



BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA

VÝROČNÍ
ZPRÁVA
ZA ROK 2024





Bezpečnostní informační služba

Výroční zpráva za rok 2024

Obsah

Slovo ředitele Bezpečnostní informační služby	5
Náplň a rozsah zpravodajské činnosti	7
Zpravodajské poznatky	9
▶ Hlavní sdělení	9
▶ Rusko jako trvající hrozba	13
▶ Zpravodajské aktivity	13
▶ Telegramoví agenti	15
▶ Další subverzní a vlivové aktivity	15
▶ Kybernetické útoky	16
▶ Obcházení sankcí	17
▶ Sociální sítě, alternativní média a šíření dezinformací	18
▶ Algoritmy sociálních sítí	18
▶ Dezinformace a jejich původ	20
▶ Nové technologie	22
▶ Trend online radikalizace mladistvých	24
▶ Energetická bezpečnost a ochrana veřejných financí	28
▶ Energetika	28
▶ Zdravotnictví	29
▶ ICT zakázky	29
▶ Kyberšpionáž	30
▶ Další důležitá témata zpravodajského zájmu	32
▶ Terorismus	32
▶ Dopady ruské agrese vůči Ukrajině na Česko	32
▶ Hrozby ze strany Číny	34
Spolupráce na národní úrovni	36
▶ Spolupráce se zpravodajskými službami ČR	36
▶ Spolupráce s Policií ČR	38
▶ Spolupráce s dalšími státními orgány a institucemi	38
Spolupráce na mezinárodní úrovni	42
Dodržování služebních předpisů	43
Rozpočet	44



Vážené čtenářky, vážení čtenáři,

dostává se Vám do rukou opět po roce veřejná výroční zpráva Bezpečnostní informační služby tentokrát za rok 2024. Ohlížíme se za událostmi čistě domácími, ale i za těmi, které mají sice původ v zahraničí, ale jejich vliv na Českou republiku byl zcela neoddiskutovatelný.

Minulý rok jsem na tomto místě vyjádřil naději, že neakceptovatelná a brutální agrese Ruské federace proti Ukrajině snad brzy skončí. To se bohužel nestalo. Pokračující konflikt na Ukrajině má přímé dopady i do života v České republice. Na našem území žije stále několik set tisíc ukrajinských uprchlíků a zároveň musíme být neustále připraveni, v případě špatného vývoje, i na případný příchod další uprchlické vlny.

Registrujeme také snahy některých tuzemských firem dostat do Ruské federace sankcionované zboží, čemuž se BIS s dalšími státními orgány snaží úspěšně bránit.

Stále také pokračují přímé i nepřímé aktivity ruských zpravodajských služeb přímo na našem území. BIS odhalila a pomohla zastavit několik pokusů o sabotážní akce podobné té, která se odehrála v autobusovém depu na pražském Klíčově.

Další oblastí, které jsme věnovali pozornost, je kyberprostor a narůstající snahy aktérů především z Ruska a Číny napadat významné státní instituce i testovat odolnost naší kritické infrastruktury. Ruku v ruce s tím kontrolujeme a cíleně oslabujeme špiónážní aktivity některých států, z nichž nejaktivnější jsou stále Rusko a Čína.

V roce 2024 se společnost i nadále potýkala s šířením dezinformací ve veřejném prostoru, a to jak přímo z produkce Ruska tak i domácích aktérů. Hlavní platformou zůstávají sociální sítě a tzv. alternativní média. Se sociálními sítěmi také úzce souvisí stále zřetelněji zaznamenávaný trend radikalizace mladistvých v online prostředí.

Stranou zájmu BIS nezůstala v roce 2024 ani oblast významných ekonomických zájmů státu, kde jsme opět popsali řadu případů klientelismu, neefektivního nakládání s veřejnými prostředky a s tím souvisejícího podezření na korupční jednání.

Rok 2024 patřil v bezpečnostní oblasti k těm nejnáročnějším v novodobé historii České republiky. Přesto si troufnu tvrdit, že jsme jako země a i jako občané obstáli na výbornou. Nadále trvá mimořádně důležitá podpora bránící se Ukrajině, většina společnosti stále odolává šířícím se dezinformacím, občané jednoznačně vyjadřují podporu našemu zakotvení v evropských i transatlantických strukturách. To vše mi dává naději, že i v současném rozkolísaném světě obstojíme a udržíme si charakter demokratické a svobodné země.

Přes tradiční obecnost Vám nabízíme vhled do práce tuzemské zpravodajské služby, necháváme nahlédnout do témat a oblastí, kterým BIS věnovala a věnuje svou pozornost. Snad Vás následující stránky ujistí, že Bezpečnostní informační služba významně přispívá k tomu, aby Česká republika zůstala jednou z nejbezpečnějších zemí světa.

Přeji nám všem bezpečné dny

genpor. Ing. Michal Koudelka



NÁPLŇ A ROZSAH ZPRAVODAJSKÉ ČINNOSTI

Činnost, postavení a působnost Bezpečnostní informační služby (BIS) 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 odst. 1 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.

ZPRAVODAJSKÉ POZNATKY

Hlavní sdělení

Rusko

Rusko se dlouhodobě snaží narušovat stabilitu a prosperitu evropských zemí. Je v jeho zájmu, aby občané Česka (a celé EU) nechovali důvěru v instituce, na kterých stojí demokratická společnost.

I přes prostředky a úsilí, které ruské zpravodajské služby vynakládají do snah o verbování tzv. telegramových agentů (za účelem páchání sabotáží v EU), vedla tato činnost v Česku jen k méně závažným bezpečnostním incidentům. Fenomén měl v Česku spíše mediální než reálný dopad.

Navzdory válečnému tažení Ruska proti Ukrajině, potažmo EU a NATO, se některé české firmy nadále snaží hledat cesty, jak do Ruska dodat sankcionované zboží. Dodávky se k ruským klientům snaží dopravit nejčastěji reexportem přes členské země Eurasijské hospodářské unie, případně přes Čínu.

Evropské sankce nemohou zabránit veškerým dodávkám sankcionovaného zboží do Ruska. Přesto ale mají svůj význam – minimálně tím, že Rusku navyšují náklady na získávání západního zboží, které na ruské území musí putovat skrytě a delšími cestami. Hlavními podporovateli ruské válečné produkce jsou Čína, Írán a KLDR.

Radikalizace

Způsob, jakým jsou nastavené algoritmy sociálních sítí, má řadu negativních dopadů na společnost (vznik závislosti a psychických problémů, radikalizace, šíření nepravdivých a zkreslených informací). Řešením je především vzdělávání uživatelů a šíření povědomí o tom, jak sociální sítě fungují a proč tomu tak je.

V Česku byl zaznamenán trend radikalizace mladistvých, zejména chlapců, v online prostředí. Jeho dominantní příčinou byly algoritmy sociálních sítí, které stále dokonaleji směřují a stupňují obsah (nejen) s radikální a násilnou tematikou uživatelům, kteří k němu inklinují. Většinou jde o osoby vyloučené z kolektivu, se špatným rodinným zázemím.





Dezinformace

Dosah aktérů a platforem, které v českém prostředí šíří dezinformace a konspirace, je omezený a v roce 2024 spíše stagnoval, neboť se těmto subjektům nepodařilo najít téma, skrze které by mohly oslovit širší obecnost. Je v zájmu státu udržet si k té části společnosti, kterou produkce dezinformací zasahuje, alespoň základní komunikační kanály a tím jí kontinuálně nabízet cestu z antisystémového prostředí.

Šíření dezinformací v českém prostředí je převážně činností domácích aktérů, jejich motivace je přitom vedle té ideové zejména finanční (jde o velmi výnosný byznys). Je stěžejní dokázat rozlišit šíření ze strany domácích aktérů a šíření sponzorované cizí mocí. Pro cizí moc je největším úspěchem, pokud se jí ovlivněnou produkcí podaří dostat do mainstreamu.

Ekonomika

Představitelé některých energetických společností v Česku využívají nadstandardní kontakty a vazby na zástupce státu a díky tomu získávají interní informace ze státních organizací. To následně využívají k prosazování svých zájmů, přičemž v některých případech svůj postup skrytě koordinují s dalšími firmami v daném sektoru.

V některých segmentech sektoru zdravotnictví je dlouhodobě průvodním jevem netransparentní jednání, čímž vzniká prostor pro neefektivní nakládání s veřejnými prostředky či přímo pro korupci.

Kyberbezpečnost

Kybernetická špionáž je často mnohem efektivnějším způsobem získávání zájmových informací než špionáž tradiční. Ke

kompromitaci elektronických zařízení většinou dochází vzdáleně (např. phishingovým útokem), možná je ale i skrze fyzický přístup. Takový typ útoku hrozí zejména během cest do rizikových zemí, např. do Číny.

Čína

Čínská společnost Emposat vybuodovala (ve spolupráci s českým partnerem) pozemní satelitní stanici na území Česka, určenou pro komunikaci a sběr dat ze satelitů na orbitě nad střední Evropou. Emposat tato data mimo jiné plánovala prodávat svým zahraničním zákazníkům. Při posuzování projektu byla detekována řada bezpečnostních rizik.

Príslušníci čínských zpravodajských služeb pokračovali v kultivaci vztahů s vybranými pročínsky smýšlejícími osobami na české politické scéně. Primárním cílem je hledání sympatizantů, kteří by propagovali zájmy Číny, tlumili česko-taiwanskou spolupráci a neotevírali téma lidských práv v Číně.

Terorismus

Úroveň ohrožení islámským terorismem v Česku zůstává nízká. I přes dění na Blízkém východě si ideologické směřování muslimů v Česku zachovává obecně umírněný charakter. Protiizraelské akce ovládli především čeští levicoví aktivisté, přičemž ani jejich projevy nebyly výrazně radikální.

