimního ovlivňování či narušování volebního procesu ze strany rizikových aktérů. Zaznamenané spontánní dezinformační a konspirační působení domácích dezinformátorů či alternativních médií týkající se voleb bylo marginální. Obdobně jako v roce 2020 se aktivity příznivců anti-covid hnutí odehrávaly zejména v prostředí internetu. Dezinformační obsah šířený anti-covid spektrem obecně odrážel společenské dění a vývoj pandemie v ČR i ve světě. BIS nezaznamenala přímý vliv cizí moci na organizování anti-covid akcí či šíření dezinformací k tématu covid-19.

Nejzávažnějšími negativními jevy, které v roce 2021 BIS zaznamenala v oblasti ochrany významných ekonomických zájmů, bylo ovlivňování rozhodovacích a legislativních procesů a manipulace s veřejnými zakázkami. V oblasti energetické bezpečnosti se BIS zabývala přípravou projektu výstavby nového jaderného zdroje v Dukovanech, zejména pak snahami ovlivnit projekt ve prospěch některého ze zájemců.

Hrozba islamistického terorismu v ČR zůstala v roce 2021 na nízké úrovni. I nadále byla prioritou BIS detekce osob, které by mohly být nositeli rizika teroristického útoku nebo jeho logistické podpory. Hrozbu islamistického terorismu v ČR nadále ovlivňovaly vnější faktory, zejména bezpečnostní situace v Evropě.

Aktivity pravicových extremistů se v roce 2021 prakticky omezily na vyjadřování se v prostředí internetu, případně na podporu veřejných akcí a protestů pořádaných jinými občanskými subjekty. Pandemie dále prohloubila i stagnaci levicově extremistických uskupení. Důvodem je zejména tematická vyprázdněnost a neschopnost zainteresovaných subjektů organizovat akce většího rozsahu, na kterých by existovala možnost oslovit zájmovou veřejnost a rozšířit v současnosti minimální počty podporovatelů. Domobranecké prostředí bylo i v roce 2021 nekompaktním shlukem několika různorodých a navzájem jen velmi volně provázaných skupin.

Zpravodajské a subverzní aktivity proti zájmům ČR

Rusko

Dne 17. dubna 2021 seznámili představitelé české vlády veřejnost s informacemi o zapojení příslušníků zvláštní subverzní jednotky ruské vojenské rozvědky GRU s označením 29155 do přípravy výbuchů muničních skladů ve Vrběticích, ke kterým došlo 16. října 2014 a 3. prosince 2014. Zveřejnění výsledků vyšetřování výbuchů vrbětických muničních skladů bezpochyby zasadilo vzájemné vztahy mezi Českou republikou a Ruskou federací do nového rámce, který symbolizovalo hromadné vyhoštění 18 ruských zpravodajských důstojníků působících pod diplomatickým krytím v ČR v rámci ruské diplomatické mise.

Vzhledem k asymetrické reakci Ruské federace a dalšímu diplomatickému vyhrocení situace došlo navíc v květnu 2021 k zavedení početní parity diplomatického zastoupení obou zemí, tj. k zastropování shodného počtu pracovníků obou ambasád. To vedlo k nucenému odjezdu dalších desítek pracovníků Velvyslanectví Ruské federace v České republice – v řadě případů osob s vazbami na ruské zpravodajské služby.

Poprvé tak bylo prolomeno disproporční diplomatické zastoupení, které ruská strana dlouhodobě využívala k zajištění krycích pozic pro důstojníky svých zpravodajských služeb. Ty jsou proto nuceny hledat alternativní možnosti využitelné k vedení špionážních operací na českém území. Vzhledem k tomu, že příslušníci ruských zpravodajských služeb dlouhodobě zneužívají volný pohyb osob uvnitř schengenského prostoru, očekává BIS zvýšení ruských zpravodajských operací prováděných ze zahraničí, zejména pak ze zemí, ve kterých si Rusko udrželo masivní diplomatickou a zpravodajskou přítomnost.

Opatření přijatá v reakci na kauzu Vrbětice vedla také k výraznému omezení možností osobního setkávání pracovníků ruské diplomatické mise se zástupci českých proruských aktivistů. Udržovat a rozšiřovat kontakty s proruskými aktivisty se nicméně dařilo jednomu z vlivových agentů působících ve prospěch orgánů ruské státní moci, který má navíc vazby i mezi novináři a zprostředkované kontakty s některými politiky. Tyto vazby využíval k nastolování proruské politické agendy, koordinaci veřejných vystoupení kontaktovaných politiků a k medializaci narativů, jež jsou v souladu se zahraničně-politickými zájmy RF.

Vlivová skupina, jejíž je tento agent součástí, disponovala dostatkem finančních prostředků k tomu, aby udržovala nebo dokonce rozšiřovala okruh proruských novinářů a aktivistů, kteří by kromě výroby alternativního mediálního obsahu pořádali veřejné akce využitelné ve prospěch ruské propagandy. Zapojeným osobám byly propláceny náklady na přípravu materiálů a v některých případech jim byly zajišťovány výjezdy do zahraničí, kde byla jejich činnost dále koordinována a kontrolována.

Obdobně se na některé české proruské aktivisty obraceli zástupci ruských státních médií, aby získali tendenční stanoviska dále využitelná zejména pro potřeby ruské vnitrostátní propagandy. Skrze spřízněné aktivisty a novináře a cestou alternativní mediální scény, která z prokremelských narativů významně čerpá, dochází v českém prostředí k šíření stanovisek podporujících zahraniční politiku režimu Vladimira Putina.

V roce 2021 došlo k dalšímu nárůstu poptávek ze strany ruského vojensko-průmyslového komplexu, který se projevoval zejména v oblastech obráběcích strojů, materiálů a know-how i vojenského materiálu cestou reexportů a nedodržování/obcházení mezinárodních sankcí. Celkově lze vyvodit závěr, že dlouhodobě platná sankční opatření EU proti Rusku jsou účinná a nutí ruské subjekty ke hledání alternativních cest získávání zboží.

Čína

Navzdory pozornosti české společnosti, která je aktuálně prioritně zaměřená na vztahy s Ruskem, představuje Čína rostoucí komplexní zpravodajskou hrozbu. Čínská zpravodajská činnost je i v České republice nadále na vysoké úrovni a BIS v roce 2021 zaznamenala vlivové operace pohybující se na celém spektru aktivit a platforem ve prospěch čínských zahraničně-politických zájmů na úkor zájmů ČR.

Čína pokračovala ve vlivovém působení, které odpovídá aktuální čínské zahraniční politice, a to zejména s ohledem na vyostřování vztahů s Tchaj-wanem. V této souvislosti se např. v čínských médiích objevila ostrá kritika ČR za údajné opakované porušování principu jedné Číny. Okamžitým ukončením spolupráce mezi ČR a Tchaj-wanem Čína rovněž podmiňovala poskytnutí čínské vakcíny proti nemoci covid-19.

Vedle vlivových aktivit působily v ČR i v roce 2021 čínské zpravodajské struktury tradičně pod diplomatickým či novinářským krytím a vykonávaly zpravodajské aktivity, do

kterých se vedle čínských zpravodajců zapojili také čínští kariérní diplomati.

S ohledem na české parlamentní volby dominovala čínskému zájmu ze zpravodajského hlediska linie politické rozvědky. Čína měla intenzivní zájem o predikce politického vývoje, povolební scénáře a možné dopady na česko-čínské vztahy. Poptávala proto služby českých expertů a agentur, které by byly schopny dodávat odpovídající analýzy a průzkumy. Poté, co volební výsledky přinesly ztrátu některých dlouhodobě budovaných kontaktů, následovala ze strany Číny intenzivní práce na tzv. damage control, včetně hledání nových partnerů na české politické scéně.

