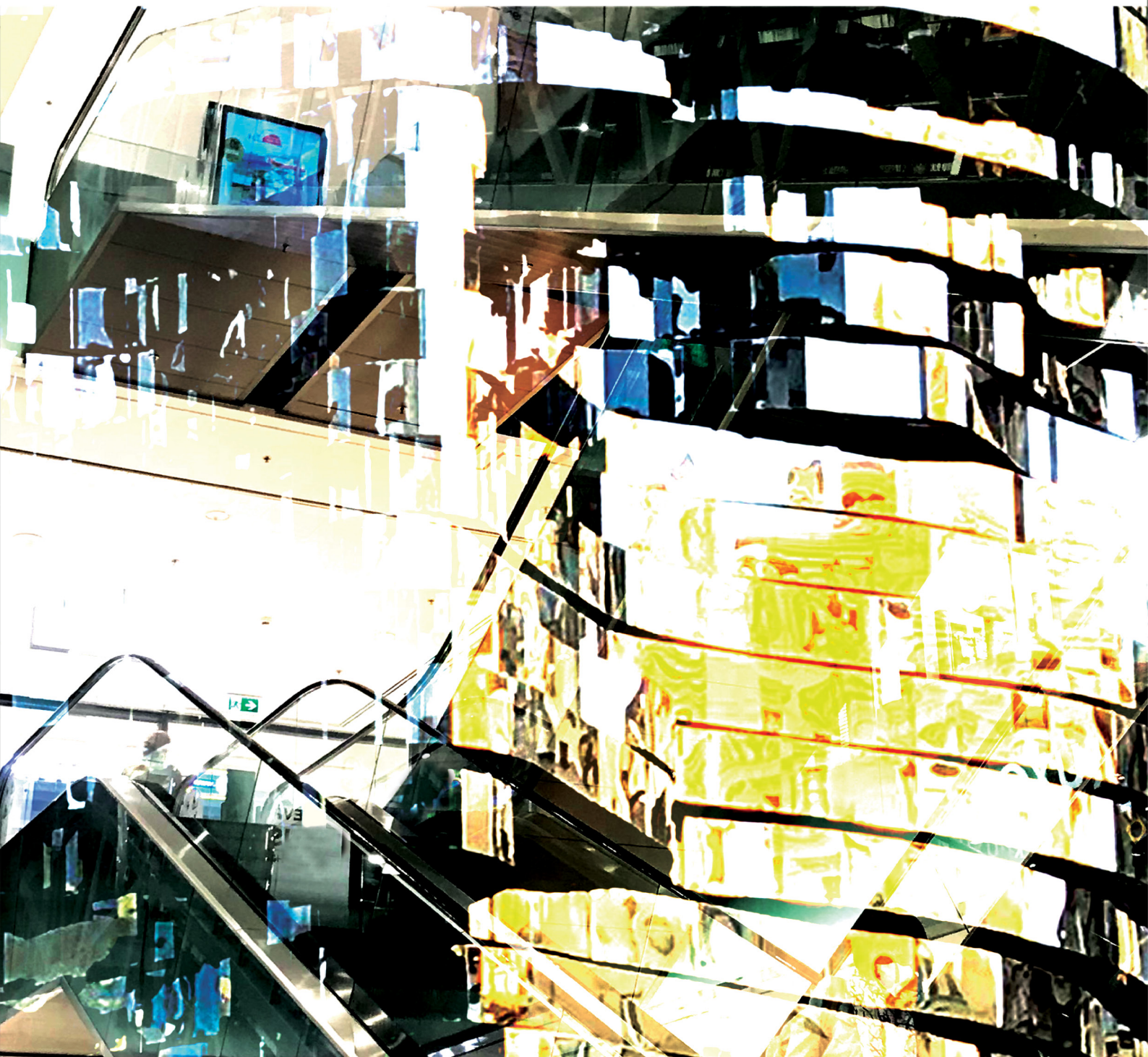
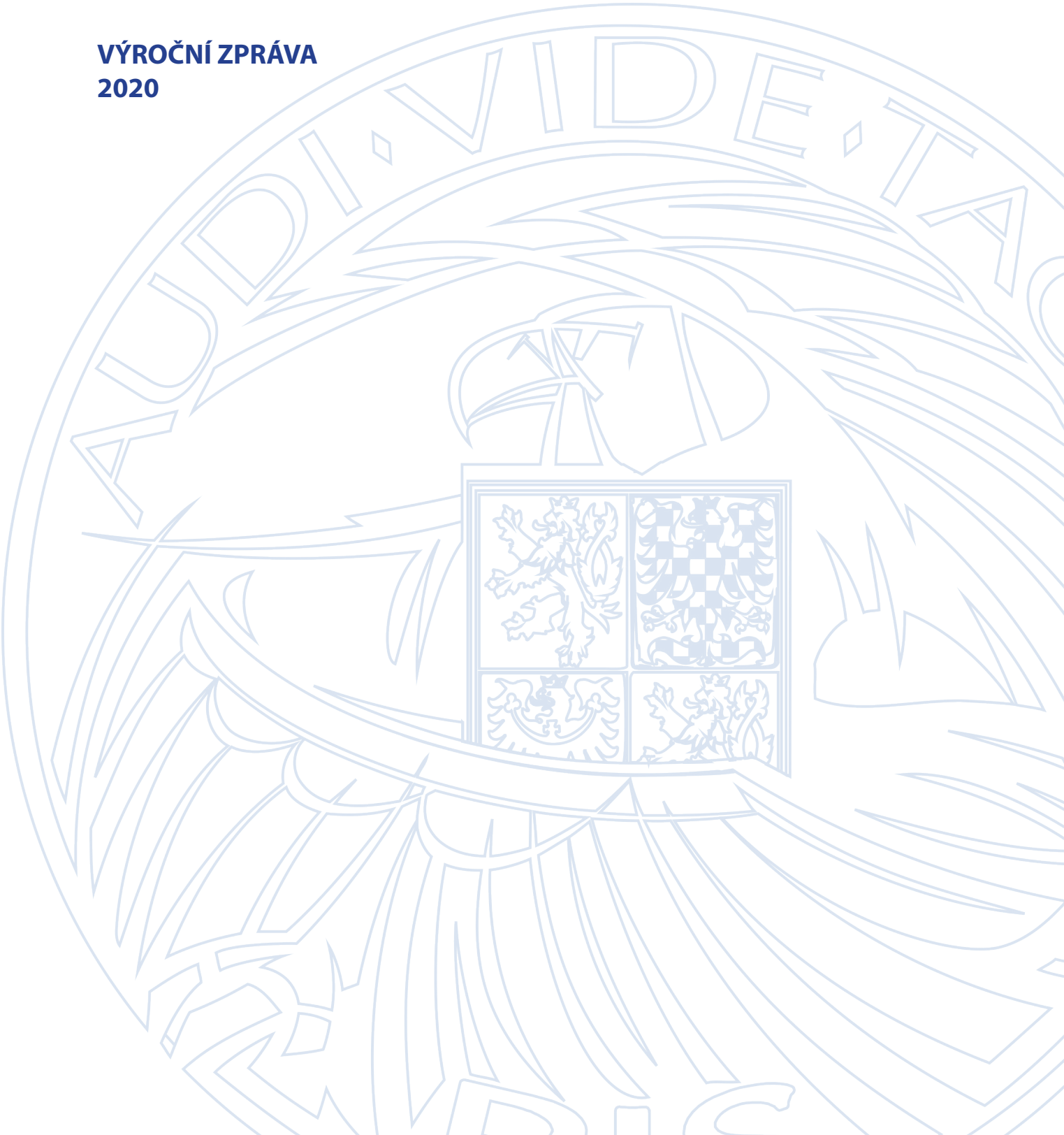
Bezpečnostní informační služba

Výroční zpráva 2020



BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA

VÝROČNÍ ZPRÁVA 2020



Obsah

Slovo ředitele Bezpečnostní informační služby

Vážení čtenáři,

jsem velmi rád, že Vám mohu představit veřejnou výroční zprávu o činnosti Bezpečnostní informační služby za rok 2020. Celá naše země má za sebou jedno z nejnáročnějších období v novodobých dějinách. Rád bych využil této příležitosti a vyjádřil neskonalý obdiv a poděkování všem zdravotníkům, záchranářům a dalším lidem, kteří v tzv. první linii bojovali s pandemií covid.

Pandemie a její důsledky se nevyhnuly ani zpravodajským službám. Na jedné straně došlo k poklesu téměř ve všech aspektech hrozeb, kterým se služba věnuje. Na straně druhé byla zejména z důvodu nejrůznějších opatření značně narušena i naše každodenní práce. Rád bych proto poděkoval i všem svým kolegům, kteří v nelehkých podmínkách dokázali plnohodnotně odvádět práci pro zajištění bezpečnosti České republiky. Přes všechna omezení se BIS podařilo i v roce 2020 dosáhnout řady úspěchů nejen v boji s působením cizích zpravodajských služeb, ale také v oblasti ochrany ekonomických zájmů státu a v eliminaci hrozeb spojených s bojem proti terorismu.