Migrace

Migrační situace v Česku v roce 2024 byla stabilní. Ukrajínští občané pokračovali v začleňování do české společnosti. Další enormní migrační vlna z Ukrajiny do Česka by hrozila pouze v případě, že by došlo ke kolapsu ukrajinské obrany a významnému prolomení frontové linie ze strany Ruska.



RUSKO

RUSKO JAKO TRVAJÍCÍ HROZBA

Zpravodajské aktivity

V roce 2024 Rusko pokračovalo ve snahách o obnovení širších špionážních struktur působících pod diplomatickým krytím na Velvyslanectví Ruské federace v Česku. Z důvodu nedostatku zkušených příslušníků umístěných dlouhodobě v Česku využívaly ruské rozvědné síly pro některé zpravodajské úkoly kromě svých vlastních důstojníků i další spolupracovníky. Konkrétní osobou pobývajícím v Česku, u které se prokázala spolupráce s ruskými zpravodajskými službami, je Natallia Sudliankova (občanka Běloruska), která proto byla v dubnu 2025 zařazena na český vnitrostátní sankční seznam a dostala lhůtu 30 dní na opuštění země.

Natallia Sudliankova dlouhodobě pobývala v Česku jako azylant. Věnovala se především žurnalistice zaměřené na tuzemské ruskojazyčné publikum a aktivitám v oblasti PR. Před rokem 2021, kdy došlo k vyloučení ruských subjektů z tendru na dostavbu jaderné elektrárny Dukovany, byla řadu let klíčovou postavou v oblasti prosazování zájmů Rosatomu v Česku (jednalo se o placenou spolupráci). Patřila také mezi dlouhodobě nejaktivnější spolupracovníky ruských zpravodajských důstojníků působících v Česku pod diplomatickým krytím a angažovala se v aktivitách hnutí Nesmrtelný pluk.

V letech 2021 a 2022 aktivity Natallie Sudliankové řídil a financoval příslušník ruské vojenské rozvědky GRU Aleksej Šavrov, na základě jehož pokynů zajistila zveřejnění několika článků, které měly nejčastěji formu rozhovoru a zaměřovaly se např. na kritiku české nevládní organizace (v roce 2021) nebo kritiku poskytování pomoci Ukrajině (v roce 2022). Finanční prostředky (v řádu nízkých desítek tisíc eur) za zveřejnění uvedených článků Natallia Sudliankova obdržela v kryptoměně skrze prostředníka.

V roce 2024 se aktivity Natallie Sudliankové zaměřovaly na podkopávání důvěry veřejnosti v oprávněnost sankcí EU uvalených např. na ruského oligarchu Ališera Usmanova v souvislosti s jeho podporou války vedené Ruskem proti Ukrajině. Tyto aktivity obnášely zveřejňování tendenčních článků v Česku i několika dalších evropských zemích a byly koordinovány a financovány (v objemu nízkých desítek tisíc eur) spolupracovníkem Ališera Usmanova.

Nekompromisní přístup v otázkách ruských špionážních kapacit působících pod diplomatickým krytím v Česku a obecně vůči osobám, které jsou ochotny spolupracovat s ruskými zpravodajskými službami, zůstává stěžejním úkolem při ochraně před nepřátelskou činností Ruska na našem území. V souvislosti s tím se BIS významně podílí na nalézání společné kontrarozvědné strategie se zahraničními partnery ze zemí schengenského prostoru.



Na českém území je nadále oficiálně přítomna Ruská pravoslavná církev Moskevského patriarchátu. Jedná se o subjekt zcela loajální ruské státní moci, jehož čelný představitel, patriarcha Kirill, je blízkým podporovatelem ruského prezidenta Vladimira Putina a ruské vojenské agrese na Ukrajině, což (již v roce 2023) vyústilo v jeho zařazení na český sankční seznam. V Česku je tato církev zastoupena prostřednictvím podvorje patriarchy moskevského a celé Rusi v České republice a byť se její zástupci snaží v Česku nepřitahovat pozornost kontroverzními prohlášeními, jejich loajalita k moskevskému vedení a podpora ruské oficiální linie je jednoznačná.

Telegramoví agenti

Rusko se i v uplynulém roce snažilo o narušení jednoty západních států a zasévání sváru mezi občany evropských zemí. Jedním z cílů subverzních aktivit Ruska bylo oslabení soudržnosti podporovatelů Ukrajiny, dodávek potřebného materiálu a vybavení a politického zastání napadeného státu. K těmto účelům Rusko začalo s nebývalou intenzitou využívat osoby bez přímého napojení na ruskou státní moc, kterým slibovalo finanční odměnu za páchání útoků na předem vytipované cíle. Tyto osoby jsou rekrutovány mezi členy skupin organizovaného zločinu s vazbami na Rusko a jemu blízké země nebo na internetu prostřednictvím inzerátů nabízejících snadný výdělek za předem nespécifikovanou práci. Nejčastější platformou k online rekrutaci je Telegram, odtud se vžil termín „telegramoví agenti“.

Tito agenti jsou úkolováni k nejrůznějším činnostem, od převozu osob či zásilek, focení a natáčení citlivých objektů, jako jsou vojenské základny či překladiště vojenské pomoci na Ukrajinu, až po žhářské útoky a ohrožení životů civilistů. V Česku v loňském roce takto došlo k zapálení autobusu v pražském depu Klíčov, které měl na svědomí občan Kolumbie zlákaný finanční odměnou nabízenou na internetu. Dalším veřejně známým případem je rozeslání samovznětlivých zásilek leteckou dopravou, za

kterým také stály osoby naverbované ruskými tajnými službami.

Právě ekonomicky slabí migranti ze zemí mimo EU nebo ze států, ve kterých má Rusko vliv, jsou častým terčem náborářů a s vyhlídkou na vysokou finanční odměnu jsou ochotni páchat nelegální činnost. Ruské zpravodajské služby využívají k náboru další prostředníky, dotyčný „telegramový agent“ si tak ani nemusí být vědom toho, že pracuje pro Rusko.

Úkoly, které jsou telegramovým agentům zadávány, vedou nejen k primárnímu efektu, tedy získání informací, dopravení zásilky či způsobení materiálních škod, ale zásadní je zejména psychologický efekt jejich konání. Tím je oslabení soudržnosti západní společnosti, vyvolání strachu a nejistoty, podkopání důvěry ve vlastní stát, že dokáže své občany ochránit, a již zmíněný tlak na omezení podpory Ukrajiny v obraně proti ruskému agresorovi.

Další subverzní a vlivové aktivity

V prvním týdnu září 2024 došlo k souběhu několika set případů nahlášení bombových útoků na školy v Česku. Podobným výhrůžkám, včetně výhrůžek školám, v různém měřítku v posledních letech čelily i další evropské státy. Dosavadní šetření jasně naznačuje vazbu výhrůžek na ruskojazyčné prostředí. Nahlášení bombových útoků v Česku navíc doprovázely konkrétní podpůrné informační aktivity (např. dezinformační kampaň provedená jedním z ruských médií).

Vlivová operace Ruska nazývaná podle stejnojmenného on-line média Voice of Europe byla přerušena na jaře 2024 zapsáním Viktora Medvečuka (ukrajinského prokremelského opozičního politika), Artěma Marčevského a společnosti Voice of Europe s.r.o. na vnitrostátní sankční seznam. Artěm Marčevskij je Medvečukův



blízký spolupracovník a operaci koordinoval z Prahy. Bezprostředně po zapsání na vnitrostátní sankční seznam opustil Česko. Následně byli oba zapsáni i na unijní sankční seznam. Operace Voice of Europe, která usilovala o ovlivňování kandidátů ve volbách do Evropského parlamentu v roce 2024, byla tímto sice efektivně zneutralizována, ale řada podobných vlivových aktivit Ruska v Evropě pokračuje i nadále.

Kybernetické útoky

Po dočasném útlumu v době začínající invaze na Ukrajinu se aktivita ruských státních a státem podporovaných kybernetických aktérů v Česku vrátila na předválečnou úroveň. BIS v roce 2024 zaznamenala aktivitu kybernetických aktérů napojených na ruské zpravodajské služby GRU, SVR i FSB. Z nich byl nejaktivnější aktér APT28 spojený s GRU, který se soustřeďuje především na oblast vojenství, mezinárodních vztahů, politiku, energetiku a obranný, letecký a vesmírný průmysl. Nejčastěji cílí na země EU a NATO a na mezinárodní organizace a v Česku útočí soustavně po řadu let.

Nejvýznamnější případ spojený s APT28 v roce 2024 byl pokračováním útoků z předchozího roku, kdy aktér zneužil zranitelnosti MS Outlook k získávání přihlašovacích údajů ve formě NTLM hashů (digitálních otisků hesla v zašifrované podobě) prostřednictvím aktérem kompromitovaných routerů. Tato kampaň, zaměřená zejména na státy EU a NATO, v Česku cílila na celou řadu státních institucí a rovněž zneužívala českou internetovou infrastrukturu k útokům na další státy. V mezinárodně koordinované akci Dying Ember došlo na počátku roku 2024 dokonce k aktivnímu zásahu Vojenského zpravodajství, který vyústil ve ztrátu přístupu útočníků k napadeným zařízením. V květnu 2024 výše popsané aktivity APT28, respektive Ruska, Česko veřejně odsoudilo společně s Německem za podpory NATO a EU.

BIS též v rámci mezinárodní spolupráce přispěla k publikaci technické zprávy, tzv. Joint Cyber Security Advisory, s názvem Russian Military Cyber Actors Target US and Global Critical Infrastructure ze září 2024. Zpráva popsala útočné techniky, taktiky a postupy Ember Bear, dalšího aktéra spojeného s GRU, při útocích na kritickou infrastrukturu v posledních letech.



Obcházení sankcí

Navzdory opakovaným prohlášením ruských představitelů o nahrazení dovozů západního zboží domácí výrobou se ruským podnikům nedařilo v řadě oblastí, včetně těch zabývajících se výrobou zbraňových systémů, eliminovat závislost na dovozech ze zahraničí. Snahy Ruska získávat sankcionované zboží z Česka proto pokračovaly i v roce 2024. Zboží, na které se vztahují omezující opatření EU, se Rusko snažilo z Česka získávat především cestou reexportů přes třetí země. Řešené případy se týkaly vývozu do členských zemí Eurasijské hospodářské unie nebo Číny.

