Bezpečnostní informační služba

Výroční zpráva 2023

Bezpečnostní informační služba

Výroční zpráva

2023

Obsah

Vážení čtenáři,

jsem rád, že mohu opět předložit veřejnosti neutajovanou výroční zprávu o činnosti BIS, tentokrát za rok 2023. Byl to rok v bezpečnostní oblasti mimořádně náročný a v mnoha ohledech velmi turbulentní. Ke zklamání nás všech stále pokračovala neakceptovatelná brutální agrese Ruska proti Ukrajině, na kterou zareagovala demokratická a svobodná část světa podporou bránící se zemi. Budu vždy hrdý na to, že v čele těchto snah je po celou dobu také Česká republika, a to nejen jako stát, ale také v podobě desítek občanských iniciativ.

Rusko zůstávalo stejně jako v předchozích letech zdaleka největší hrozbou pro bezpečnost naší země, ale i celé Evropy a světa. Snaha Ruska přepsat geopolitickou mapu světa a vybudovat „nový světový řád" je v současnosti největší hrozbou a zároveň největší výzvou pro světové společenství. Ruská federace vedle konvenční války proti sousední zemi vede proti západním demokraciím, ke kterým se hlásí také Česká republika, permanentní hybridní útoky. Rusko stále častěji využívá moderní technologie k útokům proti stabilitě, demokracii a svobodě v zemích, které označuje za nepřátelské. Jejich cílem je oslabit podporu Ukrajiny, oslabit důvěru občanů ve stát, podporovat rozdělení společnosti generováním nepřátelské propagandy na všech platformách od tzv. zpravodajských webů, přes masivní působení na sociálních sítích až po kybernetické útoky na kritickou infrastrukturu států.

Moderní technologie v čele s překotným rozvojem umělé inteligence (AI) staví před dnešní společnost a bezpečnostní složky státu obrovskou výzvu. AI může být dobrý sluha, ale velmi zlý pán. Její ovládnutí jedinou státní či soukromou entitou může mít katastrofální důsledky, proti kterým jsou dnešní útoky za pomoci deep fake videí či generováním dezinformačního obsahu jen úsměvnou epizodou. Rusko a Čína tohle velmi dobře chápou a investují obrovské finanční prostředky do této oblasti. Pro euroatlantický prostor je životně důležité nezaostávat a držet s nedemokratickými režimy v této oblasti krok.

Přes vynucenou změnu strategie ruských zpravodajských služeb, způsobenou oslabením diplomatických misí v řadě zemí, je nutné konstatovat, že pokračovaly klasické zpravodajské operace v celé Evropě. Jednu z nich odhalila, zdokumentovala a zastavila BIS ve spolupráci s dalšími evropskými zpravodajskými službami. Vyšetřování případu dnes známého jako Voice of Europe začalo v roce 2023 a pokračuje dodnes. Snaha Ruska ovlivnit nejen veřejné mínění, ale dokonce i přímo volby do Evropského parlamentu, byla brutálním zásahem do suverenity evropských států. Postup proti této zpravodajské platformě byl mimořádným úspěchem BIS, ale jedním dechem je třeba dodat, že není pochyb, že podobných aktivit vyvíjí Ruská federace v Evropě jistě mnohem víc.

Veřejná výroční zpráva je jako vždy z pochopitelných důvodů psána obecně, ale se snahou umožnit veřejnosti nahlédnout do naší práce, seznámit vás s tématy, kterým se Služba věnuje, a upozornit na hrozby, kterým čelí nejen Česká republika, ale i celý svět. Čtení to není místy lehké, ale věříme, že informovaná společnost bude také lépe připravená na to, co nás v předvídatelné budoucnosti čeká.

genmjr. 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:

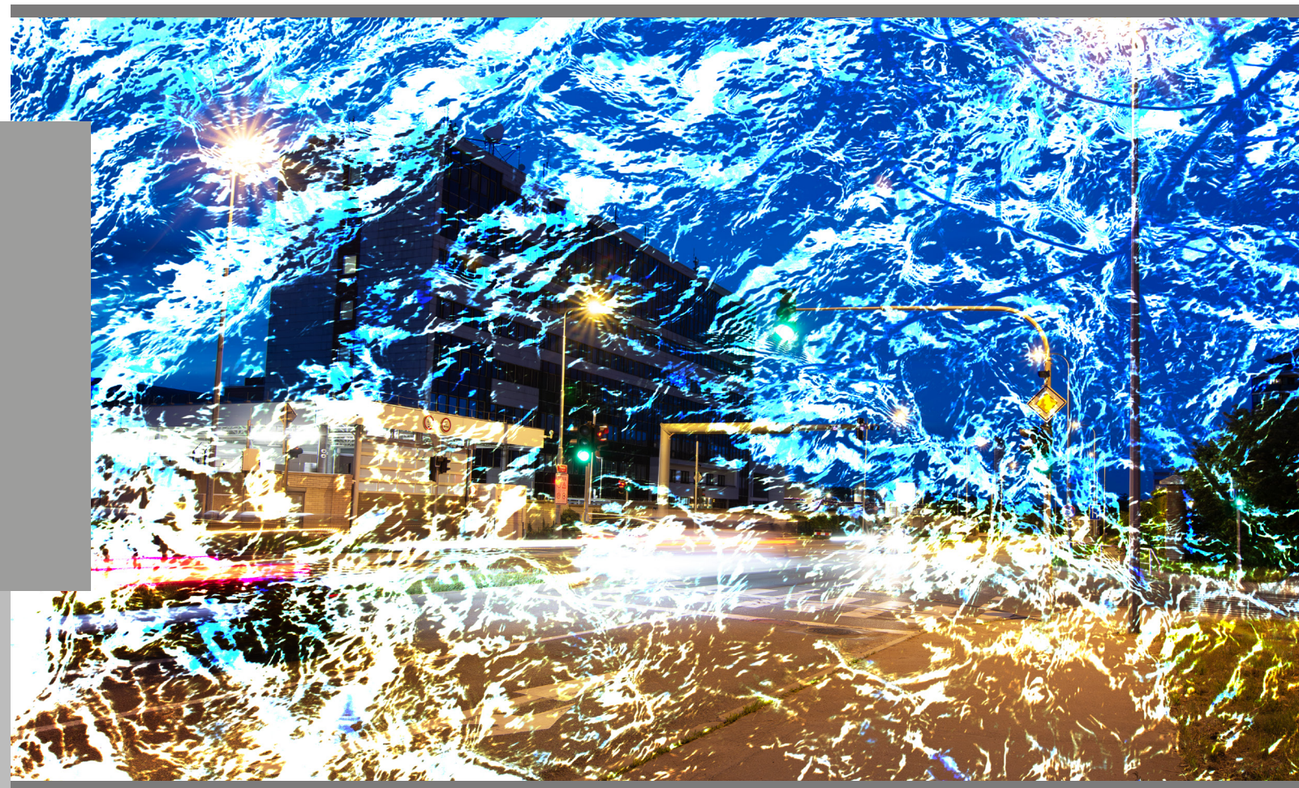
- **o záměrech a činnostech namířených proti demokratickým základům, svrchovanosti a územní celistvosti České republiky,**
- **o zpravodajských službách cizí moci,**
- **o činnostech ohrožujících státní a služební tajemství,**
- **o činnostech, jejichž důsledky mohou ohrozit bezpečnost nebo významné 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.



Zpravodajská činnost a zpravodajské poznatky

Mezi hlavní okruhy zájmu BIS v roce 2023 patřily nepřátelské aktivity Ruska, kybernetické hrozby a obecně rizika (a příležitosti) spojená s používáním nových technologií, mezery v připravenosti státu reagovat na měnící se svět a nepřátelské aktivity Číny.

Rusko, které je v současné době vnímáno především jako agresor ve válce na Ukrajině, představuje pro západní svět včetně Česka hrozbu přesahující tento konflikt. Ruské snahy o polarizaci veřejnosti, šíření dezinformací či sabotážní aktivity představují vážné bezpečnostní riziko, kterému se Česko bude muset věnovat i v předvídatelné budoucnosti.

Dnešní společnost bývá nazývána online – do virtuálního světa se přesouvá naše práce, komunikace s úřady či s bankou či seznamování. Diskutujeme na sociálních sítích, naše děti tráví u mobilů či jiných zařízení velké množství času. Stejnou měrou a rychlostí se do světa informačních technologií logicky přesouvají i rizikové aktivity – snaha obohatit se na úkor druhých, zneužít je či je obelhat a podvést. Oblast kybernetických hrozeb a nových technologií bude jedním ze zásadních bezpečnostních témat budoucnosti.

Uplynulé období ukázalo na nutnost posilovat schopnosti státu a celé společnosti reagovat na krize a nenadálé situace. Jedním z hlavních faktorů důležitých pro toto úsilí je snížení legislativních a byrokratických překážek, které zpomalují zavádění nových technologií a procesů. S tím souvisí také zvýšení schopností a kapacit některých klíčových úřadů. Z hlediska bezpečnosti je připravenost na změny klíčová zejména v energetice, aplikaci sankčních mechanismů, práci s velkými objemy dat, kyberbezpečnosti a obecně při strategických rozhodnutích státu.

Čína (ve smyslu Čínské lidové republiky) představuje zásadní hrozbu pro euroatlantický civilizační okruh včetně Česka. Dlouhodobě usiluje o pozici nejdůležitější ekonomické supervelmoci a vytvoření účinné protiváhy skupině zemí G7. Na rozdíl od svých konkurentů však představuje odlišný socioekonomický koncept založený na komunistické diktatuře, která je rozkladná vůči základním principům naší civilizace, jakými jsou demokracie a volný trh.

BIS se věnovala i dalším hrozbám, které patří do její působnosti, zejména pak hrozbě terorismu, dezinformací, extremismu, energetické bezpečnosti a obcházení mezinárodních sankcí. Bezpečnostní situaci v roce 2023 pak i nadále zásadně ovlivňovala probíhající ruská invaze na Ukrajinu.

V roce 2023 stát pokračoval v posilování své energetické bezpečnosti zvyšováním kontroly nad klíčovou infrastrukturou, získáváním kapacit v této infrastruktuře a snižováním závislosti na dodávkách z Ruska. I přes tato opatření nebylo možné u všech energetických komodit zajistit okamžité nahrazení ruských surovin. U některých alternativních dodávek hrozilo, že nebudou naplněny původně očekávané termíny jejich realizace. Pro případ výpadku dodávek těchto komodit z Ruska byla naplánována a připravena opatření, která by umožnila na vzniklou situaci reagovat, byť by se v některých případech jednalo o opatření nouzové povahy.

