POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

DIZERTAČNÍ PRÁCE

2024 **PhDr. Jan Paďourek**

POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Klíčové bezpečnostní hrozby v kontextu činnosti zpravodajských služeb České republiky

Dizertační práce

ŠKOLITEL
Doc. JUDr. Ladislav Pokorný, Ph.D.

AUTOR PRÁCE
PhDr. Jan Paďourek

PRAHA
2024

POLICE ACADEMY OF THE CZECH REPUBLIC IN PRAGUE

Key Security Threats in the Context of the Activities of the Intelligence Services of the Czech Republic

PhD THESIS SUPERVISIOR
Doc. JUDr. Ladislav Pokorný Ph.D

THE AUTHOR
PhDr. Jan Paďourek

PRAGUE
2024

Abstrakt

Dizertační práce předkládá metodu možného měření relevance 37 národních bezpečnostních hrozeb s pomocí empirického výzkumu naměřeného na vzorku názorů elitní skupiny 57 pracovníků centrální analytiky Bezpečnostní informační služby ČR (BIS). Takto zjištěná relevance analyzuje každou bezpečnostní hrozbu vyskytující se v klíčových strategických dokumentech ČR a řadí je podle naměřených skupin faktorových skladeb. Pro stanovení finální relevance hrozeb empirický výzkum využil tzv. explorační faktorovou analýzu. Zjištěné výsledky byly dále komparovány s činností a působností českých zpravodajských služeb s cílem zjistit, zda je naměřená relevance ve shodě s jejich aktivitami a kapacitami. Empirický výzkum proběhl na počátku roku 2019 a jeho výsledky nemají za cíl stanovit současnou relevanci hrozeb. Mají pouze nabídnout jednu z metod, resp. jednu z cest, jak k tomuto výsledku dospět. Aktualizované verze klíčových strategických dokumentů z roku 2023 (především Bezpečnostní strategie ČR a Obranné strategie ČR) finálně posloužily jako jedno z potvrzení správnosti zvolené metody, neboť proměna bezpečnostní situace v ČR, v Evropě a ve světě v roce 2023 plně koresponduje s názory vyslovenými analytiky BIS již v roce 2019. Z výzkumu také plyne závěr, že je stávající rozsah aktivit českých zpravodajských služeb příliš široký, a že by se jejich aktivity měly více zaměřit jen na nejzávažnější bezpečnostní hrozby v souladu s kýženou exkluzivitou zpravodajských služeb jako elitních organizací národního bezpečnostního aparátu.

Klíčová slova

Bezpečnostní hrozby; bezpečnostní rizika; bezpečnostní strategie; zpravodajské služby; empirický výzkum; faktorová skladba hrozeb

Abstract

This dissertation presents a method for measuring the potential relevance of 37 national security threats using empirical research measured on a sample of the opinions of an elite group of 57 central analysts of the Security Information Service (BIS). The relevance thus established analyses each security threat appearing in key strategic documents of the Czech Republic and ranks them according to measured groups of factor compositions. To determine the final relevance of the threats, the empirical research used the so-called exploratory factor analysis. The findings were further compared with the activities and scope of the Czech intelligence services in order to determine whether the measured relevance is in line with their activities and capabilities. The empirical research was conducted in early 2019 and the results are not intended to determine the current relevance of threats. They are only intended to offer one method or way to arrive at this result. The updated versions of key strategic documents from 2023 (especially the Security Strategy of the Czech Republic and the Defence Strategy of the Czech Republic) finally served as one of the confirmations of the correctness of the chosen method, as the transformation of the security situation in the Czech Republic, Europe and the world in 2023 corresponds with the views expressed by BIS analysts already in 2019. The research also concludes that the current scope of activities of the Czech intelligence services is too broad, and that these activities should be more focused on only the most serious security threats, in line with the desired exclusivity of the intelligence services as elite organisations of the national security apparatus.

Keywords

Security threats; Security risks; Security strategies; Intelligence services; Empirical research; Factor composition of security threats

Prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 11. 3. 2024

PhDr. Jan Paďourek

Poděkování

Děkuji upřímně mému školiteli doc. JUDr. Ladislavu Pokornému Ph.D za zcela profesionální vedení této disertační práce. Děkuji také řediteli Bezpečnostní informační služby ČR brigádnímu generálovi Michalovi Koudelkovi za možnost realizace empirického výzkumu v prostředí analytické skupiny BIS, neboť bez této velkorysé podpory by tato práce nemohla nikdy vzniknout. Děkuji upřímně i dr. Zdeňkovi Kovaříkovi, CSc., který mi odhalil taje empirického výzkumu a pomohl mi při softwarovém zpracování a prvotní analýze jeho výsledků.

Obsah

1. ÚVOD

ZÁKLADNÍ VÝCHODISKA, CÍLE, METODY A VYMEZENÍ POJMŮ

Bezpečnostní prostředí v Evropě se během několik posledních dekád velmi negativně mění, z toho v posledních měsících a letech zásadně. Lze konstatovat, že intenzita těchto změn nemá v moderních dějinách Evropy i našeho státu obdoby. Nejpodstatnější změna ve světové bezpečnostní architektuře však nastala 24. února 2022 zahájením bezprecedentní nevyprovokované války Ruska proti Ukrajině, jejíž další důsledky lze dnes jen stěží předvídat. Tento vývoj mezinárodní situace především změnil povědomí, že se již Česká republika, stejně jako všechny další státy euroatlantické civilizace, nenacházejí v relativně bezpečném prostředí, kdy bylo možné konstatovat jen minimální riziko vojenského, válečného ohrožení. Ruská vojenská agrese proti Ukrajině změnila především tento narativ a s tím spojené vyhrocení celé palety dalších hrozeb a rizik. Česká vláda a její bezpečnostní a vojenské složky, stejně jako další evropské i jiné spojenecké vlády, začaly přehodnocovat svůj pohled na nové bezpečnostní prostředí ve světě. Například tím, že iniciují zásadní aktualizaci národních strategických dokumentů a s tím spojených aktivit vedoucích ke zvýšení obranyschopnosti země, ale i zesilování nezbytné politiky odstrašení. Ta je v našich podmínkách efektivní možná především v rámci kolektivní obrany plynoucí z našeho členství v Organizaci Severoatlantické smlouvy a Evropské unie. Národní připravenost na odolnost proti všem bezpečnostním výzvám současného světa je však nezbytnou podmínkou pro efektivitu kolektivního principu obrany.

Česká republika (ČR) je také společně se svými euroatlantickými spojenci průběžně konfrontována dalším pestrým spektrem bezpečnostních hrozeb a jejich kombinací. Mnohé bezpečnostní hrozby nebyly ještě před několika lety zřetelné (např. systematické kybernetické útoky zvenčí namířené proti českým státním i nestátním institucím) nebo nebyly tak vyhrocené a časté (např. pokusy ovlivňovat různé aspekty našeho života zahraničními vlivy s použitím tzv. hybridních způsobů

válčení, zvláště v kybernetické oblasti, nebo prostřednictvím cílených zpravodajských operací, šíření dezinformací nebo tzv. fake news).

Zásadní změny bezpečnostního prostředí ve světě mají přímý vliv na bezpečnostní situaci v ČR, a to především na její tendence i na vztah k ní ze strany exekutivy i národa. Všechny vlády ČR stejně jako ostatní státy euroatlantického hodnotového prostoru dlouhodobě vzdorují výzvám některými tradičními způsoby a metodami. V hlavních národních strategických bezpečnostních dokumentech[1] identifikují, popisují a analyzují komplexní škálu bezpečnostních hrozeb a navrhují patřičná protiopatření; aktuálně organizují a využívají rozsáhlý bezpečnostní aparát se snahou těmto hrozbám účinně čelit; aktivně se angažují v mezinárodní spolupráci. Totéž činí exekutiva ČR s cílem efektivně využívat postavení ČR jako členské země Evropské unie (EU) a Organizace Severoatlantické smlouvy (NATO). Reálný popis bezpečnostních hrozeb a jejich analýza již mají a měly by mít ještě větší vliv na plánování, skladbu a výši rozpočtů a obecně i na celkovou efektivitu práce bezpečnostních institucí, které těmto hrozbám čelí, a samozřejmě by měly ovlivnit proces plánování aktivit. S tím souvisí i vymezení kompetencí v boji s bezpečnostními hrozbami. Jedním z aktuálních problémů ČR je však skutečnost, že **národní analýzy bezpečnostních hrozeb a bezpečnostního prostředí zastarávají a v mnoha ohledech již nejsou zcela aktuální**. Analýza národních bezpečnostních dokumentů obsahující identifikaci konkrétních bezpečnostních hrozeb a jejich faktorové skladby je součástí první teoretické části této dizertační práce

Dramatické bezpečnostní změny nakonec vyvrcholily skokem do války. Exekutiva zareagovala poměrně rychle, takže v říjnu 2023 byla vládou schválena jak strategie bezpečnostní, tak obranná (zatímco rok 2015 méně dramatickým vývojem poskytl prostor nejprve pro Bezpečnostní strategii a Audit národní bezpečnosti vznikl následně v roce 2016).

[1] Bezpečnostní strategie ČR z roku 2015 resp. z roku 2023, Audit národní bezpečnosti z roku 2016 nebo Obranná strategie ČR z roku 2017, resp. z roku 2023.

Změna situace a eskalace hrozeb vedly jak ke změnám v militárních složkách států, v exekutivě (vznik pozice poradce pro národní bezpečnost v Úřadu vlády ČR), tak i v méně viditelných prostorech včetně zpravodajských služeb.

Zpravodajské služby jako specifická, a přitom integrální součást bezpečnostních struktur státu jsou významným nástrojem pro zajištění bezpečnosti v boji s konkrétními hrozbami[2]. Internetová verze britské encyklopedie Collins Dictionaries definuje stručně, ale výstižně zpravodajskou službu jako „*vládní složku, která je odpovědná za shromažďování a analýzu informací o nepřátelích*“.[3] Tato definice může být doplněna nekonečnou řadou dalších definic nejen o organizacích jako takových, ale i o samotné podstatě zpravodajské práce. Tyto definice zaplňují veřejný mediální prostor a na problematiku nazírají z nejrozmanitějších perspektiv. Např. klasik dějin špionáže, britský emeritní profesor univerzity v Cambridge Christopher Andrew vidí zpravodajskou činnost jako „*získávání utajovaných informací, které nejsou přístupné v otevřených zdrojích*“[4]. Bývalý ředitel CIA George Tanet použil pro popis aktivit jím řízené organizace jen tři prostá slova – „*We steal secrets*“[5] (tj. „*Krademe tajemství*“). A nakonec český představitel zpravodajské teorie a praxe Petr Zeman definuje zpravodajství jako „*záměrnou lidskou činnost, která spočívá v utajovaném získávání a zpracovávání cizích utajených informací*“[6].

České zpravodajské služby byly nově konstituovány po rozpadu bipolárního světa na počátku 90. let minulého století. Československá a později česká vláda přijaly počátkem 90. let relativně odvážné rozhodnutí vybudovat nový národní zpravodajský aparát téměř bez přímé kontinuity s bývalými komunistickými strukturami. Šlo o bezprecedentní rozhodnutí, které takřka nemělo v zemích bývalého socialistického bloku obdoby.[7] Odstartovalo ambiciózní a

---

[2] Bezpečnostní strategie ČR, Praha 2015, s 23.
[3] Dostupné z https://www.collinsdictionary.com/dictionary/english/intelligence-service [online, cit. 2020-04-02].
[4] ANDREW Christopher (2018), The Secret World. A History of Intelligence, Allen Lane, London, s. 2
[5] Interview with DCI George Tenet, Studies in Intelligence, vol. 42 (1998), no.I.
[6] ZEMAN Petr (2008), Co je zpravodajství? Pokusy o definici pojmu a problémy překladu, webový portál Asociácie bývalých spravodajských dôstojníkov Slovenska.
[7] S výjimkou podobných rozhodnutí v některých pobaltských postsovětských státech (Estonsko, Lotyšsko a Litva). Podrobněji van HAM, Peter, ed., The Baltic States: Security and Defence after Independence, Insitute for Security Studies od WEU, 1995, 63 s., ISSN 1017-7566.

náročnou reformu českého zpravodajského systému. Tato reforma však ustrnula již v polovině 90. let minulého století a české zpravodajské služby se dále začaly rozvíjet individuálně a v podstatě nikoli jako harmonické součásti daného systému. Zmiňovaný proces sice neměl negativní vliv na postupně získávanou profesionalitu služeb, ale **organizace českých národních zpravodajských služeb je z určitého hlediska nedokončena, není zcela systémová a patrně ani dostatečně efektivní v poměru k vynaloženým prostředkům**.

Exaktně vzato vše nasvědčuje tomu, že aktuální popis zákonné působnosti českých zpravodajských služeb, který je definován v tzv. střechovém zákoně o zpravodajských službách č. 153/1994 Sb.[8] nepokrývá kompletně rozsah současných bezpečnostních hrozeb, a dokonce ani těch obsažených v českých strategických dokumentech. Nepostihuje je minimálně v exaktním slova smyslu. Některé hrozby jsou zde uvedeny zcela explicitně (např. „terorismus nebo organizovaný zločin“) a některé jen velmi implicitně, resp. skrytě zahrnuté v široce definované škále působnosti (např. v pojmu „zajišťování bezpečnosti“). Je zřejmé, že podrobnější popisy působnosti, respektive priorit činností zpravodajských služeb zadaných vládou na příslušné období nejsou součástí veřejnosti přístupných informací, avšak i tak působí zákonné vymezení působnosti českých zpravodajských služeb v zákoně č. 153/1994 Sb. značně nahodile, nekoncepčně a nesystémově. Navíc architektura českého zpravodajského systému není dnes zcela moderní (v podstatě kopíruje zpravodajskou strukturu bývalého komunistického režimu: tj. systém skládající se z civilní kontrarozvědky a civilní rozvědky a vojenské zpravodajské služby s obojí působností). Tato struktura je také v některých aspektech poněkud nelogická. Např. nesystémová podřízenost civilní zahraniční rozvědky ministrovi vnitra je z některých pohledů ne zcela koncepční. Zpravodajské služby jsou sice zprostředkovaně podřízeny jedné autoritě, ale systémová spolupráce s nimi a mezi nimi není dostatečně koordinovaná, nemluvě o jejich úkolování, financování, poskytování důležité

[8] Působnost českých zpravodajských služeb je popsána v tzv. střechovém zákoně č. 153/1994 Sb. o zpravodajských službách ČR. Některé služby mají i svůj vlastní zákon, konkrétně zákon 154/1994 Sb. o Bezpečnostní informační službě, zákon č. 289/2005 S. o Vojenském zpravodajství nebo zákon č. 205/2019 Sb. o změnách v předešlých zákonech

zpětné vazby nebo kontrole. Lze tedy konstatovat, že i když československé a později české vlády první poloviny 90. let 20. století vybudovaly zpravodajský aparát bez přímé kontinuity na bezpečnostní struktury komunistického Československa, nevyužily plně zcela unikátní a nyní již těžko se opakující příležitost zaměnit klasické členění a harmonii zpravodajských služeb nějakým aktuálnějším modelem. Přitom se nabízely modernější koncepce, kterými mohly vlády již od počátku 90. let minulého století vystavět funkčnější systém a eliminovat nebo alespoň omezit již tehdy nežádoucí nekoordinovanost a rivalitu mezi službami, které jsou přítomny dodnes. V době po nástupu současné vlády se uvažovalo o vzniku koordinačního útvaru nebo alespoň Koordinátora služeb při Úřadu vlády, problémy byly například v potřebě značných úprav legislativy; nakonec tuto roli alespoň nepřímo zastává nově vzniklá funkce poradce pro národní bezpečnost v Úřadu vlády ČR.