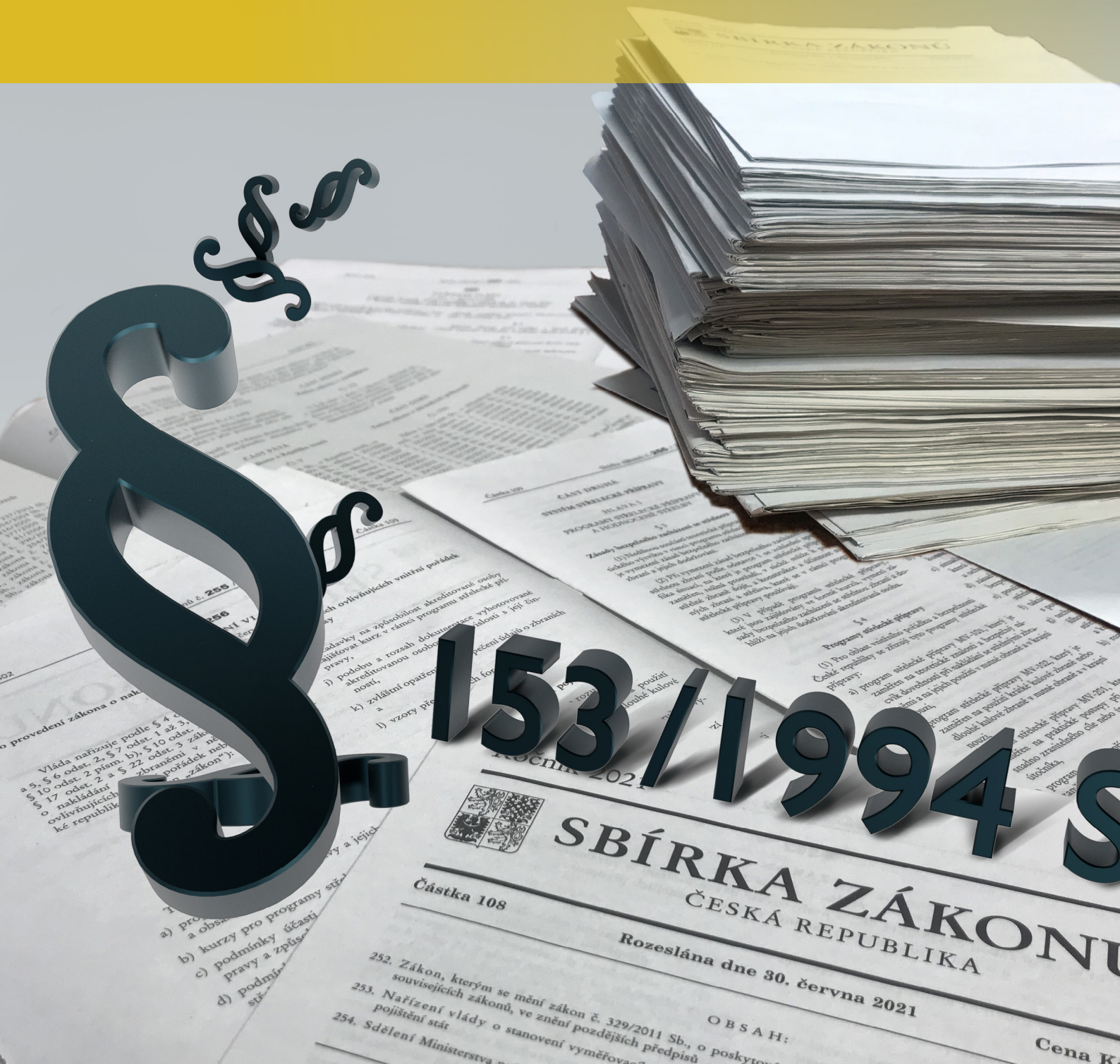
Veřejnou výroční zprávu za rok 2020 jsme se rozhodli pojmout trochu jiným stylem než v předchozích letech. Nejdeme cestou žádné revoluce, ale spíše evoluční snahou poskytnout všem zájemcům z řad laické i odborné veřejnosti trochu jiný vhled do činnosti nejvýznamnější české zpravodajské služby a také trochu zvýšit atraktivitu jejího provedení.

Jako každý rok i letos očekávám diskusi o tom, zda mají zpravodajské služby vůbec takovou veřejnou zprávu vydávat. Dokonce se v minulosti objevily ojedinělé hlasy, že tím vstupujeme na pole politiky. Chci jasně deklarovat, že veřejnou výroční zprávu považuji především za materiál, který dává každému občanovi možnost získat, byť v obecné rovině, představu, čím se služba zabývá a tím se podílet částečně na kontrole naší činnosti. Předchůdce BIS se jmenoval Úřad pro ochranu ústavy a demokracie a dodnes jsem přesvědčený, že tento název nejlépe vypovídal o našem poslání. Pokud tedy upozorňujeme na hrozby ohrožující demokratické, bezpečnostní a ekonomické základy této země, pak tak činíme v souladu s platnými zákony, které naši činnost definují, a rozhodně ani do budoucna nehodláme polevit v ochraně České republiky a jejích občanů.

Přeji všem pevné zdraví a zajímavé čtení

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.

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

Zpravodajská činnost

a zpravodajské poznatky

Rok 2020 byl nejen ze zpravodajského pohledu rokem mimořádným. Pandemii covid-19 lze zjednodušeně označit za dokonalou černou labuť zpravodajských operací.[1] Restriktivní opatření sice na jedné straně ztížila příjezdy a cestování agentů a důstojníků zpravodajských služeb cizí moci na našem území, ale současně výrazně zasáhla do zpravodajských operací BIS. Přes rozsáhlá protiepidemická omezení se nicméně po celý rok dařilo BIS plnit zákonnou působnost a průběžně informovala adresáty o ohroženích bezpečnostních zájmů státu. BIS v loňském roce předala prezidentovi a členům vlády téměř 300 dokumentů, o několik desítek více než v roce předchozím. Dalších zhruba 350 informací zaslala BIS Policii ČR, Úřadu pro zahraniční styky a informace (ÚZSI), Vojenskému zpravodajství (VZ) a dalším státním orgánům.

Za hlavní zpravodajská témata loňského roku BIS považuje snahy ovlivnit přípravu výstavby nového jaderného zdroje v Dukovanech, kybernetické útoky aktérů s vazbou na cizí moc a dezinformační působení mající potenciál oslabit demokratické základy právního státu. Důležité informace BIS zabezpečila i o aktérech proliferačních sítí s vazbou na ČR, jedincích s radikalizačním potenciálem a aktivitách zpravodajských služeb cizí moci na našem území.

Loňský rok byl také ve znamení intenzivního zapojení BIS do nově se formujících struktur bezpečnostního systému státu, jejichž hlavním cílem je sdílení informací a zkušeností v oblasti hybridních hrozeb. Pro BIS nepředstavují hybridní útoky nový či neznámý fenomén, ale jiné pojmenování pro koordinovanou kombinaci aktivit v rámci bezpečnostních hrozeb, kterým se BIS dlouhodobě věnuje. Reakce na koordinovaný přístup útočníka si žádá odpovídající spolupráci mezi jednotlivými prvky bezpečnostního systému státu, včetně zpravodajských služeb.

BIS se i v roce 2020 věnovala doplňování informací o subverzním útoku na areál ve Vrběticích, za kterým podle šetření bezpečnostních složek ČR stojí příslušníci zpravodajské služby Ruska. Veškeré zpravodajské poznatky, které BIS v uplynulém období získala, je proto nutné zasadit do kontextu zjištění, že se ČR stala cílem útoku cizího státu. Tento subverzní čin kromě velkých ekonomických škod způsobil také smrt dvou českých občanů a vedl k výraznému narušení životů tisíců obyvatel obcí v bezprostředním okolí areálu.

Pro následující období BIS předpokládá, že mezi hrozby s narůstajícím rizikem pro bezpečnostní zájmy státu budou patřit zejména aktivity ohrožující demokratické základy právního státu. Dalším z témat, jejichž význam dále poroste, bude také bezpečnost kyberprostoru a stále asertivnější chování Číny, které se projevuje i na území ČR. Velkou výzvu bude i nadále představovat nebezpečí teroristického útoku osamělého aktéra, zejména pak s přihlédnutím k zvyšující se úloze internetu při radikalizaci potenciálních útočníků a změněné bezpečnostní situaci po odchodu spojeneckých sil z Afghánistánu, která se vedle terorismu dotýká i migrace.

1 Termín černá labuť označuje vzácnou, neočekávanou událost. Sousloví v roce 2011 zpopularizoval N. N. Taleb.

Dopady pandemie covid-19 na bezpečnost

Pandemie covid-19 zasáhla aktivity zpravodajských služeb stejně jako všechny ostatní oblasti lidské činnosti. Nicméně každá krize nepřináší pouze ztráty a nepohodlí, ale také nové příležitosti či odhalení. Pandemická omezení např. ukázala, že tradiční diplomatické krytí cizích zpravodajských důstojníků má právě v krizových obdobích klíčový význam, protože legální rezidentura se stává během nich nenahraditelnou.

Pandemická krize také způsobila vzedmutí vlny negativních reakcí vůči protiepidemickým opatřením, která vedla až ke zformování tzv. anti-covid hnutí, jež se vymezuje nejen proti vládním opatřením bránícím šíření nemoci, ale zpochybňuje i závažnost onemocnění covid-19 jako takového. V tomto hnutí došlo k propojení nespokojených občanů a představitelů české dezinformační scény, kteří se na organizaci některých akcí taktéž podíleli. BIS se v rámci své

působnosti zabývala zneužitím negativních nálad vyvolaných protiepidemickými opatřeními k podněcování násilí, organizování šíření záměrně nepravdivých informací, jakož i k uplatnění nebo šíření potencionálního vlivu cizí moci.