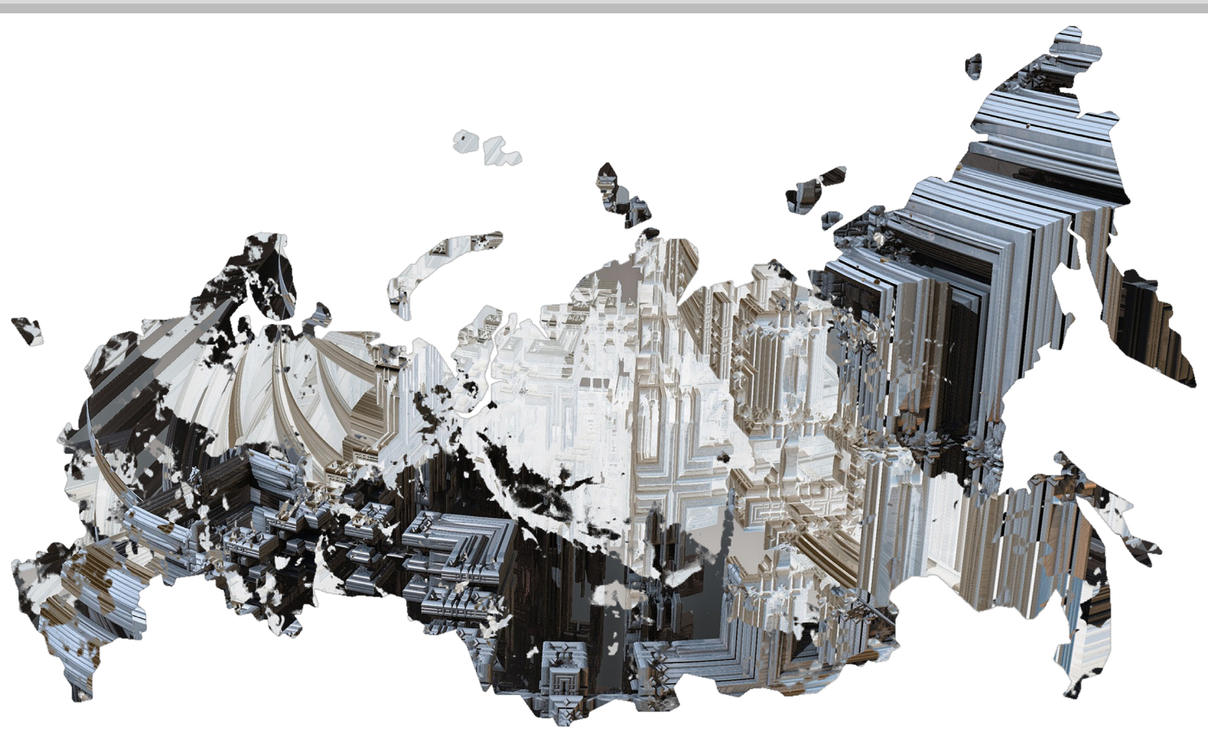
Probíhající ruská invaze na Ukrajinu zásadně ovlivňovala celkovou bezpečnostní situaci v Česku i v roce 2023. Na českém území nadále pobývá několik stovek tisíc ukrajinských občanů prchajících před tímto válečným konfliktem. Přes dílčí problémy spojené např. s integrací ukrajinských dětí do českého vzdělávacího procesu nebo se zaměstnáváním ukrajinských uprchlíků na pozicích, které neodpovídají jejich kvalifikaci, je možné zvládnutí migrační vlny z Ukrajiny, v novodobé historii Česka naprosto bezprecedentní, označit za mimořádný úspěch českého státu a celé společnosti.

České bezpečnostní složky v souvislosti s příchodem vysokého počtu uprchlíků z Ukrajiny nezaznamenaly významnější nárůst kriminality. BIS také nedisponuje informacemi, které by v souvislosti s jejich příchodem svědčily o zvyšování aktivit organizovaných zločineckých skupin v Česku. BIS dosud v souvislosti s uprchlickou vlnou z Ukrajiny nezaznamenala ani pobyt žádné rizikové osoby z hlediska islamistického radikalismu.

V průběhu roku 2023 byla vyhodnocována i další rizika související s tímto konfliktem, zejména pak nebezpečí, že se část zbraní dodaných na Ukrajinu dostane na černý trh a bude pašována zpět do EU. BIS poznatky o tom, že by ve větším měřítku docházelo k organizovaným nelegálním dovozům zbraní dodaných na Ukrajinu zpět do EU, v roce 2023 nedisponovala. Ve střednědobém horizontu lze nicméně možný nárůst nelegálních dovozů vojenského materiálu z Ukrajiny očekávat, což bude klást zvýšené nároky na příslušné státní orgány.

Rusko
trvalá hrozba pro Česko

Přestože Rusko bylo nuceno v letech 2021 a 2022 výrazně zmenšit svou diplomatickou misi v Česku, BIS nadále registruje snahy o obnovení širších rozvědných kapacit pod diplomatickým krytím vysíláním nových zpravodajských příslušníků na naše území prostřednictvím dlouhodobých diplomatických akreditací či krátkodobých víz.



Bezpečnostní informační služba
Výroční zpráva 2023

Na kapacitní ztráty způsobené vyhošťováním příslušníků či spolupracovníků působících v diplomacii reagovaly ruské zpravodajské služby různými způsoby. Řízení ruských špionážních a vlivových operací vůči některým zemím tak ve zvýšené míře probíhá přímo v Rusku nebo ve spřátelených či neutrálních státech. Vzrostlo také riziko, že se osoby navštěvující Rusko ocitnou v hledáčku tamních zpravodajských služeb, které se je pokusí využít ke špionáži proti Česku.

Ruské zpravodajské služby začaly již v předchozích letech ve zvýšené míře používat k verbování a řízení spolupracovníků různé komunikační aplikace (zejména Telegram). Zaznamenané případy potvrdily záměr ruských zpravodajských služeb využívat je mj. při přípravě subverzních útoků proti subjektům ze zemí NATO či EU, které se podílejí na distribuci pomoci pro Ukrajinu. Stejnému riziku jsou vystaveny i subjekty v Česku a stejně tak prvky naší kritické infrastruktury.

V roce 2023 byly zveřejněny další informace potvrzující angažmá jednotky 29155 spadající pod GRU (měla na svědomí přípravu útoků na muniční sklady ve Vrběticích v roce 2014) také v přípravě útoku na munici, která explodovala v bulharském Lovnidolu v roce 2011 (poté, co tam byla převezena ze skladu ve Vrběticích). Riziko vysílání tzv. cestujících důstojníků či spolupracovníků ruských zpravodajských služeb na české území zůstává vysoké.

V oblasti ruského informačního působení na českou veřejnost dominovalo téma poskytování pomoci Ukrajině. To bylo předmětem vlivové operace řízené z Ruska Viktorem Medvedčukem, ukrajinským oligarchou úzce napojeným na kremelský režim. Roli místního koordinátora této operace zastával Artěm Marčevskij, který v Praze zřídil a vedl on-line médium Voice of Europe.

Medvedčuk s skrytým financováním a řízením Voice of Europe usiloval o ovlivňování veřejného mínění v Evropě a vytváření podmínek pro ovlivňování kandidátů ve volbách do Evropského parlamentu v roce 2024. Jeho cílem bylo naplňování ruských zahraničněpolitických zájmů – především těch, které jsou v přímém rozporu se zájmy Ukrajiny. Součástí vlivové sítě byli i spolupracující novináři a vybraní politici ze zemí EU.

Do informačního působení na českou veřejnost jsou dlouhodobě zapojena také ruská státem ovládaná média, mj. Sputnik. Přestože toto médium nemůže kvůli sankcím v EU působit jako regulérní sdělovací prostředek, jeho aktivity v Česku pokračovaly i v průběhu roku 2023, a to prostřednictvím některých internetových stránek a kanálů. Osobám stojícím za jejich provozem se dařilo získávat vyjádření českých politiků či proruských aktivistů, o která následně ve zveřejňovaných příspěvcích opíraly argumenty vyhovující zájmům ruské propagandy.

Výjezdy proruských aktivistů do Ruska zůstaly utlumeny a výrazně se také snížil počet politiků, kteří se jich účastnili. Několik aktivistů se nicméně v roce 2023 v Rusku opakovaně zúčastnilo vzpomínkových akcí v souvislosti s druhou světovou válkou. V organizaci výjezdu do Moskvy v květnu 2023 se angažovala také osoba spojená s ruskou zpravodajskou službou.

Zvýšené riziko zájmu ruských zpravodajských služeb zůstává také během mezinárodních akcí, na něž vyjíždějí politici a aktivisté do nečlenských zemí NATO či EU, a to především do Srbska. Osoby působící v Srbsku (napojené na ruské zpravodajské služby) opakovaně usilovaly o navázání kontaktů s českými dezinformátory.

Průběžné zpřísňování omezujících opatření EU proti Rusku zkomplikovalo přístup ke zboží využitelnému v jeho vojensko-průmyslovém komplexu. Poptávky nicméně pokračují, stejně jako snahy o realizaci dodávek cestou reexportů zejména přes členské země Eurasijské hospodářské unie. V roce 2023 se řada rizikových poptávek týkala zejména obráběcích strojů od českých výrobců. Dosavadní průběh války na Ukrajině prokázal zásadní roli bezpilotních prostředků

Bezpečnostní informační služba
Výroční zpráva 2023

(Unmanned Aerial Vehicle, UAV) pro vedení bojových operací. Pro výrobu UAV, ale i dalších zbraňových systémů užívaných ruskou armádou, jsou přitom ve velké míře využívány součástky od západních výrobců. České společnosti byly v roce 2023 opakovaně oslovovány s poptávkami po leteckých náhradních dílech rizikovými subjekty, které se již v minulosti podílely na netransparentních vývozech do Ruska.

Na počátku roku 2023 byl uskutečněn vývoz několika kusů obráběcích strojů využitelných ve vojenském průmyslu. Jejich deklarovanou cílovou destinací byl Kyrgyzstán. Stroje nicméně do této destinace nebyly dodány, byly přesměrovány do Turecka a následně do Ruska.

Množství omezujících opatření klade výrazné nároky na kontrolní orgány, jejichž kapacity jsou omezené. Řada součástek klíčových pro výrobu ruských zbraňových systémů, na které se vztahují sankce, nespadá mezi kontrolované položky. Tato skutečnost ztěžuje identifikaci cest, kterými se české součástky do Ruska dostávají.

Po částečném poklesu aktivit státních/státem podporovaných ruských kybernetických aktérů z roku 2022 došlo opět k navýšení aktivity, zřejmě s ohledem na zpravodajské potřeby

Ruska. Pokračující izolace Ruska se projevuje na výrazném snížení tradičních operačních možností ruských zpravodajských služeb a kybernetická špionáž proto představuje důležitý nástroj k získávání informací.

Stejně jako v předchozích letech byl v Česku aktivní ruský státní/státem podporovaný aktér, který se věnuje zejména získávání informací z prostředí mezinárodní politiky s důrazem na státy EU a NATO a mezinárodní organizace. Obvyklým způsobem prvotního průniku do počítačových sítí je hromadné rozesílání phishingových zpráv. Zprávy mají obvykle podobu běžné diplomatické korespondence. České Ministerstvo zahraničních věcí bylo cílem některých kampaní, ale zároveň figurovalo i jako podvržený domnělý odesílatel škodlivých zpráv v některých vlnách zaměřených na jiné státy.

V roce 2023 probíhalo šetření aktivit dalšího ruského kybernetického aktéra, kterému je připisována řada útoků vůči Ukrajině, zemím NATO a evropským vládním a energetickým organizacím. Tento aktér prováděl již od druhé poloviny roku 2022 skenování počítačových sítí a informačních systémů různých subjektů české železniční infrastruktury. Útočník rovněž skenoval zranitelnosti počítačové infrastruktury subjektů železniční dopravy a v několika případech se mu podařilo nalezenou zranitelnost zneužít ke krátkodobému průniku do méně významných informačních systémů.

V prvním čtvrtletí 2023 stejný aktér rozšířil svůj záběr i o skenování dalších počítačových sítí, včetně subjektů kritické infrastruktury. Zpětně bylo zjištěno, že některé pokusy o spojení probíhaly již v roce 2022. Pokusy o průnik však

nebyly zjištěny, nehledě na to, že bezpečnostní řešení některých dotčených subjektů pokusy o spojení z infrastruktury útočníka automaticky zablokovala. Podobná kampaň byla zaznamenaná i v dalších zemích EU a NATO. Za přispění BIS a Vojenského zpravodajství se podařilo snížit možné negativní dopady útočníkových aktivit.