Ruské podniky historicky patřily k významným odběratelům výrobků z Česka. Po únoru 2022, kdy Rusko zahájilo plošnou agresi vůči Ukrajině, řada českých výrobců nastalou změnu geopolitické situace akceptovala a našla si odběratele v jiných teritoriích. Některé české firmy se nicméně nadále snažily najít cesty, jak své zboží klientům v Rusku dodat. Konkrétním případem, kterým se BIS zabývala, byl český výrobce, který vývozy směřující do Ruska přesměroval nejprve do členské země Eurasijské hospodářské unie a následně do Číny.

V reakci na pokračující agresi Ruska proti Ukrajině EU dále rozšiřovala seznam sankcionovaného zboží klíčového pro ruský zbrojní průmysl. Přestože omezující opatření EU nemají potenciál zastavit dodávky do Ruska, vedou k navýšení nákladů na získání západního zboží a komplikují další rozšiřování ruských výrobních kapacit.

Rozšiřování omezujících opatření EU vedlo u českých institucí zapojených do licenčního a povolovacího řízení k nárůstu zpracovávané agendy. Český systém vývozních kontrol se v důsledku nárůstu řešených případů potýkal s nedostatečnými personálními kapacitami a narůstajícími finančními náklady na provádění exportních kontrol.

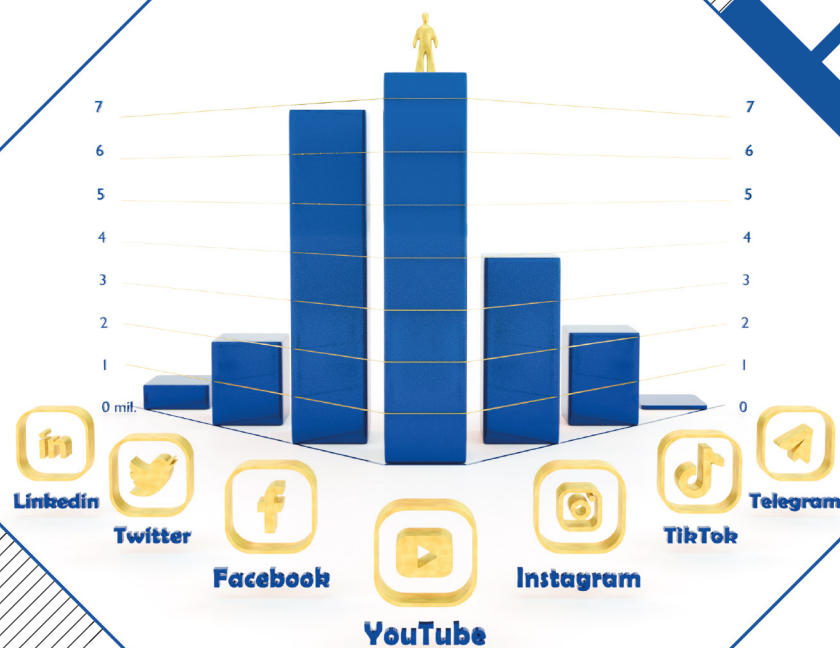
Schopnost Ruska pokračovat v agresivní válce vůči Ukrajině do značné míry závisí na přístupu Číny, odkud Rusko získává významný podíl součástek klíčových pro výrobu jeho zbraňových systémů, a na dodávkách od dalších podporovatelů, zejména Íránu a KLDR.



SOCIÁLNÍ SÍTĚ ALTERNATIVNÍ MÉDIA A ŠÍŘENÍ DEZINFORMACÍ

Algoritmy sociálních sítí

Pro část společnosti se sociální sítě staly významným zdrojem informací o světě. Způsob jejich fungování má přitom řadu rizikových aspektů – od množství falešných účtů přes nedostatek objektivitu, až po nastavení, které silně podporuje vznik závislosti.



Odhad počtu uživatelů v ČR (v milionech)

**Odhad vychází z analýzy otevřených zdrojů. Provozovatelé sociálních sítí přesné a aktuální počty uživatelů dle jednotlivých zemí nezveřejňují.*

Na sociálních sítích se nachází obrovské množství obsahu. Jednotlivým uživatelům se přitom zobrazuje pouhý zlomek ze všech zveřejněných příspěvků. Tento zlomek pro každého uživatele vybírají algoritmy (tedy speciálně naprogramované počítačové výpočty) sociálních sítí.

Ústředním cílem firem, které sociální sítě provozují, je dosáhnout co největšího zisku. Čím více času uživatelé na sítích stráví, tím větší zisk provozovatel sítě inkasuje (z placených reklam, sponzorovaných příspěvků atd.). Právě od toho se pak odvíjí také nastavení algoritmů, jejichž hlavním cílem je udržet každého uživatele co možná nejdéle „online“.

Situace, kdy sociální sítě prostřednictvím svých algoritmů uživateli nabízejí obsah, který ho více a více pohlcuje, je označována pojmem „rabbit hole“ („králičí nora“). Vzniká ve chvíli, kdy uživatel často kliká na odkazy a sleduje obsah na konkrétní téma. Algoritmy ho pak postupně do tohoto tématu vtahují stále hlouběji, výběrem stále radikálnějšího obsahu. Tento proces může vést k uzavření se do tzv. informačních bublin i k ovlivnění vnímání reality.

Algoritmy sociálních sítí upřednostňují při výběru zobrazovaných příspěvků ty, které poutají nejvíce pozornosti (tj. získávají nejvíce reakcí a komentářů – je jedno zda pozitivních, či negativních). Před „suchými“ fakty proto většinou upřednostní emočně nabitý obsah – ať už vtipný, děsivý, nebo násilný. Tímto nastavením prostředí sociálních sítí mimo jiné silně nahrává šíření nepravdivých či zkreslených informací, přičemž není v obchodním zájmu provozovatelů sítí proti tomu efektivně bojovat.

Příspěvky, které vyvolávají silné emoce a jsou manipulativní či cílí jen na určité skupiny uživatelů (za poplatek), mohou psát a šířit všichni – od extremistických skupin přes politické strany až po neziskové organizace a jednotlivce. Největší výhodu získává ten, kdo dokáže algoritmy nejefektivnějším způsobem využít (a ještě větší, pokud k tomu navíc disponuje dostatkem financí a dalších prostředků – např. k hromadné tvorbě falešných účtů). Sociální sítě jsou otevřené každému, podmínky pro šíření obsahu jsou na nich pro každého stejné. Jejich výraznější regulace je proto často kritiky označována za omezování svobody.

Ve chvíli, kdy regulace sociálních sítí je velmi pomalá a komplikovaná, je klíčové zaměřit pozornost na uživatele – na jeho vzdělání a na jeho povědomí o tom, jakým způsobem sociální sítě a jejich algoritmy fungují. Je v zájmu demokratické společnosti, aby občané toto povědomí měli a aby nečerpali informace a netvořili si názory výhradně z obsahu, který jim nejprve vyselektují sociální sítě.

BIS prostředí českých sociálních sítí monitoruje v rámci snah o zachycení možných vlivových operací a pokusů o ovlivňování veřejného mínění v Česku, a to zejména ze strany ruských zpravodajských služeb a dalších aktérů napojených na ruský stát. Monitoring probíhá také v oblasti prevence terorismu.



Dezinformace a jejich původ

Dosah aktérů a platform, které v českém prostředí šíří dezinformace a konspirace, v roce 2024 spíše stagnoval, neboť se těmto subjektům nepodařilo najít téma, skrze které by mohly oslovit nové skupiny konzumentů/širší obecnost. Aktuální vliv by tedy bylo možné interpretovat jako společensky omezený. Část společnosti nicméně konzumuje dezinformace pravidelně, což ji činí zranitelnou vůči vlivovým operacím cizí moci.

Šíření dezinformací v českém prostředí lze vnímat převážně jako činnost domácích aktérů, jejichž motivace je zejména finanční a/nebo ideová. Ve specifických případech je motivace spojená také s vyhledáváním mediální pozornosti, kterou se vybraní jedinci snaží následně přetavit v politické body. Z několika zaznamenaných případů je pak nadále patrný neustupující zájem Ruska i Číny o využívání domácí dezinformační scény pro prosazování svých zájmů. Zatímco Čína finančně podporovala média i jednotlivce ochotné šířit výhradně pozitivní obraz Číny s cílem ovlivnit její vnímání českými občany, Rusko se zaměřilo na svoji dlouhodobou strategii spočívající ve snahách využít dění v Česku s cílem podnícení neklidu v české společnosti a i pro účely domácí propagandy.

Je stěžejní rozlišovat šíření dezinformací a konspirací, jehož zdrojem jsou domácí aktéři, a šíření sponzorované cizí mocí, neboť obě varianty vyžadují jiné typy reakcí: zatímco proti šíření vnějším aktérem je potřeba se nekompromisně postavit a využít všechny prostředky k jeho omezení, domácí zdroje šířící dezinformace se stávají pro zasaženou část společnosti součástí politické diskuze a je v zájmu státu disponovat alespoň základními komunikačními kanály k těmto osobám, a tím jim kontinuálně nabízet cestu z antisystémového prostředí. Jedině důvěryhodná komunikace spojená s konkrétními kroky ve prospěch životních podmínek zasažené

populace jsou spolu s celospolečenským vzděláváním způsobilé situaci prospět.

V oblasti šíření přímo sponzorovaného Ruskem udržovaly svou aktivitu informační kanály přímo napojené na ruský státní aparát. Jednalo se především o nástupce ruského státního média Sputnik, mezi které patří web 42tcen.com a telegramový kanál neČT24, nebo z Ruska ovládaný telegramový kanál Selský rozum.