České zpravodajské služby s ohledem na význam a postavení ČR ve světě a její zájmy nepůsobí globálně a celoplošně, ale pracují výsekově na základě vládou stanovených priorit, jejichž stanovení vyplývá především ze správného popisu bezpečnostních hrozeb.

Z hlediska nově vznikající české demokracie bylo politicky důležité, že nové zpravodajské služby byly víceméně budovány jako služby informační, tj. bez přímých výkonných nebo vyšetřovacích pravomocí. Výkonné nebo vyšetřovací pravomoci jsou dány spíše několika velkým zpravodajským centrálám významných světových velmocí[9], i když i v českých podmínkách se působnost některých zpravodajských složek rozšiřuje i tímto směrem. Mám zde na mysli Vojenské zpravodajství a jeho novou agendu v oblasti kybernetické obrany státu. Je zde však na místě doplnit, že novela zákona o vojenském zpravodajství tuto výkonnou složku víceméně odděluje od zpravodajské činnosti, čímž lze

[9] Výjimku tvořilo a tvoří Vojenské zpravodajství, do jehož gesce do roku 2014 patřila 601. skupina speciálních sil. V současné době se situace opakuje, neboť Vojenské zpravodajství získalo v oblasti kybernetické obrany státu relativně zásadní výkonné pravomoci. Obě civilní služby však nadále zůstávají zpravodajskými službami čistě informačními, neboť vojenské zpravodajství odděluje v zákoně 150/2021 Sb. zpravodajskou činnost od kompetence kybernetické obrany státu.

konstatovat, že i tato zpravodajská služba je ve svém působení primárně rovněž informační službou. Obecně však platí, že pokud mají zpravodajské služby přímé výkonné pravomoci, tj. např. zasahují do trestního řízení, vyšetřování atd. jedná se o model a priori podezřelý a často i politicky zneužitelný. Proto se vyskytuje spíše v nedemokratických autoritativních zemích. Takové zpravodajské služby v podstatě dublují činnost orgánů činných v trestním řízení, především policie, avšak jejich práce je technicky i teoreticky podstatně hůře kontrolovatelná a obvykle jsou nadřazeny profesionálním strukturám. Z toho důvodu preferují demokratické a svobodné země spíše model služeb bez výkonných policejních pravomocí. Je na místě, aby i ČR pokračovala v tomto trendu s tím, že nové pravomoci Vojenského zpravodajství v kybernetické bezpečnosti nevybočují z tohoto modelu, neboť jejich kompetence při ochraně kybernetického prostoru státu je specifická a neobsahuje prvky policejních aktivit činných v trestním řízení.

České strategické dokumenty jmenují a definují konkrétní bezpečnostní hrozby[10]. Takto identifikované bezpečnostní hrozby lze zařadit do dalších konkrétních skupin – hrozeb civilních nebo vojenských, ale i vnitřních nebo vnějších, intencionálních – neintencionálních, ale především do příslušných faktorových skladeb. Analytický rozbor těchto faktorů je rovněž součástí této dizertační práce.

1.1. STRUKTURA DIZERTAČNÍ PRÁCE

1.1.1. TEORETICKÁ ČÁST

Existence a vymezení působnosti národních zpravodajských složek je obecně chápáno jako reakce státu na bezpečnostní hrozby a správný popis bezpečnostních hrozeb je základem správného využívání zpravodajského aparátu. Popis českého zpravodajského systému a jeho koordinace (s drobnými

[10] JAKUBCOVÁ, L., ŠESTÁK, B. and KOVAŘÍK, Z., Exact Estimation of factor composition of security threats for the Czech Republic, Bezpečnostní teorie a praxe, Policejní akademie ČR v Praze, 4/2017, s. 12-14, ISSN 1801-8211

historickými exkurzy[11]) je součástí **teoretické části** této dizertační práce. Tato část dizertační práce se dále zaměřuje **na rozbor a analýzu bezpečnostních hrozeb, kterým mohou zpravodajské služby účinně čelit.** V našem případě se jedná o tzv. „**hrozby intencionální***, které zamýšlí, připravuje, spouští či realizuje lidský jedinec nebo kolektivní aktér*“[12] a stranou spíše leží tzv. „hrozby **neintencionální**“, tj. takové, které jsou „*jevem přírodním definovaným fyzikálně*“[13] nebo vzniklým náhodně spontánně společenským vývojem. Na řešení „fyzikálních“ hrozeb mají zpravodajské služby vždy nulový vliv, a tak i např. koronavirová světová pandemie covid-19 či jiné rozsáhlé epidemie zůstávají spíše mimo hlavní zájem zpravodajských služeb, a tudíž i mimo zájem této dizertační práce. Prostor pro ZS je dán ve strategické predikci, a konkrétně se projevuje po vzniku jevu. I v tomto kontextu nicméně existuje oblast významná pro aktivity zpravodajských služeb. Na jaře 2020, tj. na počátku pandemické krize zveřejnily některé světové sdělovací prostředky celkem šokují obvinění některých světových lídrů o možné odpovědnosti některé z velmocí za zamoření světa tímto nebezpečnými virem[14]. Protože záležitost nebyla (alespoň podle veřejně dostupných zdrojů) doposud spolehlivě řešena domnívám se, že je nutná a užitečná spolupráce zpravodajských agentur demokratického světa prokazatelně najít a objasnit příčinu celosvětové pandemie covid-19. Výsledky tohoto šetření by měly zásadní význam pro další formování mezinárodní spolupráce (a nejenom té zpravodajské). Pokud by se však prokázalo, že byl virus vyvinut uměle a cílevědomě rozšířen, jednalo by se o bezprecedentní příklad tzv. státního terorismu nejvyššího rozsahu. I v případě pouze nechtěného úniku vyvíjeného viru by mohlo jít o porušení Úmluvy OSN o biologických zbraních. Je proto v zájmu všech, aby problém řádně vyšetřil, i kdyby to bylo proti vůli některých nedemokratických mocností. Jedna ze základních podstat svobodného světa je

---

[11] Cílem dizertační práce však není historický rozbor vzniku, existence a působení českých zpravodajských služeb.

[12] ZEMAN 2002, s. 58

[13] ZEMAN 2002, s. 58

[14] První světovou političkou, která v televizním vystoupení označila Čínu za viníka koronavirové pandemie byla australská ministryně zahraničí Merise Payne
Po ní se přidali další světové osobnosti (např. D. Trump) i s žádostí o vyšetření tohoto obvinění. Evropský parlament ve svém usnesení dokonce vyzval, aby EU požádala Čínu o plné objasnění okolností vzniku pandemie. Dostupné z https://www.abc.net.au/news/2020-04-19/foreign-minister-marise-payne-coronavirus-pandemic/12163056?nw=0. Tyto iniciativy však nakonec vyšly do ztracena.

totiž založena na pravdě a spravedlnosti, a nikoliv na skrývání skutečnosti a šíření dezinformací.[15]

Podobně byl prostor pro činnost ZS ve zdravotnické, resp. ekonomicko-sociální oblasti v otázce zabezpečení zájmu státu v nákupu vakcín, ochranných prostředků nebo mezinárodního transferu cestujících.

Není pravděpodobně v silách žádné z českých zpravodajských služeb, aby za stávajícího stavu pokryla na stejné úrovni plnou škálu bezpečnostních hrozeb definovaných v národních strategických dokumentech, tj. v komplexní intenzitě a stejně vysoké kvalitě. A to dokonce ani těch, které nazýváme hrozbami intencionálními. Každá z bezpečnostních hrozeb má však svou naléhavost, resp. každá vykazuje relativně konkrétní **relevanci** k míře bezpečnostního ohrožení ČR. Správně určená relevance bezpečnostních hrozeb může mít pozitivní vliv na kvalitnější vládní úkolování zpravodajských služeb i celého bezpečnostního aparátu, ale i na efektivnější využívání jejich kapacit, vynakládání státních prostředků z konkrétních rozpočtů, poskytování kýžené zpětné vazby nebo na eliminaci nežádoucí duplicity v činnosti jednotlivých zpravodajských služeb. Tato dizertační práce v rámci následujícího empirického výzkumu nabízí jednu z cest, která by mohla vést k přesnějšímu vymezení relevance klíčových bezpečnostních hrozeb důležitých pro zajištění bezpečnostních zájmů naší země.

1.1.2. VÝZKUMNÁ ČÁST

Výzkumná část dizertační práce čerpá z výsledků **empirického výzkumu** a nabízí **jednu z možností,** jak analyticky dospět k definování konkrétní relevance každé z identifikovaných bezpečnostních hrozeb s přiřazením kontextu působnosti zpravodajských služeb. Tato dizertační práce nenabízí a ani nemůže nabídnout definitivní a jediné řešení. Ukazuje ale možnou metodu, jak celkem logicky a víceméně přesně dospět k důležitým závěrům. Naplňuje tak smysl neoficiálního motta této dizertační práce, tj. že *„řecké slovo **méthodos** (μέθοδος)*

[15] Část z vystoupení autora této dizertační práce na mezinárodní konferenci GLOBAL INTELLIGENCE SUMMIT 2020, Institute of National Security Strategy, Soul, Jižní Korea, 17.12. 2020, konané online.

*znamená **cesta**.“* Empirický výzkum, který je základem této práce byl proveden s laskavým souhlasem vedení Bezpečnostní informační služby (BIS) v relativně malé, avšak **svou expertizou naprosto unikátní skupině 57 respondentů** – pracovníků centrální analytiky české zpravodajské služby s domácí působností. Při oslovení této skupiny jsem vycházel z předpokladu, že jsou analytici BIS ze všech příslušníků bezpečnostních sborů ČR konfrontováni denně zřejmě nejpestřejší paletou informací různých kategorií, stupňů a druhů o otázkách bezpečnostního ohrožení státu. Tyto informace pocházejí z citlivých zpravodajských informacích BIS, informací dalších bezpečnostních sborů ČR (ostatní zpravodajské služby, Policie ČR) nebo z poznatků z mezinárodní zpravodajské informační výměny. Z toho vyplývá, že hodnocení členů analytické skupiny BIS má důležitý význam pro stanovení validity relevancí konkrétních bezpečnostních hrozeb.

1.1.3. KOMPARATIVNÍ ČÁST

Komparativní část dizertační práce vychází již z konkrétních výsledků empirického výzkumu, na kterém je tato dizertace postavena. Výsledky porovnání umožňují učinit i první dílčí závěry práce, neboť dovolují popsat bezpečnostní prostředí ČR již na základě naměřené míry relevance bezpečnostních hrozeb tak, jak byly zjištěny empirickým výzkumem v expertním prostředí Bezpečnostní informační služby.

Provedená komparativní analýza umožňuje nejenom srovnat a přesně zařadit naměřenou míru relevance každé ze zkoumaných bezpečnostních hrozeb, ale umožňuje každou z hrozeb konfrontovat s působností jednotlivých českých zpravodajských služeb. Komparativní část konkrétně analyzuje i výskyt bezpečnostních hrozeb řazených podle skupin faktorových skladeb v rámci naměřené vysoké relevance, vysoké a střední relevance, vysoké, střední a nízké relevance, a to vše v kontextu působnosti českých zpravodajských služeb.

1.1.4. ZÁVĚRY

Závěry dizertační práce představují a komentují finální výsledky. Je zde prezentována setříděná relevance národních bezpečnostních hrozeb vzešlá z empirického výzkumu provedeném na exkluzivní skupině bezpečnostních analytiků BIS ve vztahu k působnosti českých zpravodajských služeb. Autor mj. dospěl k závěrům o užitečnosti přesnější aktualizace zákonného vymezení působnosti jednotlivých zpravodajských služeb v souladu s předloženou relevancí bezpečnostních hrozeb, ale i dokončení zpravodajské reformy ambiciózně započaté počátkem 90. let minulého století především s akcentem na centrální koordinaci a možná i synergii jejich práce. Další závěry se dotýkají doporučení častější aktualizace popisu bezpečnostního prostředí ČR a průběžné analýzy konkrétních bezpečnostních hrozeb formou celonárodní expertní diskuse, mj. i na základě v práci představené metody a metodologie.

Tato dizertační práce nemá ambice předložit definitivní návrh popisu nového zpravodajského systému ČR ani předložit finální aktualizaci českých národních bezpečnostních hrozeb. To jsou úkoly pro velké expertní týmy, které se musejí v koordinaci s vládou těmito otázkami zabývat. Dizertační práce tedy **ukazuje spíše cestu než cíl**. Neskromným přáním autora je prostřednictvím této analýzy přispět do již probíhající odborné diskuse, která by vedla nejen k častější relevantní aktualizaci analýzy národních bezpečnostních hrozeb, ale také k případnému dokončení reformy českého zpravodajského aparátu.

1.2. KONKRÉTNÍ CÍLE DIZERTAČNÍ PRÁCE A VÝZKUMNÉ OTÁZKY

Hlavním cílem dizertační práce je popsat a analyzovat vztah bezpečnostních hrozeb v ČR a organizaci a zákonnou působnost českých zpravodajských služeb s pomocí nově zjištěné relevance bezpečnostních hrozeb realizované empirickým výzkumem provedeným ve skupině 57 analytiků Bezpečnostní informační služby. Cílem této analýzy je mj. zjistit, zda je působnost a případně organizace a koordinace práce českých zpravodajských služeb v souladu s aktuální relevancí nebo naléhavostí národních bezpečnostních

hrozeb. S ohledem na stanovený cíl dizertační práce byly stanoveny tyto výzkumné otázky:

1. **Jaká je relevance bezpečnostních hrozeb obsažených v českých národních bezpečnostních dokumentech pohledem analytické skupiny BIS jako významné autority v oblasti analýzy národní bezpečnosti?**

2. **Je aktuální zákonná působnost a organizace a koordinace činnosti českých zpravodajských služeb v souladu se stanovenou relevancí národních bezpečnostních hrozeb?**

1.3. POUŽITÉ METODY

Během zpracování dizertační práce byly vedle dlouholetých zkušeností autora z práce ve zpravodajských službách a vedle základních postupů použity především tyto metody:

- Empirický výzkum s použitím explorativní metody dotazníkové akce provedené v exkluzivní skupině 57 analytiků BIS;

- Faktorová analýza dat získaných z empirického výzkumu;

- Obsahová a komparativní analýza zásadních dokumentů k předmětné problematice (národní bezpečnostní texty ČR, bezpečnostní strategie zemí, zákony a vládní nařízení).

- Dizertační práce rovněž předkládá jednu z možností, jakým způsobem lze provést případnou aktualizaci národních strategických dokumentů; tj. nespoléhat se pouze na akademické názory vybraných vládních expertů, ale systémově využít i názorů expertů z praxe (v tomto případě analytické skupiny BIS, ale i odborníků ostatních bezpečnostních složek státu), kteří

mají na rozdíl od akademických pracovníků aktuální a komplexní přístup k informacím popisující většinu aspektů bezpečnostního ohrožení země.

2. BEZPEČNOSTNÍ HROZBY A NÁRODNÍ BEZPEČNOSTNÍ STRATEGICKÉ DOKUMENTY

2.1. ZÁKLADNÍ DEFINICE

Výstižnou a stručnou definici pojmu „bezpečnostní hrozba“ nabízí internetová verze britského slovníku Collins Dictionaries, který pojem „bezpečnostní hrozba“ stručně definuje jako „*hrozbu pro bezpečnost země*“[16].