Realita protiepidemických opatření posunula související dezinformace a konspirace blíže i k té části veřejnosti, která se za normálních okolností vyhýbá tématům tradičně náchylným k manipulaci. Přestože však dezinformace a konspirace v loňském roce zasáhly širší vrstvu obyvatelstva než obvykle, anti-covid hnutí se širokou veřejnost zmobilizovat nepodařilo. K minimalizaci jeho společenského vlivu přispěla mimo jiné vzájemná animozita představitelů hnutí vedoucí nejen k absenci jednotné organizace a vůdčího aktéra, ale i k dalšímu tříštění celé anti-covid scény.

Na rostoucí rizika spojená s šířením lživých a manipulativních tvrzení ve společnosti upozorňuje BIS ve svých zprávách několik posledních let. Takzvaná alternativní mediální scéna prezentuje vlastní či převzatý tendenčně zmanipulovaný či přímo lživý obsah jako „alternativní pohled" na aktuální dění. Ačkoliv šiřitelé dezinformací pragmaticky rozšiřují svůj rámec o jakákoliv nová témata vzbuzující emocionální reakce u veřejnosti, jejich dlouhodobé příběhy se ve vztahu k ČR víceméně ustálily. Jedná se o kontinuální kritiku politického uspořádání a politické reprezentace, členství v EU a NATO, kritiku fungování těchto organizací a diskreditaci obecných liberálně demokratických hodnot. Tematické zaměření dezinformační produkce je tak dlouhodobě zcela v souladu se zájmy Ruské federace.

Nejaktivnějšími šiřiteli dezinformací jsou často osoby silně motivované svým ideovým přesvědčením, které tradičně inklinují k sympatiím k autoritářským mocnostem či jejich představitelům a jsou zároveň nezřídka přesvědčené, že konají „osvětu" společnosti zaslepené mainstreamovým či oficiálním výkladem událostí. Část z nich se sice považuje za moderní disidenty utlačované majoritní společností, ale paradoxně jsou to zejména tito jedinci, kteří vědomě i nevědomě přispívají k prosazování zájmů cizí moci, a to na úkor strategických zájmů ČR. Někteří autoři či šiřitelé dezinformací jsou motivováni vlastním ekonomickým prospěchem, který jim jejich šíření přináší (např. jako odměnu z reklamy nebo sponzoring od spřízněné entity).

V roce 2020 se dále stupňoval tlak, který dezinformační ekosystém vyvíjel na seriózní média včetně médií veřejné služby. Seriózní žurnalistika na manipulaci obsahu a problematiku dezinformací kontinuálně upozorňuje, čímž tvoří logický cíl verbálních útoků a diskreditace ze strany tzv. alternativní mediální scény. Kontinuální dezinformační tlak také podporuje rezignaci části společnosti na funkčnost státu v jeho současné ústavní podobě, což stát limituje ve schopnosti účinně komunikovat strategická témata zasažené části společnosti a v konečném důsledku zvyšuje zranitelnost státu a společnosti vůči vlivovým operacím cizí moci.

Pandemie nemoci covid-19 míru ohrožení ČR terorismem výrazně neovlivnila, ačkoliv u některých osob přispěla k prohloubení rizikových faktorů, jako jsou finanční tíseň a psychické problémy. Zároveň však krátkodobě znesnadnila logistiku globálních teroristických organizací, pohyb jejich členů a možnosti spáchat v ČR teroristický útok. Umírněný charakter české muslimské komunity se potvrdil, až na malé výjimky, v zodpovědném přístupu oficiálních muslimských organizací k dodržování omezujících opatření nařízených státem.

Pandemie také výrazně zasáhla do chodu české muslimské obce. Primárním zdrojem sociálního kontaktu mezi muslimy byl během pandemie internet, především sociální sítě a další komunikační platformy. Ty jsou často užívaným kanálem k šíření islamistické radikalizace a konspiračních teorií, nicméně BIS nezískala informace o tom, že by reálné riziko radikalizace českých muslimů prostřednictvím sociálních sítí vzrostlo.

Přestože byl loňský rok provázen výrazným nárůstem využívání informačních a komunikačních technologií v každodenním životě, BIS nezaznamenala významné změny v použitých technikách, prostředcích či postupech kybernetických útočníků. Mezi nejčastěji použité techniky patřil bezpochyby spear-phishing, který spočívá v zasílání e-mailů se škodlivou přílohou či škodlivým odkazem za účelem počáteční nákazy zařízení adresáta. V uplynulém roce došlo jak ke zneužití kompromitovaných českých e-mailových schránek, tak ke snaze zacílit útoky na české občany či státní instituce.

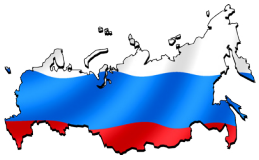
Druhým velmi častým způsobem provedení kybernetického útoku byla aktivní snaha útočníků vyhledávat zranitelnosti v sítích či systémech provozovaných a využívaných státními, ale i soukromými subjekty. Skenování zpravidla slouží jako prvotní fáze chystaného útoku, pomocí které útočník zjišťuje slabiny, které by mohl dále zneužít k průniku do vnitřní sítě.

Třetím typem byl tzv. útok hrubou silou (brute-force attack), který spočívá ve snaze o získání přihlašovacích údajů systematickým testováním jejich správnosti metodou pokus-omyl. Aktéři útoků většinou těží ze skutečnosti, že jejich cíle často nepoužívají vícefaktorové ověřování (MFA) při přihlašování do internetových služeb.

V případě úspěšné kompromitace pomocí jedné z těchto tří technik může dojít k exfiltraci dat či k pokusu o ni. Stejně jako v minulých letech BIS pozorovala zájem útočníků o e-mailové zprávy nebo konkrétní typy souborů (převážně textové či obrazové dokumenty), které slibují největší informační vytěžitelnost.

Zpravodajské
a subverzní aktivity proti zájmům ČR

Rusko



V roce 2020 mělo Rusko a jeho zpravodajské služby stále výhodu disproporčního diplomatického zastoupení. Ruská strana tak disponovala dvěma klíčovými výhodami: výhodnějším postavením v případě recipročních opatření vůči diplomatickému personálu a dostatečným počtem přítomného kvalifikovaného personálu v době omezení pohybu v rámci protiepidemických opatření.

Přesto anti-covidová opatření narušila akční plány ruské diplomacie i zpravodajských služeb – s omezeními pohybu přišly nutně i ztráty příležitostí ke zpravodajským kontaktům v tradičních oblastech zájmu, kterými jsou politika, akademická sféra či obchod. O to více se zvyšoval ruský zájem o kontakty na české proruské a protisystémové entity a snaha o maximální využití omezených příležitostí pro budování kontaktů v regionech v rámci vojensko-memoračních akcí. Ruská strana se na našem území snaží získat přístup k českým státním příslušníkům, ale také užívá ČR jako destinaci, ve které se pokouší o budování kontaktů s cizími státními příslušníky. Rusko rovněž pokračovalo v aktivitách směřujících k poškozování ČR s využitím kybernetických nástrojů.

V oblasti ruských vlivových aktivit zůstalo i v loňském roce prioritou prosazování ruských zájmů prezentovaných sice jako zájem český, nicméně skutečné české zájmy poškozujících. V globálním kontextu průběžně sílil paradox ruských vlivových operací, kdy narativ směrem k ruskému publiku hlásal, že Rusko je obklopeno nepřáteli, zatímco narativ určený k českému (resp. globálnímu) publiku zdůrazňoval, že Rusko je naše spása.

Subverzní charakter vykazovala na svém počátku tzv. ricinová kauza, kdy BIS obdržela informace o údajném dovozu a plánovaném užití jedovaté látky proti českým politikům. Po prověření zachycených signálů se však ukázalo, že se jednalo o snahu zapojit české bezpečnostní složky do interního soupeření dvou zaměstnanců ruské diplomatické mise. Přesto se BIS kloní k závěru, že tento incident byl alespoň v konečné fázi režírován ze strany zpravodajských služeb Ruské federace. Vyhodnocování toho, nakolik je hrozba reálná,

se výrazně zkomplikovalo po zveřejnění některých důležitých informací o prověřování signálu ze strany bezpečnostních složek.