S orientací v povolebním prostředí a hledáním nové strategie pomáhali Číně mimo jiné někteří akademici, o jejichž expertízy usilovali nejen čínští zpravodajci, ale rovněž někteří čínští diplomatičtí představitelé. Jejich zájem cílil zejména na otázky vnitřního vývoje EU a z něho plynoucí důsledky pro zahraniční politiku ČLR. Vytěžování dlouhodobě kultivovaných kontaktů z akademického prostředí představuje pro Čínu cenný zdroj na poli politického zpravodajství a pro ČR přináší riziko využívání kapacit české akademické sféry pro podporu zájmů cizí moci.

Zpravodajské aktivity Číny zahrnují také zpravodajské využívání čínské krajanské komunity, která je v ČR sice málo početná, zato náchylná k případné mobilizaci ze strany čínského státního aparátu. Nad rámec toho, že povinnost podílet se na zpravodajských činnostech ukládá všem čínským občanům a organizacím zákon, využívá Čína k získání bezvýhradné poslušnosti a respektu vůči vládnoucí komunistické straně rovněž státní propagandu. Kombinací vynucené poslušnosti a strachu z negativních následků protirežimního jednání si Čína v zahraničí vytváří síť loajálních krajanů využitelných pro své vlivové operace. BIS přetrvávající intenzivní čínský zájem o využívání krajanů k vlivovým operacím a zpravodajské činnosti zaznamenala i v loňském roce.

Čína se v posledních několika letech také zařadila mezi nejaktivnější aktéry na poli kybernetických útoků. Zvýšilo se nejen jejich množství, ale zejména jejich závažnost a sofistikovanost. Zpravidla se totiž jedná o velmi technicky pokročilé, dlouhodobé a především skryté a těžko odhalitelné kyberšpionážní aktivity, jejichž důsledky mohou mít dopad na chod zasažených organizací i několik následujících let od odhalení. Celosvětové pronikání čínských technologií do důležitých sítí státní infrastruktury nebo vzestup čínských technologií internetu věcí lze v kombinaci s masivním sledováním internetu hodnotit jako zásadní bezpečnostní hrozbu.

Zatímco se státy EU a NATO snaží neposkytovat Číně technologie z oblasti EDT (Emerging Disruptive Technologies), jako jsou umělá inteligence, autonomní systémy, hypersonické systémy, biotechnologie, nanotechnologie a aditivní technologie (metody výroby vrstvením s využitím 3D tiskáren) nebo blockchain, Čína se naopak snaží o naplňování programu Made in China 2025, včetně získávání pokročilých technologií v ČR. Rizikem jsou v této souvislosti zejména akvizice Číny v českých společnostech a snahy o přenášení výroby do Číny (včetně využívání reverzního inženýrství).

Írán

Zpravodajské aktivity Íránu představují dlouhodobou bezpečnostní hrozbu pro evropské státy včetně ČR. Íránští zpravodajci působí na různých pozicích íránského státního a soukromého sektoru a zaměřují se zejména na íránské opoziční entity, mapování cílů pro případný útok a obcházení platných sankčních režimů. Íránské zpravodajské aktivity lze pozorovat i na území ČR, ale jejich charakter nebyl doposud zásadní.

BIS i v roce 2021 věnovala pozornost jedincům v libanonské komunitě, kteří by mohli udržovat vazby na teroristické hnutí Hizballáh využívající evropské státy zejména jako zdroj financí. Aktivity libanonské komunity byly významně omezeny opatřeními proti pandemii covid-19 a nepředstavovaly ohrožení zájmů ČR.

Kybernetické útoky

BIS v roce 2021 zaznamenala aktivity zejména ruských a čínských státních/státem podporovaných kyberšpionážních aktérů, které se zaměřovaly na cíle nejen v ČR, ale směřovaly také proti dalším členským zemím EU a NATO.

BIS např. zachytila několik prvků infrastruktury zahraničních kyberšpionážních skupin, které sloužily k šíření špionážního malware, exfiltraci dokumentů kompromi-

tovaných obětí nebo k ovládání dalších částí infrastruktury útočníků v jiných státech. BIS se v jednom případě podařilo získat a analyzovat celou paletu nástrojů využívanou konkrétním kyberšpionážním aktérem.

Jiná část odhalené infrastruktury byla využita k provedení spear-phishingového útoku vůči desítkám diplomatických zastoupení evropských států napříč celým světem. Pro útok byla zneužita dlouho nepoužívaná legitimní e-mailová schránka, ke které získali útočníci přístup. Případů, kdy státní/státem podporovaný aktér používá v rámci svých spear-phishingových útoků legitimní e-mailové schránky skutečných osob, zaznamenala BIS několik. Zpravidla se jedná o již po mnoho let založené a často téměř nepoužívané schránky.

ČR pro útočníky neslouží jen jako místo, kde provozují svou infrastrukturu, ale jde také o jejich pravidelný cíl. Útokům se tak nevyhnuly klíčové státní instituce, jako jsou ministerstva, armáda nebo jiné státní úřady. Cílem kyberšpionážních aktérů se ale staly i nevládní neziskové či výzkumné organizace věnující se mezinárodním vztahům, lidským právům, bezpečnostním otázkám nebo jiným ekonomickým či politickým tématům spojovaným např. s podporou demokracie.

Vedle útoku na lidský prvek (phishing a spear-phishing) je jednou z nejčastějších metod průniku sofistikovaných aktérů i kyberzločineckých skupin zneužití nově objevených zranitelností, tzv. zero day. Jde o zranitelnosti HW i SW produktů, o kterých jejich výrobce ani odborná komunita neví, a proto na ně neexistuje bezpečnostní záplata. U globálně oblíbených a rozšířených produktů pak má zneužití zranitelností celosvětový dopad na kybernetickou bezpečnost jak státní, tak i soukromé sféry. ČR je tak vystavena stejným hrozbám pro kybernetickou bezpečnost jako ostatní státy.

V roce 2021 měly globální dopad zejména útoky na produkt/poštovní server Microsoft Exchange, které postupně zneužily hned několika tehdejších zero-day zranitelností. Jejich zneužitím se útočník mohl v konečném důsledku zmocnit role administrátora serveru a plně ho ovládnout (včetně přístupu k e-mailovým zprávám a účtům, případně získat přístup i do vnitřní sítě oběti). Zveřejnění bezpečnostních záplat zranitelností souhrnně nazvaných ProxyLogon na počátku března okamžitě vyvolalo globální vlnu útoků na dosud nezáplatované poštovní servery.

Za útoky stáli nejrůznější kybernetičtí aktéři (špionážní i kriminální, se záběrem od ransomware až po těžbu kryptoměn). Již od ledna 2021 však stejné zranitelnosti využívalo hned několik sofistikovaných státních/státem sponzorovaných aktérů (tzv. Advanced Persistent Threat; APT), o čemž postupně ve svých zprávách informovalo několik soukromých společností zabývajících se kybernetickou bezpečností. Část z aktérů měla vazbu na čínský stát, přičemž některé čínské skupiny tyto zranitelnosti zneužívaly již od listopadu 2020.

Přestože instalace záplat po celém světě probíhala relativně rychlým tempem, u některých serverů byla kompromitace úspěšná. I v ČR zareagovali správci sítí na varování o zranitelnostech a doporučení Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) většinou bezodkladně, a to včetně subjektů neregulovaných zákonem o kybernetické bezpečnosti. V několika případech však došlo ke kompromitaci poštovních serverů jak u regulovaných, tak neregulovaných subjektů.

Jako závažnou lze rovněž hodnotit kritickou zranitelnost open source logovací knihovny programovacího jazyku Java Log4j, která byla objevena v prosinci 2021 a která se nachází ve většině open source projektů. Tato zranitelnost byla obdobně zneužita kybernetickými aktéry všech typů, včetně státem podporovaných APT, k útokům na vybrané cíle. BIS nicméně v českém prostředí zneužití této zranitelnosti nezaznamenala.

Činnosti ohrožující demokratické základy státu

V průběhu roku 2021 se BIS věnovala hrozbám ze strany aktérů, kteří by svým kvalifikovaným působením mohli zasáhnout do volebního procesu či by jej mohli narušit. BIS se soustředila mj. na dezinformační kampaně, kybernetické útoky a možné vlivové působení cizí moci.