Kanál Selský rozum vznikl nedlouho po začátku války na Ukrajině a jeho aktivity jsou navázány na ruské zpravodajské služby. Např. v únoru 2024 kanál šířil otevřenou výzvu ke sběru informací o českém výrobci raketometů Vampire a jeho zaměstnancích. Ruská strana dlouhodobě kritizuje Česko za dodávky zbraní na Ukrajinu, včetně údajného užití českých zbraní proti ruským civilistům. Tento narativ se Rusko snažilo s malou úspěšností přenést do českého mediálního prostředí.

V roce 2024 byl mezi šířiteli a konzumenty dezinformací a konspirací v Česku patrný nárůst popularity informačních a komunikačních kanálů zaměřujících se na šíření video obsahu (platformy YouTube, Telegram a TikTok). Přestože dominantní síť zůstal v této oblasti stejně jako v předchozích letech Facebook, na rizikovosti začala významně nabírat platforma Telegram, skrze kterou došlo k propojení dezinformačního působení s klasickými subverzními aktivitami.

Komplikované nadále zůstává efektivní měření dopadu vlivových informačních operací ze strany cizí moci či obecně dopadu šíření dezinformací a konspirací. Je jisté, že cizí moc považuje za úspěch, pokud se jí ovlivněná produkce či jí nabídnutý příběh podaří dostat do mainstreamu,

a to ať už skrze média či vybrané politiky, novináře, influencery atd.

Šíření dezinformací nemusí, oproti tradiční představě, sloužit jen k ovlivnění určitého segmentu společnosti. Jak se ukázalo u případu Voice of Europe, produkce propagandy a dezinformací může také posloužit jako kouřová clona pro zakrytí závažnější zpravodajské operace. Ta může spočívat ve vytváření kontaktních kanálů na vybrané politiky či jiné osoby zájmu skrze nabídky spolupráce, rozhovorů nebo účasti v diskuzích, což zároveň poskytuje věrohodné krytí k vyplacení finančních prostředků za tyto aktivity. Tím může cizí moc vybrané osoby nepřímo podpořit či si otevřít prostor pro další zpravodajské kroky vůči nim.



Nové technologie

V současnosti i blízké budoucnosti BIS považuje za významné riziko instrumentalizaci umělé inteligence (AI) k šíření dezinformací. Řízené účty ze strany AI (boti) se už dnes umí chovat jako lidé, vést debaty, reagovat na komentáře a tím zvyšovat věrohodnost falešným informacím. Skrze AI je možné vytvářet falešný obsah v takovém množství a kvalitě, že se stává „zbraní hromadného materiálu“. Někteří aktéři již nyní tuto technologii využívají k operacím informační války, přičemž cílem není jen šířit lži, ale také vyvolávat zmatek, nejistotu, relativizovat pravdu a oslabovat schopnost veřejnosti rozeznat důvěryhodné zdroje a tím i oslabit její důvěru ve stát jako takový.

Syntetická tvorba se stala běžnou součástí informačního prostoru – včetně tzv. deepfakes, tedy falešných videí a zvukových nahrávek. Zatímco v počátečních fázích byly deepfakes často kompletně vytvořené pomocí AI, s postupem času tento trend spíše ustupuje. Namísto toho častěji dochází k vytváření vizuálních nebo audio-vizuálních záznamů, které jsou až následně upraveny nástroji AI. Takto modifikovaná média tedy vychází ze skutečných podkladů, které jsou dále pomocí AI zasazeny do nepravdivého nebo zkresleného kontextu.

Zvláště během období voleb je možné pozorovat zvýšený výskyt obsahu, který využívá AI pro manipulativní úpravu záznamu založeného na pravdivém základě. Mnohdy jsou k těmto úpravám využívány méně sofistikované AI programy, které produkují nekvalitní deepfakes.

Trh s automatizovanými detekčními nástroji nadále zaostává za vývojem syntetických médií. Současné nejzdařilejší detekční programy jsou znatelně kvalitnější než jejich předchůdci, nicméně jejich výsledky stále nejsou tak spolehlivé, aby dokázaly plně nahradit lidskou analýzu.





TREND ONLINE RADIKALIZACE MLADISTVÝCH

V roce 2024 pokračoval trend radikalizace mladých a mladistvých, který BIS pozoruje od podzimu předcházejícího roku. Šlo o zhruba dvě desítky osob, jejichž radikalizace se projevovala vyhledáváním a šířením materiálů islamistického či pravicového extremistického charakteru na internetu. Význam ideologie jako takové byl ale upozaděný, zásadní roli hrála spíše fascinace násilím a snaha být součástí širší komunity podobně smýšlejících osob.

Věk těchto mladých radikálů byl v rozmezí od 13 do 21 let a většina z nich měla českou národnost. Mladí radikálové se až na výjimky navzájem sdružovali skrze sociální sítě jako je Telegram či TikTok, byť pocházeli z různých regionů a osobně se zpravidla neznali. Obvykle šlo o mladistvé s neadekvátním rodinným zázemím a/nebo ostrakizované jedince. K radikalizaci zpravidla docházelo autonomně, bez přímé vazby na radikální organizace. Ovšem byl také zaznamenán případ 21letého občana Česka, který byl skrze Telegram v kontaktu s verbíři tzv. Islámského státu (IS).

Trend radikalizace mladých a mladistvých se současně projevoval ve více zemích Evropy. Ve většině těchto států měl zaznamenaný jev společné znaky, zejména již zmíněný zájem o násilí, sdružování se do online komunit, problémy v rodině a/nebo ve škole a minimální vazby na teroristické organizace. Na rozdíl od minulosti, kdy většina extremistických činů v souvislosti s online radikalizací končila ve verbální rovině, zaznamenané případy naznačovaly zvýšenou ochotu některých pachatelů přistoupit ke konkrétním násilným činům v reálném světě. Sofistikovanost případných útoků byla prozatím velmi nízká, což ale nijak nesnižovalo jejich hrozbu pro společnost.

Od května 2024 BIS ve spolupráci s policií a zahraničními zpravodajskými službami monitorovala pravicově extremistickou skupinu mladistvých. Ta se realizovala prostřednictvím velkého množství kanálů a skupin sociálních sítí, přičemž jejich obsah zahrnoval agresivní pravicově extremistickou propagandu s výrazným důrazem na násilí typické pro myšlenky militantního akcelerationismu a kulturu SIEGE. Největší reálné riziko vyplývající z její existence představovala výzva k teroristickému útoku proti akci Duhový pride v Bratislavě, která se konala dne 20. července 2024. Vzhledem k této hrozbě policie proti skupině zakročila a zahájila proti hlavnímu aktérovi skupiny trestní stíhání.

Významnou příčinou radikalizace byly algoritmy sociálních sítí, které stále dokonaleji směřovaly obsah, i ten s radikální tematikou, uživatelům, kteří k němu inklinovali. Tento faktor nejpřesvědčivěji vysvětloval současný vznik jevu radikalizace mladistvých ve více zemích Evropy. Sekundární roli hrály konflikty na Ukrajině a Gaze, které u některých konkrétních případů stály na počátku radikalizačního procesu. Většina monitorovaných osob těmito konflikty nežila a spíše vyhledávala i deset let staré materiály, např. propagandistická videa z vrcholné éry IS v letech 2014–2019.

Vzhledem k tomu, že motivace pro zájem o radikální materiály často vězí v osobní rovině, izolaci, nedostatku sociálních vazeb, nedostatku zájmu ze strany okolí apod., je deradikalizace těchto mladých osob možná. Zahraniční příklady úspěšné pozitivní změny chování i u velmi rizikových mladistvých zpravidla vycházely z multidisciplinárního přístupu, zahrnujícího vedle bezpečnostních složek také zejména sociální služby, školy, rodiče či imámy.



**Na osoby, které vykazují známky rizikového chování,
může veřejnost Bezpečnostní informační službu upozornit
prostřednictvím e-mailu prevence@bis.cz.**



ENERGETICKÁ BEZPEČNOST A OCHRANA VEŘEJNÝCH FINANCÍ

V oblasti ochrany významných ekonomických zájmů spočívalo hlavní riziko ve schopnosti některých soukromých společností prosazovat své partikulární zájmy ve vztahu ke státu, státem ovládaným subjektům a institucím. Tento jev byl prostoupen napříč mnoha sektory ekonomiky a jeho spojujícími prvky byl klientelismus a úzké vazby mezi zástupci státu a soukromým sektorem, které v mnoha případech představovaly zjevný střet zájmů.

Energetika

Tak jako v předchozích letech byl i v roce 2024 jedním z hlavních cílů soukromých společností energetický sektor, a to z několika důvodů. Za prvé v energetice probíhají nebo se připravují významné projekty, a to nejen z hlediska objemu financí. Za druhé se jedná o silně regulovanou oblast, kdy na nastavení některých parametrů závisí míra zisku klíčových aktérů. V neposlední řadě se v tomto odvětví přerozdělují značné prostředky z dotací či podpor.

Energetické společnosti se proto v některých případech snažily na základě utajené vzájemné koordinace svých postupů prosadit své zájmy. Představitelé energetických společností využívali také nadstandardní kontakty a vazby na zástupce státu, skrze které získávali i interní informace z prostředí státních organizací, a v některých případech skrytě využívali i zástupce zájmových sdružení či jiných – zdánlivě nezávislých – osob.

léčiv, poskytovatelé zdravotních služeb, vrcholní představitelé nemocnic, lékaři v nemocnicích, odborné společnosti apod.).