Informační infrastruktura nejrůznějších českých institucí a organizací se od začátku války na Ukrajině stává opakovaně cílem tzv. proruských patriotických hacktivistických skupin. Jejich útoky jsou krátkodobé, málo sofistikované a nemají dopad na důvěrnost nebo integritu informačních systémů. Vedle propagandistického využití mohou útoky u obyvatelstva dotčených zemí vyvolávat pocit ohrožení a snižovat důvěru ve schopnosti státu jim zamezit. Medializace takových DDoS útoků je také patrně jejich hlavním cílem v rámci informačně-psychologických operací. Proto se objevují často v souvislosti s konáním voleb a zejména jako „odveta“ u příležitosti událostí zaměřených na podporu Ukrajiny. Příkladem jsou DDoS útoky na weby Českého rozhlasu v červnu 2023 v době pořádání konference Média a Ukrajina nebo říjnová vlna DDoS útoků, která časově korespondovala s konáním druhého summitu Mezinárodní krymské platformy, pořádaného Poslaneckou sněmovnou Parlamentu ČR.

Kybernetická bezpečnost a nové technologie

Používání zařízení, která nejsou dostatečně zabezpečena či aktualizována, představuje riziko zejména pro samotného uživatele, který nad nimi ztrácí plnou kontrolu. Následně může docházet k únikům jeho soukromých dat (včetně hlasových či audiovizuálních nahrávek) a jejich zneužití. Útočník, který ovládne dostatečné množství zranitelných zařízení, může jejich prostřednictvím na internetu provádět průzkumné či přímo škodlivé aktivity. Zranitelná zařízení proto představují riziko i pro všechny sítě připojené k internetu. Příkladem jsou tzv. botnety, tedy různá zařízení sdružená do sítě ovládané útočníkem. BIS opakovaně pozorovala, že taktiku ovládnutí zranitelných zařízení používají v různých podobách i státní kyberšpionážní skupiny, některé dokonce v masovém měřítku. Jejich cílem je zakrytí své identity a zamaskování nelegitimních přístupů, špionáž, ale i exfiltrace dat dalších obětí.

Bezpečnostní informační služba
Výroční zpráva 2023

§

V roce 2023 nebyla v Česku v platnosti žádná legislativa upravující bezpečnost nejrůznějších spotřebitelských produktů schopných komunikovat přes internet (IoT). Na úrovni EU se tato legislativa teprve připravuje (Cyber Resilience Act), nicméně např. USA či Velká Británie již takové požadavky do legislativy zavedly. Pro chytrá zařízení připojená k internetu tak byly stanoveny minimální bezpečnostní standardy, např. zákaz dodávat zařízení s jednotným a slabým výchozím heslem. Ačkoli někteří renomovaní výrobci tak již dnes činí, aktuálně je odpovědnost přenesena primárně na každého uživatele. Ten by měl dbát o to, aby každé jeho zařízení s připojením k internetu bylo aktualizované a zabezpečené, čímž se sníží riziko, že se ho neoprávněně zmocní někdo cizí.

Samostatnou kapitolou jsou vysoce komplexní osobní zařízení typu chytrých mobilů, hodinek, ale i elektroautomobilů a jejich programového vybavení (aplikací), jejichž prostřednictvím lze provádět sběr údajů o poloze, datové i hlasové komunikaci a pořizovat audiovizuální záznamy. Riziko takových zařízení nespočívá primárně v instalaci vysoce sofistikovaného špionážního software, ale i ve shromažďování dat prostřednictvím mobilních aplikací či firmware (neodinstalovatelné aplikace dodané s přístrojem). Uživatelé by proto měli při výběru zařízení – od chytrých hodinek po auta – věnovat zvýšenou pozornost tomu, zda nepochází ze zemí, jejichž politický režim a legislativa zvyšují možnost zneužití dat státní mocí. Obdobné platí i pro využívání cloudových služeb nebo nejrůznějších AI asistentů.

Většina států včetně Česka nemá dostatečné možnosti a kapacity, aby dokázaly pravidelně prověřovat a stvrzovat bezpečnost technologických produktů, obzvlášť v případech, kdy je výrobci umožněna jejich vzdálená správa např. za účelem doručení bezpečnostních aktualizací. Jednotlivé státy tak zpravidla nemají pod kontrolou celý dodavatelský řetězec a musejí se spoléhat na důvěryhodnost výrobce užívaných produktů. V takových případech je klíčové spoléhat se (zejména u prvků kritické infrastruktury) na výrobce pocházející ze zemí se stejným či obdobným politickým, právním či podnikatelským prostředím. To platí ještě silněji v současnosti, kdy je celosvětovým trendem přesouvání provozu softwarových produktů včetně jejich dat do cloudového prostředí namísto jejich uchovávání v rámci vlastní infrastruktury daného subjektu.

Základní bezpečnostní zásady

- Při pořizování zařízení a aplikací věnovat pozornost důvěryhodnosti výrobce a zemi původu s ohledem na data zařízením sbíraná. U IoT zařízení dále zohlednit, že často vyžadují nainstalovanou vlastní obslužnou aplikaci pro mobilní zařízení.
- Pravidelně aktualizovat zařízení připojená k internetu – síťové prvky (routery, switche), telefony, kamery, televize, prvky chytré domácnosti, popř. další IoT zařízení. U řady z nich lze nastavit automatickou aktualizaci, například v noci.
- Vždy změnit výrobcem nastavené výchozí přihlašovací údaje. Používat dvoufaktorovou autentizaci, unikátní a komplexní hesla, popř. zabezpečené bezheslové přihlašování.
- Při výběru aplikací, zejména do mobilních zařízení, věnovat pozornost oprávněním, která aplikace požadují pro svoji činnost, zda jsou nezbytně nutná pro požadovanou funkčnost aplikace, a pravidelně toto nastavení kontrolovat.
- Odinstalovat nepoužívané nebo zřídka používané aplikace.
- V případě pochybností o zabezpečení vyčlenit pro instalaci obslužných aplikací k IoT zařízením v domácnosti jedno zařízení, kterým nebude osobní mobilní telefon.
- Vyčlenit IoT zařízení do samostatné WiFi sítě, resp. samostatného segmentu. Řada domácích routerů má možnost vytvořit tzv. síť pro hosty, ve které zařízení sice mají přístup k internetu, ale jsou izolovaná od ostatních zařízení ve stejné síti.

Vysoká míra globálního propojení se odráží i v kybernetické bezpečnosti a může mít neočekávané i nezamýšlené dopady při tzv. přelivu aktivit (spill-over efekt). Historicky patrně nejznámějším příkladem mohou být škody způsobené ruským počítačovým virem NotPetya z roku 2017, který byl vytvořen k destrukci na Ukrajině, ale způsobil škody v globálním měřítku. Dalším příkladem může být vyřazení pozemních stanic satelitního systému VIASAT/KA-SAT z provozu v den zahájení ruské invaze na Ukrajinu v roce 2022 a nejnověji přeliv izraelsko-palestinského konfliktu do českého kybernetického prostoru.

K tomu došlo v listopadu 2023 během globální kampaně propalestinského aktéra CyberAv3ngers. Ten v reakci na probíhající konflikt zneužil kritickou zranitelnost zařízení izraelského výrobce UNITRONICS používaných pro průmyslovou automatizaci. Následkem útoku displej zařízení namísto stavových informací zobrazoval vzkaz útočníka. V Česku se to týkalo několika zařízení ve vodárenském sektoru a energetice. Přestože šlo o jeden z mála zaznamenaných úspěšných útoků proti průmyslovým systémům (ISCS/SCADA) v sektorech spadajících do kritické infrastruktury, neměl závažný dopad. Mimo jiné proto, že napadené systémy byly přímo připojeny do internetu, zatímco průmyslové řídící systémy v produkčním prostředí kritické infrastruktury takovou přímou a nezabezpečenou konektivitu zpravidla nemají.

Rok 2023 byl přelomovým pro umělou inteligenci. Technologický pokrok zejména v oblasti generativní umělé inteligence spojený s vyšší uživatelskou přívětivostí umožnil proliferaci syntetických médií (deepfakes) do běžného informačního prostoru.

BIS experimentálně ověřovala možnosti vytváření syntetického obsahu, který by byl přizpůsobený českému prostředí. Zlepšování velkých jazykových modelů potvrdilo, že vzniku syntetického textu v masivním měřítku již nic nebrání. Zároveň je syntetický text téměř nemožné odhalit. Zatímco u vizuálního obsahu je stále možné forenzní analýzou odhalit artefakty automatizované manipulace, text produkovaný velkým jazykovým modelem je zaměnitelný s lidským výstupem. Pro neexistenci vstupních bariér a nízkou detekovatelnost považuje BIS tento typ syntetického média za aktuálně nejrizikovější.

Jako druhé nejrizikovější syntetické médium hodnotí BIS syntetický hlas. Lze očekávat, že volně dostupné nástroje budou velmi brzy schopny vytvořit hodnověrný hlasový klon v českém jazyce.

Přes veškerou pokročilost a aktuální dostupnost technologií nebylo využití syntetických multimédií ve vlivových kampaních v ČR doposud zaznamenáno. V zahraničí, kde k tomu již došlo, byl nicméně dopad jejich využití velmi malý.

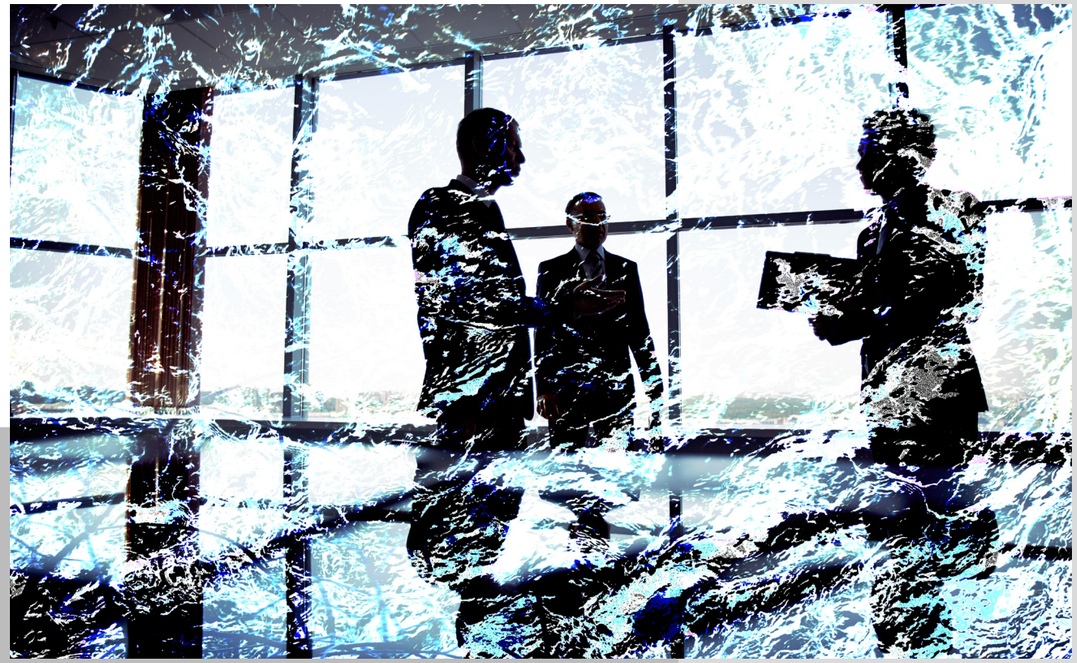
Výzvy pro připravenost státu reagovat na měnící se svět

Česko a celý západní svět procházejí výraznými technologickými, ekonomickými a společenskými změnami, které mají významný dopad i na bezpečnost a práci zpravodajských služeb. Aby státy mohly na tyto změny reagovat a potenciálně je využít, musí být adaptabilní a připravené na rychle se měnící prostředí, což platí i pro jejich instituce.