Český bezpečnostní teoretik, bývalý zpravodajec a ředitel civilní rozvědky Petr Zeman definuje hrozbu v příručce o české bezpečnostní terminologii mj. takto:

„Hrozba je primární, mimo nás nezávisle existující, vnější fenomén, který může nebo chce poškodit nějakou konkrétní hodnotu. Závažnost hrozby je úměrná povaze hodnoty a toho, jak si danou hodnotu ceníme. Hrozba může být jevem přírodním, definovaným fyzikálně – takovou hrozbu nazýváme hrozbou neintencionální. Realizace neintencionální hrozby je stochastické povahy. Zcela jiného původu je hrozba působená či zamýšlená činitelem nadaným vůlí, úmyslem (hrozba intencionální) – zamýšlí ji, připravuje, spouští či realizuje lidský jedinec nebo kolektivní aktér. Termín ohrožení je synonymem termínu hrozba“.[17]

České strategické dokumenty, ale i další odborné texty zabývající se problematikou národní bezpečnosti používají vedle termínu ***hrozba*** i termín ***riziko***. Je zde na místě upozornit na rozdíl ve významu těchto pojmů, neboť **hrozba** je „*primární, mimo nás nezávisle existující, vnější fenomén, který může*

[16] Dostupné z https://www.collinsdictionary.com/dictionary/english/security-threat, [online, cit. 2020-04-01].

[17] ZEMAN, Petr a kol. (2002) Perspektivy vývoje bezpečnostní situace, vojenství a obranných systémů do roku 2015 s výhledem do roku 2025. Část 1: Perspektivy bezpečnostní situace a politického vývoje států střední a východní Evropy do roku 2015, Česká bezpečnostní terminologie, Výklad základních pojmů, heslo 18. Hrozba a riziko, s. 58, ÚSS/202-S-1-031, Ministerstvo obrany, Brno

nebo chce poškodit nějakou konkrétní hodnotu. Závažnost hrozby je úměrná povaze hodnoty a toho, jak si danou hodnotu ceníme…“[18], kdežto **riziko** je „*pravděpodobnost, že dojde ke škodlivé události, jež postihne danou hodnotu. Jinak je riziko možnost, že s určitou pravděpodobností vznikne událost, jež se liší od toho, co si přejeme. Riziko je odvozená závisle proměnná a dá určit nebo odhadnout tzv. analýzou rizik. Riziko je reakcí na hrozbu, též na stav naší připravenosti (zranitelnosti) a je spojeno s rozhodováním“*[19].

Samotný pojem **národní bezpečnost** je definován českým bezpečnostním badatelem a pedagogem Masarykovy univerzity v Brně prof. Miroslavem Marešem jako *„stav, kdy objektu (národnímu státu jako celku nebo jeho podstatným atributům) nehrozí závažné ohrožení svrchovanosti, uzemní celistvosti, základům politického uspořádání, vnitřního pořádku a bezpečnosti, životů a zdraví občanů, majetkových hodnot a životního prostředí. Ani jeho spojenci nejsou vystaveni hrozbám, které by v případě jejich aktivace vyžadovaly ozbrojenou či jinou rizikovou spoluúčast. Objekt je schopen a ochoten potenciální hrozby rozpoznat a v maximální možné míře jim zamezovat, popřípadě je eliminovat“*[20]. Podle člena americké senátní Národní rady pro humanitní vědy a bývalého amerického diplomata Kima R. Holmese lze z globálního pohledu definovat národní bezpečnost i „*jako moc národa nad kontrolou jeho suverenity a osudu, tj. jako určitou míru kontroly nad skutečností, do jaké míry mohou vnější síly poškodit zemi. Tvrdá, resp. vojenská moc je o kontrole, zatímco měkká moc je hlavně o vlivu – snaží se přesvědčit ostatní, aby kromě války, využili metody s cílem něco udělat – cosi ovlivnit*[21]“.

Česká národní bezpečnost je oboustranně nedílnou součástí mezinárodní bezpečnosti, a to především bezpečnosti euroatlantického prostoru, kterého je ČR prostřednictvím svého členství v klíčových mezinárodních organizacích (NATO, EU) aktivním aktérem. V současné době se vzhledem k expanzivní politice Číny

[18] ZEMAN 2002, s. 58
[19] ZEMAN 2002, s. 58
[20] ZEMAN 2002, s. 15
[21] HOLMES Kim R. (2015), What is National Security? The Heritage Foundation, 2015 Index of US Military Strength, Washington D.C. s. 17-26

objevují hrozby i v tamním prostoru. Ten je ČR sice geograficky vzdálen, ale je zřejmé, že je třeba jej nově systematicky pojímat v sumě hrozeb (viz např. COVID, ale i problémy se zdroji surovin apod.) – dopad na bezpečnost je globální. Systém mezinárodní bezpečnosti má, opět podle Kima R. Holmese, několik myšlenkových směrů, jako je např. kolektivní obrana, kolektivní bezpečnost, globální bezpečnost nebo mezinárodní právo[22]. Význam bezpečnosti státu však zůstává důležitý i v regionálním/globálním komplexu.

2.2. VÝVOJ TVORBY ČESKÝCH STRATEGICKÝCH DOKUMENTŮ

Vývoj moderních českých, resp. československých národních strategických bezpečnostních dokumentů zpracovaných na základě bezpečnostních podnětů a s odkazem na reálnou bezpečnostní situaci doma i ve světě lze zaznamenat od roku 1991, kdy byl přijat první porevoluční strategický dokument – Vojenská doktrína České a Slovenské federativní republiky[23]. Ta reagovala především na skutečnost, že se Československo po zániku bipolárně rozděleného světa v podstatě ocitlo zcela mimo jakékoliv kolektivní bezpečnostní struktury. Vojenská doktrína ČSFR z roku 1991 hledala své místo především v již existujících strukturách OSN. Po vzniku samostatného státu byla v roce 1995 vydána Bílá kniha o obraně[24], která poprvé oficiálně deklarovala snahu ČR vstoupit do Organizace severoatlantické smlouvy (NATO). Zcela přelomovou událostí bylo přijetí Ústavního zákona o bezpečnosti z roku 1998[25] a následně v roce 1999 byla vydána první Bezpečnostní strategie ČR[26], která byla brzy novelizována dalším vydáním v roce 2003[27]. V roce 2001 byla aktualizována Doktrína Armády ČR[28] a

[22] HOLMES (2015), s. 18-19
[23] Dostupné z https://www.mocr.army.cz/images/Bilakniha/CSD/1991%20Vojenska%20doktrina%20CSFR.pdf [online, cit. 2021-02-16].
[24] Dostupné z https://www.mocr.army.cz/images/Bilakniha/CSD/1995%20Bila%20kniha%20o%20obrane%20CR.pdf [online, cit. 2021-02-16].
[25] Ústavní zákon o bezpečnosti č. 110/1998 Sb. Detailně MAREŠ Miroslav, NOVÁK Daniel (2019), Ústavní zákon o bezpečnosti ČR. Komentář, Wolters Kluwer ISBN: 978-80-7598-202-5, 236 s.
[26] Dostupné z https://www.mocr.army.cz/images/Bilakniha/CSD/002.pdf [online, cit. 2021-02-16].
[27] Dostupné z https://www.mocr.army.cz/images/Bilakniha/CSD/2003%20Bezpecnostni%20strategie%20CR.pdf [online, cit. 2021-02-16].
[28] Dostupné z https://www.mocr.army.cz/images/Bilakniha/CSD/003.pdf [online, cit. 2021-02-16].

v rychlém sledu několik aktualizovaných vydání Vojenské strategie ČR z roku 2002[29], 2004[30] a 2008[31]. V roce 2011 vydalo MO ČR tzv. Bílou knihu o obraně[32] a v témže roce byla publikována i nová redakce Bezpečnostní strategie ČR 2011[33]. V roce 2012 vyšla Obranná strategie ČR[34]. V roce 2023 byly oba poslední dokumenty zásadně aktualizovány.

2.3. NÁRODNÍ STRATEGICKÉ DOKUMENTY ČR

Česká republika společně s ostatními státy euroatlantického prostoru aktuálně disponuje relativně kvalitním popisem národního bezpečnostního prostředí i relativně hodnotnou analýzou konkrétních bezpečnostních hrozeb. Aktuální národní analýza bezpečnostního prostředí ČR, která definuje i jednotlivé okruhy bezpečnostních hrozeb s výčtem skutečně konkrétních hrozeb je primárně obsažena v ***Bezpečnostní strategii ČR*** (BS ČR 2015, resp. 2023). ČR na rozdíl od mnohých jiných států disponuje i hodnotnou rozšířenou verzí národní bezpečnostní analýzy a strategie, tzv. ***Auditem národní bezpečnosti*** (ANB) z r. 2016[35]. ANB na základě příkladné celonárodní expertní diskuse podrobil každou konkrétní bezpečnostní hrozbu mj. i detailnímu analytickému rozboru[36].

---

[29] Dostupné z https://www.mocr.army.cz/images/Bilakniha/CSD/2002%20Vojenska%20strategie%20CR.pdf [online, cit. 2021-02-16].
[30] Dostupné z https://www.mocr.army.cz/images/Bilakniha/CSD/2004%20Vojenska%20strategie%20CR.pdf [online, cit. 2021-02-16].
[31] Dostupné z https://www.mocr.army.cz/images/Bilakniha/CSD/2008%20Vojenska%20strategie%20CR.pdf [online, cit. 2021-02-16].
[32] Dostupné z https://www.mocr.army.cz/images/Bilakniha/bila_kniha_o_obrane.pdf [online, cit. 2021-02-16].
[33] Dostupné z https://www.mocr.army.cz/images/Bilakniha/CSD/011.pdf [online, cit. 2021-02-16].
[34] Dostupné z https://www.mocr.army.cz/images/id_40001_50000/46088/STRATEGIE_ce.pdf online, cit. 2021-02-16].
[35] Audit národní bezpečnosti z roku 2016 (142 stran) rozšiřuje a v mnohém konkretizuje bezpečnostní strategii 2015 a je v kontextu střední Evropy neběžným materiálem, který vznikl na základě celonárodní debaty klíčových bezpečnostních expertů pod vedením MZV ČR. Navzdory své kvalitě i tento text zastarává a podle autorů této stati také vyžaduje aktualizaci. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2020-04-01].
[36] SWOT analýza je jedna z metod strategické analýzy, zkoumající jevy na základě čtyř principů: S = Strengths (silné stránky), W = Weaknesses (slabé stránky), O = Oportunities (příležitosti) a T = Threats (hrozby). Podrobněji např. SARSBY, Alan: SWOT ANALYSIS, London 2016

V podobném duchu byly zpracovány i další dvě důležité, i když rozsahem nevelké studie – ***Obranná strategie ČR*** (OS) z roku 2017, resp. 2023 popisující bezpečnostní situaci ČR z vojenského hlediska[37] nebo ***Koncepce české zahraniční politiky*** z roku 2015, která spíše akcentuje hlavní proudy české zahraniční politiky, včetně oblastí prosazování našich zájmů ve světě.[38] Aktualizovaná ***Obranná strategie [39] byla schválena na podzim 2023***, na ***Koncepci zahraniční politiky ČR*** pracuje MZV jako gestor. Problém většiny strategických textů tkví v tom, že – ačkoliv jsou nutně formulovány volněji s ohledem na možný vývoj v nejdéle střednědobém horizontu - jejich aktuálnost zastarává a exekutiva tak často stojí před úkolem jejich aktualizace. Výjimkou z tohoto tvrzení a v souladu s moderními trendy byl příklad jednoho z nejnovějších strategických dokumentů České republiky, který byl vládou schválený koncem roku 2020 - **Národní strategie kybernetické bezpečnosti České republiky 2020–2025[40]**. Česká národní kybernetická strategie na pět let zaměřuje hlavní pozornost vedle tradiční ochrany státní kritické infrastruktury i na ochranu soukromých cloudů, internetu věcí nebo i zvyšování mediální gramotnosti širokých vrstev obyvatelstva[41]. I tato oblast však podléhá dynamickému vývoji (a to dokonce i v rámci EU). Promítnutí kybernetické strategie spolu s implementací evropské směrnice NIS2 do nového Zákona o kybernetické bezpečnosti bude vycházet ze skutečně komplexní expertní i politické diskuse, v připomínkovém řízení vlády i v odborných fórech.

BS ČR (2015) slouží jako východisko pro komparativní analýzu této dizertace, neboť byla platná v době konání empirického výzkumu (2019). Nová

---

[37]Text Obranné strategie ČR, 2017, 8 s. dostupný z http://www.mocr.army.cz/images/id_40001_50000/46088/OS.pdf [online, cit. 2020-04-01].

[38] Celý text aktuální Koncepce české zahraniční politiky, 2015, 18 s. dostupný z https://www.mzv.cz/file/1565920/Koncepce_zahranicni_politiky_CR.pdf [online, cit. 2020-04-01].

[39] https://www.vlada.cz/assets/ppov/brs/dokumenty/obranna__strategie_c_r_2023_final.pdf [online, cit. 2020-08-24].

[40] Text Národní strategie kybernetické bezpečnosti 2020–2025 je plně dostupný z https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf [online, cit. 2020-08-24].

[41] Národní strategie kybernetické bezpečnosti 2020–2025 navazuje na předešlý dokument Akční plán Národní strategie kybernetické bezpečnosti 2015-2020. Dostupné z https://www.dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/akcni-plan-nskb-2015-2020-final-150408.pdf [online, cit. 2020-08-24].

bezpečnostní strategie 2023 byla vzata v potaz v závěru při srovnání s výsledky empirického výzkumu. BS ČR 2015 identifikuje celkem 11 faktorových skladeb bezpečnostních hrozeb.[42] Tyto okruhy i konkrétní hrozby jsou dále detailně rozpracovány v **ANB (2016)**, kde je pozornost zaměřena na konkrétní bezpečnostní hrozby popsané v 10 faktorových skladbách.[43] Stále se však jedná o systémově podobný model prezentovaný již v BS ČR (2015). **OS ČR** z roku 2017 doplňuje trojici strategických dokumentů o popis bezpečnostního prostředí ČR a jeho východisek z obranného a vojenského hlediska a jednotlivé bezpečnostní hrozby jmenuje spíše nahodile s odvoláním na BS ČR (2015). Jednoznačně však akcentuje nové vojenské trendy bezpečnostního ohrožení ČR, ať již se jedná o ruský vliv v našem regionu nebo o cílené šíření dezinformací a zneužívání kybernetického prostoru.[44]

Ohrožení ČR v kybernetické oblasti jako relativně nové, avšak dynamicky se rozvíjející bezpečnostní hrozby akcentuje jak BS ČR (2023, 2015), tak i ANB (2016). Tempo rozvoje tohoto nebezpečí a určitá zaostalost ČR v této oblasti přiměla vládu ke schválení klíčového zákona č. 181/2014 sb. **o kybernetické bezpečnosti** s dalšími novelizacemi,[45] který především vymezuje práva a povinnosti osob i konkrétní pravomoci orgánů státní moci v kybernetické oblasti. Na základě novely zákona č. 181/2014 Sb. prostřednictvím zákona č. 205/2017 Sb. byl zřízen samostatný **Národní úřad pro kybernetickou a informační bezpečnost** (NÚKIB) se sídlem v Brně. Do té doby se otázkami celostátní koordinace kybernetické bezpečnosti zabýval Národní bezpečnostní úřad. NÚKIB

---

[42] 1) oslabování mechanismu kooperativní bezpečnosti i politických a mezinárodněprávních závazků v oblasti bezpečnosti, 2) nestabilita a regionální konflikty v euroatlantickém prostoru a jeho okolí, 3) terorismus, 4) Šíření zbraní hromadného ničení a jejich nosičů, 5) kybernetické útoky, 6) Negativní aspekty mezinárodní migrace, 7) extremismus a nárůst interetnického a sociálního napětí, 8) organizovaný zločin, zejména závažná hospodářská a finanční kriminalita, korupce, obchodování s lidmi a drogová kriminalita, 9) ohrožení funkčnosti kritické infrastruktury, 10) přerušení dodávek strategických surovin nebo energie a 11) pohromy přírodního a antropogenního původu a jiné mimořádné události. Bezpečnostní strategie ČR, Praha 2015, s. 11-13.