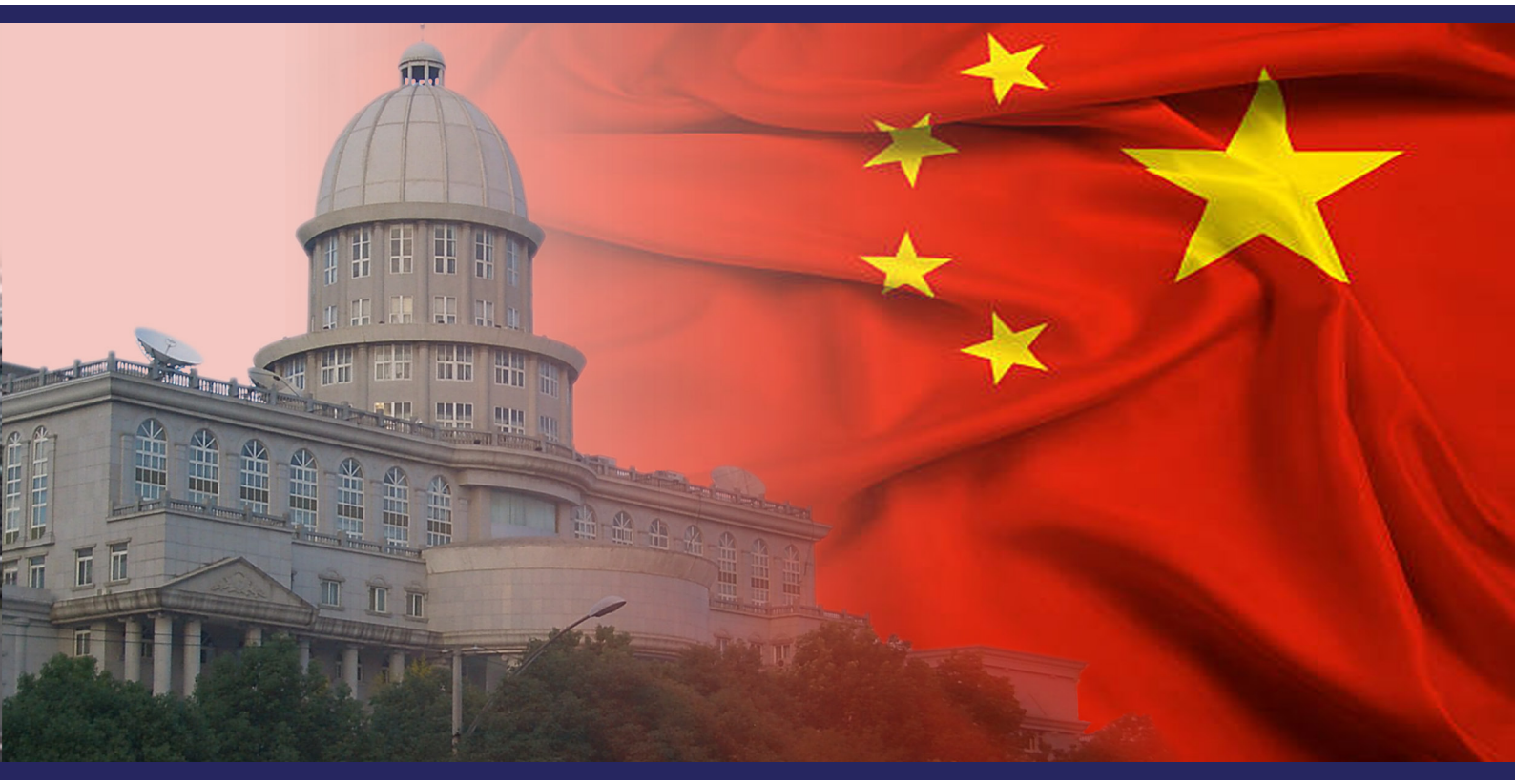
Pokračovaly rovněž snahy ruských společností spojených s tamním vojensko-průmyslovým komplexem získávat v ČR výrobky zařazené na seznamech mezinárodně kontrolovaných položek. Důvodem nárůstu poptávek byly zejména obměny a modernizace obráběcích strojů dodaných do Ruska v minulosti. U obchodu s vojenským materiálem se projevila účinnost sankčních opatření EU proti Rusku, která takové obchody neumožňují.

Čína

Stejně tak Čína představuje rostoucí komplexní zpravodajskou hrozbu. Podružnou se zároveň stává otázka, kdo je či není čínský zpravodajský důstojník – podle čínského zákona o národním zpravodajství je každý čínský občan potenciální vykonavatel vůle a zájmů čínských zpravodajských služeb. Dle platné legislativy musí každá organizace i občan podporovat, napomáhat a podílet se na národní zpravodajské činnosti. Spolupráce s čínskými silovými složkami je tak pro čínské subjekty i jednotlivce ze zákona povinná a odmítnutí součinnosti s sebou nese vážné důsledky.

Navzdory omezením pohybu vyvíjely čínské zpravodajské struktury aktivity na českém území i v loňském roce, a to zejména pod diplomatickým a novinářským krytím. Nejintenzivnější byla čínská zpravodajská činnost v oblastech politické a vědecko-technické rozvědky. Z pohledu možných ekonomických škod a ztráty know-how jsou nicméně nejrizikovější čínské zpravodajské zájmy a aktivity v rámci českých akademických institucí, vůči kterým čínské zpravodajské služby intenzivně budují nejen informační, ale také vlivové přístupy. Po linii politické rozvědky jsou příslušníci čínských zpravodajských služeb velmi úspěšní v kultivaci vztahů s osobami, které se pohybují na politické scéně (popř. ji ovlivňují), a to bez rozdílu v ideologické orientaci.

V segmentu vlivových operací se čínský zájem a aktivita soustřeďovaly na přenesení viny za pandemii nemoci covid-19 na západní země a na narušení česko-tchajwanských



politických a ekonomických vztahů. Součástí vlivového působení bylo i to, že čínští zpravodajci, diplomaté a členové stranických organizací hledali v ČR způsoby, jak ovlivňovat veřejné mínění, šířit čínskou propagandu a budovat pozitivní obraz Číny prostřednictvím otevřeného i skrytého ovlivňování mediálního obsahu v ČR. V kontextu pandemie covid-19 lze zmínit i čínskou snahu o nákup ochranných pomůcek v ČR.

Čína se v rámci svého programu „Made in China 2025" i nadále pokoušela obstarávat zahraniční pokročilé technologie a související know-how, a to i z ČR. Aktuálně Čína usiluje o získávání nově vyvíjených technologií, mezi které obecně patří robotické a autonomní systémy, aditivní výroba 3D tisku nebo nanotechnologie. Čínské subjekty také pokračovaly v akvizicích zájmových českých společností a ve snahách o přenesení výroby do Číny nebo využívání metod reverzního inženýrství.

Írán

V posledních letech lze, po desetiletích útlumu, pozorovat opětovný nárůst aktivit íránských speciálních služeb v Evropě, stejně jako jejich rostoucí agresivitu zejména vůči odpůrcům režimu v exilu. I v roce 2020 se tak BIS zaměřovala na možná bezpečnostní rizika spojená s činností íránského exilu v Evropě (možné útoky na opoziční novináře nebo politické aktivisty z řad kurdské, sunnitské a obecně progresivní názorové opozice duchovního režimu). Těmito aktivitami Íránu může být v ČR dotčeno působení perské redakce Rádia Fardá v rámci Rádia Svobodná Evropa/Rádia Svoboda, které Írán vnímá jako opoziční entitu. BIS nicméně v této souvislosti v roce 2020 nezaznamenala indicie o bezprostředním nebezpečí.

Írán také projevoval snahu získávat proliferačně využitelné poznatky na českých vědeckých pracovištích a univerzitách zejména s technickým zaměřením či na konferencích se zahraniční účastí. Snaha získávat proliferačně využitelné poznatky je součástí tzv. nehmotného přenosu technologií a poskytování tzv. technické pomoci, která zahrnuje i předávání poznatků a znalostí jak ve vědě a výzkumu, tak v podnikatelské sféře. Proliferační rizika související s problematikou tzv. nehmotného přenosu technologií je možné zmírňovat i kontinuálním zvyšováním povědomí o jejich existenci.

Kybernetické útoky

Přestože i v loňském roce se většina útoků identifikovaných a šetřených BIS týkala státních institucí, BIS zaznamenala i kybernetické útoky cílené na české politické strany nebo nevládní či neziskové organizace. U šetřených útoků se jednalo především o snahy o kompromitaci počítačové sítě či e-mailových schránek a následnou exfiltraci dat. Ta byla potvrzena u jedné státní instituce, ze které bylo exfiltrováno značné množství dokumentů a jiných souborů do infrastruktury útočníků.

Kompromitací vládních institucí získají aktéři nejen informace o záměrech a postojích ČR v určitých tématech, ale rovněž informace o konkrétních zaměstnancích nebo vrcholných představitelích státu včetně jejich názorů na určitá témata (např. komentáře a revize u exfiltrovaných dokumentů) či mezilidských vztazích pracovníků (např. z uniklé korespondence). Odcizené informace pak činí dotčené osoby zranitelnějšími vůči metodám klasické špionáže.

Soukromé (ale samozřejmě i pracovní) e-mailové schránky státních zaměstnanců navíc zpravidla obsahují nespočet osobních údajů, včetně kopií dokladů, nebo další přihlašovací údaje do nejrůznějších služeb (jiných e-mailových schránek, sociálních sítí, e-shopů atd.). Takové údaje mohou být pro útočníky, resp. státní/státem podporované aktéry v některých případech mnohem cennější než interní dokumenty institucí, v nichž zaměstnanci pracují. Výše uvedené údaje jsou totiž dále využitelné pro cílený kybernetický útok na vybraného zaměstnance či vrcholného představitele státu nebo jej opět činí zranitelnějším vůči metodám klasické špionáže.

V případě kompromitace sítě státní instituce nebo e-mailové schránky vysokého státního představitele či zaměstnance může dojít k tzv. hack and leak scénáři, tj. postupnému selektovanému uvolňování exfiltrovaných informací a jejich využití v předpřipravené dezinformační kampani, která může být zacílena na diskreditaci kompromitované instituce, konkrétního státního představitele/zaměstnance či ČR jako takovou. Dalším stupněm v takové hack and leak dezinformační kampani je zahrnutí zcela vyfabulované informace (falešný dokument, text e-mailu, fotografie) mezi skutečné uveřejňované dokumenty získané v rámci útoku. Oběť dezinformační (diskreditační) kampaně prakticky nemá reálnou možnost, jak se bránit a dopad na důvěryhodnost instituce či jednotlivce, vůči kterým je tato kampaň vedena, může být u veřejnosti enormní a v konečném důsledku již nevratný.