V šíření dezinformací zaměřených na volební proces hráli dominantní roli již tradičně domácí multiplikátoři dezinformačního obsahu spíše než externě koordinované kampaně. Potvrzuje se, že česká dezinformační scéna pragmaticky rozšiřuje svůj rámec o jakákoliv nová témata vzbuzující emocionální reakce. Ačkoliv se vyskytly dezinformace mající za cíl podlomit důvěru ve volební proces, nemá BIS poznatky o tom, že by je někdo koordinoval. Jejich dopad lze hodnotit jako zcela marginální.

Domácí dezinformátoři v souvislosti s parlamentními volbami opakovaně recyklovali fámy, lži a manipulace, které si mezi sebou sdílely zejména autentické komunity. Naopak prvek koordinovaného neautentického šíření

dezinformací byl spíše upozaděn. Dominantní postavení v dezinformačním ekosystému zaujímaly weby, které integrovaly dezinformační obsah či které využívaly manipulativní práce s informacemi. Tyto weby svým vysokým dosahem ovlivňovaly zbytek alternativní mediální scény a mj. dosáhly vysoké sdílenosti svých článků na sociálních sítích. Antipatie zástupců antisystémové scény vůči určitým kandidujícím subjektům rovněž vedla ke zvýšenému dezinformačnímu tlaku vůči nim.

Z hlediska vlivového působení zájem o parlamentní volby projevovaly mj. také organizace prezentující se jako nezávislé a civilní, jež ve skutečnosti ovšem sloužily jako vlivové platformy plně kontrolované ruským státem.

Dezinformační scéna byla v roce 2021 vzájemně propojená, avšak decentralizovaná, přičemž dezinformace a konspirační teorie šířila převážně sama mezi sebou. Dezinformátoři svými aktivitami cílili na osoby ve zhoršené životní situaci a na nespokojené frustrované jedince. Jednou z hlavních motivací pro ně byla vidina zisku mj. formou příspěvků od publika. Někteří z nich na dezinformacích finančně profitovali. Řada dezinformačních platforem měla do značné míry netransparentní organizační strukturu, finanční zázemí i personální složení. Běžnou praxí byla snaha zakrýt vlastníky platforem či anonymizovat autory a členy redakcí. Dezinformační ekosystém je provázaný. Primárním prostorem pro šíření dezinformací byly nadále sociální síť Facebook, dezinformační weby a řetězové e-maily. K radikálnější komunikaci využívala část antisystémového spektra taktéž síť Telegram. Dominantní alternativní weby slouží jako hlavní zdroj sdílení dezinformací a svou produkcí ovlivňují dění v dezinformačních skupinách na sociálních sítích.

Na dezinformačních platformách se často objevovaly narativy, které byly prospěšné zájmům cizí moci (zejména Ruské federace a Číny). Řada dezinformátorů však fungovala nadále samostatně z vlastní iniciativy a těmito narativy se pouze volně inspirovala. Do jejich šíření se na dezinformačních platformách zapojovali i někteří představitelé antisystémových a populistických politických subjektů.

V průběhu koronavirové pandemie došlo ke zvýšení pronikání dezinformačních narativů do české společnosti a zároveň k akceleraci šíření dezinformací zejména na sociálních sítích. V průběhu roku 2021 převládaly v dezinformačním online prostředí narativy spojené s onemocněním covid-19, očkováním a protipandemickými restrikcemi. Část politických kandidátů šířila dezinformace také v rámci volební kampaně, čímž se dosah dezinformací do širší veřejnosti zvyšoval.

Jedním z hlavních zdrojů informací sdílených mezi příznivci anti-covid hnutí byly články z produkce dezinformační mediální scény. BIS zaznamenala i přejímání dezinformačních narativů původem z cizojazyčných webů. U části anti-covid aktivistů docházelo v průběhu roku k pozvolné radikalizaci postojů i rétoriky, svými názory a protestními aktivitami však nedokázali oslovit širší spektrum veřejnosti. Proruští aktivisté využívali covid-19 jako užitečné téma pro šíření konspirací, dezinformací a prokremelské propagandy a fungovali s anti-covid hnutím do značné míry v symbióze.

Před parlamentními volbami v říjnu 2021 se někteří představitelé anti-covid hnutí pokusili využít mediální pozornost získanou skrze své veřejné anti-covid aktivity a zapojili se do volebního soutěžení. Po volebním debaklu těchto subjektů došlo k přeskupení anti-covid scény, která se propojila a začala více koordinovat své aktivity. V závěru roku tito hybatelé scény uspořádali sérii demonstrací, kterých se účastnily rovněž osoby působící na české antisystémové scéně (včetně extremistických či domobraneckých subjektů). Anti-covid hnutí tak poskytlo otevřený prostor pro šíření radikálních a extremistických tezí do společnosti. Obdobnou kooperaci napříč antisystémovým prostředím lze v českých poměrech považovat za unikátní, mobilizační potenciál hnutí však zůstal nízký a z pohledu celospolečenského vlivu marginální.

Ekonomické zájmy státu

Obdobně jako v předchozím roce se BIS zabývala přípravou projektu výstavby nového jaderného zdroje v Dukovanech. S ohledem na významnost tohoto projektu pro českou energetiku byla největším rizikem zvažovaného tendru potenciální účast subjektů, které by mohly v budoucnu využít svého postavení v projektu k prosazování vlastních partikulárních zájmů či zájmů cizí státní administrativy.

Na začátku roku pokračovaly snahy o ovlivnění mediálního prostoru a veřejného mínění ve prospěch některého ze zájemců. Zároveň zástupci jednoho z uchazečů o realizaci projektu využívali kontakty na osoby ze zájmových a profesních organizací českého průmyslu k získávání informací či koordinaci budoucích kroků. Po postupném zúžení okruhu potenciálních uchazečů došlo k výraznému omezení těchto aktivit a nebezpečí účasti rizikových subjektů na tendru se výrazně snížilo. V budoucnu nicméně může toto nebezpečí opět akcentovat v rámci subdodavatelského řetězce, a proto byly možné změny vlastnické struktury potenciálních subdodavatelů předmětem zájmu BIS.

Dlouholetým negativním jevem, který BIS zaznamenává, je snaha ovlivňovat regulované sektory ekonomiky ze strany regulovaných subjektů s cílem prosadit vlastní partikulární zájmy. Dlouhodobě jsou z jejich strany využívány dva způsoby – jednak snaha ovlivnit přímo činnost regulatorních a dohledových orgánů, jednak snaha ovlivnit legislativní proces u jednotlivých návrhů regulace.

Ačkoliv v roce 2021 došlo obecně ke snížení aktivit směřujících k ovlivnění dohledových orgánů, řádný výkon pravomocí některých z nich byl ohrožen jejich nedostatečnou personální či odbornou kapacitou. Tato omezená kapacita vytvořila prostor pro regulované subjekty, které využily svou odbornou převahu a mohly ovlivňovat přípravu regulatorní legislativy. Co do četnosti takové aktivity dokonce oproti předchozímu roku ještě zintenzivnily. Prosazování zájmů regulovaných subjektů velmi často doprovázela snaha zakrýt místo skutečného vzniku návrhu s cílem dodat mu tak zdání objektivity. To umožňovalo zdůvodňovat navrhované legislativní úpravy oprávněnými zájmy (např. výhodnou cenou pro konečného spotřebitele), ačkoli ve skutečnosti tyto návrhy konvenovaly se zájmy regulovaných subjektů.