Válka na Ukrajině byla katalyzátorem systémových změn v mnoha aspektech fungování státu. Významný dopad měla např. v oblasti ekonomických zájmů státu, zejména v sektoru energetiky. Nutnost rychlé reakce na překotný vývoj v ekonomice ukázala na nevyrovnanou připravenost státu na nastalé změny. Zatímco soukromé subjekty se v této situaci rychle zorientovaly a obratem se snažily využít nové podmínky (např. nové podpory v energetice) pro maximalizaci vlastního užitku, státní sektor se potýkal s řadou problémů pramenících zejména z nedostatečného odborného a personálního zázemí. Regulatorní orgány nejsou často ochotny jít do střetu s regulovanými subjekty, ať už z důvodu lhostejnosti, liknavosti, nebo právě nedostatku pracovníků. Takové jednání mělo i konkrétní dopady v oblasti regulace, kdy v některých případech probíhala kontrolní činnost pouze formálně, bez detailní analýzy či náležité kontroly dat vykázaných regulovanými subjekty.

Kapacity veřejné správy

Zmíněný nedostatek odborníků se sice plně ukázal v souvislosti s dynamikou změn v posledních letech, nicméně jedná se o dlouhodobý jev, se kterým se potýká velká část stání správy. Největší problém to činí v oblasti IT, ale týká se mnoha dalších oblastí, kde stát prohrává souboj o odborníky se soukromým sektorem. To velmi často vede k outsourcování důležitých rolí státu na třetí subjekty. Takové subjekty jsou pak obvykle ve střetu zájmů, kdy na jedné straně se podílí na přípravě podkladových materiálů a na straně druhé jsou zároveň následně adresáty legislativních norem vzniklých na základě těchto podkladů.



V roce 2023 BIS zaznamenala několik případů zcela flagrantního střetu zájmů pramenícího právě z neschopnosti státu dostatečně konkurovat soukromým zaměstnavatelům. Zástupci některých státních institucí přijímali finanční prostředky pro dorovnání svých nízkých platů ve státním sektoru od třetích subjektů. Takové subjekty se přitom ucházely o veřejné zakázky instituce daného zaměstnance nebo na ně měly dopadat legislativní návrhy úřadu zaměstnávajícího takového pracovníka.

BIS v souvislosti se snahou ovlivňovat legislativu či zástupce státu zaznamenala i vzrůstající trend soukromých subjektů využívat pro takové účely různá sdružení či spolky. Ty se sice (alespoň dle názvů či oficiálně prezentovaných obecně prospěšných cílů) tváří jako nezávislá uskupení, ve skutečnosti jsou však pod vlivem zmíněných subjektů a jednají v souladu s jejich partikulárními zájmy.

V některých případech opakovaně využívali nedostatečné schopnosti zástupců státu vykonávat náležitou kontrolu i představitelé státem ovládaných subjektů, kteří i v roce 2023 pokračovali v účelových úpravách obsahu podkladových nebo strategických materiálů, na základě nichž se následně rozhoduje mimo jiné o budoucnosti a dalším rozvoji těchto subjektů.

Dalším příkladem prosazování soukromých zájmů na úkor státu je klientelismus, tedy poskytování neoprávněných výhod vybraným osobám či firmám. K takovým jevům docházelo u veřejných zakázek, výběrových řízení či při přerozdělování veřejných financí spravovaných státními institucemi. V minulosti taková jednání často doprovázelo poskytování přímého protiplnění (korupce), které bylo odpovědnými orgány snáze odhalitelné a postižitelné. To lze v dnešní době označit za překonané. V posledních letech totiž představitelé státních institucí často využívají prosazování partikulárních zájmů různých skupin především k posilování vlastní pozice a zejména k zajištění svého budoucího uplatnění (např. zaměstnání) u takových subjektů. Jejich motivace spočívá především v očekávání budoucího prospěchu, což je ovšem velmi obtížně doložitelné. BIS sklony k takovému jednání paradoxně zaznamenala zejména v případech, kde ve vedoucích pozicích státních orgánů působí silné osobnosti, či v případech, že vedení dané instituce je postaveno na monokratickém principu.

Žádoucí rozšiřování omezujících opatření vůči Rusku přináší pro český systém vývozních kontrol bezprecedentní nárůst vykonávané agendy, aniž by tato skutečnost byla kompenzována přidělením odpovídajících lidských a finančních zdrojů. Instituce zabývající se povolováním vývozů v některých vyspělých státech zaměstnávají technické odborníky na kontrolované položky (jejich identifikaci, zařazení) či mají samostatná oddělení zaměřená pouze na problematiku povolování

vývozů know-how a poskytování odborných znalostí při studiu a vědeckém výzkumu (tzv. nehmotný přenos technologií). Česká státní správa obdobnými kapacitami nedisponuje. Některé státní úřady rovněž čelí nedostatku pracovníků s adekvátní bezpečnostní prověrkou, což omezuje výměnu některých informací se zpravodajskými službami. Rostoucí náklady, které jsou spojeny s prověřováním subjektů, ale zejména se správou a zabezpečením utajovaných dat, povedou nevyhnutelně k debatě o tom, jaké informace je opravdu nezbytné utajovat, popř. na jaké úrovni.

V posledních letech se tak v řadě klíčových oblastí veřejné správy, které jsou naprosto nezbytné pro řádné fungování státu, projevuje nikoliv nadbytek, ale naopak nedostatek kvalitních zaměstnanců. Nedostatečné finanční ohodnocení znemožňuje nábor kvalifikovaných pracovníků, což dále podvazuje schopnost státu reagovat na měnící se globální prostředí. Existují však také útvary a úřední pozice, jejichž činnost je naopak pro fungování moderního státu zbytná. Funkční veřejná správa je nezbytným předpokladem pro funkční stát. A funkční stát je jedinou formou státu, který svým občanům zajistí bezpečnost a osobní svobodu. Bez systémové změny přístupu k české veřejné správě se budou tyto schopnosti v budoucnu snižovat.

Zvládání migrace

BIS dlouhodobě sleduje migrační situaci v Česku i v Evropě a vyhodnocuje informace získané vlastní činností, od zahraničních partnerů i v rámci mezirezortní spolupráce. Vlastní informace o projevech nelegální migrace, které BIS v předcházejícím období získala, nemají parametry bezpečnostní hrozby. Migrační trendy nicméně směřují k růstu počtu imigrantů přicházejících do Evropy. Česko, stejně jako další země EU, čelí vlivu dlouhodobých push faktorů ve zdrojových zemích migrace (nízká úroveň a nestabilita životních standardů, válečné, náboženské, národnostní střety, politické tlaky) i pull faktorů v cílových zemích (politická stabilita, ekonomická prosperita, kvalita života, společenská a osobní svoboda, vnitřní bezpečnost), které přivádějí imigranty na naše území. Reálné možnosti oslabení push faktorů jsou omezené a změny pull faktorů nežádoucí.

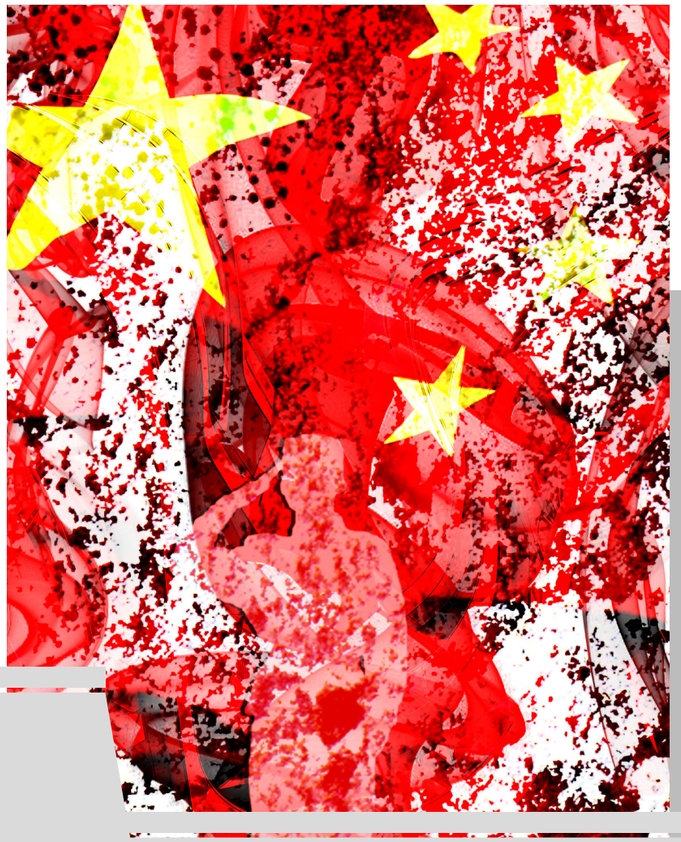
Administrativní řešení migrace spočívající v restrikci legálních možností migrantů, jak do Česka vstoupit a pobývat zde, proto budou mít jen krátkodobý efekt a povedou k přesouvání cizinecké agendy z působnosti státu do sféry neregulérních či přímo nelegálních aktivit různých zprostředkovatelů, agentur a společností parazitujících na migrantech. V případě zvýšeného přílivu osob si stát navíc není schopen zajistit dostatečné informace o žadatelích o pobytová oprávnění, což je mimo jiné způsobeno omezenou kapacitou příslušných úřadů. Klíčová je pak schopnost veřejného sektoru vytvářet podmínky pro aktivní integraci migrantů, což působí nejen jako důležitý prvek prevence před radikalizací, ale přispívá i k celkové společenské soudržnosti. Zvládnutý proces integrace lze opětovně dokumentovat na úspěšném začleňování Ukrajinců do české společnosti.

Ochrana kritické infrastruktury

Česko doposud pracuje na budování a posilování funkčního systému ochrany kritické infrastruktury, který bude bránit sběru informací ze strany nepřátelských států a snižovat riziko sabotáží. Jeho cílem je, aby poznatky o případných bezpečnostních incidentech byly systematicky sbírány a analyzovány. Zkušenosti z řady západních zemí a ostatně i případ českých Vrbětic potvrzují obavy BIS, které pramení ze schopností a vůle některých nepřátelských zemí provádět na našem území sabotáže mající rozličnou podobu. Schopnost státu na obdobné hrozby rychle a efektivně reagovat bude pro jeho bezpečnost v budoucnosti klíčová.

Čína - velké bezpečnostní téma současnosti

Demokratickým světem rezonuje sousloví čínská hrozba. Zatímco však jiní aktéři v čele s Ruskem sami definují to, čím nás ohrožují, zejména pak veřejně páchanými zločiny a otevřeně deklarovanými nenávistnými záměry, u Číny (myšleno Čínské lidové republiky) je pochopení nezbytnosti bránit se jejímu vlivu obtížnější. To, že aktuálně nevnímáme přímou čínskou vojenskou hrozbu namířenou proti nám, nezaznamenáváme hrozbu terorismu mířenou z Číny a ani se neobáváme masivní nelegální migrace z tohoto teritoria, neznamená, že pro nás Čína nepředstavuje iminentní a zásadní hrozbu.



Čína je demokratickému světu vzdálená, a to nejen geograficky (v případě euroatlantického prostoru), ale především mentálně. O to více musíme vynaložit úsilí, abychom pochopili její záměry a cíle, modus operandi a nástroje, které pro budování své kýžené pozice světového lídra používá. Stejně jako Čína nikdy nečiní rozhodnutí, které by nepropojovalo ekonomické zájmy s politikou, což je jeden ze základních postulátů Komunistické strany Číny, tak ani my nesmíme zapomínat na globální kontext, jehož jsme součástí. Je to o to náročnější, že s Čínou budeme muset vést dialog a že není možné s ní nespolupracovat.