[43] 1) terorismus, 2) extremismus, 3) organizovaný zločin, 4) působení cizí moci, 5) bezpečnostní aspekty migrace, 6) přírodní hrozby, 7) antropogenní hrozby, 8) hrozby v kyberprostoru, 9) energetická, surovinová a průmyslová bezpečnost, 10) hybridní hrozby a jejich vliv na bezpečnost občanů ČR Audit národní bezpečnosti ČR, Ministerstvo vnitra ČR, Praha 2016, s. 10-138

[44] Obranná strategie ČR, Ministerstvo obrany ČR, Praha 2017, s.

[45] Zákon č. 181/2014 Sb. s následujícími novelizacemi – novela prostřednictvím zákona č. 104/2017 Sb., č. 183/2017 Sb., č. 205/2017 Sb., č. 35/2018 Sb., č. 111/2019 Sb. a č. 12/2020 Sb.

má jako správní orgán ve své působnosti relativně široké vymezení a vedle problematiky kybernetické bezpečnosti garantuje i otázky ochrany utajovaných informací v oblasti kybernetiky a informatiky i informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku veřejně regulované služby v rámci družicového systému Galileo[46]. NÚKIB ale nemá přímou působnost v otázkách kybernetické obrany státu. Tato gesce byla vládním rozhodnutím svěřena do působnosti Vojenského zpravodajství. Stalo se tak novelou zákona č. 298/2005 Sb. prostřednictvím zákona č. 150/2021 Sb. o Vojenském zpravodajství z července 2021. Toto vládní rozhodnutí zásadně změnilo postavení jedné ze tří českých zpravodajských služeb, které dosud měly výhradně informační, tj. nevýkonnou působnost. Rozšířením pravomocí Vojenského zpravodajství o problematiku kybernetické obrany, která v sobě mj. zahrnuje vedle aktivit Velitelství kybernetických sil a informačních operací AČR[47] i aktivní zapojení Vojenského zpravodajství v oblasti kybernetické obrany státu. Vojenští zpravodajci v tomto kontextu budují Národní centrum kybernetických operací s cílem aktivně odvrátit nebo zastavit kybernetický útok[48], ale také preventivně reagovat na možná kybernetická rizika.

S riziky v kybernetické oblasti jsou úzce spojeny i nepřátelské aktivity některých státních i nestátních aktérů realizované tzv. hybridními metodami působení. Vláda ČR s odkazem na BS ČR (2015) schválila v dubnu 2021 vedle již zmíněné **Národní strategie kybernetické bezpečnosti 2020-2025** další významný strategický dokument **Národní strategii pro čelení hybridnímu působení[49]**. Tato strategie je příkladem konkrétní reakce státu na jednu fakticky pojmenovanou a proti ČR (a integracím) reálně působící bezpečnostní hrozbu. Koncepce byla zpracována za široké účasti zástupců české bezpečnostní komunity z rezortů vnitra, obrany, zahraničí, zpravodajských služeb, úřadu vlády,

---

[46] Dostupné z https://www.nukib.cz/cs/o-nukib/ [online, cit. 2021-05-26].
[47] KySIO – Velitelství kybernetických sil a informačních operací „působí nezávisle, společně nebo v součinnosti s pozemními, vzdušnými a speciálním silami".
Dostupné z https://www.acr.army.cz/struktura/generalni/kyb/velitelstvi-kybernetickych-sil-a-informacnich-operaci-214169/ [online, cit. 2021-05-26].
[48] Dostupné z https://www.vzcr.cz/kyberneticka-obrana-46. [online, cit. 2021-05-26].
[49] Dostupné z https://www.mocr.army.cz/assets/informacni-servis/zpravodajstvi/narodni-strategie-pro-celeni-hybridnimu-pusobeni.pdf [online, cit. 2021-05-26].

NÚKIB nebo Armády ČR. Strategie mj. předpokládá vytvoření indikátorů hybridního působení, které budou využitelné i pro veřejnou správu.[50] Na MV ČR působí Centrum proti hybridním hrozbám[51], pozice na úrovni předsednictva vlády se v době psaní této práce ještě hledá, i když byla tato problematika dočasně svěřena do gesce poradce pro národní bezpečnost.

2.4. VÝZKUM FAKTOROVÉ SKLADBY BEZPEČNOSTNÍCH HROZEB PROVEDENÝ NA POLICEJNÍ AKADEMII ČR V PRAZE

Důležitým příspěvkem k přesnějšímu vymezení aktuální faktorové sklady bezpečnostních hrozeb ČR byl výzkum organizovaný v letech 2016–2019 na Policejní akademii ČR v Praze[52]. Jedná se celkem o tři navazující fáze empirického výzkumu, jejichž závěry byly průběžně publikovány v několika statích[53]. Tento výzkum byl zaměřen především na problematiku modelování faktorové sklady bezpečnostních hrozeb v takřka identicky provedených šetřeních. Jednotlivá zkoumání však byla provedena na odlišných skupinách respondentů. **První etapa** vědeckého výzkumu modelování exaktního odhadu faktorových skladeb hrozeb byla zaměřena na odbornou veřejnost v České republice (konkrétně na zástupce policie, hasičů, celníků, ministerských úředníků nebo akademických pracovníků, tj. na celkem 233 respondentů)[54]. **Druhá etapa**

---

[50] Vláda schválila Národní strategii pro čelení hybridnímu působení Dostupné z https://mocr.army.cz/assets/informacni-servis/zpravodajstvi/narodni-strategie-pro-celeni-hybridnimu-pusobeni.pdf / [online, cit. 2021-06-08].

[51] https://www.mvcr.cz/chh/

[52] V jeho prozatím poslední třetí části byl spoluřešitelem i autor této dizertační práce.

[53] 1) JAKUBCOVÁ, L., ŠESTÁK, B. a KOVAŘÍK, Z., (2017) Exaktní odhad faktorové skladby bezpečnostních hrozeb pro Českou republiku, Bezpečnostní teorie a praxe, 4/2017, s. 5-21, ISSN 1801-8211

2) JAKUBCOVÁ, L. (2018), Vnímání bezpečnostních hrozeb pro Českou republiku, Bezpečnostní teorie a praxe, 1/2018, s. 65-83, ISSN 1801-8211

3) JAKUBCOVÁ, L., KOVAŘÍK, Z., BLAŽEK, V. (2018), Odhad faktorové skladby bezpečnostních hrozeb pro Slovenskou republiku a její porovnání s Českou republikou, Bezpečnostní teorie a praxe, 3/2018, s. 45-63, ISSN 1801-8211

4) JAKUBCOVÁ, L., ŠESTÁK, B. and KOVAŘÍK, Z., (2017-2) Exact Estimation of factor composition of security threats for the Czech Republic, Bezpečnostní teorie a praxe, Policejní akademie ČR v Praze, 4/2017, s. 5-19, ISSN 1801-8211

5) PAĎOUREK, J., KOVAŘÍK, Z. (2019), Modelling the Factor Composition of Security Threats from the Perspective of Czech and Slovak Respondents and Experts in the CR, Bezpečnostní teorie a praxe, Policejní akademie ČR v Praze, 4/2019, s. 69-91, ISSN 1801-8211

[54] JAKUBCOVÁ, L., ŠESTÁK, B. a KOVAŘÍK, Z. (2017), s. 5-21. JAKUBCOVÁ, L. (2018) s. 65-83.

se zaměřila na stejný výzkum s takřka identickým složením profesní skladby respondentů ve Slovenské republice (zde celkem 407 respondentů)[55]. **Třetí etapa** výzkumu, které se již aktivně zúčastnil autor této dizertace, rozšířila dříve získané poznatky o konkrétní reakce skupiny již zmiňovaných 57 analytiků BIS.[56] Publikované závěry třetí etapy výzkumu jsou výsledkem celkového počtu oslovených respondentů všech tří výzkumů dohromady, jejichž konečný počet se navýšil na 731 osob. Takto zjištěné výsledky jsou logicky nejkomplexnější a také korigují některé dříve zjištěné poznatky i učiněné závěry. Nebyla však změněna sktruktura faktorových skladeb bezpečnostních hrozeb, která v porovnání s 11 faktorovou skladbou z BS (2015) a s 10 faktorovou skladbou z ANB (2016) je strukturovanější a přesněji a vykazuje jen pětibodovou faktorovou škálu. Bezpečnostní hrozby obsažené v této faktorové skladbě tvořily během posledně jmenovaného empirického výzkumu s analytiky BIS páteř použitého dotazníku k problematice relevance bezpečnostních hrozeb. Dotazník byl však rozšířen o další tři klíčové geopolitické elementy (Rusko, Čína, Severní Korea), které jsou v ČR obecně vnímány jako významná bezpečnostní hrozba.

V empirickém výzkumu této dizertace byla dotazována relevance konkrétních bezpečnostních hrozeb, které se explicitně vyskytují nebo mají oporu v českých bezpečnostních strategických dokumentech, souhrnně především v ANB (2016). Jedná se konkrétně o tyto položky (řazeno abecedně):

1) dlouhodobé sucho
2) hrozba neúspěšné integrace
3) hybridní hrozby
4) islámský radikalismus
5) kriminalita spojená s insolvenčním řízením
6) kybernetická špionáž
7) kyberterorismus
8) legalizace výnosů z trestné činnosti
9) levicový extremismus
10) narušení bezpečnosti e-governmentu

[55] JAKUBCOVÁ, L., KOVAŘÍK, Z., BLAŽEK, V. (2018), s. 45-63.
[56] PAĎOUREK, J., KOVAŘÍK, Z. (2019) s. 69-91.

11) narušení dodávek elektrické energie velkého rozsahu
12) narušení dodávek pitné vody velkého rozsahu
13) narušení dodávek plynu velkého rozsahu
14) narušení dodávek potravin velkého rozsahu
15) narušení dodávek ropy velkého rozsahu
16) narušení odolnosti IT infrastruktury
17) nepřátelské kampaně
18) neřízená migrace
19) organizovaná daňová kriminalita
20) ovlivňování veřejné správy cizí mocí
21) ovlivňování veřejného mínění cizí mocí
22) politický extremismus
23) povodně
24) pravicový extremismus
25) prorůstání organizovaného zločinu do veřejné správy
26) průmyslová bezpečnost
27) působení a vliv Číny
28) působení a vliv Ruska
29) působení a vliv Severní Koreje
30) radiační havárie
31) surovinová bezpečnost
32) terorismus osamělých vlků
33) únik nebezpečné látky
34) zahraniční bojovníci
35) získávání zákonem chráněných informací cizí mocí
36) zneužití legitimních služeb pro účely organizovaného zločinu
37) zneužívání veřejných zakázek a rozpočtů[57]

[57] Použitý výčet bezpečnotsních hrozeb je kompletně obsažený v Auditu národní bezpečnosti ČR (2016). Jedinou výjimkou jsou tři geopolitické hrozby: působení a vliv Ruska, působení a vliv Číny a působení a vliv Severní Koreje. Tyto tři položky byly do dotazníku doplněny autorem dizertace s tím, že se ruská a čínská bezpečnostní hrozba s přímým ohrožením ČR v textu ABN 2016 opakovaně vyskytuje.

Z pohledu aktuálních zkušeností je zřejmé, že v seznamu chybí např. pandemické hrozby a rozsáhlé virové epidemie, které v době realizace empirického výzkumu (přelom let 2019/2020) nebyly v českých bezpečnostních strategických textech příliš akcentovány, byť zmínky o nich se vyskytují jak BS ČR (2015)[58], tak v ANB (2016)[59]. V obou případech se však jednalo o popis přírodních, tedy tzv. neintencionálních hrozeb, na jejichž výskyt nemají zpravodajské služby žádný vliv. Jiná situace by nastala, pokud by se podařilo prokázat, že celosvětová pandemie covid-19 byla způsobena uměle, tzn. že vir byl rozšířen buď neúmyslně nebo úmyslně jednotlivci nebo kolektivními (státními) aktéry. Může se zdát, že byla světová pandemická krize Covid-19 spíše hrozbou způsobenou neúmyslně, tj. bez prokázaného lidského zásahu. Všechny vlády světa aktuálně řeší následky pandemie covid-19. Je však legitimní otázka, zda pandemii covid-19 způsobil přírodní nebo lidský faktor? Na jaře 2020 zveřejnily světové sdělovací prostředky podezření některých světových představitelů o možné odpovědnosti některé z velmocí za zamoření světa tímto virem[60]. Protože záležitost nebyla doposud uspokojivě řešena, bude patrně nezbytné v rámci spolupráce demokratických zpravodajských agentur prokazatelně najít a objasnit příčinu pandemie Covid-19. Pokud by se prokázalo, že byl virus vyvinut uměle v laboratořích některého státu a unikl mimo kontrolu bez varování ostatních, byl by to vážný problém nejenom z hlediska Úmluvy o biologických zbraních. Pokud by se dokonce prokázalo, že byl virus vyvinut uměle a úmyslně rozšířen, jednalo by se o bezprecedentní příklad tzv. státního terorismu nejvyššího rozsahu[61]. Tato problematika je v podstatě obsažena v otázce boje s terorismem.

---

[58] Bezpečnostní strategie ČR 2015, s. 10, Pohromy přírodního a antropogenního původu a jiné mimořádné události. Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2021-06-08].

[59] Audit národní bezpečnosti 2016, Přírodní hrozby, VI) Epidemie – hromadné nákazy osob, s.76, dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2021-06-08].

[60] První světovou političkou, která v televizním vystoupení označila Čínu za viníka koronavirové pandemie byla australská ministryně zahraničí Merise Payne. https://www.abc.net.au/news/2020-04-19/foreign-minister-marise-payne-coronavirus-pandemic/12163056?nw=0
Po ní se přidali další světové osobnost (např. D. Trump) i s žádostí o vyšetření tohoto obvinění. Evropský parlament ve svém usnesení dokonce vyzval, aby EU požádala Čínu o plné objasnění okolností vzniku pandemie a naposledy summit G7 v jihoanglickém Cornwallu (červen 2021) vyzval k prošetření této kauzy i za účasti Činy.

[61] Tyto teze byly autorem práce předneseny na světové konferenci World Intelligence Summit konané v prosinci 2020 v jihokorejském Soulu (online formou).

Ve výzkumu není rovněž samostatně zohledněna hrozba proliferace, resp. nešíření zbraní hromadného ničení, neboť je rovněž širší součástí zkoumané problematiky boje s terorismem. Otázka proliferace se však logicky objevuje v českých strategických textech. Např. ANB (2016) konstatuje, že *některé mezinárodní teroristické organizace přímo deklarovaly snahu o získání zbraní hromadného ničení, obecně ale platí, že stále převládá soustředění se na „konvenční" formy útoků… pravděpodobnost útoku za využití zbraní hromadného ničení je v ČR poměrně nízká, významné by ale v takovém případě byly dopady takové události*[62]. Nukleární proliferace se zdá být především militárním rizikem, za války Ruska proti Ukrajině se ukazuje i rostoucí (a zneužitelný) význam pro psychiku společnosti; z hlediska vojenského by použití taktických jaderných zbraní mělo patrně sporný přínos, ale dopad politický a psychologický by byl daleko horší. Podobné riziko aktuálně zesiluje na Blízkém východu (např. Írán), Opět v obou dimenzích, a možná i přesahující taktickou kapacitu.