V sektoru zdravotnictví se projevila úskalí monokratického řízení jednotlivých institucí či pracovišť, která BIS zaznamenala již v minulých letech. V situaci, kdy jsou v řídících pozicích silné osobnosti, dochází v některých případech ke kumulaci vlivu těchto osob a jeho zneužívání pro vlastní prospěch nebo zvýhodnění jiného soukromého subjektu s úzkou vazbou na tyto osoby. Příkladem takového jednání je zasahování do stanovisek jednotlivých útvarů dané instituce, zrychlené vyřizování požadavků preferovaných subjektů, vycházení vstříc farmaceutickým společnostem apod. To vytváří prostor pro neefektivní nakládání s veřejnými prostředky či přímo korupci. Motivem jednání zástupců státních institucí však nemusí být nutně finanční profit, ale může se jednat i o udržování a kultivování oboustranně výhodných kontaktů a vazeb.

Zdravotnictví

Další oblastí, ve které BIS zaznamenala případy klientelismu či ovlivňování rozhodování představitelů státem ovládaných subjektů, bylo zdravotnictví. Oproti energetice se jednalo o případy s řádově nižším potenciálním dopadem na veřejné finance, avšak četnost jejich výskytů byla naopak vyšší. K netransparentnímu jednání dlouhodobě dochází u různých zainteresovaných subjektů v sektoru zdravotnictví (zdravotní pojišťovny, farmaceutické společnosti, distributoři

ICT zakázky

Dlouhodobým problémem některých státních subjektů je nevyhovující stav IT infrastruktury, včetně některých strategicky významných informačních systémů či projektů. Příčinou tohoto stavu byla např. několikaletá nečinnost vedení konkrétní instituce, kdy docházelo k oddalování přijetí klíčového rozhodnutí o budoucí podobě informačního systému a výběru způsobu realizace. V některých případech zpoždění při realizaci potřebné IT infrastruktury ohrožovalo získání předpokládané dotace či vyvolávalo časový tlak, který zvyšoval riziko volby nevhodného postupu. V jiném případě neschopnost připravit včas zakázku vedla i k situaci, kdy zástupce státního subjektu požadoval po potenciálních dodavatelích skrytou participaci na zpracování zadávací dokumentace, což však takovému subjektu mimo jiné poskytlo konkurenční výhodu. Zmíněné jevy jsou často provázány nedostatečným či zavádějícím informováním odpovědných zástupců státu, kteří pak nemohou plně vykonávat svou kontrolní funkci.



KYBERŠPIONÁŽ

Kybernetická špionáž je v případě jejího úspěšného provedení mnohem efektivnějším prostředkem pro získání zájmových a zpravodajsky využitelných informací, než je tomu v případě tradiční špionáže. Ve prospěch kybernetické špionáže navíc svědčí nejen množství potenciálně získaných informací, ale také jejich kvalita a přesnost.

Stejně jako v minulých letech i v roce 2024 byly detekovány již tradiční pokusy či úspěšné kompromitace zařízení nebo sítí, ke kterým zpravidla dochází vzdáleně např. zneužitím zranitelnosti či phishingovým útokem. Kromě těchto případů se BIS zabývala mimo jiné i získáváním poznatků o infikovaném zařízení, ke kterému měl útočník dočasně umožněn fyzický přístup. K tomuto typu útoku zpravidla nedochází na českém území, ale v rizikových zemích, do kterých občan Česka přicestuje a stane se cílem zvýšeného zpravodajského zájmu. Za rizikové země považujeme zpravidla nedemokratické státy, které nejsou členy EU či NATO a zároveň disponují ofenzivními kybernetickými schopnostmi.

Typicky se jedná o pracovní návštěvu, během které hostící strana využije výhod a kapacit na svém území a nastaví či pozmění program cesty takovým způsobem, aby její účastníci neměli dočasně přístup ke svému osobnímu nebo pracovnímu elektronickému zařízení (zpravidla notebook či telefon). Během této doby k němu mají útočníci fyzický přístup a jsou schopni ho kompromitovat škodlivým kódem, aniž by o tom měl jeho majitel jakékoli tušení. Vzhledem k tomu, že takto nainstalovaný malware má především špionážní funkce, pravděpodobným účelem těchto aktivit je získání informační výhody do dalších obchodních, diplomatických nebo jiných jednání.

V souvislosti s cestami (především pracovními) do rizikových zemí je vhodné držet se bezpečnostních zásad, které výrazně snižují riziko úspěšné provedené špionáže:

1. Před cestou

Pro pracovní záležitosti využívejte výhradně pracovní komunikační zařízení. Ujistěte se, že vaše zařízení má nejnovější aktualizace.

Používejte dlouhá hesla ve formě frází a/nebo použijte správce hesel.

Změňte hesla před vaší pracovní cestou i po ní.

Zvažte použití dočasně mobilního zařízení, které využijete pouze v této rizikové destinaci.

Povolte služby pro určování polohy v telefonu pouze tehdy, když je potřebujete.

Instalujte pouze aplikace, které skutečně potřebujete.

Pokud je to možné, využívejte vícefaktorové ověřování (MFA).

Použijte zámek obrazovky k zabezpečení svých mobilních zařízení.

Při používání zařízení na veřejných místech buďte opatrní: ostatní vás mohou nepozorovaně sledovat.

2. Během cesty

Pravidelně restartujte svůj telefon.

Vypněte Bluetooth na všech svých zařízeních.

Vždy využívejte své mobilní datové připojení. Rovněž používejte VPN připojení. Nepoužívejte Wi-Fi připojení.

Během cestování nestahujte ani neinstalujte jakékoli aplikace.

Věnujte pozornost neočekávaným nebo zvláštním (bezpečnostním) upozorněním na telefonu, notebooku nebo tabletu. Taková oznámení mohou indikovat kybernetický útok.

Pokud chcete volat, použijte komunikační aplikaci, která používá standardní koncové šifrování.

V případě telekomunikačních zařízení nikdy nepoužívejte přídatná vybavení nebo kabely třetích stran. Rovněž nepřipojujte svá zařízení k jiným neznámým zařízením (např. tiskárny či nabíječky).

Pokud vložíte USB flash disk do zařízení třetí strany, může se nakazit malwarem. Toto USB zařízení již během cesty nepoužívejte. Přivezte ho zpět, abyste jej zničili nebo vyčistili.

Nevkládejte žádná USB třetích stran do svých zařízení. Zejména USB flash disky mohou být nakaženy malwarem. Pokud obdržíte USB flash disk, který má obsahovat zájmová data, ověřte, jak můžete bezpečně přenést tato data do pracovní sítě.

Nikdy neopouštějte svá zařízení. Pokud je to z bezpečnostních důvodů nezbytně nutné, přenechte je např. u kolegy, který nejde s vámi. Pokud to není možné, zařízení vypněte, dejte ho do těsního sáčku a uložte nejlépe do trezoru, ke kterému máte klíč.

Nedovolte ostatním používat vaše zařízení.

3. Po cestě

Změňte hesla ke všem zařízením, která jste měli s sebou. Stejně tak změňte hesla ke všem emailovým schránkám nebo účtům na sociálních sítích, které jste v zahraničí používali.



DALŠÍ DŮLEŽITÁ TÉMATA ZPRAVODAJSKÉHO ZÁJMU

Terorismus

Úroveň ohrožení terorismem v Česku v průběhu roku 2024 zůstala na nízké úrovni. Došlo nicméně ke dvěma neúspěšným pokusům občanů Česka o připojení se k zahraničním teroristickým organizacím v Somálsku a Libanonu. Jednalo se o první takové případy od roku 2017. Znepokojivým trendem byl výše popsán nárůst případů mladých a mladistvých se zájmem o radikální obsah na internetu. Bezprostřední ohrožení území ČR terorismem ale zjištěno nebylo.

I v souvislosti s blízkovýchodní situací zůstalo ideologické směřování muslimů v Česku neměnné a i nadále si zachovalo obecně umírněný charakter. Stejně jako v předchozích letech bylo zaznamenáno několik radikálnějších projevů, které ovšem nerepresentovaly hlavní názorový proud komunity. Naprostá většina těchto projevů byla navíc zaznamenána v prostředí sociálních sítí.

Hlavním radikalizačním faktorem byl v průběhu roku 2024 trvající palestinsko-izraelský konflikt, ačkoliv nešlo o natolik silné téma jako v zemích s početnou muslimskou komunitou. S narůstajícím počtem obětí na straně rodin a blízkých Palestinců žijících v Česku se sporadicky začala objevovat radikálnější vyjádření k situaci, šlo však pouze o jednotlivce. Protiizraelské akce ovládli především levicoví aktivisté, muslimové v Česku se soustředili na reálnou pomoc blízkým v Gaze. Téma se v průběhu roku přeneslo i na akademickou půdu, kde byly české univerzity vyzývány k ukončení nekritické podpory univerzit v Izraeli. Ani zde nebyly projevy natolik radikální, jako tomu bylo na univerzitách v zahraničí.