Na atribuci kybernetických útoků konkrétním aktérům je nezbytné pohlížet jako na dlouhodobý proces, který, ačkoliv může trvat měsíce, nemusí v některých případech dospět k požadovanému konci. Atribuce kybernetických útoků je z převážné většiny založena na technické analýze útoku a dále na tzv. všezdrojové analýze.

V rámci technické analýzy útoku jsou z hlediska atribuce posuzovány zejména nástroje používané útočníky, jejich typické postupy a identifikovaná infrastruktura. Všeobecně lze konstatovat, že lze v poslední době pozorovat určitý posun útočníků od užívání jejich vlastních nástrojů (např. malware) směrem k nástrojům, které jsou volně dostupné a používané (např. Mimikatz, PowerShell, Cobalt Strike). Stejně tak již velmi zřídka dochází k využívání tzv. vlastní infrastruktury, tj. typicky serverů zřízených a provozovaných samotnými aktéry, a je stále zřetelnější trend posunu aktérů směrem k pronajímané infrastruktuře (pronajaté VPS u velkých poskytovatelů na velmi krátkou dobu, užívání komerčních VPN v anonymizačním řetězci a dále služby Dropbox, Google Drive apod.). Tyto skutečnosti značně ztěžují a ovlivňují jednoznačnost atribuce prováděných útoků.

U tzv. všezdrojové analýzy jsou klíčovými částmi především analýza otevřených a odborných zdrojů (např. reportů výzkumných společností) a dále korelace útoků vycházejících z informací získaných v rámci zahraniční spolupráce, přičemž právě zahraniční spolupráci lze v případě šetření kybernetických útoků označit za naprosto stěžejní.

Atribuci kybernetických útoků také paradoxně komplikují velice kvalitní výzkumné reporty bezpečnostních společností detailně popisující proběhlé útoky státních/státem podporovaných aktérů. Tyto reporty v mnohých případech obsahují značně podrobný popis technik a nástrojů používaných identifikovanými aktéry a pro jiné pokročilé státní/státem podporované aktéry pak není problém tyto techniky a nástroje použít či napodobit a provádět útoky „pod cizí vlajkou“ (tzv. false flag).

Ekonomické zájmy státu

I v roce 2020 pokračovala příprava tendru na výstavbu nového jaderného zdroje v Dukovanech. Vzhledem k tomu, že se jedná o významný ekonomický projekt, ve kterém se český stát zaváže ke strategickému partnerství v oblasti energetiky na další desítky let, bylo v oblasti významných ekonomických zájmů stěžejní vyhodnotit jednotlivá rizika, která tento projekt potenciálně ohrožovala. Největší hrozbu pro projekt představovala potenciální účast subjektů, u kterých existovalo odůvodněné riziko, že budou zneužívat své postavení k prosazování vlastních zájmů nebo zájmů třetí strany (typicky geopolitické zájmy cizí státní administrativy) na úkor zájmů českých.

Ve fázi před vyhlášením tendru spočívalo hlavní riziko v možném ovlivňování přípravy projektu a rozhodování o podstatných otázkách a parametrech tendru. BIS v této souvislosti zaznamenala např. snahu získávat interní informace z prostředí české státní správy a subjektů zapojených do přípravy projektu. Zároveň pokračovaly aktivity, které měly za cíl ovlivnit mediální prostor a rovněž osoby s klíčovým vlivem na rozhodování. Nejednalo se o cestu běžného lobbingu, ale naopak byla evidentní snaha zakrýt původ informací objevujících se v médiích, k čemuž byly využívány zdánlivě nezávislé osoby.

Obdobné riziko ovlivňování nezávislého výkonu svěřených pravomocí či podsouvání zdánlivě nezávislých materiálů dlouhodobě existuje také v činnosti regulatorních a dohledových orgánů státu, zejména v oblasti energetiky, telekomunikací či zdravotnictví. Aktivity některých regulovaných subjektů v roce 2020 uvedená rizika potvrzovaly,

přičemž docházelo k pokračování obdobných jevů, které byly zaznamenány již v minulosti. Regulované subjekty se pokoušely skrytě podsouvat pozměňovací návrhy v rámci legislativního procesu u některých důležitých právních norem s potenciálně významnými ekonomickými dopady pro český stát. Při tom se snažily zakrýt sebe jako skutečného původce návrhu a vytvořit tak zdání objektivity.

Vedle tohoto dlouhodobého postupu se objevil i nový fenomén, kdy byly regulované subjekty zapojeny do tvorby regulatorního prostředí již v okamžiku příprav, čímž získaly významný vliv poskytující jim prostor ovlivnit podobu návrhu. Zapojení regulovaných subjektů do přípravy legislativy samo o sobě není nežádoucí, naopak může být v určitém okamžiku přínosné. Nicméně dochází-li k přesouvání odpovědnosti státní správy za zpracování klíčových dokumentů na regulované subjekty již na počátku, např. z důvodu nedostatečné kapacity kompetentních úřadů, získávají tím regulované subjekty značnou volnost k přizpůsobení si legislativy ve prospěch svých zájmů.

V oblasti regulace rovněž BIS opakovaně zaznamenala snahy regulovaných subjektů získat nestandardní kontakty a vazby na představitele regulačních orgánů a státní správy. Nadstandardní přístup vůči vybraným regulovaným subjektům vedl k poskytování řady dílčích vzájemných služeb a protislužeb, v jejichž rámci subjekty vstřícné ustoupit v některých regulatorních záležitostech získávaly výhody v jiných projednávaných věcech.

V oblasti telekomunikací byla významnou událostí aukce kmitočtů pro mobilní sítě 5G. Vzhledem k tomu, že v minulosti elektronické aukce realizované v rámci veřejné správy provázely netransparentní jevy negativně ovlivňující jejich výsledky, existovalo riziko, že se snahy o manipulaci objeví i v případě aukce kmitočtů 5G. S ohledem na dosavadní zkušenosti toto riziko spočívalo zejména v případné existenci skrytých dohod mezi účastníky aukce. Zjištění BIS potvrdila, že v minulosti existovala vzájemná provázanost některých účastníků v roce 2020 probíhající aukce kmitočtů 5G spočívající zejména v historické personální vazbě či předchozí spolupráci. Nicméně konkrétní dohody v souvislosti s aukcí kmitočtů nebyly v průběhu roku 2020 zaznamenány.

Hrozba skrytých dohod mezi účastníky veřejných soutěží dlouhodobě existuje i v případě zadávání veřejných zakázek, přičemž uvedené riziko se naplňovalo i v roce 2020. Kartelové dohody mezi zájemci o zakázky byly uzavírány zejména u infrastrukturních staveb v oblasti dopravy. Jako jev s potenciálně značnými dopady na výslednou cenu soutěžených zakázek se nově ukázal střet zájmů u některých subjektů poskytujících poradenské a servisní služby veřejným zadavatelům. Zadávání veřejných zakázek citelně ovlivnila pandemická situace a vyhlášený nouzový stav. Vyvstala nutnost pořídit některé zboží v relativně krátkém čase (zejména ve zdravotnictví), což mělo vliv na prověřování potenciálních dodavatelů, kdy zakázky získávaly i subjekty bez historie či s nejasným původem kapitálu.

Prodej významného českého výrobce strojírenských zařízení ruským investorům byl typickým příkladem, kdy stát neměl k dispozici účinný nástroj, jak zamezit rizikovým investicím na svém území či jejich rizikovost omezit. Přes trvající sankce EU proti Rusku management české společnosti vzápětí po prodeji veřejně oznámil akceptaci ruských zakázek, přičemž nový vlastník pohrozil, že v případě jejich odmítnutí přenese výrobu do Ruska. Vzhledem k tomu, že u řady zařízení z produkce této společnosti jde o mezinárodně kontrolované položky, hrozí při přenesení výroby do Ruska ztráta kontroly ČR nad dalším nakládáním s proliferačně využitelným zbožím. V průběhu roku 2020 došlo k finalizaci české legislativní úpravy zavádějící mechanismus prověřování navazující na předpisy EU, což do budoucna umožní českému státu lépe chránit svou bezpečnost a veřejný pořádek.

Činnosti a násilné aktivity ohrožující demokratické základy státu

Pandemie covid-19 pouze akcelerovala dlouholetý vývoj extremistické scény, který potvrdil, že scéna prošla výraznou transformací. Byť je činnost některých extremistů mediálně atraktivní a jejich případné excesy přitahují pozornost, reálný mobilizační potenciál i kompetence členů organizovaných extrémistických skupin zůstávají malé a tyto subjekty víceméně stagnují. Ve vztahu k ochraně demokratických základů státu nejsou organizované extremistické skupiny již několik let v ČR závažným bezpečnostním rizikem.

Z činnosti paramilitárních a domobraneckých uskupení rovněž nevyplývalo relevantní ohrožení. Domobranci sami sebe sice prezentovali jako profesionální polovojenskou skupinu, ale ve skutečnosti šlo jen o mediální fikci a jejich reálný dosah byl velmi malý. Hlavní náplní činnosti domobranců byla různá setkání spojená s polovojenskými cvičeními a paramilitárně zaměřenými přednáškami. V průběhu roku se domobranci také angažovali na poli šíření dezinformací a konspirací spojených s nemocí covid-19 a opatřeními proti ní. Primárně k tomu využívali své internetové stránky a účty na sociálních sítích.