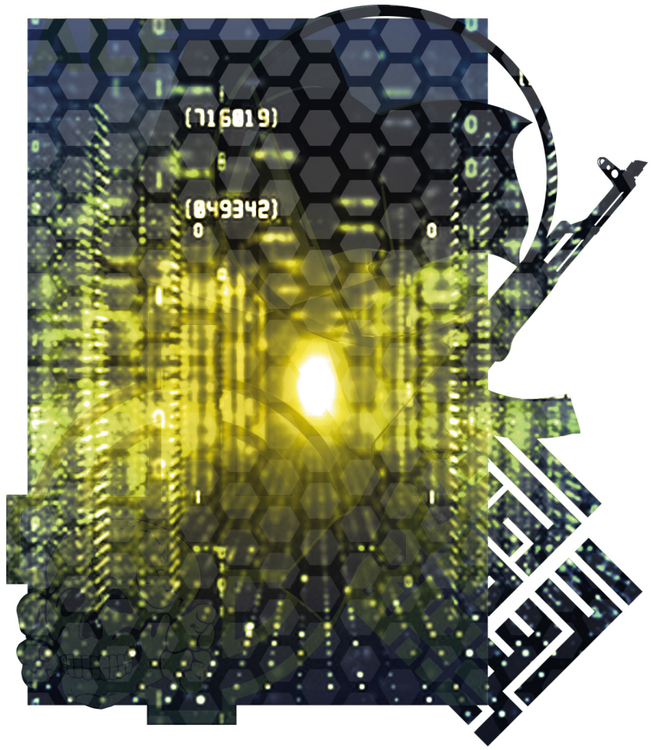
Vedle skryté účasti byly do vytváření regulatorní legislativy v některých případech regulované subjekty zapojeny i oficiálně, např. prostřednictvím účasti v různých pracovních skupinách. Ačkoliv transparentní zapojení regulovaných subjektů může být obecně přínosné, v konkrétních případech vznikaly legislativní návrhy jen ve velmi úzkém kruhu regulovaných subjektů a existence široké platformy pro oficiální zapojení subjektů v rámci pracovních skupin měla tento fakt jen zakrýt.

Rizika spojená s přenášením odborných kompetencí odpovědných státních orgánů na regulované subjekty jsou značná zejména v oblasti energetiky, kde v důsledku ruské invaze na Ukrajinu bude pravděpodobně docházet k přenastavení fungování celého sektoru a vytváření nových podmínek na mnoho let dopředu.

Při zadávání veřejných zakázek docházelo v několika oblastech ke zvýhodňování některých dodavatelů, souvisejícímu vyvádění finančních prostředků či získávání neoprávněného prospěchu ze strany osob, které o zadání zakázek rozhodovaly. Zvýhodňování bylo uskutečňováno např. poskytováním neveřejných materiálů či úpravou zadávacích podmínek, přičemž příčinou byla často existence osobních vazeb představitelů zadavatelů a dodavatelů. Častým způsobem byly nákupy nadhodnocených či nepotřebných poradenských, marketingových, IT či právních služeb.

Dalšími negativními jevy provázejícími tuto oblast bylo dále např. opakované zneužívání postavení dodavatelů stavebních zakázek, kteří se snažili omezovat vstup konkurence na trh či měli zájem získávat zakázky pro majetkově či personálně propojené společnosti. V některých sektorech pokračovala dlouhodobá závislost na konkrétním dodavateli (zejména v oblasti IT), která přetrvávala i přes snahy tento vendor lock-in stav eliminovat či alespoň omezit.

V roce 2021 BIS zaznamenala i zhoršující se finanční situaci některých státních nebo státem ovládaných subjektů. Tento stav byl zapříčiněn jak objektivními důvody, tak i nedodržením plánů na zlepšení situace, pochybením v minulosti apod. V konkrétním případě se situace jevila natolik závažná, že ohrožovala možnosti budoucího financování (např. získávání úvěrů) či dokonce běžný provoz podniku. Vzhledem k ekonomickému vývoji může být situace některých subjektů v blízké budoucnosti ještě tíživější.



Násilné aktivity, extremismus a radikalizace

Hlavní islamistické teroristické organizace, tzv. Islámský stát (IS) a Al-Qáida (AQ), měly nadále zájem páchat útoky v západních zemích, ale jejich schopnost je zorganizovat zůstávala v roce 2021 oslabena. Pragmaticky se proto soustředily na regionální konflikty v Africe a Asii s cílem získat zázemí pro další globální teroristickou činnost. Ve vztahu k Západu se omezily na nabádání svých sympatizantů k provedení jednoduchých útoků. Jejich propaganda ovlivnila některé pachatele útoků v Evropě i v loňském roce. Pokračoval tak trend málo sofistikovaných útoků osamělých aktérů bez přímé vazby na teroristické organizace, ale ovlivněných jejich propagandou. U pachatelů byly často se opakujícím faktorem psychické problémy, přičemž v některých případech bylo obtížné určit, zda byl čin skutečně ideologicky motivovaný, nebo způsobený primárně duševní nemocí. Psychické potíže v každém případě snižují odolnost vůči manipulativní propagandě.

Ve srovnání s érou před porážkou IS v březnu 2019 radikálních projevů v ČR ubylo. To ilustruje, jak silně úspěchy IS a jeho propagandou idealizovaný obraz v minulosti ovlivňovaly úroveň hrozby islamistického terorismu v ČR. Počet osob vykazujících známky islamistické radikalizace byl v roce 2021 v jednotkách a obvykle se jednalo o vazby na rizikové osoby v zahraničí. Ojedinělé pak bylo schvalování teroristických útoků či sdílení džihádistické propagandy. Zpravidla se jednalo o osoby původem z muslimských zemí, nejčastěji z Maghrebu, nebo etnické Albánce, a v jednom případě pak o českého konvertitu.

Nadále přetrvávala hrozba ze strany bývalých bojovníků IS a jejich rodin vracejících se nepozorovaně do Evropy. Ačkoliv BIS v této souvislosti prověřovala nižší jednotky osob, v roce 2021 nepotvrdila výskyt žádného navrátilce z oblasti džihádu na území ČR. Co se týká osudu více než desítky osob s vazbou na ČR, které se v minulosti připojily k IS nebo jiné džihádistické organizaci v Sýrii a Iráku, většina z nich již zesnula nebo byla nadále nezvěstná. Dva občané ČR, kteří se připojili k syrské teroristické organizaci Hayat Tahrir Al Sham, zůstávali na území kontrolovaném touto organizací.

Přestože se hrozba, kterou pro západní svět představuje Afghánistán, příchodem Tálibánu k moci zvýšila, změna afghánského režimu zásadní vliv na bezpečnostní situaci v ČR doposud neměla. Ani u afghánské komunity BIS nezaznamenala výraznější projevy podpory radikálních islamistických hnutí.

Stejně jako v roce 2020 byla i v roce 2021 česká muslimská komunita citelně zasažena pandemií koronaviru a s ní spojenými omezeními. Společenský a náboženský život muslimských organizací, včetně provozu jednotlivých modliteben a mešit nebo oslav svátků, byl po značnou část roku paralyzován, protože oficiální muslimské organizace přistupovaly k dodržování protiepidemických nařízení převážně zodpovědně.

Prakticky všechny oficiální muslimské organizace byly velmi pasivní ať už směrem k veřejnosti, tak i dovnitř organizací samotných. I v roce 2021 pokračovaly úvahy o vzniku nové mešity za podpory zahraniční organizace se silným ruským vlivem. Aktivity naopak doznaly útlumu v kazašské sektě tzv. čistého islámu.

Přestože internet zůstal významným prostředkem komunikace mezi muslimy, nedošlo jeho prostřednictvím k nárůstu míry potenciálního rizika radikalizace jednotlivců z muslimské komunity. BIS zaznamenala pouze několik ojedinělých profilů na sociálních sítích, které projevily zájem o skupiny či osobní profily a stránky spojené s islamismem. Ve všech případech se jednalo o kontakty nepřímé a málo významné.

Dominantním tématem extremistické scény v roce 2021 bylo vyjádření negativního postoje ke způsobu boje proti nemoci covid-19, ale zapojení extremistů (mimo účast na některých proticovidových demonstracích) bylo minimální. Samostatné akce pořádali extremisté jen výjimečně. Kontakty českých a zahraničních extremistů byly marginální a probíhaly primárně na individuální úrovni. Celkově činnost extremistických subjektů nadále stagnovala. Riziko BIS nicméně spatřuje v případné seberadikalizaci některých psychicky labilnějších jedinců, kteří mohou

být mj. ovlivněni právě i postoji a informacemi prezentovanými zástupci extremistické, populistické či konspirační scény.