Empirický výzkum této dizertace byl až na malé výjimky zaměřen na zkoumání relevance intencionálních hrozeb. Do seznamu byly zařazeny jen dvě neintencionální hrozby – *povodně a dlouhodobé sucho*, jako příklady dlouhodobě se vyskytujících přírodních katastrof s velmi negativním potencionálem na život české společnosti[63].

2.5. FAKTOROVÁ SKLADBA BEZPEČNOSTNÍCH HROZEB A JEJICH ČLENĚNÍ DO INTENCIONÁLNÍCH A NEINTENCIONÁLNÍCH SKUPIN

[62] Audit národní bezpečnosti (2016), III. Teroristická hrozba z hlediska nástrojů terorismu, a) Zneužití zbraní hromadného ničení, konvenčních zbraní, výbušnin a položek dvojího užití, s. 16.
[63] Absence pandemických hrozeb v empirickém výzkumu však z aktuálního pohledu vyznívá jako chyba. Nemá však smysl provádět dodatečný empirický výzkum zaměřený na pandemickou krizi, neboť získané výsledky by byly již ovlivněny aktuálními zkušenostmi s touto problematikou a celkové výsledky výzkumu by tím byly negativně zkresleny.

V této dizertaci byla použita původně pětibodová, později šestibodová faktorová skladba s konkrétně obsaženými bezpečnostními hrozbami rozšířenými o hrozby geopolitické povahy (nebezpeční vlivu Ruska, Číny a Severní Koreje):

1. **ohrožení působnosti státu a jeho ekonomické stability**

   (**9** bezpečnostních hrozeb,
   ve všech případech se jedná o hrozby intencionální, tj. v gesci zpravodajských služeb, řazeno abecedně)

   (kriminalita spojená s insolvenčním řízením, legalizace výnosů z trestné činnosti, organizovaná daňová kriminalita, ovlivňování veřejné správy cizí mocí, ovlivňování veřejného mínění cizí mocí, prorůstání organizovaného zločinu do veřejné správy, získávání zákonem chráněných informací cizí mocí, zneužití legitimních služeb pro účely organizovaného zločinu, zneužívání veřejných zakázek a rozpočtů);

2. **hrozby v kyberprostoru**

   (**6** bezpečnostních hrozeb,
   ve všech případech se jedná o hrozby intencionální, tj. v gesci zpravodajských služeb, řazeno abecedně)

   (hybridní hrozby, kybernetická špionáž, kyberterorismus, narušení bezpečnosti eGovernmentu, narušení odolnosti IT infrastruktury, nepřátelské kampaně);

3. **hrozby spojené s hrozbami migrace a terorismu**

   (**5** bezpečnostních hrozeb,
   ve všech případech se jedná o hrozby intencionální, tj. v gesci zpravodajských služeb, řazeno abecedně)

   (hrozba neúspěšné integrace, islámský radikalismus, neřízená migrace, terorismus osamělých vlků, zahraniční bojovníci);

4. **hrozby extremismu**

   (**3** bezpečnostní hrozby,

ve všech případech se jedná o hrozby intencionální, tj. v gesci zpravodajských služeb, řazeno abecedně)

(levicový extremismus, *politický extremismus, pravicový extremismus);*

5. **hrozby energetické, surovinové, průmyslové a environmentální**

(**11** bezpečnostních hrozeb,
V 9 případech se jedná o hrozby intencionální, tj. v gesci zpravodajských služeb, 2 posledně jmenované hrozby – povodně a dlouhodobé sucho – jsou hrozbami neintencionálními, tedy mimo přímou působnost zpravodajských služeb)

(dlouhodobé sucho, *narušení dodávek elektrické energie velkého rozsahu, narušení dodávek pitné vody velkého rozsahu, narušení dodávek plynu velkého rozsahu, narušení dodávek potravin velkého rozsahu, narušení dodávek ropy velkého rozsahu, povodně, průmyslová bezpečnost, radiační havárie, surovinová bezpečnost, únik nebezpečné látky*[64]*);*

6. **hrozby geopolitické**

(**3** bezpečnostní hrozby,
ve všech případech se jedná o hrozby intencionální, tj. v gesci zpravodajských služeb, řazeno abecedně)

(nebezpečí čínského vlivu, nebezpečí ruského vlivu, nebezpečí severokorejského vlivu).

V šesti faktorových skladbách je celkově obsaženo 37 významných bezpečnostních hrozeb, z toto 35 bezpečnostních hrozeb je intencionální povahy a pouze 2 hrozby neintencionální povahy (*dlouhodobé sucho a povodně)*. Je zde na místě konstatovat, že s rozvojem umělé inteligence (AI) přichází i nový druh hrozby, totiž neintencionální škody vysokého rozsahu.

[64] Původní návrh faktorové sklady bezpečnostních hrozeb v článku JAKUBCOVÁ, L., ŠESTÁK, B. and KOVAŘÍK, Z., Exact Estimation of factor composition of security threats for the Czech Republic, Bezpečnostní teorie a praxe, Policejní akademie ČR v Praze, 4/2017, s. 12-14, ISSN 1801-8211, finální podoba názvů faktorových skladeb je upřesněná, resp. došlo k rozšíření názvů 3. a 5. faktoru v článku PAĎOUREK, J., KOVAŘÍK, Z., Modelling the Factor Composition of Security Threats from the Perspective of Czech and Slovak Respondents and Experts in the CR, Bezpečnostní teorie a praxe, Policejní akademie ČR v Praze, 4/2019, s. 69-91, ISSN 1801-8211.

2.6. FAKTOROVÁ SKLADBA BEZPEČNOSTNÍCH HROZEB A JEJICH ČLENĚNÍ DO SKUPIN PODLE DOMÁCÍHO NEBO ZAHRANIČNÍHO PŮVODU

Zkoumané bezpečnostní hrozby lze rozdělit do dalších tří faktorových skupin zohledňující domácí nebo zahraniční původ aktérů:

- **bezpečnostní hrozby realizované spíše zahraničním aktérem**
  (*řazeno abecedně, 12 bezpečnostních hrozeb*)
  hrozba neúspěšné integrace
  hybridní hrozby
  islámský radikalismus
  kybernetická špionáž
  nebezpečí čínského vlivu
  nebezpečí severokorejského vlivu
  nebezpečí ruského vlivu
  nepřátelské kampaně
  neřízená migrace
  ovlivňování veřejné správy cizí mocí
  ovlivňování veřejného mínění cizí mocí
  získávání zákonem chráněných informací cizí mocí

- **bezpečnostní hrozby realizované spíše domácím aktérem nebo probíhající doma**
  (*řazeno abecedně, 6 bezpečnostních hrozeb*)
  dlouhodobé sucho
  kriminalita spojená s insolvenčním řízením
  povodně
  průmyslová bezpečnost
  radiační havárie
  únik nebezpečné látky

- **bezpečnostní hrozby realizované domácím i zahraničním aktérem**

(řazeno abecedně, 19 bezpečnostních hrozeb)

kyberterorismus

legalizace výnosů z trestné činnosti

levicový extremismus

narušení bezpečnosti eGovernmentu

narušení dodávek elektrické energie velkého rozsahu

narušení dodávek pitné vody velkého rozsahu

narušení dodávek plynu velkého rozsahu

narušení dodávek potravin velkého rozsahu

narušení dodávek ropy velkého rozsahu

narušení odolnosti infrastruktury

organizovaná daňová kriminalita

politický extremismus

pravicový extremismus

prorůstání organizovaného zločinu do veřejné správy

surovinová bezpečnost

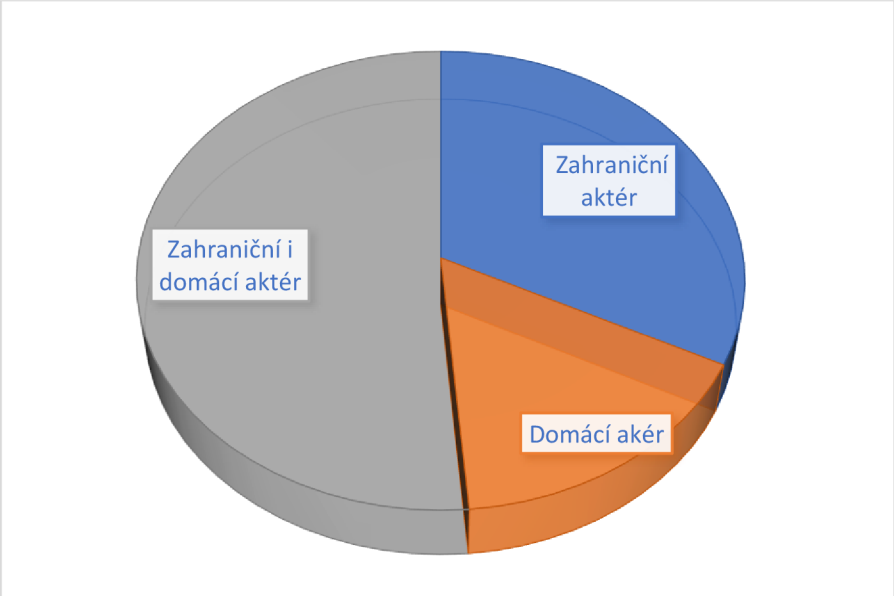
terorismus osamělých vlků

zahraniční bojovníci

zneužití legitimních služeb pro účely organizovaného zločinu

zneužívání veřejných zakázek a rozpočtů

Graf č. 1 – Faktorová skladba zkoumaných bezpečnostních hrozeb podle původu aktérů



2.7. FAKTOROVÁ SKLADBA BEZPEČNOSTNÍCH HROZEB V KONTEXTU ZÁKONEM AKTUÁLNĚ VYMEZENÉ PŮSOBNOSTI ČESKÝCH ZPRAVODAJSKÝCH SLUŽEB

České strategické dokumenty, tj. především BS ČR (2023 i 2015) a ANB (2016), popisují vztah zpravodajských služeb v oblasti zajišťování národní bezpečnosti v kontextu konkrétních bezpečnostních hrozeb takto:

BS ČR (2023) je výrazně změněna proti BS ČR (2015). Má méně popisný a více akční charakter, je komplexnější z hlediska hrozeb i z hlediska obrany proti nim. BS ČR (2023) zřejmě zpravodajské služby považuje za součást státních struktur natolik, že je ani přímo nezmiňuje a hovoří o povinnostech státu. Obrana je v textu traktována intenzivně, ale z toho, že není zmíněno ani VZ, lze usuzovat, že nezmínění služeb není dáno jen obranným zaměřením BS ČR, vyvolaným blízkými válkami, ale je součástí koncentrovaného konceptu. Naproti tomu BS ČR (2015) popisně konstatuje, že *nezastupitelnou roli při získávání, shromažďování a vyhodnocování informací potřebných pro zajišťování bezpečnosti ČR mají zpravodajské služby ČR*[65]. ANB (2016) nad rámec toho uvádí, že *zpravodajské služby mají vzhledem k povaze hodnocených hrozeb významnou úlohu při*

[65] Bezpečnostní strategie ČR (2015), V. Strategie prosazování bezpečnostních zájmů ČR, Institucionální rámec zajištění bezpečnosti, čl. 99, s. 21.

získávání, shromažďování a vyhodnocování informací v celém širokém spektru, zahrnující samozřejmě i zabezpečování informací o původcích propagandy, nepřátelské vůči zájmům ČR, a o dalších okolnostech a jevech, souvisejících s jejím šířením a pronikáním. Základní metodou ZS je získávání informací a jejich vyhodnocování, k čemuž mají v příslušné legislativě upraveny nástroje pro získávání informací, které je nutné s ohledem na narůstající a zcela nové hrozby modifikovat a přizpůsobit novému bezpečnostnímu prostředí, stejně jako i kapacity a prostředky k jejich uplatňování[66].

V souladu se zjištěnými a upřesněnými faktorovými skladbami (tj. rozdělení hrozeb na intencionální a neintencionální hrozby a upřesnění domácího, zahraničního nebo obojího vlivu bezpečnostních hrozeb) do příslušných okruhů působnosti práce zpravodajských služeb lze stanovit a popsat aktuální působnost českých zpravodajských služeb v kontextu aktuálně definovaných a popsaných bezpečnotsních hrozeb. K vytvoření tohoto souhrnu byl využit zvláště střechový zákon o zpravodajských službách (1994) a novela zákona o VZ realizovaná prostřednictvím zákona č. 150/2021 Sb., kde je exkluzivně ve veřejně přístupných zdrojích konkretizována zákonná působnost českých zpravodajských služeb. Vedle toho byly využity informace z veřejných částí výročních zpráv dvou zpravodajských služeb (BIS a VZ[67]) a v neposlední řadě i popis bezpečnotsních hrozeb a bezpečnostního prostředí vyjádřené v BS ČR (2015) a ANB (2016). Z poznatků zjištěných z těchto zdrojů byly stanoveny faktorové skladby obsahující základní kategorie zákonem daných aktivit českých zpravodajských služeb.

1. **ekonomická bezpečnost**
2. **kybernetická bezpečnost**
3. **migrace**
4. **terorismus**
5. **extremismus**

---

[66] Audit národní bezpečnosti (2016), Odpovědné instituce v rámci bezpečnostního systému ČR a základní nástroje (legislativa, strategie, koncepce) pro eliminaci hrozeb a rizik, Zpravodajské služby, s. 56.

[67] ÚZSI jako jediná z českých zpravodajských služeb nezveřejňuje žádné informace z jinak povinně zpracovávaných výročných zpráv.

6. **energetická bezpečnost**
7. **špionáž – nepřátelské aktivity cizích mocností**.

2.7.1. Ekonomická bezpečnost

Zpravodajským gestorem ekonomické bezpečnosti státu je v domácích podmínkách BIS a v zahraniční oblasti ÚZSI. BIS v této problematice v rámci mezinárodní zpravodajské spolupráce komunikuje napřímo i s důležitými zahraničními partnery. VZ tuto gesci přímo nepokrývá, v omezeném segmentu ekonomické bezpečnosti působí jen v případech majících vliv na rezort ministerstva obrany (MO). BS ČR (2023 i 2015) mj. řadí mezi strategické zájmy ČR *zajištění ekonomické bezpečnosti ČR a posilování konkurenceschopnosti ekonomiky*[68]. Rovněž ANB (2016) zmiňuje otázku ekonomické bezpečnosti v mnoha ohledech, avšak ekonomickou bezpečnost jako samostatný fenomén neuvádí. Zákonná působnost vyjádřena zákonem o zpravodajských službách (1994) BIS vymezuje tyto kompetence explicitně takto: BIS zabezpečuje informace *o činnostech, jejichž důsledky mohou ohrozit bezpečnost nebo významné* ***ekonomické*** *zájmy ČR*[69]. Rovněž ÚZSI, který podle stejného zákona zabezpečuje informace *„mající původ v zahraniční, důležité pro bezpečnost a ochranu zahraničně politických a* ***ekonomických*** *zájmů České republiky“*[70]. Pouze v případě VZ zákon nejmenuje konkrétně působnost vojenské zpravodajské služby v oblasti ekonomické bezpečnosti státu.

[68] Bezpečnostní strategie (2015), III. Bezpečnostní zájmy ČR, 14. strategické zájmy, s. 7 nebo Ekonomický rámec zajištění bezpečnosti, body 90-96, s. 20-21.
[69] Zákon č. 153/1994 Sb. o zpravodajských službách České republiky, §5 Působnost zpravodajských služeb (1) d.
[70] Zákon č. 153/1994 Sb. o zpravodajských službách České republiky, §5 Působnost zpravodajských služeb (2).