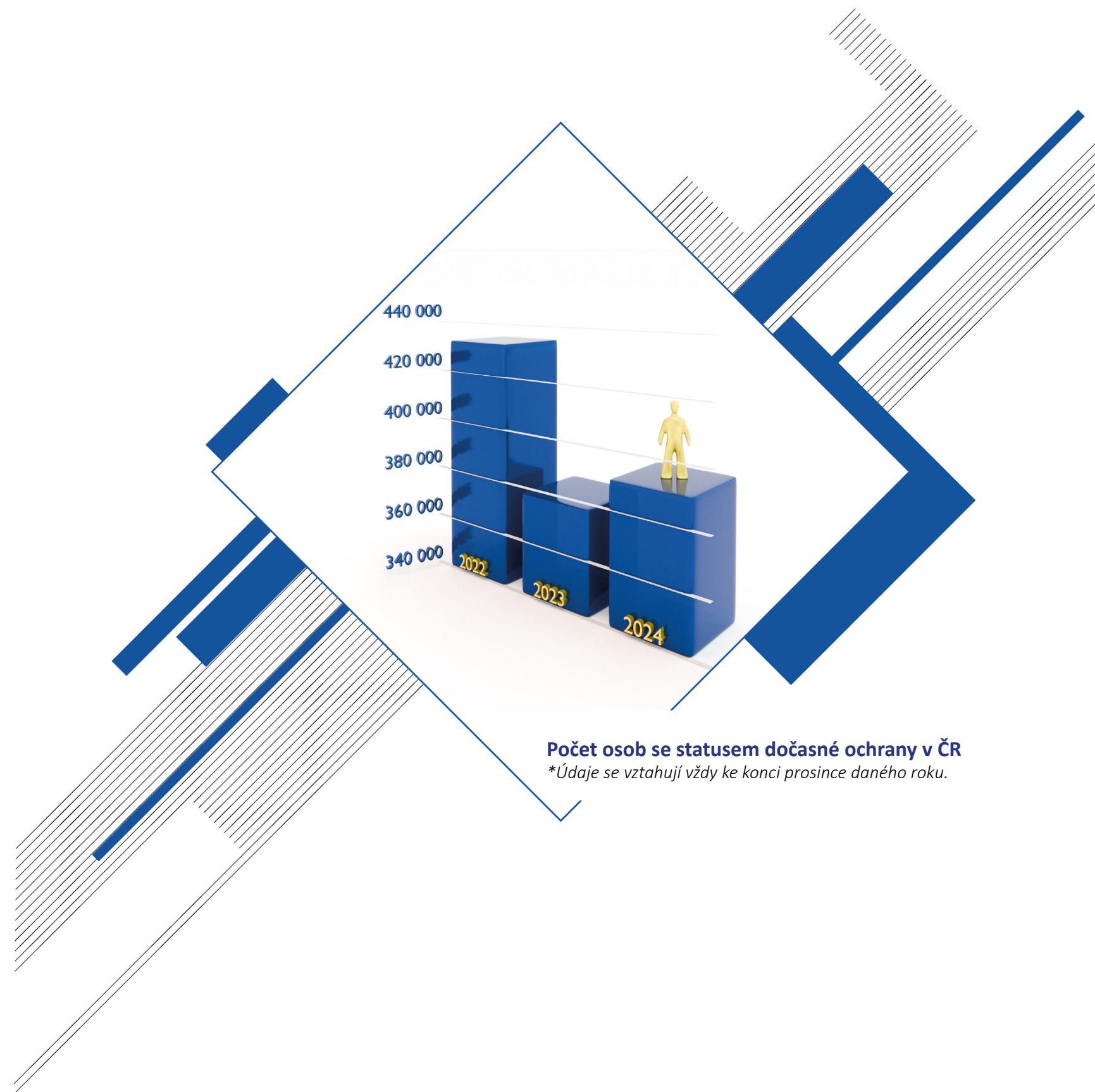
Turbulentní situace na Středním východě přinášela mnohá rizika, která bylo nezbytné průběžně sledovat a vyhodnocovat. Politiku Íránu v roce 2024 významnou měrou poznamenal konflikt Izraele s hnutími Hamás a Hizballáh vedoucí ke smrti jejich vůdců, izraelské útoky na

Írán, smrt některých významných představitelů íránského režimu a překvapivý pád režimu syrského prezidenta Baššára al Asada. Situaci v Evropě negativně ovlivňovala spolupráce íránského režimu s místními kriminálními sítěmi za účelem provádění násilných útoků proti zdejším „nepřátelům režimu“. Žádná z výše uvedených událostí se však výrazně nepropsala do situace v íránské, libanonské či syrské komunitě v Česku a nezměnila jejich dosavadní umírněný charakter.

Dopady ruské agrese vůči Ukrajině na Česko

Na Ukrajině v průběhu roku 2024 pokračovaly evakuace z oblastí válečné frontové linie. V zemi je evidováno přes tři miliony vnitřně vysídlených osob, z nichž více než polovina spoléhá na nějakou formu humanitární pomoci.

V Česku na konci roku 2024 pobývalo přes 390 tisíc osob se statutem dočasné ochrany. Další enormní migrační vlna z Ukrajiny do Česka by hrozila pouze v případě, že by ze strany Ruska došlo k významnému průlomů na frontové linii nebo k ovládnutí ukrajinského státu. Aktuálně je migrační situace v Česku stabilní a ukrajinští občané zde pokračují v začleňování do společnosti, přičemž hodnota jejich ekonomického přínosu již dávno přesáhla hodnotu finanční podpory a sociálních dávek, které od českého státu od začátku války obdrželi. Na míru kriminality v Česku jejich přítomnost neměla negativní dopad.





BIS sleduje dopady ruské agrese proti Ukrajině rovněž s ohledem na předpokládané riziko využívání struktur organizovaného zločinu k subverzním akcím plánovaným ruskými zpravodajskými službami. Zapojení členů skupin organizovaného zločinu nebo jiných osob z kriminálního prostředí do sabotážních akcí nebylo zatím v Česku zaznamenáno, ale zkušenosti z ostatních zemí EU nebo Ukrajiny ukazují, že toto riziko je relevantní, stejně jako využitelnost členů těchto struktur pro vlivové operace Ruska namířené proti EU.

Ani v roce 2024 BIS nedisponovala informacemi o zapojení představitelů organizovaného zločinu do nelegálního obchodu se zbraněmi z Ukrajiny. S ukončením válečného konfliktu se však z nelegálního obchodu se zbraněmi a vojenským materiálem z Ukrajiny může stát nový rizikový fenomén.

Hrozby ze strany Číny

Významnou rizikovou aktivitou čínských subjektů v Česku byla investice společnosti Emposat do vybudování pozemní satelitní stanice na českém území. Čínské společnosti jsou vázány zákony Číny ke spolupráci s čínským státem. Při provozu takového zařízení tedy mohlo dojít k situaci, kdy by na pokyn čínské strany byla společnost Emposat povinna jednat v souladu s nařízením čínských autorit, a to i v případech, kdy by toto jednání bylo proti českým zájmům. Existovala tedy reálná rizika využití satelitního zařízení pro vojenské či zpravodajské účely, v rozporu s bezpečnostními nebo zahraničně-politickými zájmy Česka. Tato rizika byla identifikována v oblastech obrazového a signálového zpravodajství, ohrožení signálové komunikace a kybernetické bezpečnosti.

Snahy čínských subjektů o provozování satelitních stanic ve státech EU nejsou ojedinělé a dotčené státy se snaží výše uvedená rizika eliminovat dle svých zákonných možností. Popsaný případ je zatím v Česku první svého druhu v řadě oblastí. Možnosti zastavení takových rizikových aktivit a omezení popsanych hrozeb řešila BIS s kompetentními orgány v rámci jejich zákonných pravomocí. Ke konci roku 2024 nebyl případ Emposat dořešen, v květnu 2025 ale došlo k odstranění satelitní stanice, a to v souladu s rozhodnutím Ministerstva průmyslu a obchodu (MPO), které navazovalo na vládní usnesení o zákazu dalšího trvání této investice.

stranách, kteří by podporovali sbližování obou zemí, propagovali zájmy Číny a tlumili pro ni nežádoucí česko-taiwanskou spolupráci, a zároveň neotevírali téma lidských práv a demokratických principů v Číně. Součástí čínských aktivit na českém území je i sběr zájmových informací, které jsou následně posílány do Číny a mohou být využity např. k přesnějšímu formování přístupu Číny vůči Česku na mezinárodním poli.

Čínská snaha o obchodní a technologickou dominanci představuje výzvu pro ochranu českých společností, jejich know-how a dodavatelských řetězců. Po zavedení prověřování zahraničních investic do české legislativy mohou být Čínou více využívány joint venture projekty realizované na území Číny, které znesnadňují kontrolu vlastnictví a využití českého know-how. V případě vybudování výrobního závodu na území Číny tak hrozí aktivní snaha o vyvedení technologií dodaných druhou stranou v rámci joint venture projektů. I čistě civilním technologiím následně hrozí zneužití v čínském vojenském průmyslu, neboť Čína intenzivně uplatňuje politiku fúze civilní a vojenské sféry.

Co se týče čínské kyberšpionáže, zpravodajské služby Číny obsahují své vlastní (vnitřní) kybernetické jednotky. Ty jsou ale pouze dílčí součástí celého komplexního, systémově řízeného a vzájemně provázaného ekosystému, který tvoří i další subjekty. Podstatným prvkem jsou minimálně některé soukromé IT společnosti, které spolupracují právě se zpravodajskými službami, popř. dalšími státními subjekty. Jak dokázala i uniklá data čínské společnosti i-SOON, je pravidlem, že jedna společnost může poskytovat své služby pro různé účely (včetně vojenských nebo určených pro vnitřní bezpečnost) mnoha státním subjektům. Hlavní síla celého čínského kybernetického ekosystému tkví v tom, že jeho jediným cílem je působit v zájmu čínské vlády, respektive Komunistické strany Číny.

Kybernetičtí aktéři z řad soukromých IT společností zapadají do aplikace tzv. celospolečenského přístupu Číny, který je těsně provázan se zákonem o národním zpravodajství. Jedná se o metodu, kdy Čína nad rámec činností zpravodajských služeb zapojuje do sběru zájmových informací svou diplomatickou reprezentaci, čínskou komunitu, stranické organizace či soukromé subjekty (např. kybernetické aktéry). Spolupráce všech zmíněných subjektů se zpravodajskými složkami Číny je zmíněným zákonem vynutitelná.

Čínská společnost Emposat, ve spolupráci s českým partnerem, zprovoznila na pozemku v obci Vlkoš u Kyjova satelitní anténu určenou pro komunikaci, řízení a sběr dat ze satelitů nad územím střední Evropy pro zahraniční zákazníky. Cílem provozu čínské antény bylo navázat komunikaci se satelitní sítí Jilin. Družicový systém Jilin spravuje státem vlastněná čínská společnost Chang Guang Satellite Technology, která byla zařazena na sankční seznamy EU a USA za poskytnutí satelitních snímků ve vysokém rozlišení Wagnerově soukromé vojenské skupině působící na Ukrajině.