Významnějším problémem se naopak stávají ad hoc tematicky zaměřené skupiny či radikalizovaní jedinci, u nichž není důležitá propracovanější soustava postojů a hodnot, ale pouze negativní, často iracionální postoj vůči určitému fenoménu.

Obecně pak platí, že riziko představuje zejména možná seberadikalizace některých jedinců, kteří díky své neprovázanosti s extremistickou scénou snáze unikají pozornosti bezpečnostních složek. Prozatím se činnost takovýchto osob v ČR soustředila na méně závažné kriminální činy, ale zkušenosti ze zahraničí naznačují, že se mohou stát pachateli činů násilných či dokonce páchat teroristické útoky.

Navzdory vyššímu počtu úspěšných útoků v Evropě zůstala míra ohrožení nábožensky motivovaným terorismem v ČR na nízké úrovni. BIS sice zaznamenala známky příklonu k radikálnímu výkladu islámu u několika jednotlivců původem zejména ze severní Afriky, kteří měli různě silnou vazbu na ČR (pobytový status, dočasný tranzit v rámci svého pohybu po Evropě), ale bezprostřední ohrožení bezpečnosti dle poznatků BIS nehrozilo. Stejně tak BIS nezaznamenala pobyt žádného z navrátilců z oblasti bojů, kde působí džihádistická uskupení, na území ČR. BIS i v roce 2020 monitorovala průjezdy a příjezdy rizikových osob s přímou vazbou na teroristická uskupení – ani v jednom případě však nebyl účel jejich cesty příprava teroristického útoku v ČR.

V roce 2020 došlo v Evropě k více než deseti úspěšným teroristickým útokům islamistů, což je násobně více než v předešlém roce. Jednalo se o první meziroční nárůst počtu útoků od roku 2016. V drtivé většině šlo o málo sofistikované útoky s nízkým počtem obětí, jejichž pachatelé byli inspirováni džihádistickou propagandou na internetu. Islamistické útoky se nově odehrály i v zemích bez předchozí historie islamistických teroristických útoků (v Rakousku a Švýcarsku). Loňský rok tak ukázal, že teroristická hrozba je nadále aktuální a netýká se pouze zemí s dlouholetými zkušenostmi s útoky.

Konkrétními faktory ovlivňujícími počet útoků v roce 2020 byly především narůstající počet propuštěných radikálů z vězení a znovuoživení tématu karikatur proroka Muhammada. Útoky inspirované karikaturami i reakce muslimského světa ukázaly, že napadení symbolů islámu má mnohdy širší radikalizační potenciál než myšlenka globálního džihádu. K nim se přidávalo působení dlouhodobých faktorů, zejména pak džihádistické propagandy na internetu, a také psychické problémy. Ty u některých pachatelů útoků v Evropě snížily odolnost vůči manipulativním technikám propagandy teroristických organizací jako al Qá´ida a tzv. Islámský stát.

Islamistické sítě, trvalé zdroje džihádistického terorismu, stále přetrvávají a jsou přiživovány internetovou džihádistickou propagandou. Po uplynutí období zdánlivého klidu dochází k jejich aktivaci souhrou mnoha událostí a okolností. Mezi nejdůležitější z nich patří vznik nebo obnovení zahraničních ohnisek konfliktů se zapojením muslimů nebo nárůst napětí mezi muslimskými menšinami a většinovou společností, důsledky klimatických nebo ekonomických změn či jiné zdroje nestability. Hlavní podmínkou pro eskalaci současného islamistického terorismu je akumulace nespokojenosti či frustrace v rozrůstajících se řadách psychicky zranitelnějších jedinců, kteří jsou snadným cílem ideologické manipulace.

Události jako např. karikatury proroka Muhammada, diskuse okolo zavedení tzv. šátkových zákonů či projevy islamofobie působí jako spouštěče dalších vln teroristických útoků. Džihádističtí propagandisté, často radikální kazatelé nenávisti vůči osobám považovaným muslimy za nevěřící, dokáží výše zmiňovaných momentů efektivně využívat pro získávání dalších stoupenců. Přestože je mezinárodní boj s islamistickým terorismem efektivní a zaznamenal mnoho úspěchů, nelze zabránit každému útoku ve jménu islámu, protože islamisticko–džihádistická ideologie vychází z nejednoznačných myšlenkových zdrojů s velkým mobilizačním potenciálem. Státy se tak i nadále budou potýkat s útoky tzv. osamělých aktérů radikalizovaných prostřednictvím internetu.


لا إله إلا الله
الله
رسول
محمد

Ochrana utajovaných informací, bezpečnost a krizové řízení

V oblasti ochrany utajovaných informací nedošlo ke změnám. Stejně jako v předchozích letech byla vyhotovována odborná vyjádření v rámci BIS, dokumenty byly posuzovány z hlediska stanovení stupně utajení podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, byl podáván výklad seznamu utajovaných informací v působnosti BIS a příslušných vnitřních předpisů a poskytována metodická pomoc organizačním útvarům.

Zajišťování bezpečnosti informací se řídí bezpečnostní politikou informačních systémů BIS, která klade důraz 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 Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). V roce 2020 byla provedena úspěšná recertifikace informačních systémů zpracovávajících utajované informace stupně utajení Důvěrné a Tajné.

Všichni uživatelé certifikovaných informačních systémů byli v souladu se zákonem č. 412/2005 Sb. proškoleni před jejich prvním přístupem do systému a následně prochází jednou ročně pravidelným proškolením, včetně zvyšování povědomí v oblasti kybernetické bezpečnosti. V průběhu roku 2020 nebyl ve Službě zaznamenán žádný závažný bezpečnostní incident.

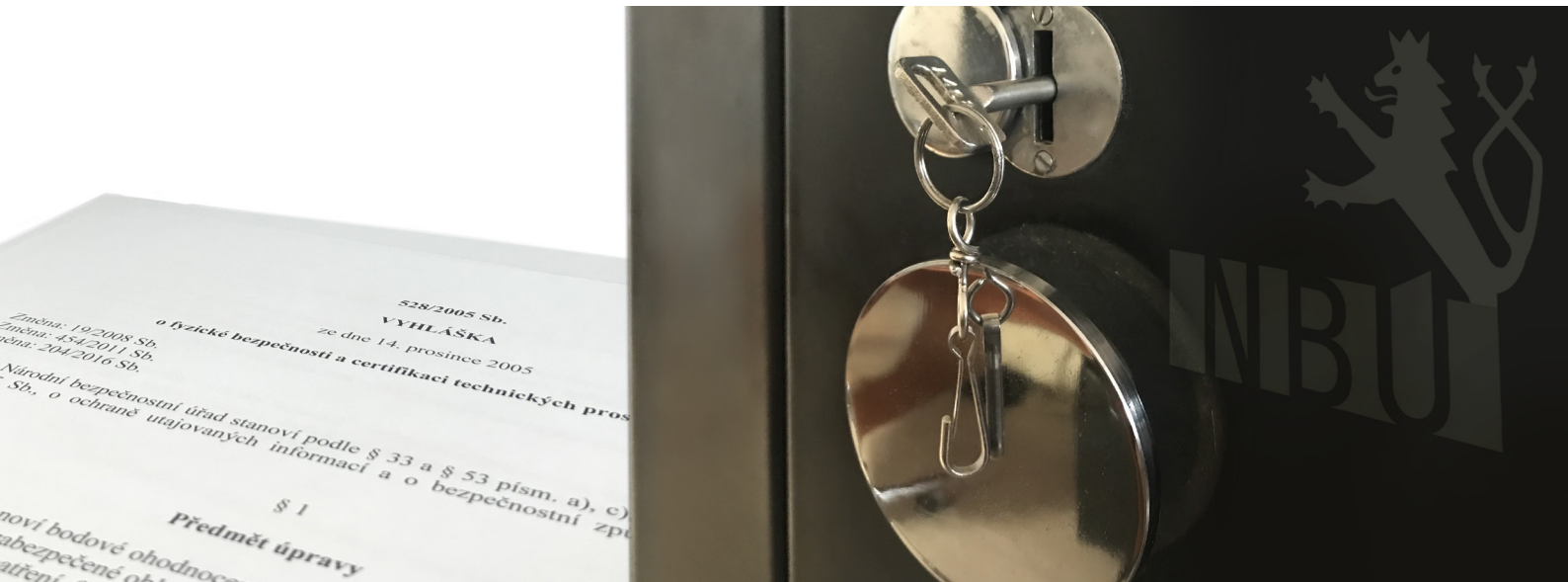
V oblasti kryptografické ochrany utajovaných informací probíhala příprava nového systému utajeného spojení s partnerskými zpravodajskými službami. Na základě požadavků NÚKIB proběhla reorganizace pracovišť kryptografické ochrany systému a vzniká pracoviště pro generování klíčového materiálu pro tento komunikační systém. V průběhu roku proběhly aktualizace režimových opatření v důsledku certifikací nových i stávajících kryptografických prostředků.

V roce 2020 nebyl v BIS zaznamenán žádný závažný incident nebo kompromitace kryptografických prostředků. Pravidelné inventury kryptografického materiálu nezjistily žádné nedostatky ve správě a manipulaci s kryptografickým materiálem.