2.7.2. Kybernetická bezpečnost

České zpravodajské služby pokrývají svou působností bezpečnostní hrozby z oblasti kybernetické bezpečnosti v otázkách kybernetické obrany a kybernetické ochrany. Aktivní role zde byla exkluzivně svěřena VZ, které je zodpovědné za kybernetickou obranu státu a spolu s civilními zpravodajskými službami BIS a ÚZSI je aktivní i v oblasti kybernetické ochrany. Kybernetickou ochranu státu gesčně zajišťuje Samostatné oddělení kybernetické bezpečnosti Ministerstva vnitra ČR, které je součástí sekce vnitřní bezpečnosti MV. Zatímco střechový zákon o zpravodajských službách (1994) se v popisu zákonné působnosti u civilních zpravodajských služeb BIS a ÚZSI o kybernetice vůbec nezmiňuje, novela zákona o VZ (2021) rozpracovává gesci kybernetické obrany do nejmenších podrobností[71]. Problematika zákonem popsané působnosti zpravodajských služeb v oblasti kybernetické bezpečnosti ilustruje zastaralost některých důležitých právních norem, které tomuto důležitému bezpečnostnímu fenoménu nevěnují dostačující pozornost. To lze s odkazem na dobu vzniku zákona (1994) sice pochopit, otázkou však zůstává, proč dosud nebyl tento zákon již kompletně novelizován tak, jak se tomu stalo v případě novely zákona o VZ (2021). Lze ale konstatovat, že BS ČR (2023 i 2015) a ANB (2016) na problém upozorňují především z pohledu kybernetické ochrany ČR. BS ČR (2023) v seznamu bezpečnostních hrozeb konkrétně jmenuje kybernetické útoky a v textu se už v roce 2015 BS ČR zabývá otázkami kybernetické bezpečnosti i dalšími druhy kybernetických hrozeb [72] (např. zajištění kybernetické bezpečnosti a obrany řadí mezi strategické zájmy ČR[73]). ANB (2016) zmiňuje otázku kybernetiky více jak 300krát a v kapitole Bezpečnostní hrozby v kyberprostoru třídí

[71] Novela zákona č. 289/2005 Sb. prostřednictvím zákon č. 150/2021 Sb. s účinností od 1.7. 2021. Touto novelou byla do zákona přidána nová Část čtvrtá – Činnost Vojenského zpravodajství při zajišťování obrany České republiky v kybernetickém prostoru. Např. § 16g poskytuje VZ i pravomoc provést aktivní zásah v kybernetickém prostoru po předchozím schválení ministra obrany a §16l zřizuje institut inspektora pro kybernetickou obranu. Zároveň byla rovněž k 1.7. 2021 novelizována část střechového zákona o zpravodajských službách ČR č. 153/1994 Sb. týkající se pravomocí VZ v tom smyslu, že zde přibyl odstavec, který konstatuje, že „*Vojenské zpravodajství se v rozsahu a způsobem stanoveným zákonem o Vojenském zpravodajství podílí na zajišťování obrany České republiky v kybernetickém prostoru*“ (novela zákona č. 153/1994 Sb., článek II, odst. 1.-5.).

[72] Bezpečnostní strategie ČR (2015), Bezpečnostní hrozby, Kybernetické útoky, s. 9.

[73] Bezpečnostní strategie ČR (2015), III. Bezpečnostní zájmy ČR, 14. Strategické zájmy, s. 7

toto ohrožení na hrozby kybernetické špionáže; narušení nebo snížení odolnosti IT infrastruktury; nepřátelské kampaně; narušení nebo snížení bezpečnosti eGovernmentu a kyberterorismus[74].

2.7.3. Migrace

Největší novodobá migrační vlna prošla Evropou právě v době, kdy se finalizoval text BS ČR (2015) i text ANB (2016). BS ČR (2015) hodnotí negativní aspekty mezinárodní migrace jako jednu ze základních bezpečnostních hrozeb pro ČR a dále se věnuje i otázkám tzv. nelegální migrace. BS ČR (2015) konkrétně uvádí, že *nelegální migrace … je následně zdrojem či katalyzátorem řady bezpečnostních problémů. Nicméně i nedostatečná integrace zcela legálních migrantů může být zdrojem sociálního napětí*[75]. Poučení vývojem a komplexní přístup jsou patrny např. v b. 35 BS ČR (2023): ..*hrozbou je jak nelegální migrace, tak i neřízená a nekontrolovaná legální migrace, kdy stát není schopen účinně rozhodovat o objemu migračních toků či kontrolovat, kdo na jeho území vstupuje. Cílené zesilování nelegálních migračních toků se stává i nástrojem nepřátelského působení třetího státu. Hrozbou je též nedostatečná nebo neúspěšná integrace pobývajících cizinců, která s sebou přináší riziko vytváření uzavřených komunit cizinců, včetně paralelních mocenských struktur, riziko sociální fragmentace společnosti a nárůstu xenofobie, netolerance a extremismu ve společnosti.*

ANB (2016) zmiňuje migraci téměř 200krát a problematiku analyzuje v samostatné kapitole Bezpečnostní aspekty migrace, kde mj. uvádí, že *důležité je sdílení zpravodajských informací v rámci národních států, stav propojení informačních systémů a databází, a to jak na úrovni mezinárodní, tak na úrovni meziresortní v rámci státních orgánů a orgánů samosprávy, které na jedné straně snižuje administrativní náročnost procesu a na druhé straně efektivně odhaluje obcházení legislativy*[76]. Zákonem vyjádřená působnost zpravodajských služeb se však konkrétně o migraci ani v jednom případě nezmiňuje. Veřejné části výročních

[74] Audit národní bezpečnosti, 2. třídění hrozeb, s. 96-103, Praha 2016.
[75] Bezpečnostní strategie ČR (2015), Bezpečnostní hrozby, Negativní aspekty mezinárodní migrace, s. 9 a s.11.
[76] Audit národní bezpečnosti (2016), Bezpečnostní aspekty s. 62-75.

zpráv českých zpravodajských služeb (BIS a VZ) však jednoznačně dokazují, že je i problematika migrace součástí jejich aktivit. Velký důraz na tuto problematiku klade především BIS[77], VZ a ÚZSI mají gesci spíše v oblasti zahraničního zpravodajství.

2.7.4. Terorismus

Aktivní boj proti terorismu je jednou z klíčových aktivit každé zpravodajské služby a výjimkou nejsou ani domácí zpravodajské služby. ČR sice patří mezi země, které dosud nebyly zasaženy přímým teroristickým útokem většího rozsahu, avšak s ohledem na celkovou bezpečnostní situaci ve světě identifikují české strategické dokumenty hrozbu terorismu jako velmi vážnou. BS ČR 2015 jmenuje terorismus jako zásadní bezpečnostní hrozbu a konkrétně uvádí, že *hrozba terorismu jako metody násilného prosazování politických cílů je trvale vysoká*[78]. Podle BS ČR (2015) i BS ČR (2023) ČR *v rámci NATO přispívá k podpoře boje proti terorismu sdílením zpravodajských informací, rozvojem odpovídajících schopností, rozšířením konzultací s partnery a svojí aktivní účastí v aliančních operacích a misích*[79]. BS ČR (2023) terorismus zmiňuje nejenom co do obrany proti němu, ale i v zásadní části ve vztahu k budování resilience populace, resp. státu. ANB 2016 zmiňuje terorismus téměř 250x a bezpečnostní hrozbu terorismu detailně analyticky rozpracovává v samostatné kapitole[80]. ABN (2016) mj. uvádí, že *za terorismus lze označit takové jednání, které je politicky, nábožensky či jinak ideologicky motivováno a užívá násilí či jeho hrozby zejména s cílem vyvolat strach. Proti hrozbě terorismu není v současné době zcela imunní žádná země, ČR nevyjímaje*[81]. Konkrétní zmínka o působnosti zpravodajských služeb v oblasti terorismu je však ve střechovém zákoně o zpravodajských službách (1994) explicitně uvedena jen u BIS[82]. Je však nasnadě, že se otázkami terorismu aktivně zabývají i zbylé zpravodajské službě (ÚZSI, VZ), i když je tato

[77] Např. Výroční zpráva BIS za rok 2016 – veřejná část, Migrace, s. 8
[78] Bezpečnostní strategie ČR (2015), Bezpečnostní hrozby, Terorismus, s. 11.
[79] Bezpečnostní strategie ČR (2015), V. Strategie prosazování bezpečnotsních zájmů ČR, Strategie, prevence a potlačování bezpečnostních hrozeb, čl. 57, s 15.
[80] Audit národní bezpečnosti (2016), Terorismus, s. 10-27.
[81] Audit národní bezpečnosti (2016), Terorismus, 1. Úvod, s. 10.
[82] Zákon č. 153/1994 Sb. o zpravodajských službách ČR, § 5, (1) odst. e).

gesce, jako u mnohých jiných aktivit, ukryta v obecném popisu jejich zákonné působnosti (např. v případě ÚZSI, v odstavci *zabezpečuje informace mající původ v zahraničí, důležité pro bezpečnost a ochranu zahraničně politických a ekonomických zájmů České republiky*[83] nebo VZ *zabezpečuje informace mající původ v zahraničí, důležité pro obranu a bezpečnost České republiky*[84] a v domácím prostředí již jen v oblasti obrany ČR).

V celém světě existuje nekonečné množství definic terorismu. Uvádím zde definici izraelského profesora Boaze Ganora, neboť jeho ve světě citovaná definice má zcela jednoznačně definované parametry, které musí být naplněny, aby násilný akt mohl být klasifikován jako terorismus: „*Terorismus je záměrné použití násilí namířené proti civilním cílům za účelem dosažení politických cílů; nacionalistických, socioekonomických, ideologických, nábožensko-politických"*[85].

Dle české trestní legislativy je terorismus definován paragrafem 311 Teroristický útok a paragrafem 312 Teror Trestního zákoníku ČR. Česká republika, coby součást euroatlantického hodnotového prostoru, čelí novodobé teroristické hrozbě prakticky od roku 2001, kdy se stala součástí koalice bojující proti Al-Káidě a mezinárodnímu terorismu. ČR si je toho dobře vědoma a již 15 let zavádí do své legislativy i koncepčních materiálů nejrůznější prostředky boje s terorismem. V praxi se však ukazuje, že počáteční přesvědčení o výhradně zahraničním terorismu je nutném změnit a soudy tak příslušné paragrafy aplikovaly jak na případy českého terorismu (např. útok na trať), tak nejnověji na účast jednotlivců z ČR v teroristických operacích RF na území Ukrajiny.

---

[83] Zákon č. 153/1994 Sb. o zpravodajských službách ČR, § 5, (2).
[84] Zákon č. 153/1994 Sb. o zpravodajských službách ČR, § 5, (3) odst. a).
[85] *„Terrorism is the deliberate use of violence aimed against civilian targets in order to achieve political ends; nationalistic, socio-economic, ideological, religious-political."* GANOR, Boaz (2005), The Counter – Terrorism Puzzle: A Guide for Decision Makers, New Brunswick, NJ, Transaction Publishers, s. 17.

Tabulka č. 1 Působnost českých zpravodajských služeb na základě bezpečnostních hrozeb konkrétně jmenovaných v národních strategických dokumentech a podle stanovené faktorové sklady

Bezpečnostní hrozba	Působnost zpravodajských služeb	Poznámka
EKONOMICKÁ BEZPEČNOST	BIS, ÚZSI	VZ se této působnosti účastní pouze v specifickém segmentu ekonomických otázek mající vliv na rezort obrany.
KYBERNETICKÁ BEZPEČNOST	VZ, BIS, ÚZSI	VZ má exkluzivní gesci v otázkách kybernetické obrany státu. Kybernetická bezpečnost je však zajišťována i aktivitami a spoluprací zbývajících zpravodajských služeb ČR – BIS a ÚZSI.
MIGRACE	BIS, ÚZSI, VZ	Klíčovou gesci má BIS, je však náplní činnosti i ÚZSI a VZ.
TERORISMUS	BIS, ÚZSI, VZ	V domácí i zahraničí oblasti má klíčovou gesci BIS, i zbylé zpravodajské služby zde mají významnou aktivitu.
EXTREMISMUS	BIS, VZ, ÚZSI	V civilním sektoru má hlavní gesci BIS. VZ problematiku sleduje v rámci působnosti rezortu MO. ÚZSI má na starosti jen mezinárodní (zahraniční) přesah.
ENERGETICKÁ BEZPEČNOST	BIS, ÚZSI, částečně VZ	
NEPŘÁTELSKÉ AKTIVITY CIZÍCH MOCNOSTÍ (ŠPIONÁŽ)	BIS, VZ, částečně ÚZSI	

3. AKTUÁLNÍ ORGANIZACE A PŮSOBNOST ZPRAVODAJSKÝCH SLUŽEB ČR

Zpravodajské služby[86] jsou při zajišťování otázek národní bezpečnosti jedním z páteřních pilířů bezpečnostního aparátu státu. V literatuře, včetně té odborné, se vedle termínu „zpravodajské služby“ používá i nepřesný název „tajné služby“. Domnívám se, že je výstižnější používání termínu zpravodajské než tajné služby. Nabízejí se i další varianty, např. špionážní nebo výzvědné služby. Toto označení však spíše evokuje aktivity externích služeb a nemůže být obecně použito pro všechny typy zpravodajských agentur. Mezi českou politickou elitou, ale i v domácím mediálním prostoru spíše převládá termín tajné služby. Naprosto opačně však hovoří všechny právní dokumenty, které mluví jen o zpravodajských službách[87].

ČR disponuje relativně sofistikovaným zpravodajským aparátem, který tvoří tři samostatné zpravodajské služby. Právní status národních zpravodajských služeb ČR je komplexně obsažen v tzv. střechovém zákoně o zpravodajských službách č. 153/1994 Sb.[88], kde § 3 mj. uvádí, že v ČR působí **Bezpečnostní informační služba (BIS)** jako domácí civilní kontrarozvědka, **Úřad pro zahraniční styky a informace (ÚZSI)** jako zahraniční civilní rozvědka a **Vojenské zpravodajství (VZ)** jako vojenská vnější i vnitřní zpravodajská služba.

Všechny tři české zpravodajské služby plnily do roku 2021 specifické úkoly většinou bez konkrétních výkonných pravomocí, které jsou jinak typické pro

---

[86] Text kapitoly 3. byl již z velká části autorem publikován v samostatné kapitole kolektivní monografie PAĎOUREK, Jan (2020), Civilní zpravodajské služby v kontextu spolupráce s pořádkovou policií, kapitola 11, kniha HRINKO, Martin a kolektiv, Pořádková činnost policie, nakladatelství Aleš Čeněk, s. 307–320.

[87] PAĎOUREK, Jan, Tajné nebo zpravodajské služby? The Conservative.online, 9.5. 2021. Dostupné z https://theconservative.online/article/tajne-nebo-zpravodajske-sluzhby, [online, cit. 2020-011-06].

[88] Zákon č. 153/1994 Sb. O zpravodajských službách ČR, vedle vymezení statusu všech českých zpravodajských služeb (proto tzv. „střechový zákon“) ještě obsahuje právní status vnější zahraniční zpravodajský služby ÚZSI, která nemá vlastní zákon. Na rozdíl od BIS a VZ, jejichž existence je upravena samostatnými zákony o BIS č. 154/1994 Sb. a o VZ č. 150/2021 Sb.

orgány činné v trestním řízení. České civilní zpravodajské služby (BIS, ÚZSI) zůstaly i nadále organizacemi čistě informačními. Výjimku z ustáleného pravidla tvoří nová agenda kybernetické obrany, kterou byla od roku 2021 rozšířena působnost Vojenského zpravodajství[89]. Tato koncepčně a systémově důležitá změna, realizovaná novelou zákona o Vojenském zpravodajství[90], změnila dosud kompaktní charakter českých porevolučních zpravodajských služeb tím, že jedné z nich vymezila výkonné pravomoci, které byly dosud pro aktivity českých zpravodajských služeb nepřípustné. Vojenské zpravodajství však tuto kompetenci ve svém novém zákoně č. 150/2021 Sb. od zpravodajské činnosti odděluje.