Případ splňoval definici rizikové zahraniční investice na území ČR ve smyslu zákona č. 34/2021 Sb., o prověřování zahraničních investic, získané poznatky proto umožnily gestorovi zákona MPO zahájit proces prověření celé investice. Na základě identifikovaných bezpečnostních rizik Český telekomunikační úřad neudělil pro anténní systém Emposatu umístěný na pozemní stanici povolení k využívání rádiových kmitočtů družicové služby.

V roce 2024 příslušníci čínských zpravodajských služeb pokračovali v kultivaci vztahů s pročínskými osobami na české politické scéně. Primárním cílem je hledání sympatizantů ve všech politických

SPOLUPRÁCE NA NÁRODNÍ ÚROVNI

Spolupráce se zpravodajskými službami ČR

BIS v roce 2024 zaslala ÚZSI více než 70 informací a VZ obdrželo od BIS více než 40 informací. Spolupráce s oběma službami probíhá i v dalších činnostech operativního, analytického či servisního charakteru.

Spolupráce BIS s ÚZSI na prověřování žadatelů o diplomatickou akreditaci pro území ČR je jedním z nástrojů, jak snížit bezpečnostní riziko plynoucí z nepřátelských aktivit osob působících v diplomatických službách cizích států na našem území. Tato spolupráce plynule pokračovala i v roce 2024, kdy bylo prověřeno 145 diplomatických zástupců, pracovníků diplomatických misí a jejich rodinných příslušníků.



Počet osob prověřených v souvislosti
s žádostmi o diplomatickou akreditaci

BIS, VZ a ÚZSI spolupracovaly rovněž při přípravě a v průběhu cvičení orgánů krizového řízení NATO a při aktualizaci Národního systému reakce na krize.



Spolupráce s Policií ČR

BIS v roce 2024 pokračovala ve spolupráci s Ředitelstvím služby cizinecké policie (ŘSCP) na prověřování žadatelů o krátkodobá a dlouhodobá víza. V roce 2024 BIS prověřila 1 800 000 žádostí, což znamenalo nárůst o 100 000 oproti roku 2023.

V rámci prověřování byl zaznamenán nárůst žádostí ruských státních příslušníků. Zatímco v roce 2023 bylo prověřeno přibližně 470 000 žádostí ruských státních příslušníků, v roce 2024 se jednalo již o téměř 600 000 žádostí. Ve většině případů šlo o žádosti o vízum podané na zastupitelských úřadech členských států schengenského prostoru. Na zastupitelských úřadech Česka bylo podáno pouze okolo 700 žádostí ruských státních příslušníků, protože Česko vůči Rusku i nadále uplatňuje přísná pravidla pro vydávání víz spočívající v omezení okruhu osob, která mohou žádost o vízum podat. Možnost vyjádřit se i k žádostem o vízum občanů Ruské federace, podaných na zastupitelských úřadech členských států v kombinaci s omezením okruhu osob ruské státní příslušnosti, které si mohou o vízum na zastupitelských úřadech Česka požádat, jsou významným prvkem snižujícím bezpečnostní hrozbu, kterou představuje pohyb ruských zpravodajských důstojníků v zemích schengenského prostoru.

V roce 2024 BIS s ŘSCP pokračovala ve spolupráci při prověřování osob, které žádají o osvědčení spolehlivosti. Jeho účelem je vyloučit bezpečnostní riziko u fyzických osob žádajících o povolení vstupu do vyhrazených bezpečnostních prostor letiště. V roce 2024 bylo prověřeno přes 20 000 osob, což je ve srovnání s rokem 2023 dvojnásobný počet. Nárůst byl pravděpodobně způsoben zkrácením doby platnosti osvědčení spolehlivosti z pěti let na jeden rok a z toho plynoucí vyšší frekvencí prověřování žadatelů o toto osvědčení.

ŘSCP je pro BIS důležitým partnerem při zařazování cizinců do evidence nežádoucích osob, která je důležitým nástrojem pro zamezení vstupu cizince, který by mohl ohrozit bezpečnost státu, na území ČR.

Standardní spolupráce a pravidelná výměna poznatků probíhala také s dalšími útvary Policie ČR – zejména s Národní centrálou proti organizovanému zločinu (NCOZ) a Národní centrálou proti terorismu, extremismu a kybernetické kriminalitě (NCTTEK).

Spolupráce s dalšími státními orgány a institucemi

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

Spolupráce BIS s NBÚ se realizuje na několika úrovních na denní bázi. V oblasti bezpečnostního prověřování BIS odpovídá na žádosti NBÚ nebo se na průběhu bezpečnostních řízení v oblasti personální a průmyslové bezpečnosti a bezpečnostní způsobilosti aktivně podílí formou zabezpečování informací v prostředí. BIS rovněž zabezpečuje relevantní informace o okolnostech nasvědčujících tomu, že držitelé osvědčení nebo dokladu přestali splňovat podmínky pro jejich vydání.

Nadále probíhá intenzivní spolupráce na opatřeních souvisejících s elektronizací veřejné správy v mezirezortní pracovní skupině „Dopady elektronizace veřejné správy na činnost bezpečnostních složek ČR“, a to zejména s bezpečnostním odborem MV i ostatními zainteresovanými bezpečnostními složkami.



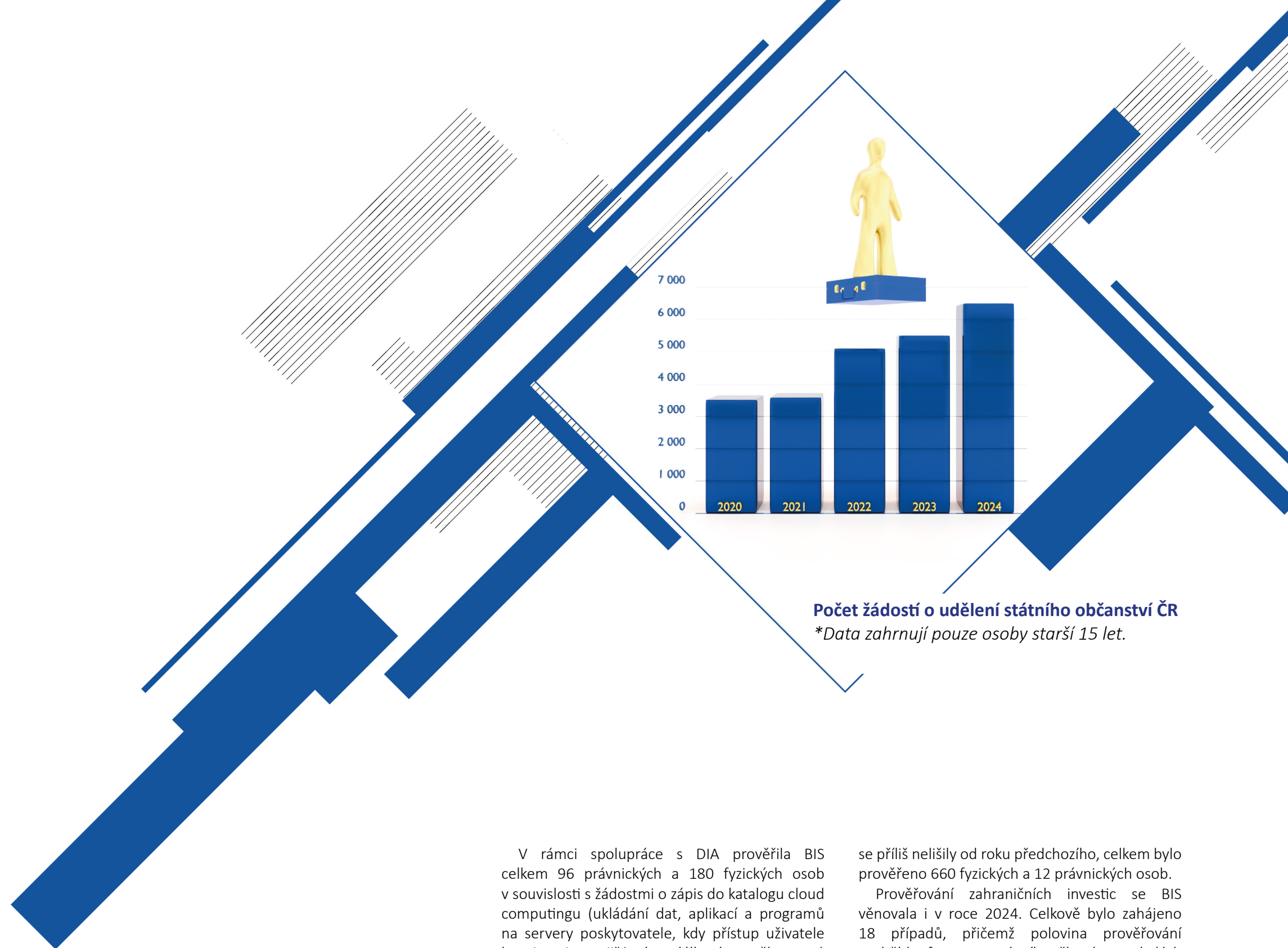


S odborem bezpečnostní politiky MV BIS i v roce 2024 spolupracovala na prověřování fyzických a právnických osob žádajících o udělení povolení ke zprostředkování zaměstnání podle zákona o zaměstnanosti. V souvislosti s trváním válečného konfliktu na Ukrajině pokračovalo i v roce 2024 prověřování osob žádajících podle zákona o branné povinnosti o povolení vstupu do ozbrojených sil Ukrajiny.

Spolupráce s Odborem azylové a migrační politiky MV (OAMP) se týká především prověřování osob žádajících na území ČR o udělení nebo prodloužení mezinárodní ochrany a osob žádajících o pobyťová oprávnění. Stejně jako v letech 2022 a 2023 se válečný konflikt na Ukrajině promítl i v roce 2024 do struktury žadatelů. BIS se vyjádřila k 624 žadatelům o mezinárodní ochranu, největší zastoupení měli žadatelé z Ukrajiny, se značným odstupem následování žadatelé ze Sýrie, Běloruska a Ruska. BIS se dále vyjádřila k cca 150 000 žadatelů o pobyťová oprávnění a k necelým 327 000 žadatelů o udělení nebo prodloužení dočasné ochrany. Oproti roku 2023 došlo u dočasné ochrany k mírnému nárůstu, což svědčí o přetrvávajícím zájmu o tento pobyťový institut.