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 v souladu s prováděcí vyhláškou NBÚ č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.

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.

V období pandemie covid-19 byl aktivován a pravidelně se scházel krizový štáb ředitele BIS.



Spolupráce

se zpravodajskými službami ČR a ostatními státními orgány

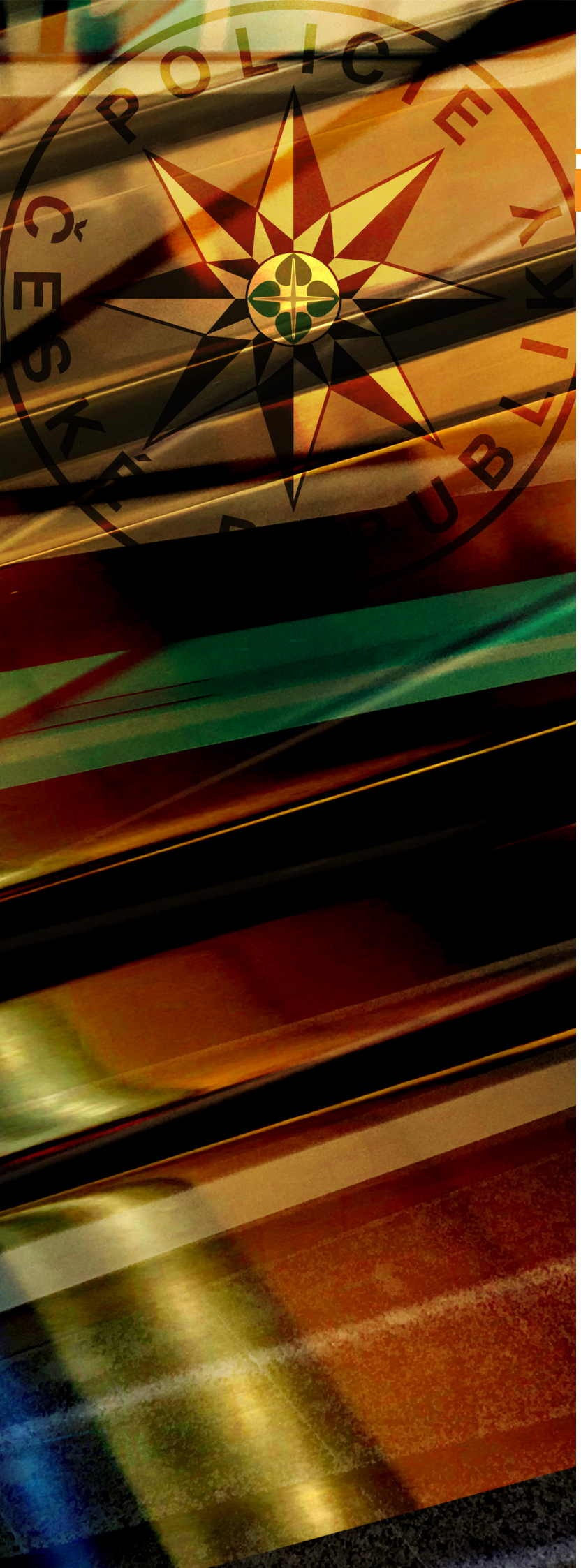
Spolupráce se zpravodajskými složkami ČR

BIS v roce 2020 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. BIS se v roce 2020 vyjádřila k více než stovce diplomatických zástupců a pracovníků diplomatických misí cizích států.

I v roce 2020 probíhala spolupráce s Ministerstvem obrany, resp. Vojenským zpravodajstvím, 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

BIS se jako garant jednotného stanoviska zpravodajských služeb ČR podílí na hodnocení bezpečnostních rizik spojených s udělováním víz. V roce 2020 se BIS na žádost Ředitelství služby cizinecké policie (ŘSCP) vyjádřila k více než 400 tisícům žádostí o krátkodobá schengenská víza, která byla podána na zastupitelských úřadech ČR, nebo v rámci konzultačního mechanismu na zastupitelských úřadech ostatních států schengenského prostoru. Rok 2020 byl ovlivněn celosvětovou pandemií covid-19, která se projevila výrazným snížením počtu žádostí. Ve srovnání s rokem 2019 nedosahoval jejich počet v loňském roce ani jedné čtvrtiny.

Pokračovala spolupráce BIS s ŘSCP, která vyplývá ze zákona č. 49/1997 Sb., o civilním letectví, ve znění pozdějších předpisů, dle kterého byla pro fyzické osoby vstupující do vyhrazeného bezpečnostního prostoru letiště zavedena povinnost prokázat svoji spolehlivost. V roce 2020 BIS prověřila více než 10 tisíc žadatelů o ověření spolehlivosti, což bylo o několik tisíc více než v předchozím roce. Nárůst počtu prověřovaných osob souvisel s nutností opětovného posouzení spolehlivosti žadatele, vyplývající z platnosti dokladu, která je nyní zákonem stanovena na pět let.

Spolupráce s Národní centrálou proti organizovanému zločinu (NCOZ) spočívala ve výměně poznatků zejména po linii problematik významných ekonomických zájmů, terorismu, kontrašpionáže a kybernetické bezpečnosti. Jedním z okruhů spolupráce bylo prověřování zájmových subjektů, konkrétně příslušníků zahraničních bezpečnostních složek usilujících o specializovaný výcvik v České republice. Dále byly sdíleny poznatky v oblasti ekonomické kriminality či rizik vůči strategickým objektům.

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 2020 provedla BIS na základě žádosti NBÚ více než 18 tisíc evidenčních šetření. Po realizaci činnostního šetření se BIS vyjádřila k 107 fyzickým a k 7 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.

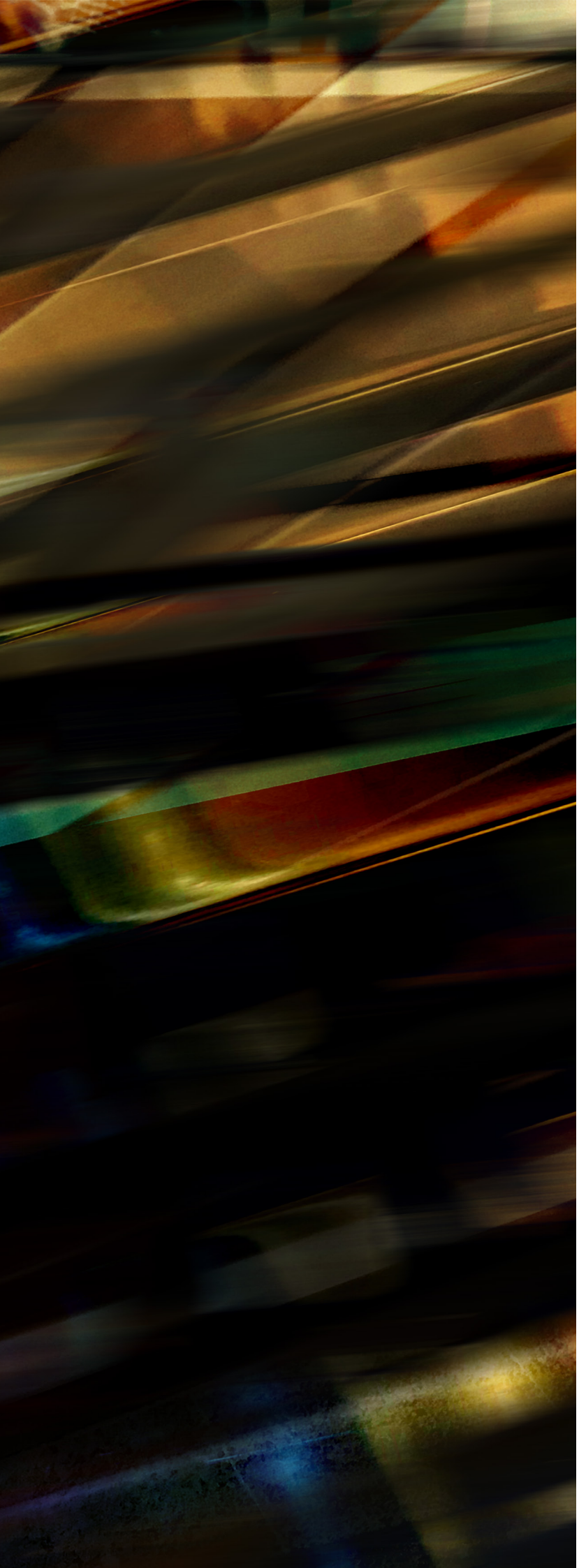
I v roce 2020 pokračovala spolupráce s Ministerstvem vnitra při posuzování cizinců – žadatelů o pobytová oprávnění a žadatelů o udělení státního občanství ČR. Další formou spolupráce byla součinnost při prověřování právnických nebo fyzických osob žádajících o povolení ke zprostředkování zaměstnání.

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 hospodářství, životního prostředí a též v oblasti závodního stravování. Ve spolupráci s MV byla dále připravována stanoviska BIS pro jednání Výboru pro civilní nouzové plánování. V rámci Generálního ředitelství Hasičského záchranného sboru pak v době pandemie covid-19 probíhala spolupráce v oblasti ochranných pomůcek, protiepidemických opatření apod.