Krátkým exkurzem do minulosti můžeme úvodem konstatovat, že bývalé československé a později české vlády nevyužily na počátku 90. let minulého století exkluzivní možnost relativně snadnou cestou vybudovat nový model zpravodajského aparátu v odlišné organizaci, než byla v podstatě převzatá klasická struktura zpravodajských služeb bývalého totalitního režimu (tj. I. správa FMV Hlavní správa rozvědky – dnes **ÚZSI**, II. správa FMV Hlavní správa kontrarozvědky –dnes **BIS** a III. správa FMV Hlavní správa vojenské kontrarozvědky – dnes částečně **VZ**). Počátkem 90. let minulého století se sice posuzovaly i jiné modely. Z řady možností lze zmínit např. návrh na zpravodajskou strukturu organizovanou jen dvěma službami – civilní a vojenskou nebo dvojicí služeb s vnitřní a vnější působností anebo jedné velké národní zpravodajské agentury absorbující všechny aktuální větve českého zpravodajského aparátu atd. I když série pokusů použít jiný model byla učiněna např. již v roce 1993, díky neshodám mezi tehdejším MV a MZV však k tomuto rozhodnutí nakonec nedošlo.[91]

---

[89]Vojenské zpravodajství disponovalo na rozdíl od obou civilních zpravodajských služeb – ÚZSI a BIS – již v minulosti konkrétními výkonnými pravomocemi. Do r. 2015 byla jeho součástí 601. skupina speciálních sil generála Moravce, účastnící se významných vojenských zahraničních misí např. v zemích bývalé Jugoslávie nebo v Afghánistánu.

[90] Novela zákona č. 289/2005 Sb. o Vojenském zpravodajství prostřednictvím zákona č. 150/2021 Sb.

[91] Civilní rozvědka 1990-1993, kolektiv autorů, vydal ÚZSI 2020, s. 44. Dostupné z https://www.uzsi.cz/files/Kniha_UZSI_nahled.pdf [online, cit. 2020-04-04].

Cesta k dnešní podobě národního zpravodajského systému vedla analogicky s procesy budování demokracie v naší zemi po roce 1989. Pád komunistického režimu v roce 1989 s sebou přinesl nekonečnou řadu systémových změn, které mj. způsobily i zásadní přeměnu a transformaci zpravodajského systému bývalého Československa a po roce 1993 samostatné České republiky.

Československý zpravodajský systém se po 2. světové válce, resp. po roce 1948, vyvíjel až do roku 1989 jako pevně ukotvený ve strukturách československého ministerstva vnitra pod přímým vlivem Komunistické strany. Komunistické zpravodajské služby byly jedním z klíčových mocenských, vlivových a represivních nástrojů tehdejší moci[92] a byly prostřednictvím tzv. sovětských poradců[93] přímo formovány a napojeny na nedůstojný dozorující protektorát sovětských bezpečnostních složek.

Příchod Sametové revoluce v roce 1989 tuto tendenci zcela změnil. Československá transformace národních zpravodajských služeb po roce 1989 začala v porovnání se zeměmi střední a východní Evropy **bezprecedentním rozhodnutím tehdejší československé vlády zcela ukončit činnost dosavadních komunistických zpravodajských složek**. Tyto služby byly v minulosti zformovány do organizační soustavy tzv. Státní bezpečnosti (StB) v gesci federálního ministerstva vnitra. Na jejich místě v rámci politiky absolutní diskontinuity s totalitním režimem byl po roce 1990 v ČR **vybudován nový národní zpravodajský aparát**[94]. Vedle systémových změn v podřízenosti

---

[92] Federální ministerstvo vnitra Československé socialistické republiky řídilo a využívalo činnost většiny tehdejších zpravodajských složek: vnitřní kontrarozvědku, zahraniční rozvědku i vojenskou kontrarozvědku, čímž v rámci jednoho resortu koncentrovalo nebývalou moc.

[93] KAPLAN, Karel. *Sovětští poradci v Československu 1949–1956*. Praha: Ústav pro soudobé dějiny AV ČR, 1993. Sešity Ústavu pro soudobé dějiny, sv. 14. ISBN 80-85270-26-9 nebo ŽÁČEK, Pavel, První garnitura sovětských poradců v Praze. Ovládnutí a řízení československého bezpečnostního aparátu, 1949–1953, Securitas Imperii, 2018/01, s. 40-69, ISSN 1804-1612.

[94] Při budování nového demokratického zpravodajského systému využily tento princip diskontinuity společně s Československem ještě vlády států Pobaltí. Naproti tomu většina postkomunistických zemí převzala větší část zpravodajské agentury z totalitní minulosti. Tento princip kontinuity s bývalým režimem byl využit např. v Polsku, Maďarsku, Rumunsku, Bulharsku nebo částečně po rozpadu ČSFR i na Slovensku.

jednotlivých nově se formujících českých zpravodajských služeb vůči různým autoritám[95] přestaly být nově budované české zpravodajské služby také zneužívány k mocenskému boji jako vlivový nástroj s důležitými výkonnými pravomocemi. Přestaly být represivním nástrojem politické zvůle. Nebyly již také napojeny na vnější zpravodajské a bezpečnostní vlivy a staly se zcela nezávislými a plně apolitickými. Obdobně jako ve většině zemí tradičních demokracií začaly i české zpravodajské služby vykonávat čistě informační aktivity ve prospěch konkrétně stanovených ústavních činitelů státu[96]. Hlavní rozdíl mezi komunistickým a demokratickým zpravodajským aparátem tedy leží v rozsahu jeho výkonných pravomocí a kompetencí,[97] v oblasti politizace vs. apolitizace, ale i v závislosti, resp. nezávislosti zpravodajských služeb na nedůstojné podřízenosti cizím zpravodajským nebo mocenskopolitickým centrálám.

Zpravodajské služby ČR jsou dnes organizovány tak, aby mohly naplnit potřeby tzv. zpravodajského cyklu, tedy procesu, který vede od zadání úkolu zpravodajské službě kompetentní státní autoritou až po předání požadované informace tomuto legálnímu zadavateli[98]. Řeč je o mnohdy dlouhé, složité a často i velice nákladné cestě od **zadání** zpravodajského úkolu kompetentními ústavními orgány zpravodajské službě; přes **převzetí** konkrétního zadání; jeho **rozboru a vyhodnocení**; **plánování** dalšího postupu včetně výběrů nebo vyhledávání či vytvoření vhodných informačních zdrojů; **sběru relevantních informací**; **analýzy** získaných informací a jejich případného zasazení do příslušného konkrétního

---

[95] Do roku 1989 spadaly všechny složky StB pod jurisdikci Federálního ministerstva vnitra ČSSR. Dnes Ministerstvo vnitra ČR řídí činnost ÚZSI, ministerstvo obrany řídí činnost VZ a vláda řídí aktivity BIS.

[96] … „*Výhradními příjemci výstupních informací jsou vláda a prezident republiky a pouze tito adresáti mohou zadávat službě konkrétní úkoly, ale vždy jen v zákonem daném rámci*“... Dostupné z *https://www.bis.cz/poslani-zasady-a-kredo/* [online, cit. 2019-11-21].

[97] Většina zpravodajských služeb malých a středně velkých zemí euroatlantického prostoru má pouze informační působnost a neúčastní se přímo aktivit orgánů činných v trestním řízení. Existují však i velké výjimky. Například americká FBI (Federální úřad vyšetřování), která má tyto aktivity i ve svém názvu, má vyšetřovací pravomoci v oblasti rozsáhlých federálních zločinů a podobně analogicky působí např. i ruská FSB (Federální bezpečnostní služba RF), i když její další zaměření je víceméně analogické se službami dříve působícími v totalitních státech sovětského bloku a dnes v podobných nedemokratických režimech.

[98] Podrobné informace o zpravodajském cyklu např. ve studii PHYTHIAN, Mark, Understanding of Intelligence Cycle (Studies of Intelligence), New York 2013, ISBN-10: 1138856320 nebo COLLONA Vilasi, A, The Intelligence Cycle. Open Journal of Political Science, 2018/8, 35-46, dostupné z https://www.scirp.org/pdf/OJPS_2017122815101250.pdf [online, cit. 2019-11-20].

rámce; **vypracování finálního výstupu**; **předání** konečné informace zadavateli a případně získání **zpětné vazby (tzv. feedback)** od zadavatele zpět ke zpravodajské službě.[99]

Současný model systémové podřízenosti českých zpravodajských služeb je do jisté míry nesystémový a neodpovídá současným potřebám prostředí i řízení zpravodajských služeb. I když po Sametové revoluci došlo relativně rychlým sledem událostí k odluce nových zpravodajských služeb od struktur bývalé Státní bezpečnosti, není dodnes proces systémové podřízenosti zpravodajských služeb uspokojivě dořešen. Rychlé odloučení od totalitních struktur bylo i výsledkem úsilí některých reaktivovaných příslušníků, jmenovitě Přemyslem Holanem nebo Zdeňkem Jodasem. Skupina vedená těmito muži mj. iniciovala sepsání klíčového koncepčního dokumentu s názvem „*Model zpravodajské služby*“, který mj. předpokládal i vyčlenění všech nově konstituovaných služeb ze struktury ministerstva vnitra.[100]

Ve sledu porevolučních událostí však došlo ke dvěma zásadním změnám. Byl schválen tzv. **střechový zákon o zpravodajských službách 153/1994 Sb.**, kde byla nově mj. vymezena i působnost a kompetence jednotlivých služeb a již v roce 1992 vznikla tzv. **Rada pro zpravodajskou činnost** jako pokus o koordinaci spolupráce mezi jednotlivými službami, ale i spolupráce zpravodajských služeb s vládou a klíčovými vládními resorty.

Střechový zákon o zpravodajských službách vyčlenil BIS z působnosti ministerstva vnitra a přeřadil jeho podřízenost přímo vládě[101]. Tento krok byl zřejmě důsledkem porevolučního přesvědčení představitelů nových politických elit o větším významu vnitřní zpravodajské služby pro potřeby státu na úkor zbývajících služeb.[102] I když podobný osud byl původně zvažován i ve vztahu k vnější zpravodajské službě ÚZSI (v r. 1993 byl zvažován koncept přeřazení

[99] PYTHIAN 2013. Z českých badatelů se problematice věnoval např. ZEMAN Petr, Zpravodajský cyklus – klišé nebo nosný koncept? Obrana a strategie 10/1 2010, ISSN 1214-6463, s. 45-64. článek dostupný z https://www.obranaastrategie.cz/filemanager/files/30274.pdf [online, cit. 2019-11-20].
[100] ÚZSI 2020, s. 32
[101] Zákon č. 153/1994 Sb., § 2.
[102] ÚZSI 2020, s. 41

podřízenosti ÚZSI z MV na MZV) nakonec díky nesouhlasu tehdejšího ministra zahraničí J. Zieleniece[103] zůstal rozpočet rozvědky jako samostatné organizační jednotky státu součástí rozpočtu MV s tím, že ředitele ÚZSI se souhlasem vlády jmenuje i odvolává ministr vnitra a ředitel ÚZSI je i ministru vnitra přímo odpovědný.[104] Analogický model podřízenosti byl uplatněn i ve vztahu Vojenského zpravodajství vůči ministerstvu obrany a konkrétně vůči ministrovi obrany,[105] i když z právního hlediska je ÚZSI od ministerstva vnitra oddělen výrazněji než VZ od ministerstva obrany, jehož je součástí.

Vznik Rady pro zpravodajskou činnost byl důležitým pokusem o zřízení jednotného vládního koordinačního místa činnosti zpravodajských služeb a jejich spolupráce s vládou po vzoru britského Joint Intelligence Committee[106] (JIC). Vznik tohoto orgánu byl i významným signálem o nové československé snaze apoliticky a demokraticky řídit zpravodajské služby. K tradičnímu britskému modelu JIC se však český ekvivalent nikdy ani nepřiblížil. Britský model mj. zahrnuje i významnou analytickou kapacitu s pravomocemi práce s konkrétními zpravodajskými informacemi a přímé zajišťování komunikace mezi službami a úřadem britského premiéra[107], což český VZČ postrádá. Dnes toto těleso pracuje pod názvem Výbor pro zpravodajskou činnost (VZČ) a je součástí Bezpečnostní

---

[103] ÚZSI 2020, s. 44

[104] Zákon č. 153/1994 Sb., § 3.

[105] Zákon č. 153/1994 Sb., § 4.

[106] Úkolem britského Joint Intelligence Committee mj. je:

- hodnotit události a situace související s vnějšími záležitostmi, obranou, terorismem, významnou mezinárodní trestnou činností, vědeckými, technickými a mezinárodními ekonomickými záležitostmi a dalšími nadnárodními otázkami, vycházet z tajných zpravodajských informací, diplomatických zpráv a otevřených zdrojů
- sledovat a včas varovat před vývojem přímých a nepřímých hrozeb a příležitostí v těchto oblastech pro britské zájmy nebo politiky a pro mezinárodní společenství jako celek
- pravidelně sledovat ohrožení bezpečnosti doma i v zámoří a řešit bezpečnostní problémy, které mu mohou být postoupeny
- přispívat k formulaci prohlášení o požadavcích a prioritách pro shromažďování zpravodajských informací a další úkoly, které mají zpravodajské agentury provádět
- udržovat dohled nad analytickými schopnostmi zpravodajské komunity prostřednictvím profesionálního vedoucího zpravodajské analýzy
- udržovat styk s Commonwealthem a zahraničními zpravodajskými organizacemi podle potřeby a zvažovat, do jaké míry jim může být jejich produkt zpřístupněn. Podrobněji v https://www.gov.uk/government/groups/joint-intelligence-committee [online, cit. 2020-04-04].

[107] Další informace o činnosti britského Joint Intelligence Committee dostupné z https://www.gov.uk/government/groups/joint-intelligence-committee [online, cit. 2020-04-04].

rady státu. Integrální součástí VZČ je i tzv. Společná zpravodajská skupina (SZS), jakýsi zúžený koordinační zpravodajský orgán příležitostně se scházející pod vedením ministerského předsedy a za účasti ředitelů služeb a ministrů vnitra a obrany.[108] Činnost těchto institucí však za uplynulých 30 let nikdy nepředstavovala skutečně systematickou a koncepční koordinaci práce zpravodajských služeb navzdory tomu, že v čele stojí autorita ministerského předsedy. Důvodem je mimo jiné fakt pouhého administrativního, technického nebo organizačního charakteru působnosti VZČ bez jakýchkoliv manažerských pravomocí, tj. bez jakékoliv autority VZČ vůči jednotlivým zpravodajským službám. Ani postavení premiéra nemůže za stávajícího stavu v této věci mnoho změnit. Premiérovy koordinační aktivity vůči zpravodajským službám logicky nemohou být díky mnoha dalším aktivitám a povinnostem systematické a koncepční, neboť se omezují pouze na nestálou a spíše nahodilou frekvenci společných setkání. Bez příslušných pravomocí VZČ vůči zpravodajským službám bude tento systém i nadále odkázán na pokračování relativně formálního postavení své existence.