Hrozbu nepředstavuje čínský lid, byť jeho postupná sílící indoktrinace prostřednictvím informační izolace je vysoce rizikovým faktorem, a už vůbec ne čínská kultura a tradice. Naše technologická a strategicko-surovinová závislost na tomto autokratickém režimu, který má globální ambice na vytvoření účinné protiváhy zemím G7, je nicméně stav, na který je nutné aktivně reagovat. Dostávat se do orbitu vlivu Číny totiž znamená postupně odevzdávat technologické a strategické know-how systému představujícímu odlišný socioekonomický koncept založený na komunistické diktatuře, která je rozkladná vůči základním principům naší civilizace, jakými jsou demokracie a volný trh.

Čína svůj geopolitický vliv rozšiřuje dravými úvěrovými a obchodními praktikami užívanými celosvětově, rozvojovou iniciativou se snahou politicky si zavázat chudé země globálního Jihu a ekonomickou dominancí v nekompromisním ovládání světového trhu se strategickými nerostnými surovinami. Česko – člen EU, NATO a řady dalších mezinárodních platforem – nestojí v tomto globálním soupeření stranou. Naše stanovisko či podpora nejen vůči Číně, ale také vůči Tchaj-wanu, který je pro Peking bytostně neuralgickým bodem a který považuje za své území, má pro Čínu nezanedbatelný význam.

Česku se nevyhýbají čínské útoky na postpandemické pokusy západního světa o diverzifikaci dodavatelských řetězců, které mají přímý dopad i naši ekonomiku, kyberšpionáže usilující o extrahování strategických dat a v konečném důsledku ani gradující vojenské hrozby v Indo-Pacifiku. V globalizovaném světě by totiž případná anexe Tchaj-wanu znamenala i přímé důsledky pro Česko – odstavení dominantní světové produkce polovodičů by přineslo drastickou inflaci a nedostatek některých produktů. Čínská hrozba roste i v kontextu pro naši bezpečnost zásadní války na Ukrajině. Osa

KLDR – Čína nepřetržitě kultivuje vztahy s Ruskem, které jej v současném konfliktu výrazně posilují.

Čínský zastupitelský úřad se na našem území logicky zaměřuje na získávání informací o české politické scéně. Příslušníci čínských zpravodajských služeb kultivovali vztahy s vlivnými osobami a BIS zaznamenala zájem Číny o potírání aktivit spojených s tzv. pěti jedy, které vnímá jako hrozbu pro stabilitu vlády komunistické strany. Kdykoliv se čínská strana dozví o nějaké akci v Česku, na které by se mohly objevit negativní komentáře o Číně, začne podnikat systematické kroky s cílem získat citlivé informace o místě konání, obsahu a účastnících události.

Významnou úlohu hraje čínská komunita, protože může být kdykoli využita mimo jiné i k podpoře utajovaných operací. Takové operace probíhají i v Česku, kde je provádějí vedle zpravodajských služeb také členové čínských stranických organizací Mezinárodní oddělení Ústředního výboru Komunistické strany Číny (IDCPC) a Oddělení práce na jednotné frontě (UFWD).

Cenný zdroj zájmových informací a kontaktů představuje také akademická sféra. Čína využívá české akademiky k získávání neveřejných informací i k lepší orientaci v českém prostředí. K tipování i prvotnímu oslovení akademiků Čína nejčastěji využívá profesní sociální síť LinkedIn. Za účelem navázání kontaktu používají čínské zpravodajské služby krycí profily zaměstnanců fiktivních konzultantských či headhunterských společností nejčastěji se sídlem v Singapuru či Hongkongu. Pod záminkou navázání odborné spolupráce a s příslibem finanční odměny žádá od akademiků tvorbu zpráv a studií z oblastí odpovídajících politickým zájmům Číny. Tyto studie představují zpravidla předstupeň k další spolupráci spočívající v dodání konkrétních informací. Další kultivace zahrnuje mimo jiné pozvání do Číny, přičemž čínská strana hradí veškeré náklady.

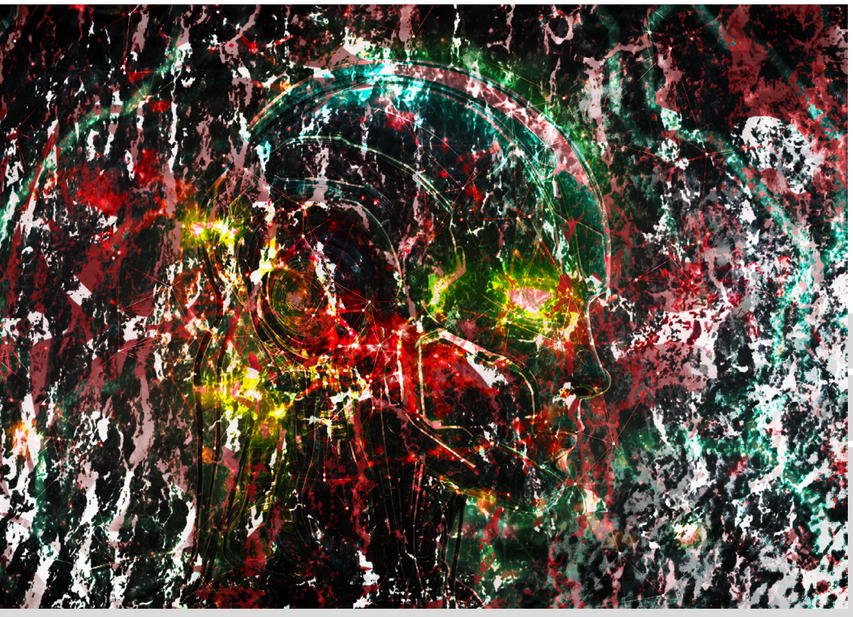
Oficiální pozvání k návštěvě Čína tradičně využívá k vytváření kontaktní sítě osob, které se jí cítí být zavázány a v budoucnu mohou být nakloněny podpoře čínských zájmů v Česku. Pozvání cílí na bývalé i stávající politiky, zástupce státní správy i samosprávy, významné akademiky i významné podnikatele. Tyto výjezdy jsou rizikové nejen s ohledem na nebezpečí oslovení čínskými zpravodajskými službami či využití návštěvy k propagandistickým účelům, ale také kvůli vzniku závazku za čínskou pohostinnost, který může být čínskou stranou v budoucnu využit.

Pro Čínu je důležitý její obraz před domácím publikem i zahraničními partnery, proto se dlouhodobě snaží o potírání jakýchkoliv informací poškozujících budovanou image hegemona prosazujícího celosvětový mír a pořádek. V průběhu roku 2023 tak BIS sledovala pokračování spolupráce české a čínské mediální scény, při které dochází k distribuci čínské produkce zejména do menších českých televizních stanic. Čínské pořady slouží k ovlivnění vnímání Číny českou veřejností a zobrazují jen pozitivní stránku komunistického režimu, zatímco pošlapávání lidských práv, utlačování národnostních menšin či teritoriální agrese jsou zcela vynechány či popírány.

Čína pokračuje ve svém úsilí získat pokročilé technologie a know-how, kterými disponují západní země, a to za využití všech prostředků včetně špionážních aktivit. Lze vysledovat zájem Číny a její podporu joint venture projektům, při kterých se výrobní proces přesouvá na čínské území, kde je snazší používanou západní technologii odcizit. Dalším tradičním způsobem získání přístupu k západním technologiím a know-how je vysílání čínských studentů na zahraniční univerzity, kde se podílí na vývoji a výzkumu.

V reakci na to pokračuje úsilí EU a NATO neposkytovat Číně zejména technologie z oblasti nově vyvíjených technologií (Emerging Disruptive Technologies, EDTs), mezi které patří pokročilé polovodičové technologie, umělá inteligence, kvantové technologie, biotechnologie, vesmírné technologie, autonomní systémy, pokročilé materiály – nanotechnologie ad. V případě vývozu technologií do Číny hrozí ztráta kontroly nad dalším nakládáním s proliferačně využitelným zbožím. Kromě kontrolního režimu týkajícího se jaderných technologií není Čína členem žádného dalšího mezinárodního kontrolního režimu upravujícího obchody s položkami dvojího užití nebo vojenským materiálem. Riziko, že budou vyvezené technologie využity ve prospěch navýšení kapacit ozbrojených složek, umocňuje strategie čínské vlády propojení civilního a vojenského sektoru. Realizace vývozů čínským subjektům zapojených do reexportů vede také k navýšení výrobních kapacit v zemích jako Írán nebo Rusko.

V kyberprostoru v roce 2023 došlo k významnému poklesu spear-phishingových útoků přisuzovaných konkrétní čínské kyberšpionážní skupině, které byly vedeny vůči českým státním institucím v době po zahájení ruské invaze na Ukrajinu. K tomuto poklesu pravděpodobně došlo v důsledku změn v cílení této skupiny, která se začala zaměřovat na cíle v jiném regionu. Avšak tento pokles rozhodně neznamenal úbytek jiných sofistikovaných špionážně motivovaných kybernetických útoků vůči českým státním institucím.



Kybernetické útoky přisuzované čínským aktérům jsou zpravidla velmi sofistikované. Často dochází ke zneužívání zranitelností v softwarových produktech, přičemž v některých případech se jedná o zranitelnosti tzv. nultého dne, na které v době útoku neexistují účinné záplaty. Zneužitím takové zranitelnosti se útočníkovi podaří uskutečnit prvotní vstup do sítě oběti, kterou dále dokáže efektivně využít pro svůj prospěch. Začne se v ní nepozorovaně pohybovat, prozkoumávat vnitřní prostředí a její nastavení. V dalších fázích útoku zpravidla dochází k zajištění perzistence v síti pomocí dodatečně nainstalovaných škodlivých nástrojů nebo mazání stop. V závěrečné fázi útočník ze sítě exfiltruje zájmová data na jím ovládané servery, což se mu v případě nedostatečné nebo opožděné detekce ze strany oběti může dařit i opakovaně. Jedna takto vhodně zneužitá zranitelnost může ovlivnit nejen organizaci, která se stala obětí kybernetického útoku, ale i další subjekty, které jsou s ní v pracovním, obchodním či jiném vztahu.

Další důležitá témata zpravodajského zájmu

BIS v průběhu roku 2023 nezjistila bezprostřední ohrožení islamistickým terorismem na území Česka. Projevy islamistické radikalizace BIS prověřovala pouze u několika mála jedinců, což představovalo pokračování pozitivního trendu z posledních let. V Evropě se úroveň hrozby islamistického terorismu ve druhé polovině roku 2023 začala zvyšovat. Spíše než o náhodný výkyv šlo o důsledek oživení tradičních mobilizačních vlivů, konkrétně četných případů znesvěcování Koránu a eskalace izraelsko-palestinského konfliktu. Úroveň hrozby ovlivňoval i další faktor, a sice zájem afghánské odnože tzv. Islámského státu (IS) motivovat k útokům v Evropě. Při nedostatku vlastních kapacit k vyslání vycvičených teroristů do Evropy se IS snažil útoky podněcovat skrze online komunikaci. Cíleně oslovoval primárně osoby z ruskojazyčných diaspor v Evropě, často původem ze střední Asie.

V květnu 2023 přes Česko tranzitoval Kyrgyz prověřovaný evropskými zpravodajskými službami pro kontakty na osoby patřící k IS, přičemž jednu noc strávil v Praze. Mezi jeho kontaktní osoby patřil i Tádžik, který byl v červnu 2023 v Nizozemsku zatčen pro přípravu terorismu. V souvislosti s uvedenou cestou, ani s cestami dalších prověřovaných Středoasiatů přes Česko, nebyla zjištěna riziková činnost na našem území. Tranzit rizikových osob přes Česko není novým jevem, v roce 2023 ale takových případů přibylo.

Rok 2023 nepředstavoval z pohledu ideologické orientace české muslimské komunity žádnou změnu. Ta si zachovávala umírněný charakter, který narušilo jen několik individuálních projevů jedinců s radikálnějšími sklony, jejichž projevy absolutně neodpovídaly většinovým názorům českých muslimů. Komunitu mohl v roce 2023 v otázce potenciální radikalizace nejvýrazněji ovlivnit konflikt mezi Izraelem a teroristickou organizací Hamás. Zájmové arabské a muslimské komunity ve většině případů podporovaly Palestince, nicméně podporu hnutí Hamás vyjádřilo v průběhu konfliktu jen několik jednotlivců a v komunitě tento názor nepřevládal.