BIS spolupracovala s Odborem bezpečnostní politiky Ministerstva vnitra na prověření fyzických a právnických osob žádajících o udělení povolení ke zprostředkování zaměstnání podle zákona č. 435/2004 Sb., o zaměstnanosti. BIS prověřila téměř 700 právnických a více než 1 300 fyzických osob.

Spolupráce BIS a Odboru azylové a migrační politiky Ministerstva vnitra (OAMP) je zaměřena na vyloučení bezpečnostního rizika u žadatelů o pobytová oprávnění, udělovaných podle zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, a u žadatelů o mezinárodní ochranu podle zákona 325/1999 Sb., o azylu.

V roce 2020 se BIS vyjádřila k více než 124 tisícům žadatelů o pobytová oprávnění. V porovnání s předchozím rokem bylo posouzeno přibližně o 15 tisíc osob méně, v rámci meziročního srovnání jde o první pokles od roku 2016. Tato skutečnost byla pravděpodobně způsobena celosvětovou pandemií covid-19 a s ní souvisejícími opatřeními.



V roce 2020 spolupracovala BIS s OAMP při prověřování osob v rámci zdravotně humanitárního projektu MEDEVAC. V tomto roce byl projekt zaměřen na pomoc občanům Běloruska. Bylo prověřeno 90 osob státní příslušnosti BLR a RUS, které byly přesunuty do ČR v souvislosti s konfliktem v Bělorusku.

V roce 2020 zaslala BIS na základě žádostí Odboru všeobecné správy Ministerstva vnitra vyjádření podle zákona č. 186/2013 Sb., o státním občanství České republiky, k více než 3 500 žadatelům o udělení státního občanství ČR.

Pokračovala také spolupráce BIS s odborem eGovernmentu MV při prověřování žadatelů o akreditaci pro správu kvalifikovaného systému elektronické identifikace podle zákona č. 250/2017 Sb., o elektronické identifikaci.

Dlouhodobá je také spolupráce BIS a bezpečnostního odboru Ministerstva zahraničních věcí. Její stěžejní formou je vyloučení bezpečnostního rizika u fyzických, ale i právnických osob, které s ministerstvem spolupracují anebo o spolupráci žádají. V roce 2020 BIS posoudila bezpečnostní riziko u více než 500 fyzických a 30 právnických osob.

BIS pravidelně sdílela zpravodajské poznatky v rámci Společné zpravodajské skupiny (SZS) a Národního kontaktního bodu pro terorismus (NKBT). V rámci platformy SZS BIS informačně přispívala k vyhodnocování bezpečnostní situace z hlediska možného ohrožení ČR. Hlavními tématy byly vliv karanténních opatření na hodnocení hrozeb teroristických útoků, dopady aktuálních teroristických útoků a situace v zahraničních misích Armády ČR v Mali a Afghánistánu. Hlavní náplní spolupráce v rámci NKBT 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, 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, Celní správou ČR, 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 Generálního ředitelství cel, 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 Ministerstvem vnitra, Ministerstvem obrany, Ministerstvem zahraničních věcí, Licenční správou Ministerstva průmyslu a obchodu, 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.

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 Úřadu pro ochranu hospodářské soutěže byly předávány informace spadající do jejich působnosti. Dále probíhaly odborné konzultace s gesčními úřady, a to především s Ministerstvem průmyslu a obchodu a Ministerstvem vnitra v oblasti přípravy výstavby nového jaderného zdroje a Ministerstvem průmyslu a obchodu v oblasti prověřování zahraničních investic.

Pokračovala aktivní spolupráce v rámci Mezirezortního orgánu pro potírání nelegálního zaměstnávání cizinců. Činnost orgánu je mj. zaměřena na kontrolní činnost ve vztahu k ekonomickým aktivitám a pobytu cizinců v ČR, na legislativní i nelegislativní materiály v oblasti pobytu cizinců a jejich zaměstnanosti, dále na působení agentur práce a v neposlední řadě na činnosti označované jako nedeklarovaná práce.

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

V roce 2020 BIS dále spolupracovala se státními orgány v rámci boje proti pandemii covid-19. Konkrétně se jednalo o zajišťování ochranných pomůcek a dezinfekcí v součinnosti s Ministerstvem průmyslu a obchodu 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. Aktuálně je BIS 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 2020 aktivně účastnila spolupráce v několika mezinárodních platformách a uskupeních (např. Counter-Terrorism Group a NATO Civilian Intelligence Committee).

Vzhledem k omezené možnosti cestování do zahraničí a pořádání mezinárodních jednání probíhala interakce s partnerskými službami především prostřednictvím elektronických komunikačních nástrojů, jejichž nasazení a rozvoj se dá očekávat i v roce 2021.

V rámci mezinárodní spolupráce BIS v roce 2020 přijala více než 10 000 zpráv a postoupila cca 1 800 dokumentů. Na strategické a expertní úrovni se zástupci BIS zúčastnili více než 500 mezinárodních jednání.

Celkový počet přijatých a odeslaných zpráv v roce 2020 v porovnání s předchozím rokem mírně poklesl, což je možné připsat zejména nutnosti prioritizace oblastí mezinárodní spolupráce, které služby musely čelit vzhledem k omezujícím protipandemickým opatřením.

Prioritními oblastmi spolupráce BIS se zahraničními zpravodajskými službami jsou boj proti terorismu, kontrašpionáž, proliferace, kybernetická bezpečnost a oblast ochrany utajovaných informací a 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 svých pro účely kontroly zpravodajských služeb zřízených zvláštních kontrolních orgánů. 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 5 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 11 kontrol, jejichž cílem bylo zejména 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, 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 a sledování využití vozidel. V rámci kontrolních akcí nebyla zjištěna závažná porušení předpisů.

Orgánem nemocenského pojištění BIS byly provedeny tři kontroly dodržování režimu dočasně práce neschopného pojištěnce s tím, že v žádném případě nebylo shledáno jakékoliv porušení ze strany pojištěnce.

Pracovníci archivní služby a kontrolní skupiny provedli celkem 20 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 2020 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.

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 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 250 podání nebylo ani jedno vyhodnoceno jako stížnost na jednání příslušníků BIS. 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 Policie České republiky, 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 2020 stanoven zákonem č. 355/2019 Sb., o státním rozpočtu České republiky na rok 2020. Příjmy byly kapitole určeny ve výši 190 000 tis. Kč a výdaje ve výši 2 147 315 tis. Kč. Vedle rozpočtových prostředků evidovala BIS také nároky z nespotřebovaných výdajů jako jediný mimorozpočtový zdroj. Celkové příjmy kapitoly dosáhly částky 254 573 tis. Kč. Celkové výdaje včetně použití nároků z nespotřebovaných výdajů byly k 31. 12. 2020 čerpány ve výši 2 208 004 tis. Kč.

Kapitálové výdaje směřovaly vedle výstavby technicko-administrativního objektu především k udržení provozuschopnosti materiálně technické základny a jejímu nejnutnějšímu rozvoji v rámci pořízení a technické obnovy dlouhodobého majetku BIS včetně běžné periodické obměny. Kromě těchto výdajů realizovala BIS v rámci kapitálových výdajů i nezbytné investice do informačních a komunikačních technologií a do vlastní zpravodajské techniky. 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 a v neposlední řadě i na pravidelnou obměnu dopravní techniky.

V objemu čerpání běžných výdajů představovaly nejvýznamnější položku osobní výdaje. Vedle výdajů na platy a příslušenství sem patří také výsluhové nároky, což jsou mandatorní výdaje vyplácené bývalým příslušníkům po skončení služebního poměru.

Významný podíl v ostatních běžných výdajích tradičně zaujímaly výdaje na speciální zpravodajskou techniku. Další výdaje provozního charakteru, jako jsou ostatní běžné materiálové výdaje, výdaje na nákup energií a služeb, zajišťujících běžný provoz kapitoly, a výdaje na dodavatelské zajištění oprav a údržby majetku a objektů BIS nevybočovaly z vývoje uplynulých let. Neplánované výdaje s sebou nesla hygienická a organizační opatření v souvislosti s epidemií covid-19 na zajištění bezpečného a zdraví neohrožujícího režimu na pracovištích. Lze konstatovat, že i díky včas přijímaným opatřením nebyla akceschopnost BIS v roce 2020 zásadně narušena.

Základní provozní i rozvojové potřeby BIS byly v roce 2020 pokryty. Čerpání výdajů však mělo oproti předchozím letům svá specifika. Pro rozvojové aktivity v oblasti zpravodajské techniky, informačních a komunikačních technologií a v oblasti financování výstavby technicko-administrativního objektu bylo stejně jako v předchozích letech nezbytné do financování zapojit nároky z nespotřebovaných výdajů z minulých let. Naopak v některých oblastech běžných výdajů, např. školení, konference a zahraniční služební cesty, nebylo možné vzhledem k platným epidemiologickým opatřením plánované prostředky čerpat a odloženy nebo zrušeny byly i některé menší investiční akce z důvodů jak na straně BIS, tak i na straně některých dodavatelů.

Bezpečnostní informační služba
Výroční zpráva 2020

Kontakty

Adresa pro písemný styk:
Bezpečnostní informační služba
P. O. BOX 1
150 07 Praha 57

Kontakt pro veřejnost:
Telefon: +420 235 521 400
Fax: +420 235 521 715
E-mail: info@bis.cz
Datová schránka: cx2aize

Kontakt pro média:
E-mail: press@bis.cz
Telefon: +420 257 142 007

Kontakt pro prevenci:
E-mail: prevence@bis.cz