Ideologický extremismus (neonacismus, fašismus, komunismus atp.) dlouhodobě přestává být hlavním hybatelem protidemokratických nálad. Naopak docházelo ke spolupráci jedinců a skupin se zcela rozdílnými hodnotami, které jejich nositelé v rámci „boje proti společnému nepříteli“ byli schopni aspoň částečně upozadit. Tento trend pandemická krize jen prohloubila. S jejím postupným odezníváním se zřejmě navrátí tradičnější témata extremistické scény (migrace, rasové či genderové otázky, postoj k Evropské unii atp.), nicméně stále klesající význam ideologického extremismu bude velmi pravděpodobně pokračovat.

České domobranecké prostředí je heterogenní skupinou několika různorodých a navzájem jen velmi volně provázaných skupin. Řada z nich reálnou činnost vyvíjí pouze sporadicky a značně nekoordinovaně. Ideologické pozadí jednotlivých domobraneckých skupin je velmi nevyhraněné a není hlavním hybatelem jejich fungování. Mezi domobranci se vyskytují jedinci silně protisystémově zaměření, ale i osoby, které žádný ideologický postoj nezastávají a jejich hlavní motivací jsou militaristicky zaměřené schůzky. Obecně lze smýšlení domobranců charakterizovat jako směsici ultranacionalismu, pozitivního přístupu k autoritářským režimům (primárně k Rusku) a celkové nedůvěry k demokratickému fungování společnosti. S nástupem pandemie covid-19 se mezi domobranci rozšířil i silný nesouhlas s opatřeními státu při boji proti této nemoci a výrazný odpor vůči očkování. Za nejrizikovější aktivity domobranců lze považovat jejich snahy o nelegální výrobu palných zbraní a výbušnin.

Kontakty českých a zahraničních domobranců jsou sporadické a navzdory deklarovaným prohlášením spolupráce probíhala dominantně pouze na základě osobních kontaktů několika jednotlivců.

Ochrana utajovaných informací, bezpečnost a krizové řízení

Bezpečnost informačních a komunikačních systémů BIS je zaměřena zejména na zajištění důvěrnosti a integrity informací. Velký důraz je kladen na neustálé zlepšování zabezpečení ICT systémů a poskytovaných služeb aplikováním vhodných technologií, a to jak v systémech zpracovávajících utajované informace, tak v neutajovaných systémech. Všechny informační systémy BIS zpracovávající utajované informace mají platný certifikát NÚKIB. V roce 2021 byla provedena úspěšná akreditace informačního systému určeného pro komunikaci mezi zpravodajskými službami států NATO.

Všichni uživatelé certifikovaných informačních systémů jsou v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, proškoleni před jejich prvním přístupem do informačního systému. Následně prochází jednou ročně pravidelným proškolením zaměřeným na dodržování bezpečnostní politiky informačních systémů BIS a zvyšování povědomí v oblasti kybernetické bezpečnosti.

V průběhu roku 2021 nebyl v BIS zaznamenán žádný závažný bezpečnostní incident.

V oblasti kryptografické ochrany utajovaných informací probíhá příprava dalšího nového systému utajeného spojení s partnerskými zpravodajskými službami. Na základě ustanovení vyhlášky NÚKIB proběhly recertifikace kryptografických pracovišť včetně aktualizace jejich režimových opatření.

V průběhu uplynulého roku nebyl v BIS zaznamenán žádný závažný incident nebo kompromitace kryptografických prostředků. Průběžně probíhá proškolování pracovníků kryptografické ochrany a pracovníků provozní obsluhy jednotlivých kryptografických prostředků, a to jak stávajících, tak nových.

V průběhu roku 2021 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., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Byla prováděna tvorba nových povinných složek objektové dokumentace pro pracoviště a objekty BIS a probíhaly novelizace objektových dokumentací tak, aby odpovídaly aktuálnímu stavu.

Oblast běžné činnosti fyzické bezpečnosti byla v průběhu roku 2021 ovlivněna stavbou administrativně-technického objektu. Byla prováděna režimová opatření na zabezpečení perimetru a režimu vstupu do prostor stavby tak, aby byla v co nejmenší míře narušena obvyklá činnost BIS.

S cílem ochrany utajovaných informací při krizových situacích byly aktualizovány plány zabezpečení objektů či oblastí, které jsou součástí bezpečnostních projektů. V souladu se zákonem č. 240/2000 Sb., o krizovém řízení, byl průběžně aktualizován krizový plán BIS a plán krizové připravenosti subjektu kritické infrastruktury.

Byl aktivován a pravidelně se scházel krizový štáb ředitele BIS, který vydával organizační a systémová rozhodnutí či doporučení s cílem zajištění chodu BIS a minimalizace rizik spojených s nemocí covid-19.

Spolupráce se zpravodajskými službami ČR a ostatními státními orgány

Spolupráce se zpravodajskými službami ČR

BIS v roce 2021 zaslala Úřadu pro zahraniční styky a informace (ÚZSI) a Vojenskému zpravodajství (VZ) desítky informací. Spolupráce s oběma službami probíhá i v dalších činnostech operativního, analytického či servisního charakteru.

BIS dlouhodobě spolupracuje s ÚZSI v oblasti prověřování osob žádajících o akreditaci diplomatických zástupců a pracovníků diplomatických misí. Cílem je vyloučit bezpečnostní riziko, které by z působení těchto osob na našem území mohlo plynout.

Pokračovala spolupráce s Ministerstvem obrany (MO), resp. VZ, v oblasti rozvoje agendového informačního systému pro potřebu zpravodajských služeb.

BIS s VZ a ÚZSI dále spolupracovala při cvičení orgánů krizového řízení EU či NATO či v oblasti opatření proti šíření onemocnění covid-19.

Spolupráce s Policií ČR

Policie České republiky (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.

BIS se jako garant jednotného stanoviska zpravodajských služeb ČR podílí na hodnocení bezpečnostních rizik spojených s udělováním víz. V roce 2021 se BIS vyjádřila k 558 578 žádostem o krátkodobá jednotná schengenská víza. Počet žádostí je i nadále ovlivněn pokračující pandemií covid-19. Proti roku 2020 došlo k mírnému nárůstu, nadále však zůstávají počty podaných žádostí výrazně nižší, než tomu bylo před začátkem pandemie.

V roce 2021 pokračovala spolupráce mezi BIS a Ředitelstvím služby cizinecké policie (ŘSCP), která plyne ze zákona č. 49/1997 Sb., o civilním letectví. Spolupráce spočívá ve vyloučení bezpečnostního rizika u fyzických osob vstupujících do vyhrazeného bezpečnostního prostoru letiště. V roce 2021 bylo prověřeno 4 137 žadatelů o vydání osvědčení spolehlivosti dle zákona o civilním letectví, což je ve srovnání s rokem 2020 o více než polovinu méně. Vyšší počet prověřovaných osob v roce 2020 byl ovlivněn tím, že v tomto roce uplynula většině již vydaných osvědčení platnost, která je zákonem stanovena na pět let, a proto vznikla žadatelům povinnost požádat o vydání nového. Zároveň nedošlo k přijetí plánované novely zákona, která měla zkrátit platnost osvědčení.

Spolupráce s Národní centrálou proti organizovanému zločinu SKPV PČR (NCOZ) spočívala ve výměně poznatků zejména po linii problematik významných ekonomických zájmů, terorismu a kybernetické bezpečnosti.

Spolupráce s dalšími státními orgány a institucemi

BIS poskytuje informace a stanoviska vybraným orgánům státní správy, které se týkají bezpečnostního prověřování osob a firem, ať už na základě ustanovení zákona, nebo na základě dohody o mezirezortní spolupráci. Mezi nejvýznamnější adresáty informací patří Národní bezpečnostní úřad (NBÚ), Ministerstvo vnitra (MV) a Ministerstvo zahraničních věcí (MZV).