S narůstající délkou trvání konfliktu a zvyšujícím se počtem obětí na straně Palestinců se postupně začala objevovat kritika českých státních představitelů a médií, která je obviňovala

z jednostranné podpory Izraele. Palestinci žijící v ČR se věnovali reálné pomoci svým blízkým zasaženým situací v Gaze, a tak dominantní roli při propalestinských a protiizraelských akcích převzali již od začátku především levicově orientované subjekty a aktivisté. Ti obviňovali Izrael z dlouhodobého útlaku Palestinců v Gaze, kolonialismu a genocidy. Ve srovnání s obdobnými demonstracemi ve světě byl průběh akcí v Česku poklidný.

Jedním z významných trendů ovlivňujících hrozbu islamistickým terorismem je autoradikalizace prostřednictvím internetu. Dlouhodobě klesá věk radikalizovaných osob, přičemž jde nejen o mladistvé, ale i o děti ve věku okolo 13 let. Dalším rysem je poměrně

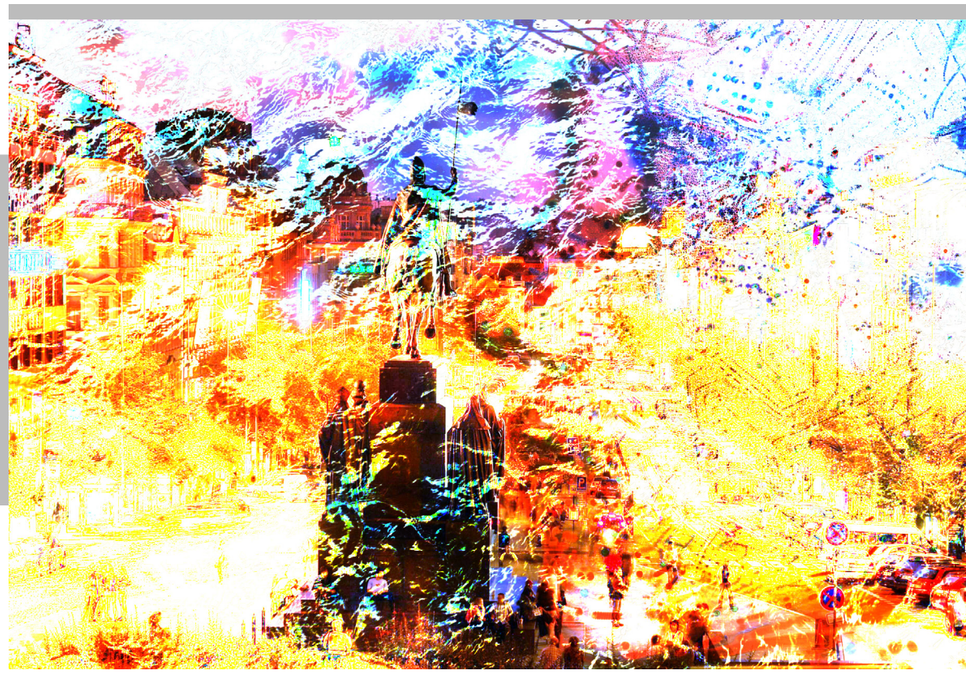
rychlá radikalizace (řádově jde o týdny až měsíce) pod vlivem zahraničních událostí a jejich jednostranné či účelové intepretace, jako např. znesvěcování náboženských symbolů či situace v pásmu Gazy. Důležitým faktorem je rovněž skutečnost, že některé radikalizované osoby trpí psychickou poruchou. V reakci na tento vývoj dochází k zintenzivnění mezinárodní a hlavně mezirezortní spolupráce v oblasti analýzy rizik radikálních projevů na internetu.

Dezinformační narativy šířené v průběhu roku 2023 se zaměřovaly na válečný konflikt na Ukrajině a s ním provázaná ekonomická a sociální témata. Stejně jako v předchozích letech byly jedním z hlavních kanálů šíření dezinformací webové stránky a sociální sítě. Za výrazný trend lze však označit nárůst popularity sdílení obsahu ve formě videí, což způsobilo zvýšení vlivu platforem jako je např. Youtube či TikTok.

Aktivity české dezinformační scény zůstávaly nadále z převážné části autonomní, bez koordinace či řízení cizím aktérem. BIS nicméně zachytila několik případů zneužití tuzemských alternativních médií či dezinformačních aktivistů k šíření proruských narativů v českém informačním prostoru. Např. již v roce 2022 takto ruský vlivový agent dlouhodobě působící v Česku zajistil na žádost jednoho z nejvyšších orgánů ruské státní moci šíření ruské propagandy. Informační kampaň s rozpočtem několika tisíc eur zpochybňovala smysluplnost poskytování pomoci Ukrajině nebo sankcí EU a byly do ní zapojeny některé veřejně známé osobnosti.

V tomto prostředí působily rovněž platformy přímo napojené na Rusko, které šířily prorusky orientované dezinformace např. prostřednictvím upravených lživých videí. Takovéto video bylo do českého informačního prostředí vneseno např. během prezidentských voleb v lednu 2023 telegramovým kanálem „neČT24“ s cílem zdiskreditovat jednoho z prezidentských kandidátů.

Extremistická scéna jako celek nepředstavovala významné bezpečnostní riziko. Počet osob inklinujících k násilným projevům byl marginální. Potenciálně nebezpeční zůstávali sociálně neukotvení jedinci, u nichž hlavním motivem nenávistných projevů není ideologie, ale spíše fascinace násilím. Populární je v této souvislosti zejména Siege kultura (extrémní forma neonacismu). Až na výjimky se tyto osoby angažují pouze ve virtuálním prostoru. Česká domobranecká a paramilitární scéna se potýkala s personální vyprázdněností a počet jejích členů se nadále snižoval. Přetrvávající a nejnebezpečnější aktivitou spojenou s činností domobranců byla snaha o výrobu nelegálních palných zbraní a výbušnin.



V prosinci 2023 došlo na Filozofické fakultě Univerzity Karlovy v Praze k útoku aktivního střelce, při kterém pachatel zastřelil 14 osob a desítky dalších zranil. Tento čin byl nejtragičtější událostí svého druhu v moderní české historii. Útok byl ukončen sebevraždou pachatele. Těsně před útokem vrah zabil i svého otce a dříve zastřelil v Praze Klánovicích dvaatřicetiletého muže a jeho dvouměsíční dceru. Ti byli náhodnými obětmi, bez jakéhokoliv vztahu k pachateli.

Dle získaných poznatků šlo o individuální útok osamělého střelce. Skutek nebyl teroristicky či extremisticky motivovaný, ale jednalo se o kriminální čin jednotlivce. Vrah nebyl napojen na žádnou extremistickou či teroristickou skupinu, což velmi komplikovalo jeho včasnou identifikaci. Tato tragédie ukázala, že ani Česku se podobné trestné činy nevyhýbají. Přestože je nelze zcela eliminovat, lze alespoň minimalizovat jejich důsledky systémovými opatřeními (ochranou měkkých cílů, nácvikem chování potenciálních obětí, systémem včasného varování, adekvátní zbraňovou legislativou atp.). Nezbytná je také úzká kooperace orgánů státní správy a bezpečnostních složek, do které je BIS rovněž zapojena.

Spolupráce se zpravodajskými službami ČR a ostatními státními orgány

Spolupráce se zpravodajskými službami ČR

BIS v roce 2023 zaslala Úřadu pro zahraniční styky (ÚZSI) více než 100 informací a Vojenské zpravodajství (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 akreditaci diplomatického zástupce a pracovníka diplomatické mise cizího státu je jedním z nástrojů, jak lze snížit bezpečnostní riziko plynoucí z nepřátelských aktivit osob působících v diplomatických službách na našem území. Tato spolupráce plynule pokračovala i v roce 2023, kdy bylo prověřeno 199 diplomatických zástupců, pracovníků diplomatických misí a jejich rodinných příslušníků, což znamená mírný nárůst ve srovnání s rokem 2022.

Probíhala i spolupráce s Ministerstvem obrany, resp. VZ, v oblasti rozvoje agendového informačního systému pro potřebu zpravodajských služeb.

BIS s VZ a ÚZSI dále spolupracovala při cvičení orgánů krizového řízení EU či NATO.

Spolupráce s Policií ČR

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

BIS, stejně tak jako v minulých letech, spolupracovala s Ředitelstvím služby cizinecké policie (ŘSCP) na prověřování žadatelů o krátkodobá a dlouhodobá schengenská víza. V roce 2023 BIS prověřila téměř 1 700 000 žadatelů o tato víza. Jedním z faktorů, který ovlivnil počet prověřovaných žádostí o vízum, bylo zpřísnění vízové politiky vůči Rusku, ke kterému EU přistoupila po zahájení konfliktu na Ukrajině. V Česku byla přijata přísná pravidla pro podávání žádostí o vízum ze strany ruských a běloruských občanů, což mělo za následek nejen snížení jejich počtu, ale i omezení možnosti zneužití víz osobami spolupracujícími s cizí mocí. Ke zpřísnění pravidel patřilo i opatření, na základě kterého se BIS může vyjadřovat k žádostem o víza ruských občanů, které jsou podány na zastupitelských úřadech všech členských států EU. V roce 2023 byla zamítnuta více než 4 % z celkového počtu víz podaných občany Ruska, zatímco v roce 2020 se jednalo o pouhé promile. Česká opatření patří mezi nejpřísnější v Evropě a významně přispívají ke snížení bezpečnostní hrozby, kterou pohyb ruských zpravodajských důstojníků představuje.

V roce 2023 BIS s ŘSCP pokračovala ve spolupráci při prověřování osob pro účely zákona o civilním letectví, které žádají o osvědčení spolehlivosti. Jeho účelem je vyloučit bezpečnostní riziko u fyzických osob žádajících o povolení vstupu do vyhrazeného bezpečnostního prostoru letiště.

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

Spolupráce s Národní centrálou proti organizovanému zločinu (NCOZ) a Národní centrálou proti terorismu, extremismu a kybernetické kriminalitě (NCTEKK) spočívala ve výměně poznatků zejména po linii problematik významných ekonomických zájmů, terorismu, organizovaného zločinu, proliferace a kybernetické bezpečnosti.

Spolupráce s dalšími státními orgány a institucemi

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

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

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. V roce 2023 provedla BIS na základě žádosti NBÚ více než 22 000 evidenčních šetření.