V rámci zdravotně humanitárního projektu MEDEVAC a Programu humanitární, stabilizační, rekonstrukční a hospodářské asistence Ukrajině BIS prověřila 39 osob. Ve většině případů se jednalo o zdravotnický personál, který se v Česku účastnil odborných stáží. Ve dvou případech se jednalo o doprovod dítěte, které mělo na našem území podstoupit léčbu.

V roce 2024 pokračovala BIS ve spolupráci s Odborem všeobecné správy MV s prověřováním osob starších 15 let žádajících o udělení státního občanství ČR. V roce 2024 se BIS vyjádřila k 6 500 žadatelům, což je o téměř 1 000 více, než v roce předchozím. Kromě výhod spojených s udělením občanství členského státu EU může být důvodem zvyšování počtu žadatelů i aktuální bezpečnostní situace ve světě.



Počet žádostí o udělení státního občanství ČR

**Data zahrnují pouze osoby starší 15 let.*

V rámci spolupráce s DIA prověřila BIS celkem 96 právnických a 180 fyzických osob v souvislosti s žádostmi o zápis do katalogu cloud computingu (ukládání dat, aplikací a programů na servery poskytovatele, kdy přístup uživatele k nim je zajišťován dálkovým přístupem) a opakovaným prověřením společností již zapsaných. V souvislosti s žádostí o vydání akreditace pro správu kvalifikovaného systému elektronické identifikace udělované podle zákona o elektronické identifikaci, byla prověřena jedna právnická osoba a 14 fyzických osob.

Spolupráce s MZV, stejně jako v minulých letech, spočívala ve vyloučení bezpečnostního rizika u osob, které se ucházejí o spolupráci s tímto ministerstvem. Počty prověřovaných osob

se příliš nelišily od roku předchozího, celkem bylo prověřeno 660 fyzických a 12 právnických osob.

Prověřování zahraničních investic se BIS věnovala i v roce 2024. Celkově bylo zahájeno 18 případů, přičemž polovina prověřování proběhla formou správního řízení, ve zbylých případech šlo o zrychlený konzultační proces. MPO několikrát využilo možnost, kterou mu dává zákon o prověřování zahraničních investic, a zahájilo řízení z moci úřední, tedy aniž by investor o prověření požádal. Stejně jako v předchozích letech BIS v oblasti prověřování zahraničních investic vyhodnocovala a předávala MPO podněty získané na základě své vlastní zpravodajské činnosti či monitoringu neveřejných i otevřených zdrojů.



SPOLUPRÁCE NA MEZINÁRODNÍ ÚROVNI

Spolupráce se zahraničními zpravodajskými službami je v řadě oblastí působnosti BIS klíčovým faktorem umožňujícím zabezpečování informací důležitých z hlediska bezpečnosti ČR. Na základě souhlasu české vlády je BIS oprávněna spolupracovat s více než stovkou zpravodajských služeb z více než 80 zemí světa. Informační výměnu a aktivní kontakty BIS rozvíjí především se službami zemí EU a NATO. Na multilaterální úrovni se BIS v roce 2024 zapojovala v rámci všech uskupení, jichž je členem (např. Counter-Terrorism Group a NATO Civilian Intelligence Committee).

Hlavními oblastmi spolupráce BIS se zahraničními zpravodajskými službami byly boj

proti terorismu, kontrašpionáž a subverzní aktivity, proliferace, kybernetická bezpečnost a ochrana utajovaných informací a oblast bezpečnostní způsobilosti. V rámci mezinárodní spolupráce BIS v roce 2024 přijala přes 14 000 zpráv a postoupila více než 2 500 dokumentů. Na strategické a expertní úrovni zástupci BIS absolvovali více než 1 000 mezinárodních jednání.

Evropské zpravodajské služby se v roce 2024 taktéž intenzivně zabývaly ochranou voleb do Evropského parlamentu s cílem zamezit vměšování cizích, často státem sponzorovaných, aktérů. Pokračovala i spolupráce s institucemi EU v rámci evropských iniciativ a reforem.

DODRŽOVÁNÍ SLUŽEBNÍCH PŘEDPISŮ

V rámci BIS působí odbor inspekce, který vyřizuje dožádání orgánů činných v trestním řízení či jiných orgánů státní správy a prošetřuje oznámení, podněty a stížnosti směřující na pracovníky BIS. Odbor inspekce prošetřuje případy podezření ze spáchání jednání, které má znaky přestupku, a kázeňských přestupků, včetně prošetřování mimořádných událostí. Dále má odbor inspekce v případech podezření ze spáchání trestného činu příslušníkem BIS postavení policejního orgánu ve smyslu ustanovení § 12 odst. 2 písm. f) trestního řádu. V případech podezření ze spáchání trestného činu příslušníkem BIS je odbor inspekce dozorován věcně i místně příslušným státním zastupitelstvím.

Naprostá většina šetření podezření ze spáchání kázeňského přestupku nebo jednání, které má znaky přestupku, se i v roce 2024 týkala dopravy, např. 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, které má

znaky přestupku, ze strany příslušníka BIS, byly postoupeny ke kázeňskému řízení.

Z celkového počtu 126 podání, jejichž šetření bylo v roce 2024 ukončeno, byla dvě vyhodnocena jako stížnost na jednání příslušníků BIS, z toho jedna věc byla postoupena příslušnému služebnímu funkcionáři ke kázeňskému projednání. Obsah všech dalších podání byl prověřen a vyhodnocen. Některá podání byla postoupena zpravodajským útvarům BIS k dalším opatřením, jiná byla postoupena např. věcně příslušným orgánům státní správy nebo Policie ČR. Obsahově jsou oznámení od občanů odrazem celospolečenského dění v Česku a také dění v zahraničí, kdy odrážejí situaci kolem válečného konfliktu na Ukrajině a na Blízkém východě.

V právní úpravě kontroly zpravodajských služeb nedošlo v roce 2024 k žádné změně. Nicméně významnou faktickou změnou je, že v červenci 2024 zahájil činnost Orgán nezávislé kontroly zpravodajských služeb České republiky, který byl do zákona č. 153/1994 Sb. zakotven s účinností již od 1. ledna 2018, avšak do roku 2024 nebyl personálně naplněn.



ROZPOČET

Rozpočet BIS pro rok 2024 byl stanoven zákonem č. 433/2023 Sb., o státním rozpočtu ČR na rok 2024. Příjmy stanovené rozpočtem kapitole ve výši 260 000 tis. Kč byly naplněny ve výši 298 094 tis. Kč. Výdaje rozpočtem určené ve výši 2 149 787 tis. Kč byly uskutečněny ve výši 2 257 172 tis. Kč, a to i za přispění zbývajících nároků z nespotřebovaných výdajů, kterými BIS dosud disponovala.



Výdaje BIS za posledních pět let (v tis. Kč)

V objemu čerpání běžných výdajů představovaly nejvýznamnější položku osobní výdaje. Vedle výdajů na platy a příslušenství sem patří také výsluhové nároky vyplácené bývalým příslušníkům po skončení služebního poměru. Výdaje na platy a příslušenství byly v roce 2024 negativně zasaženy opatřeními ke konsolidaci veřejných výdajů, což se projevilo snížením jejich rozpočtované výše o 2 % a následně nutností posílit je z nároků z nespotřebovaných výdajů. Další významnou skupinou běžných výdajů jsou výdaje na speciální techniku specifickou pro činnost zpravodajské služby a zvláštní finanční prostředky určené pro přímou zpravodajskou činnost.

Do běžných výdajů dále patří výdaje provozního charakteru, což jsou zejména výdaje na služby a komodity k zajištění provozních potřeb včetně dodavatelského zajištění oprav a údržby majetku, se kterým BIS hospodář. Výši běžných výdajů ovlivnil i významný nárůst objemu výdajů na získání oprávnění k užití počítačových programů a databází, které obecně souvisí se změnami v oblasti licenčních politik dodavatelů softwaru. Dále BIS musela v roce 2024 pokrýt nárůst výdajů na energetické komodity, který byl důsledkem nových smluvních podmínek po vypršení cenových fixací v roce 2023 a obecně situace na trhu energetických komodit. Výdaje na elektrickou energii vzrostly meziročně o 88,7 % a u plynu o 23 %, výdaje na pohonné hmoty se podařilo udržet téměř na úrovni roku 2023.

Hlavní investiční akcí z hlediska strategického významu pro BIS byly práce na novém zpravodajském informačním systému, u něhož byly provedeny kroky k vypsání výběrového řízení na nového dodavatele. Na základě proběhlých předběžných tržních konzultací došlo k identifikaci vhodného směru pokračování projektu. Vedle toho významná část investic směřovala do pořízení a modernizace zpravodajské techniky a do informačních a komunikačních technologií. Prostředky směřovaly i na nezbytnou obměnu dopravních prostředků. Stavební investice byly po dokončení výstavby technicko-administrativního objektu utlumeny v roce 2024 na nezbytné minimum.

Výši výdajů, které směřovaly v roce 2024 do investic a pořízení technických prostředků, lze považovat za minimální udržovací úroveň, která ale není dlouhodobě slučitelná s potřebou či spíše nutností reagovat na změny v prostředí vyvolané zejména bouřlivým rozvojem informačních a komunikačních technologií. Tyto změny se neobejdou bez potřebného posílení kapacit BIS včetně odpovídajícího personálního a rozpočtového zabezpečení.

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 2024 byly ukončeny čtyři 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
Výroční zpráva za rok 2024

P.O.BOX 31
155 00 Praha 515
Česká Republika
Tel: 235 521 400
Fax: 235 521 715
E-mail: info@bis.cz
Data box: cx2aize