BIS v oblasti bezpečnostního prověřování odpovídá na žádosti NBÚ podle § 107 odst. 1, § 108 odst. 1 a § 109 odst. 1 zákona č. 412/2005 Sb. (tzv. evidenční šetření) nebo se na průběhu bezpečnostních řízení v oblasti personální a průmyslové bezpečnosti a bezpečnostní způsobilosti aktivně podílí formou zabezpečování informací v prostředí, a to na základě žádostí NBÚ podle ustanovení § 107 odst. 2 a 3, § 108 odst. 2, 3 a 4 a § 109 odst. 2 zákona č. 412/2005 Sb. (tzv. činnostní šetření). Při činnostním šetření je prováděna standardní zpravodajská činnost včetně používání specifických prostředků získávání informací a jejich kombinací.

V roce 2021 provedla BIS na základě žádosti NBÚ více než 18 000 evidenčních šetření. Po realizaci činnostního šetření se BIS vyjádřila k 93 fyzickým a třem právnickým osobám.

BIS v této oblasti i bez žádosti NBÚ zabezpečuje v rámci své působnosti informace o okolnostech nasvědčujících tomu, že držitelé osvědčení nebo dokladu přestali splňovat podmínky pro jejich vydání. Případná relevantní zjištění jsou NBÚ neprodleně předávána, neohrozí-li to důležitý zájem sledovaný BIS.

MV a jemu podřízené subjekty dlouhodobě poskytují BIS na základě dohody některé služby komunikačních technologií, činností v oblasti požární ochrany, bezpečnosti a ochrany zdraví při práci, energetiky, vodního hospo-

dářství, životního prostředí a též v oblasti stravování.

Pokračovala i spolupráce s MV na prověření fyzických a právnických osob žádajících o udělení povolení ke zprostředkování zaměstnání. BIS prověřila 629 právnických a 1 068 fyzických osob.

V roce 2021 se BIS vyjádřila na žádost Odboru azylové a migrační politiky MV (OAMP) k téměř 163 000 žadatelům o pobytová oprávnění. Vypovídající meziroční porovnání nelze provést, neboť v roce 2020 došlo v souvislosti s pandemií covid-19 k poklesu počtu žádostí. V porovnání s předchozími roky můžeme konstatovat rostoucí trend v zájmu cizinců o pobytová oprávnění.

BIS se dále na základě žádosti OAMP vyjádřila celkem k 547 žadatelům o udělení nebo prodloužení mezinárodní ochrany. O mezinárodní ochranu nebo její prodloužení v roce 2021 požádalo nejvíce žadatelů z Afghánistánu, a to v důsledku politických změn a z nich plynoucí nestabilní bezpečnostní situace v zemi. Další početnější skupiny žadatelů pocházely ze Sýrie, Běloruska, Ukrajiny, Číny, Kazachstánu nebo Iráku. BIS spolupracovala s OAMP opět při prověřování osob v rámci zdravotně humanitárního projektu MEDEVAC. Stejně jako v roce 2020 byl i v roce 2021 projekt zaměřen zejména na pomoc občanům Běloruska.

BIS se na základě žádosti Odboru všeobecné správy MV vyjádřila k 3 585 žadatelům o udělení státního občanství ČR. Počet osob žádajících o udělení státního občanství se v porovnání s roky 2019 a 2020 výrazně nezměnil.

Spolupráce s odborem eGovernmentu MV spočívá v prověřování žadatelů o akreditaci pro správu kvalifikovaného systému elektronické identifikace. BIS prověřila dvě právnické a 27 fyzických osob. V souvislosti s připravovanou elektronizací státní správy bude okruh prověřovaných subjektů z této oblasti narůstat. Jako příklad lze uvést novelu zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých zákonů, která je účinná od 1. září 2021, a která umožňuje MV požadovat od zpravodajských služeb, ale i dalších státních orgánů, informace k subjektu, žádajícímu o zápis do katalogu cloud computingu, který je veden na MV.

V rámci mezirezortní pracovní skupiny „Dopady elektronizace veřejné správy na činnost bezpečnostních složek ČR“ probíhala s MV a ostatními zainteresovanými bezpečnostními složkami spolupráce na opatřeních souvisejících s elektronizací veřejné správy.

BIS spolupracovala s bezpečnostním odborem MZV na vyloučení bezpečnostního rizika u osob, které se o spolupráci s MZV ucházejí. V roce 2021 bylo prověřeno 652 fyzických a 56 právnických osob. Jednalo se například o 25 kandidátů na pozici honorárního konzula, 24 žadatelů o akreditaci vojenského přidělence, 30 žadatelů o udělení či prodloužení dlouhodobé novinářské akreditace, 95 osob žádajících o přijetí na zastupitelský úřad (ZÚ) jako místní síly a 148 osob, které měly zájem o stáž na MZV či na ZÚ České republiky v zahraničí. Oproti roku 2020 došlo k mírnému navýšení počtu prověřovaných subjektů.

V roce 2021 nabyl účinnosti zákon č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů. BIS je jedním ze subjektů, které v rámci procesu prověřování zahraničních investic poskytují informace Ministerstvu průmyslu a obchodu (MPO), do jehož gesce tato problematika spadá. Zákon upravuje práva a povinnosti zahraničních investorů, jejichž konečný vlastník je ze třetích zemí, a to v konkrétních oblastech, uvedených v zákoně. Účelem zákona je zajištění ochrany bezpečnosti ČR a vnitřního a veřejného pořádku. Zároveň by však zákon měl svými předem nastavenými pravidly zvýšit právní jistotu pro přicházející zahraniční investory.

Investice a subjekty, kterých se investice týká, jsou prověřovány na třech úrovních, přičemž BIS se podílí na všech z nich. První z nich jsou notifikace, kdy jsou prověřovány investice ze třetích zemí, které směřují do jiného členského státu EU a ke kterým se má možnost ČR vyjádřit. Další jsou konzultace, v rámci nichž se prověřují investice zákonem specifikované, nebo takové, u nichž se investor sám dobrovolně rozhodne z důvodu právní jistoty prověřit investici mající potenciál ohrozit bezpečnost ČR nebo vnitřní či veřejný pořádek. Poslední jsou řízení, která jsou povinná pro úzkou skupinu nejcitlivějších oblastí a kde je vyžadován k povolení investice souhlas státu. V případě opomenutí investorů je též možné v pětiletém období od investice zahájit proces prověřování z moci úřední.

Od počátku účinnosti tohoto zákona prověřila BIS 78 právnických osob a 54 fyzických osob v rámci evropských notifikací a 57 právnických osob a 69 fyzických osob v rámci prověřování investic směřujících na území ČR (konzultace a řízení).

BIS pravidelně sdílela zpravodajské poznatky v rámci Společné zpravodajské skupiny a informačně přispívala k vyhodnocování bezpečnostní situace z hlediska možného ohrožení ČR. BIS rovněž průběžně sdílela informace v rámci platformy Národního kontaktního bodu pro terorismus, která působí jako jedno z oddělení NCOZ. Hlavní náplní spolupráce byly prověrky identit získaných ve spojitosti s vyšetřováním teroristických útoků na území EU.

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

Mimo výše uvedené spolupracovala BIS také s Generální inspekcí bezpečnostních sborů, Finančním analytickým úřadem (FAÚ), Celní správou ČR, Generálním ředitelstvím cel (GŘC), Vězeňskou službou ČR, Generálním finančním ředitelstvím (GFŘ) a se soudy a státními zastupitelstvími.

Předmětem spolupráce s dalšími orgány státní správy bylo také řešení konkrétních případů v problematice proliferace zbraní hromadného ničení 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 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 (SÚJB) 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 pokračovala v koordinaci plnění úkolu VZČ k problematice vývozů zařízení, která nejsou na seznamech mezinárodních kontrolních režimů, a která mohou být využita dvojím způsobem při vývozech do rizikových oblastí. Na plnění úkolu se podíleli zástupci MV, MZV, MPO, SÚJB, GŘC, FAÚ, ÚZSI a VZ.