V rámci mezirezortní pracovní skupiny „Dopady elektronizace veřejné správy na činnost bezpečnostních složek ČR“ probíhala s MV a ostatními zainteresovanými bezpečnostními složkami i nadále velmi dobrá spolupráce na

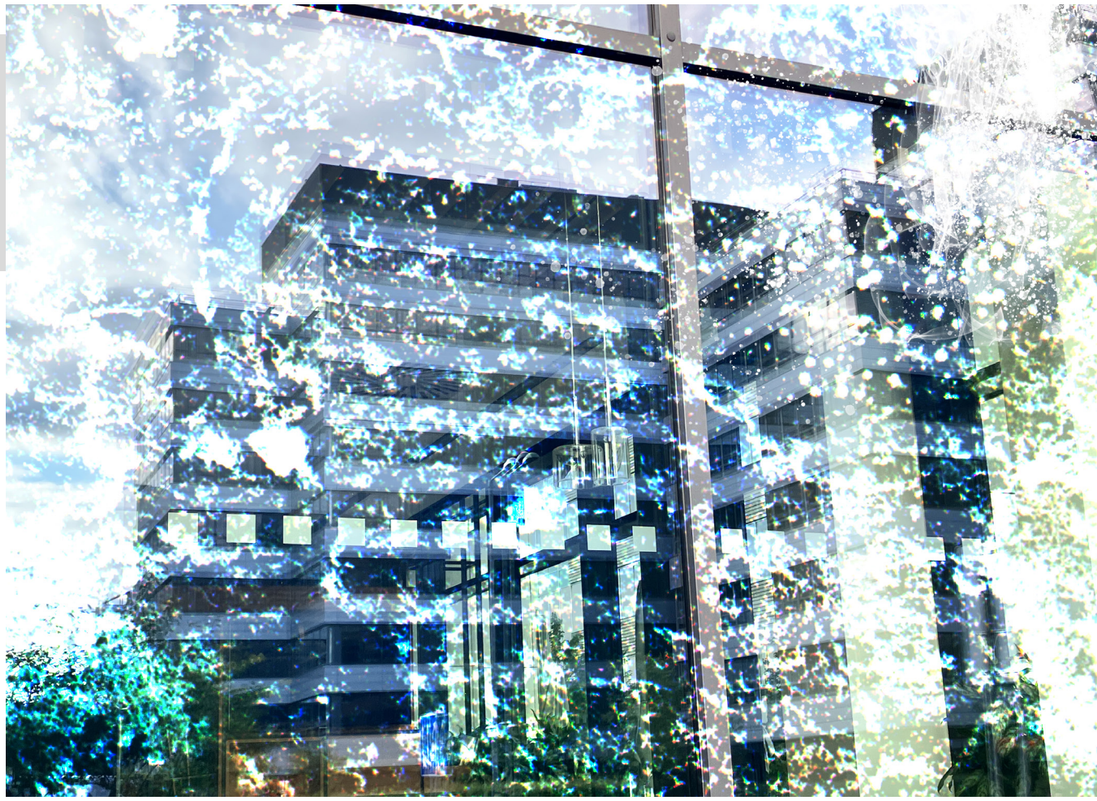
opatřeních souvisejících s elektronizací veřejné správy.

MV a další subjekty napojené na rozpočet jeho kapitoly dlouhodobě poskytují BIS na základě dohody některé služby v oblasti elektronických komunikací, činnosti v oblasti požární ochrany, bezpečnosti a ochrany zdraví při práci, energetiky, vodního hospodářství, životního prostředí a též v oblasti stravování.

V roce 2023 pokračovala spolupráce s MV při vyloučení bezpečnostního rizika u cizinců žádajících o mezinárodní ochranu, pobytové oprávnění a o udělení státního občanství. BIS se také podílela na prověřování právnických a fyzických osob žádajících o povolení ke zprostředkování zaměstnání a pokračovala i v prověřování osob žádajících o povolení vstupu do služeb ozbrojených sil Ukrajiny. Pokračovala i spolupráce dle zákona o elektronické identifikaci a nově i při posuzování žadatelů o zápis do katalogu cloud computingu.

S odborem bezpečnostní politiky MV (OBP MV) BIS i v roce 2023 spolupracovala na prověřování fyzických a právnických osob žádajících o udělení povolení ke zprostředkování zaměstnání podle zákona o zaměstnanosti. Z důvodu přetrvávání válečného konfliktu pokračovalo i v roce 2023 ve spolupráci s OBP MV prověřování osob žádajících dle zákona o branné povinnosti o povolení vstupu do ozbrojených sil Ukrajiny.

Pokračovala spolupráce s MV na prověřování osob žádajících na území ČR o udělení nebo prodloužení mezinárodní ochrany a osob žádajících o pobytová oprávnění. Stejně jako v roce 2022, tak i v roce 2023 měl na strukturu žadatelů dopad válečný konflikt na Ukrajině.

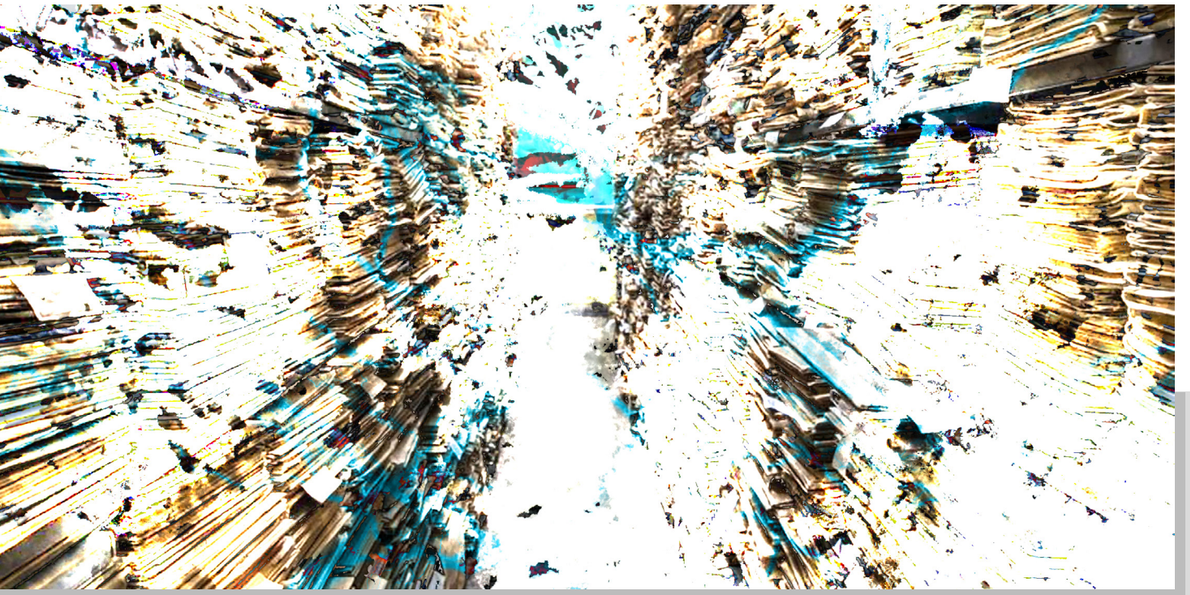


V roce 2023 se BIS vyjádřila k 789 žadatelům o mezinárodní ochranu, kdy největší zastoupení měli žadatelé z Ukrajiny se značným odstupem následováni žadateli ze Sýrie, Afghánistánu, Ruska a Běloruska. BIS se dále vyjádřila k 157 000 žadatelům o pobytová oprávnění a 303 000 žadatelům o dočasnou ochranu.

V souvislosti s ozbrojeným konfliktem na Ukrajině vyvolaným invazí ruských vojsk v roce 2022 a s ohledem na změnu bezpečnostní situace byl u některých osob jejich pobyt v Česku vyhodnocen jako možné bezpečnostní riziko. V několika případech došlo ke zrušení povolení k pobytu a vycestování osob z území.

Při prověřování osob v rámci zdravotně humanitárního projektu MEDEVAC a Programu humanitární, stabilizační, rekonstrukční a hospodářské asistence Ukrajině bylo prověřeno 57 osob. Ve všech případech se jednalo o zdravotní personál, který se účastnil v ČR odborných stáží.

V roce 2023 se BIS v rámci prověřování osob starších 15 let žádajících o udělení státního občanství vyjádřila k 5 500 žadatelů. Údaj je v souladu s dlouhodobým trendem zvyšujícího se počtu žadatelů. V roce 2023 bylo dokončeno opětovné prověření žadatelů, kteří byli ruskými občany, a u kterých nebylo do počátku válečného konfliktu ukončeno řízení.



Významný nárůst negativních stanovisek BIS k žadatelům o udělení občanství z řad občanů Ruska v roce 2023 byl důsledkem změny bezpečnostní situace po zahájení válečného konfliktu.

V průběhu roku 2023 obdržela BIS 50 žádostí o zápis do katalogu cloud computingu (jde o ukládání dat, aplikací a programů na servery poskytovatele, kdy přístup k nim je pro uživatele zajišťován vzdáleným přístupem) dle zákona o informačních systémech veřejné správy, v rámci kterých bylo prověřeno 85 právnických a 182 fyzických osob. BIS v roce 2023 neobdržela žádnou žádost o vydání akreditace pro správu kvalifikovaného systému elektronické identifikace, udělované dle zákona o elektronické identifikaci.

Spolupráce s MZV spočívala ve vyloučení bezpečnostního rizika u osob, které se ucházejí o spolupráci s ministerstvem. Počty prověřovaných osob se příliš nelišily od roku předchozího, celkem bylo prověřeno 555 fyzických a 19 právnických osob.

Již třetím rokem se BIS podílela na prověřování zahraničních investic. V roce 2023 došlo k oživení investic a prověřováním prošel dvojnásobek případů než v roce předchozím. 15 investic prověřovala BIS v rámci konzultačního procesu a šest v rámci řízení. Také systém evropských notifikací zaznamenal nárůst v počtu prověřovaných investic, a to o 14 %. V roce 2023 věnovala BIS zvýšenou pozornost identifikaci investic, které dle zákona nelze uskutečnit bez předchozího povolení Ministerstva průmyslu a obchodu (MPO), ale kde investor řádně a včas o povolení nezažádal. Prioritou bylo sledování vlastnických změn u právnických osob, jejichž koneční vlastníci se ocitli na sankčním seznamu EU. Konkrétní podněty pak BIS řešila v rámci úzké spolupráce s MPO.

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

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

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

Předmětem spolupráce s dalšími orgány státní správy bylo také řešení konkrétních případů v problematice proliferace zbraní hromadného ničení a jejich nosičů a obchodů s vojenským materiálem. Probíhala spolupráce zejména s orgány celní správy, a to jak na úrovni GŘC, tak na úrovni jednotlivých celních úřadů. Pokračovala i spolupráce s orgány celní správy týkající se rizik možných transportů kontrolovaných položek, především vojenského materiálu a položek dvojího použití, do sankcionovaných zemí. V konkrétních případech probíhala spolupráce také s MV, MO, MZV, Licenční správou MPO, Státním úřadem pro jadernou bezpečnost (SÚJB) a na ně navázanými organizacemi, a to i v probíhajících povolovacích a licenčních řízeních a při informování o dodržování licenčních podmínek a mezinárodních kontrolních režimů.

BIS pokračovala v koordinaci plnění úkolu VZČ k problematice vývozů zařízení, která nejsou na seznamech mezinárodních kontrolních režimů a která mohou být využita dvojím způsobem při vývozech do rizikových oblastí. Na plnění úkolu se podíleli zástupci MV, MZV, MPO, SÚJB, GŘC, FAÚ, ÚZSI a VZ.

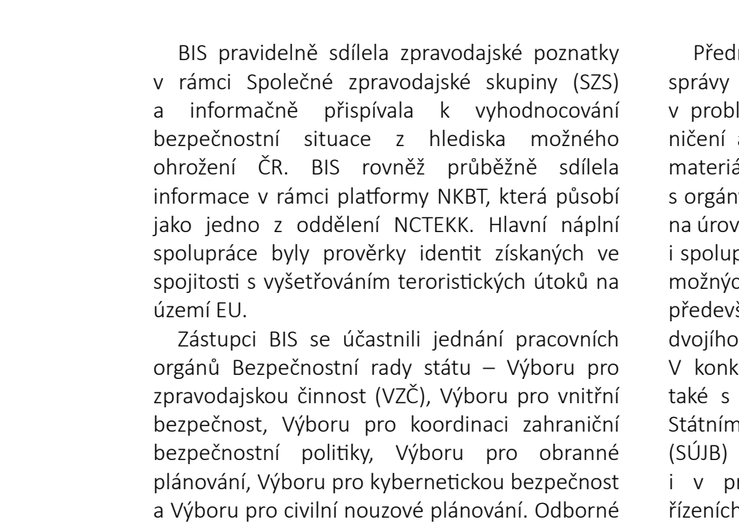
Při zabezpečování informací k činnostem ohrožujícím významné ekonomické zájmy spolupracovala BIS s dalšími orgány státní správy. Komunikace s GFŘ se týkala oprávnění BIS získávat informace z daňových řízení. Orgánům činným v trestním řízení, SÚJB a Úřadu pro ochranu hospodářské soutěže byly předávány informace spadající do jejich působnosti.