Při zabezpečování informací k činnostem ohrožujícím významné ekonomické zájmy spolupracovala BIS s dalšími orgány státní správy. Komunikace s GFŘ se týkala oprávnění BIS získávat informace z daňových řízení. Orgánům činným v trestním řízení, SÚJB a ÚOHS byly předávány informace spadající do jejich působnosti. Dále probíhaly odborné konzultace s gesčními úřady, a to především s MPO a MV v oblasti přípravy výstavby nového jaderného zdroje.

Spolupráce s NÚKIB spočívala nejen v oblasti zabezpečení utajovaných informací v rámci fyzické bezpečnosti, ale také v předávání zpravodajských poznatků.

V roce 2021 BIS dále spolupracovala se státními orgány při zajišťování ochranných pomůcek a dezinfekce v rámci čelení pandemii covid-19 (součinnost s MPO a Správou státních hmotných rezerv).

Spolupráce se zpravodajskými službami cizí moci

BIS realizuje spolupráci se zpravodajskými službami cizí moci na základě § 10 zákona č. 153/1994 Sb., o zpravodajských službách České republiky. Na základě souhlasu vlády ČR je BIS aktuálně oprávněna spolupracovat s více než stovkou zpravodajských služeb z celého světa. Informační výměna a aktivní kontakty jsou rozvíjeny především se službami členských zemí EU a NATO a některých dalších zemí. Na multilaterální úrovni se BIS v roce 2021 zapojovala v rámci všech uskupení, jejichž je členem (např. Counter-Terrorism Group a NATO Civilian Intelligence Committee).

S částečným uvolněním protipandemických restrikcí jednotlivých států a za využití zkušeností z předchozího roku mezinárodní zpravodajská komunita přizpůsobila formu a způsob spolupráce, což se odrazilo i v meziročním nárůstu počtu jednání. S ohledem na efektivní čerpání zdrojů a proměnlivou pandemickou situaci byly nadále využívány a rozvíjeny elektronické komunikační nástroje.

V rámci mezinárodní spolupráce BIS v roce 2021 přijala více než 12 000 zpráv a postoupila zhruba 2 200 dokumentů. Na strategické a expertní úrovni se zástupci BIS zúčastnili více než 700 mezinárodních jednání. Po loňském mimořádném poklesu tak došlo k návratu k rostoucím trendu četnosti jednání a vyměněných zpráv. Prioritními oblastmi spolupráce BIS se zahraničními zpravodajskými službami zůstávají boj proti terorismu, kontrašpionáž, proliferace, kybernetická bezpečnost, oblast ochrany utajovaných informací a oblast bezpečnostní způsobilosti.

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 ČR.

Ačkoliv zákon nestanoví konkrétní rozsah ani způsob provádění kontrolní činnosti vládou, kontrola vlády vůči BIS se odvíjí od jejího oprávnění ukládat BIS úkoly a hodnotit jejich plnění. Vláda za činnost BIS odpovídá, koordinuje ji a jmenuje a odvolává jejího ředitele. BIS je rovněž 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.

Poslanecká sněmovna je o činnosti zpravodajských služeb informována vládou prostřednictvím svého příslušného orgánu pro zpravodajské služby. Tím je ve vztahu k BIS Stálá komise pro kontrolu činnosti Bezpečnostní informační služby, jejíž členové jsou např. oprávněni vstupovat v doprovodu ředitele BIS nebo jím pověřeného příslušníka do objektů BIS. Kontrolní orgán také může požadovat od ředitele BIS potřebné vysvětlení v případě, že má 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.

Zákon 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, předpokládá zřízení pětičlenného Orgánu nezávislé kontroly zpravodajských služeb České republiky voleného Poslaneckou sněmovnou na dobu pěti let na návrh vlády, který by měl vykonávat kontrolu na základě podnětu některého ze zvláštních kontrolních orgánů. Tento orgán, který bude oprávněn požadovat od zpravodajské služby až na několik výjimek všechny potřebné informace o její činnosti, které souvisejí s prováděnou kontrolou, 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, 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.

Ochranu utajení činnosti zpravodajských služeb zajišťují zvláštní způsoby, jakým se kontroly provádějí. Například v zařízeních zpravodajské služby může být kontrola vykonána jen se souhlasem jejího ředitele. Nebude-li souhlas udělen, zajistí zpravodajská služba výkon kontroly sama a následně podá zprávu o jejím výsledku kontrolnímu orgánu, který o souhlas požádal. 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 jejího výkonu.

V případech používání zpravodajské techniky podle zákona č. 154/1994 Sb. podléhá činnost BIS i soudní kontrole. O povolení k použití zpravodajské techniky rozhoduje předseda senátu Vrchního soudu v Praze, který také provádí kontrolu průběhu jejího použití. Předseda senátu Vrchního soudu v Praze dále rozhoduje o žádostech BIS o poskytování zpráv o záležitostech týkajících se klienta, které jsou předmětem bankovního tajemství. Soud nejen vydává předchozí povolení k písemné žádosti BIS, ale také kontroluje, zda důvody žádosti trvají. V opačném případě povolení odejme, resp. odebere.

Veřejnost kontroluje činnost BIS zejména prostřednictvím hromadných sdělovacích prostředků nebo přes internetové stránky BIS, na kterých jsou volně přístupné např. výroční zprávy či aktuální sdělení týkající se bezpečnostní situace.

Vnitřní kontrola a interní audit

Odborné útvary provedly celkem 20 kontrol, jejichž cílem bylo metodicky a věcně usměrňovat činnost organizačních útvarů ve finanční a materiálové oblasti a rovněž předcházet možnosti vzniku nežádoucích jevů. Jednotlivé kontroly byly zaměřeny především na oblast účetnictví a rozpočtu, materiálně technické zabezpečení a vedení evidence majetku BIS, dále na evidenci pro výplatu služebních příjmů příslušníků a platů zaměstnanců, poskytování náhrad cestovních výdajů a příspěvků z fondu kulturních a sociálních potřeb, sledování technického stavu vozidel a provádění technických kontrol, dodržování kontrolních norem spotřeby pohonných hmot, sledování využití vozidel a stav a využití stavebních objektů, energetické služby a na prováděné povinné kontroly a revize. V rámci kontrolních akcí nebyla zjištěna závažná porušení předpisů.

Orgánem nemocenského pojištění BIS byly provedeny čtyři kontroly dodržování režimu dočasně práce neschopného pojištěnce a ze strany BIS jako zaměstnavatele byla provedena jedna kontrola dodržování stanoveného režimu dočasně práce neschopného pojištěnce v období prvních 14 kalendářních dnů dočasné pracovní neschopnosti u zaměstnanců v pracovním poměru. V žádném z kontrolovaných případů nebylo shledáno porušení ze strany pojištěnce.

Pracovníci archivní služby a kontrolní skupiny provedli celkem 30 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.

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. V roce 2021 byly ukončeny tři auditní zakázky. V průběhu roku nebyly identifikovány závažné nedostatky, které by nepříznivě ovlivnily činnost BIS a signalizovaly sníženou kvalitu vnitřního kontrolního systému.