Pokračovala aktivní spolupráce v rámci mezirezortního orgánu pro potírání nelegálního zaměstnávání. Činnost orgánu je mj. zaměřena na kontrolní činnost ve vztahu k působení agentur práce a v neposlední řadě na činnosti označované jako nedeklarovaná práce.

Spolupráce s NBÚ spočívá v konzultacích o zabezpečení utajovaných informací v rámci fyzické bezpečnosti.

S Národním úřadem pro kybernetickou a informační bezpečnost BIS spolupracuje především na tématech ochrany utajovaných informací v ICT, včetně certifikace těchto systémů, dále pak v oblasti kompromitujícího vyzařování a kryptografické ochrany utajovaných informací.

BIS se také aktivně podílela na činnosti Národní skupiny pro boj proti proliferaci, která byla zaměřena především na operativní spolupráci.



Spolupráce se zpravodajskými službami cizí moci

Spolupráce se zpravodajskými službami cizí moci je v řadě oblastí působnosti BIS klíčovým faktorem umožňujícím zabezpečování informací důležitých z hlediska bezpečnosti ČR pro zákonné adresáty BIS. Na základě souhlasu vlády ČR je BIS oprávněna spolupracovat s více než stovkou zpravodajských služeb z celého světa. Informační výměna a aktivní kontakty BIS rozvíjí především se službami EU, NATO a některých dalších zemí. Na multilaterální úrovni se BIS v roce 2023 zapojovala v rámci všech uskupení, jejichž je členem (např. Counter-Terrorism Group a NATO Civilian Intelligence Committee).

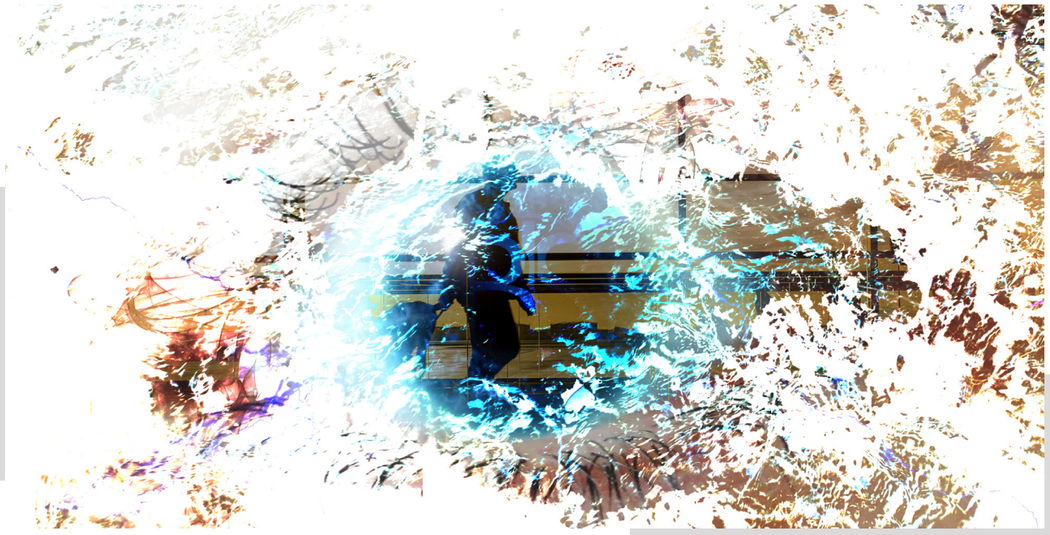
Hlavními oblastmi spolupráce BIS se zahraničními zpravodajskými službami zůstávají boj proti terorismu, kontrašpionáž, proliferace, kybernetická bezpečnost a ochrana utajovaných informací a oblast bezpečnostní způsobilosti. V rámci mezinárodní spolupráce BIS v roce 2023 přijala více než 14 000 zpráv a postoupila více než 2 500 dokumentů. Na strategické a expertní úrovni se zástupci BIS zúčastnili více než 900 mezinárodních jednání.

Kontrola

Základ právní úpravy kontroly činnosti BIS je zakotven v § 12 odst. 1 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, z něhož vyplývá, že činnost BIS podléhá kontrole vlády, Poslanecké sněmovny a Orgánu nezávislé kontroly zpravodajských služeb ČR.

Ačkoliv zákon nestanoví konkrétní rozsah ani způsob provádění kontrolní činnosti vládou, kontrola vlády vůči BIS se odvíjí od jejího oprávnění ukládat BIS úkoly a hodnotit jejich plnění. Vláda za činnost BIS odpovídá, koordinuje ji a jmenuje a odvolává jejího ředitele. BIS je rovněž povinna podávat prezidentovi republiky a vládě jednou za rok a kdykoliv o to požádají zprávy o své činnosti. Z této úpravy je zřejmé, že kontrolní činnost vlády se zaměřuje na všechny oblasti činnosti BIS.

Poslanecká sněmovna je o činnosti zpravodajských služeb informována vládou prostřednictvím svého příslušného orgánu pro zpravodajské služby. Tím je ve vztahu k BIS Stálá komise pro kontrolu činnosti Bezpečnostní informační služby, jejíž členové jsou např. oprávněni vstupovat v doprovodu ředitele BIS nebo jím pověřeného příslušníka do objektů BIS. Kontrolní orgán také může požadovat od ředitele BIS potřebné vysvětlení v případě, že má za to, že činnost BIS nezákonně omezuje nebo poškozuje práva a svobody občanů. Na druhé straně je ředitel BIS povinen předkládat kontrolnímu orgánu zákonem určené informace a písemnosti.



Zákon č. 325/2017 Sb., kterým se mění zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů, a další související zákony, předpokládá zřízení pětičlenného Orgánu nezávislé kontroly zpravodajských služeb České republiky voleného Poslaneckou sněmovnou na dobu pěti let na návrh vlády, který by měl vykonávat kontrolu na základě podnětu některého ze zvláštních kontrolních orgánů. Tento orgán, který bude oprávněn požadovat od zpravodajské služby až na několik výjimek všechny potřebné informace o její činnosti, které souvisejí s prováděnou kontrolou, nebyl v roce 2023 personálně obsazen.

Kontrolu plnění úkolů BIS v oblasti hospodaření se státním majetkem a plnění státního rozpočtu vykonávají příslušné státní orgány např. podle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finnační kontrole), 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.

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.

Dodržování kázně, vyřizování žádostí a oznámení

Působnost odboru inspekce spočívá ve vyřizování dožádání orgánů činných v trestním řízení či jiných orgánů státní správy a v prošetřování oznámení, podnětů a stížností směřujících na pracovníky BIS. Odbor inspekce prošetřuje případy podezření ze spáchání jednání majících znaky přestupku a kázeňských přestupků, včetně prošetřování mimořádných událostí. V neposlední řadě má odbor inspekce v rámci své působnosti v případech podezření ze spáchání trestného činu příslušníkem BIS, postavení policejního orgánu ve smyslu ustanovení § 12 odst. 2 písm. f) trestního řádu.

Naprostá většina šetření podezření ze spáchání kázeňského přestupku nebo jednání majícího znaky přestupku se i v roce 2023 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 93 podání nebylo ani jedno vyhodnoceno jako stížnost na jednání příslušníků BIS. Obsah všech podání byl prověřen a vyhodnocen. Některá podání byla postoupena zpravodajským útvarům BIS k dalším opatřením. Další podání byla postoupena např. věcně příslušným orgánům státní správy nebo PČR. Obsahově jsou oznámení od občanů odrazem celospolečenského dění, kdy současně odrážejí situaci kolem válečného konfliktu na Ukrajině a v Izraeli.

Odbor inspekce spolupracuje s ostatními orgány státní správy především ve formě dožádání, která nejčastěji zasílají orgány PČR, které jsou činné v trestním nebo přestupkovém řízení.

Odbor inspekce v postavení policejního orgánu plní úkoly vyplývající z trestního řádu a v rámci své činnosti je dozorován věcně i místně příslušným státním zastupitelstvím.

Rozpočet

Rozpočet BIS pro rok 2023 byl stanoven zákonem č. 449/2022 Sb., o státním rozpočtu České republiky na rok 2023. Příjmy byly kapitole určeny ve výši 250 000 tis. Kč a výdaje ve výši 2 227 190 tis. Kč.

Vedle rozpočtových prostředků disponovala BIS v roce 2023 nároky z nespotřebovaných výdajů (dále jen „NNV"). Konečný rozpočet výdajů, který představuje celkové disponibilní zdroje včetně zapojených a spotřebovaných NNV, činil ke konci sledovaného období 2 568 530 tis. Kč.

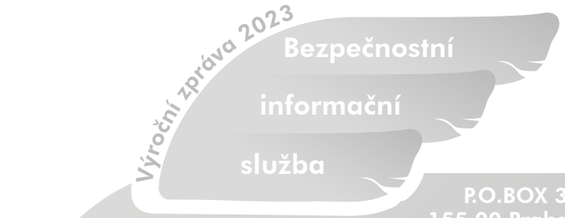
Celkové skutečně realizované výdaje v roce 2023 dosáhly výše 2 375 501 tis. Kč, což představuje 107 % upraveného, resp. 92,5 % konečného rozpočtu kapitoly.

Kapitálové výdaje schválené pro rok 2023 byly čerpány s cílem udržení provozuschopnosti materiálně-technické základny a jejího nezbytného rozvoje. I v roce 2023 byla nejvýznamnější akcí tohoto programu výstavba technicko-administrativního objektu, která byla po necelých pěti letech výstavby úspěšně dokončena ve druhém čtvrtletí roku 2023. Vedle této nejdůležitější investiční akce byly zahájeny práce na další zásadní víceleté investiční akci, kterou je budování nového zpravodajského informačního systému. Ostatní investiční akce spočívaly především v prosté reprodukci a nezbytném rozvoji dlouhodobého majetku BIS. Významná část investic směřovala též do pořízení a modernizace zpravodajské techniky a do informačních a komunikačních technologií. Opomenout nelze ani výdaje na nezbytnou obměnu dopravních prostředků.

Největší část běžných výdajů tvořily osobní výdaje a v jejich rámci výdaje na platy a příslušenství, jejichž meziroční růst byl důsledkem navýšení základních tarifů u služebních příjmů příslušníků k 1. 1. 2023. Výdaje na výsluhové nároky, které při splnění předepsané délky trvání služebního poměru náleží bývalým příslušníkům, zůstaly v roce 2023 na úrovni roku předchozího.

Další významnou skupinou běžných výdajů jsou v souladu se zvláštními postupy finančního hospodaření BIS 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 zajišťující běžný provoz a na dodavatelské zajištění oprav a údržby majetku a objektů BIS. Na výši těchto provozních výdajů měl v roce 2023 vliv růst cen řady komodit a služeb nezbytných pro zajištění chodu BIS i pro výkon její působnosti. Rok 2023 byl charakteristický vysokými cenami energií a pohonných hmot. Pro BIS však vzhledem k tomu, že pro většinu odběrných míst měla i pro rok 2023 smluvně zajištěné pevné ceny na úrovni před energetickou krizí, nepředstavoval vývoj tržních cen těchto komodit zásadní problém, který by významně ovlivnil rozpočtové hospodaření roku 2023.



P.O.BOX 31
155 00 Praha 515
Telefon: +420 235 521 400
Fax: +420 235 521 715
E-mail: info@bis.cz
Datová schránka: cx2aize