Bezpečnostní informační služba

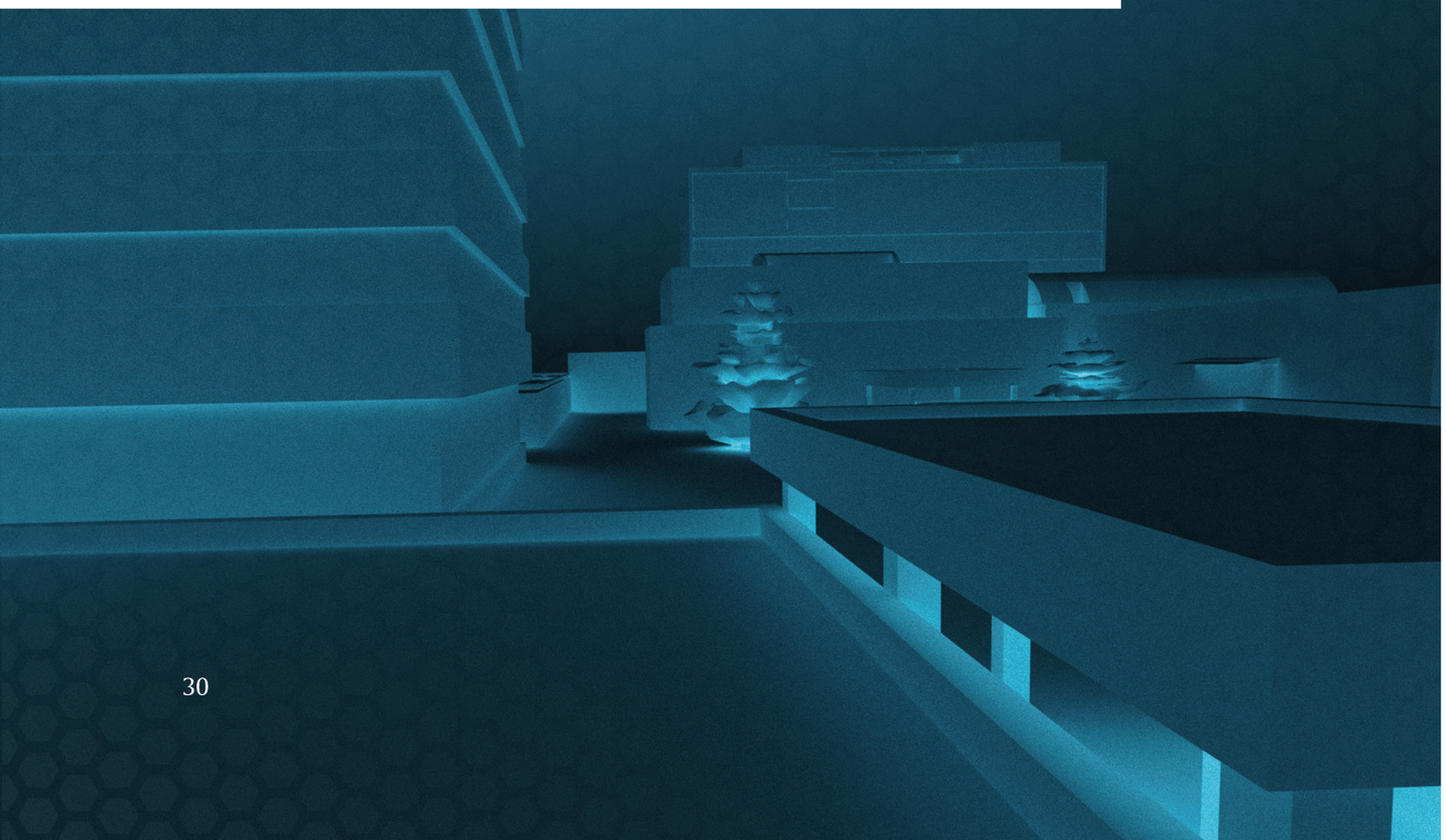
Dodržování kázně, vyřizování žádostí a stížností

Působnost odboru inspekce lze rozdělit do čtyř hlavních oblastí – činnost v postavení policejního orgánu BIS ve smyslu § 12 odst. 2 písm. f) trestního řádu, a to v případech podezření ze spáchání trestného činu příslušníkem, činnost při prošetřování případů podezření ze spáchání jednání majících znaky přestupku a kázeňských přestupků příslušníky, včetně prošetřování mimořádných událostí, činnost v rámci prošetřování stížností, oznámení a podnětů příslušníků BIS a subjektů mimo BIS a činnost v rámci vyřizování dožádání jiných orgánů činných v trestním řízení podle ustanovení trestního řádu a ostatních orgánů státní správy.

Naprostá většina šetření podezření ze spáchání kázeňského přestupku nebo jednání majícího znaky přestupku se i v roce 2021 týkala dopravy, tj. například dopravních nehod se služebními nebo soukromými vozidly, poškození služebních vozidel a podezření z jiného porušení zákona o provozu na pozemních komunikacích. Případy, u nichž bylo zjištěno podezření ze spáchání kázeňského přestupku nebo jednání majícího znaky přestupku ze strany příslušníka BIS, byly postoupeny ke kázeňskému řízení.

Z celkového počtu 157 podání bylo jedno vyhodnoceno jako stížnost na jednání příslušníků BIS. Stížnost byla shledána jako nedůvodná. Všechna podání byla prověřena a vyhodnocena s tím, že nedošlo k porušení interních ani obecně závazných právních předpisů příslušníkem BIS, a bylo rozhodnuto o dalším postupu. Obsahově jsou oznámení od občanů odrazem celospolečenského dění nejen v ČR, ale i v zahraničí, a odrážela situaci kolem pandemie covid-19.

Odbor inspekce spolupracuje s ostatními orgány státní správy především ve formě dožádání, která nejčastěji zasílají orgány PČR, které jsou činné v trestním nebo přestupkovém řízení. Trend počtu zpracovávaných žádostí a dožádání je po celou sledovanou dobu rostoucí.



Rozpočet

Rozpočet BIS byl pro rok 2021 stanoven zákonem č. 600/2020 Sb., o státním rozpočtu České republiky na rok 2021. Příjmy byly kapitole určeny ve výši 250 000 tis. Kč a výdaje ve výši 2 297 315 tis. Kč.

Vedle rozpočtových prostředků evidovala BIS nároky z nespotřebovaných výdajů. Konečný rozpočet výdajů, který představuje celkové disponibilní zdroje včetně zapojených nároků z nespotřebovaných výdajů, činil ke konci sledovaného období 2 726 655 tis. Kč. Celkové skutečně realizované výdaje BIS v roce 2021 dosáhly výše 2 260 154 tis. Kč.

Kapitálové výdaje byly čerpány s cílem udržet provozuschopnost materiálně technické základny a zajistit její nezbytný rozvoj. V současné době je nejvýznamnější akcí výstavba technicko-administrativního objektu. Významná část investic směřovala také do zpravodajské techniky a do informačních a komunikačních technologií. Další výdaje byly vynaloženy na opatření posilující bezpečnost zpravodajské činnosti a zpravodajských informací a do pravidelné obměny dopravních prostředků. Čerpání výdajů v této oblasti významně ovlivnila nedostupnost některých požadovaných technologií v posledním čtvrtletí roku 2021.

Objemově nejvýznamnější položku v rámci běžných výdajů představovaly osobní výdaje reprezentované zejména výdaji na platy a příslušenství. Významnou součástí osobních výdajů jsou i výsluhové nároky vyplácené bývalým příslušníkům po skončení služebního poměru.

Další důležitou součástí běžných výdajů byly výdaje na speciální zpravodajskou techniku a zvláštní finanční prostředky určené pro přímou zpravodajskou činnost. Opomenout nelze ani výdaje provozního charakteru, ke kterým se řadí běžné materiálové výdaje, výdaje na nákup energií a služeb zajišťujících každodenní chod organizace a výdaje na dodavatelské zajištění oprav a údržby majetku a objektů BIS.

I v roce 2021 byla BIS nucena zajistit ochranné pomůcky, desinfekční prostředky, zdravotnický materiál a testovací sady související s opatřeními proti epidemií covid-19. Výše těchto mimořádných výdajů na úrovni 1,7 mil. Kč však nebyla v relaci celkových výdajů zásadní. Díky včasnému nastavení řady preventivních hygienických a organizačních opatření nebyla činnost BIS ani přes vážnost epidemické situace v roce 2021 výrazně omezena.

Čerpání běžných výdajů probíhalo vzhledem k jejich charakteru a struktuře v průběhu roku 2021 pravidelně a průběžně. Platná protiepidemická opatření ovlivnila čerpání v některých oblastech běžných výdajů, jako např. školení, konference a zahraniční služební cesty, takže objemy realizovaných výdajů v těchto položkách byly nižší než v letech neovlivněných epidemií covid-19.

Bezpečnostní informační služba
Výroční zpráva 2021

Bezpečnostní informační služba
P. O. BOX 1
150 07 Praha 57
Telefon: +420 235 521 400
Fax: +420 235 521 715
E-mail: info@bis.cz
Datová schránka: cx2aize