ČR aktuálně zřídila novou pozici poradce premiéra (vlády) v otázkách národní bezpečnosti, tzn. jakéhosi „superúředníka“ pro národní bezpečnost. Tato pozice má jistou analogii v jiných zemích, např. v USA. Ve Spojených státech dlouhodobě působí národně bezpečnostní poradce prezidenta, který „*je federální vládní úředník, který radí prezidentovi v záležitostech týkajících se národní bezpečnostní politiky… Kromě poradenství prezidentovi Spojených států je poradce pro národní bezpečnost členem Rady národní bezpečnosti, která pracuje z Bílého domu, je formálně vedena prezidentem nebo, když je prezident nepřítomný, viceprezidentem. Pracuje jako asistent prezidenta pro záležitosti národní bezpečnosti a jeho role není funkcí na úrovni kabinetu. Nevyžaduje tedy potvrzení Senátu.*[109] Americký národně bezpečnostní poradce však není

[108] Detailnější informace o VZČ a SZS dostupné z https://www.vlada.cz/cz/ppov/brs/pracovni-vybory/zpravodajska-cinnost/vybor-pro-zpravodajskou-cinnost-3858/ [online, cit. 2020-04-04].

[109] What Does the National Security Advisor Do? Master Class, 12.9. 2022. Dostupné z https://www.masterclass.com/articles/what-does-the-national-security-advisor-do [online, cit. 2022-11-10].

koordinátorem zpravodajských služeb. Tím je v USA ředitel národního zpravodajství (Director of National Intelligence), který je „*vedoucím představitelem americké zpravodajské komunity, dohlíží na implementaci Národního zpravodajského programu a řídí jej a působí jako hlavní poradce prezidenta, Národní bezpečnostní rady a Rady vnitřní bezpečnosti pro zpravodajské záležitosti týkající se národní bezpečnosti. Prezident jmenuje DNI na radu a souhlas Senátu*“.[110]

Ve Velké Británii existuje model vládního sekretariátu pro bezpečnost (The National Security Secretariat), sídlící přímo v úřadu britského premiéra, který „*zajišťuje koordinaci bezpečnostních a zpravodajských otázek strategického významu napříč vládou. Samostatná Společná zpravodajská organizace vytváří nezávislá hodnocení ze všech zdrojů týkající se otázek národní bezpečnosti a důležitosti zahraniční politiky. Podporuje práci Národní bezpečnostní rady a Smíšeného zpravodajského výboru poskytují rady v těchto otázkách předsedovi vlády a dalším ministrům*“.[111] Vedle zpravodajského sekretariátu ve Velké Británii samostatně působí národně bezpečnostní poradce ministerského předsedy (Prime Minister's National Security Adviser), který předsedá Národní bezpečnostní radě (National Security Council).[112] V obou uvedených případech, v americkém i britském je zřejmé, že jsou pozice národně bezpečnostních poradců odděleny od funkcí koordinátorů zpravodajských služeb. V českém případě s odvoláním na studium otevřených zdrojů není zcela patrné, zda se počítá se stejným modelem nebo zda nově vytvářená pozice národně bezpečnostního poradce bude absorbovat i koordinaci zpravodajských služeb. Z logiky věci však vyplývá, že by bylo účelnější tyto funkce oddělit i v ČR.

[110] Oficiální stránky kanceláře ředitele amerického národního zpravodajství. Dostupné z https://www.dni.gov/index.php/who-we-are [online, cit. 2022-11-10].

[111] Oficiální stránky The National Security Secretariat. Dostupné z https://www.gov.uk/government/organisations/national-security/about [online, cit. 2022-11-10].

[112] Podrobněji dostupné z https://www.gov.uk/government/groups/national-security-council [online, cit. 2022-11-10].

3.1. ZÁKONNÉ VYMEZENÍ PŮSOBNOSTI ČESKÝCH ZPRAVODAJSKÝCH SLUŽEB

Střechový zákon o zpravodajských službách č. 153/1994 Sb. konkretizuje vymezení působností zpravodajských služeb následujícím způsobem:

*„**(1) Bezpečnostní informační služba** zabezpečuje informace*
***a)** o záměrech a činnostech namířených proti demokratickým základům, svrchovanosti a územní celistvosti České republiky,*
***b)** o zpravodajských službách cizí moci,*
***c)** o činnostech ohrožujících státní a služební tajemství,*
***d)** o činnostech, jejichž důsledky mohou ohrozit bezpečnost nebo významné ekonomické zájmy České republiky,*
***e)** týkající se organizovaného zločinu a terorismu.*
***(2) Úřad pro zahraniční styky a informace** zabezpečuje informace mající původ v zahraničí, důležité pro bezpečnost a ochranu zahraničně politických a ekonomických zájmů České republiky.*
***(3) Vojenské zpravodajství** zabezpečuje informace*
***a)** mající původ v zahraničí, důležité pro obranu a bezpečnost České republiky,*
***b)** o zpravodajských službách cizí moci v oblasti obrany,*
***c)** o záměrech a činnostech namířených proti zabezpečování obrany České republiky,*
***d)** o záměrech a činnostech ohrožujících utajované skutečnosti v oblasti obrany České republiky*
***e)** kybernetickou obranu ČR[113].*

***(4)** Zpravodajské služby plní další úkoly, pokud tak stanoví zvláštní zákon nebo mezinárodní smlouva, jíž je Česká republika vázána“*.[114]

[113] Novela zákona o Vojenském zpravodajství, zákon č. 150/2021 Sb. § 16 a – n.
[114] Zákon č. 153/1994 Sb., § 5

Tabulka č. 2
Zákonné vymezení působnosti zpravodajských služeb ČR s konkrétními příklady hrozeb obsažených ve strategických dokumentech

IMPLICITNĚ	TYP HROZBY
Záměry a činnosti namířené proti demokratickým základům, svrchovanosti a územní celistvosti ČR (BIS)	**Intencionální**
Činnosti ohrožující služební a státní tajemství (BIS)	**Intencionální**
Činnosti ohrožující bezpečnost ČR (BIS)	**Intencionální**
Činnosti ohrožující významné ekonomické zájmy ČR (BIS)	**Intencionální**
Informace původem ze zahraničí důležité pro bezpečnostní zájmy ČR (ÚZSI)	**Intencionální**
Informace původem ze zahraničí důležité pro zahraničněpolitické zájmy ČR (ÚZSI)	**Intencionální**
Informace původem ze zahraničí ohrožující důležité ekonomické zájmy ČR (ÚZSI)	**Intencionální**
Informace původem ze zahraničí důležité pro obranu ČR (VZ)	**Intencionální**
Informace původem ze zahraničí důležité pro bezpečnost ČR (VZ)	**Intencionální**
Záměry a činnosti ohrožující utajované skutečnosti v oblasti obrany ČR (VZ)	**Intencionální**
Kybernetická obrana (VZ)	**Intencionální**
Další úkoly, pokud tak stanoví zvláštní zákon nebo mezinárodní smlouva jíž je ČR vázána (BIS, ÚZSI, VZ)	**Intencionální**

Tabulka č. 2 ilustruje **složitost, nejednoznačnost, asymetrii a dublování** (i jistou míru chaotičnosti) zákonné působnosti českých zpravodajských služeb tak jak je patrná z otevřených zdrojů.

Některé velmi vágně vymezené působnosti v podstatě připouští jakoukoliv aktivitu zpravodajských služeb (např. působnost v oblasti *„činnosti ohrožující bezpečnost ČR“* nebo *„záměry a činnosti namířené proti demokratickým základům, svrchovanosti a územní celistvosti ČR“*). Lze konstatovat, že do takto

nepřehledně a nejasně koncipované působnosti českých zpravodajských služeb je možné zařadit prakticky cokoliv, tj. i všechny bezpečnostní hrozby, které jsou obsaženy v národních strategických dokumentech. Není však v silách ani možnostech žádné ze zpravodajských služeb ČR pokrýt ve stejné kvalitě tak velký rozsah odpovědnosti. I z tohoto důvodu je žádoucí stanovení jasné prioritizace (relevance) jednotlivých bezpečnostních hrozeb nezbytné k plánování činnosti, ale i lidských technických a finančních kapacit jednotlivých služeb.

Z textu je rovněž patrné, že střechový zákon o zpravodajských službách č. 153/1994 Sb. ne zcela aktuální zákon, nereflektující některé nové bezpečnostní výzvy současného světa s akcentem např. na kybernetickou bezpečnost. Text v podstatě vynechává některé důležité reakce na nové výzvy, například rychle se rozvíjející proces vývoje tzv. umělé inteligence (AI); možná rizika při zavádění moderních 5G a 5,5G sítí, kvantové počítače a rozbíjení šifer vč. již existujících digitálních archivů atd. Tento trend byl v současné době transparentně svěřen pouze do gesce Vojenského zpravodajství[115], přijetím novely zákona č. 150/2021 Sb. Zbývající dvě civilní zpravodajské služby – BIS a ÚZSI zůstávají informačními agenturami bez zákonem konkrétně vymezené působnosti v oblasti kybernetické bezpečnosti. Lze namítnout, že tato aktivita může být obsažena např. v popisu působností typu *„získávání informací původem ze zahraničí důležitých pro bezpečnostní zájmy ČR“* (ÚZSI) *nebo „činnosti ohrožující bezpečnost ČR (BIS)“.* Avšak tímto způsobem by bylo možné přistupovat ke všem dalším bezpečnostním hrozbám.

Střechový zákon o zpravodajských službách připouští duplicitu působnosti. Konkrétně se jedná o zákonné působení vnější zpravodajské služby ÚZSI a VZ v oblasti zajišťování „*Informací původem ze zahraničí důležitých pro bezpečnostní zájmy ČR*“. VZ je jedinou českou zpravodajskou službou, která pokrývá působnost v oblasti obrany i bezpečnosti současně. Kromě vyjmenovaných oblastí zákonné působnosti střechový zákon připouští úkolování služeb i v oblasti plnění *„dalších úkolů, pokud tak stanoví zvláštní zákon nebo mezinárodní smlouva jíž je ČR*

[115] Novela zákona o Vojenském zpravodajství. Zákon č. 150/2021 Sb.

vázána". Takto nekonkrétně definovaná působnost s otevřenou možností rozšířit priority práce služeb kdykoliv a jakýmkoliv směrem může zpravodajským službám způsobit problémy, neboť se ze samé podstaty jedná o velmi konzervativní instituce. Příslušné nastavení působnosti zpravodajské služby novým směrem je velmi dlouhodobá záležitost s nutností nalezení nových zpravodajských zdrojů, nalezení agentury atd. I zde je až nebezpečná absence centrální koordinace činnosti zpravodajských služeb, kdy například dvě citlivé operace vůči témuž zahraničnímu subjektu mohou mít zhoubné následky.

Ve vyspělých demokraciích je typické, že jsou zpravodajské služby považovány za elitní bezpečnostní složky státu, jejichž kapacitami se neplýtvá. Jejich expertíza totiž může mít klíčový význam pro zajišťování bezpečnosti země. Z tohoto důvodu je i jejich zákonná působnost většinou přesně vymezena a soustřeďuje se pouze na nejvýznamnější hrozby, kterým každá konkrétní země čelí. Popis působnosti bývá konkrétnější v případě vnitřních zpravodajských služeb a poněkud obecnější v případě vnějších zpravodajských služeb. Posledně jmenované kritérium se uplatňuje i v ČR a má svou logiku. Konkrétní popis působnosti vnitřních služeb má i svůj odstrašující potencionál pro nepřátelské špionážní aktivity. Naopak obecně pojatý popis působnosti vnějších služeb chrání tyto složky před potencionálními aktivitami cizích kontrarozvědných orgánů.

3.2. VELKÁ BRITÁNIE: KLÍČOVÉ BEZPEČNOSTNÍ HROZBY vs. PŮSOBNOST BRITSKÝH CIVILNÍCH ZPRAVODAJSKÝCH SLUŽEB JAKO PŘÍKLAD FUNKČNÍHO A TRANSPARENTNÍHO MODELU

Při hledání příkladu funkčního vzoru je na místě představit dlouhodobě fungující model, který v mnohých aspektech může posloužit i jako vzor vhodný následování. Velká Británie je jednou ze zemí, která relativně přesně definuje bezpečnostní hrozby a má dlouhodobou, více jak stoletou kontinuitu existence zpravodajských služeb. Hrozby definované britskými bezpečnostními experty jsou pojmenovány a popsány zcela transparentně. Relativně přesně je vymezena i působnost bezpečnostních složek – zpravodajské služby nevyjímaje.

Seznam klíčových bezpečnostních hrozeb lze najít ve veřejně publikovaných dokumentech vládního Centra pro ochranu národní infrastruktury.[116] Zákonná působnost jednotlivých zpravodajských služeb je dostupná na webových stránkách dvou britských civilních zpravodajských služeb – MI5 a MI6 (SIS).[117] Protože na rozdíl od některých českých zpravodajských služeb britské zpravodajské služby nezveřejňují žádnou část svých výročních zpráv, jsou tyto informace spolu s naprosto výjimečnými projevy či rozhovory vedoucích činitelů služeb fakticky jedinými relevantními zprávami o konkrétním zaměření aktivit britského zpravodajského aparátu. Základní úkoly i zaměření britských zpravodajských služeb je i součástí tzv. Intelligence Service Act z roku 1994[118].

Britská MI5 stejně jako MI6 každoročně vypracovává výroční zprávu (MI5/MI6 Annual Report). Tento dokument je podle zákona The Security Service Act z roku 1989[119] určený výhradně ministerskému předsedovi a ministrovi vnitra a žádná z jejích částí není veřejná. Nezávislé instituce jako je Úřad komisaře pro vyšetřovací pravomoci[120] (dříve Komisař pro dohled nad zpravodajskými službami[121]) a Výbor pro zpravodajství a bezpečnost[122] ale zveřejňují své vlastní zprávy o práci MI5[123]. Další podrobnosti spojené s britskou národní bezpečností

---

[116] Center for the Protection of National Infrastructure (https://www.cpni.gov.uk/national-security-threats) [online, cit. 2021-01-07].
[117] MI5 – britská vnitřní zpravodajská služba, ekvivalent české BIS: https://www.mi5.gov.uk/what-we-do [online, cit. 2021-01-07]. MI6 nebo tzv. SIS (Secret Intelligence Service) – britská vnější zpravodajská služba, ekvivalent českého ÚZSI: https://www.sis.gov.uk/about-us.html [online, cit. 2021-01-07].
[118] Intelligence Service Act, podrobně viz https://www.legislation.gov.uk/ukpga/1994/13/contents [online, cit. 2021-03-01].
[119] Dostupné z https://www.legislation.gov.uk/ukpga/1989/5/contents [online, cit. 2021-03-01].
[120] Investigatory Powers Commissioner's Office. Dostupné z https://www.ipco.org.uk/ [online, cit. 2021-03-01].
[121] Intelligence services Commissioner. Dostupné z https://www.gov.uk/government/organisations/intelligence-services-commissioner https://www.ipco.org.uk/ [online, cit. 2021-03-01].
[122] Intelligence and Security Committee of Parliament. Dostupné z https://isc.independent.gov.uk/ [online, cit. 2021-03-01].
[123] Dostupné z https://www.mi5.gov.uk/faq/does-mi5-produce-an-annual-report [online, cit. 2021-01-07].

lze získat v textu Národní bezpečnostní strategie Velké Británie z roku 2010: Silná Británie v časech nejistoty[124].

Experti Spojeného království fakticky definují pouze čtyři, resp. pět bezpečnostních hrozeb, resp. faktorových skupin bezpečnostních hrozeb, které obsahují náplň práce britských zpravodajských služeb:

- Terorismus
- Špionáž
  (MI5 domácí kontrarozvědná činnost/MI6 činnost proti nepřátelským aktivitám cizích mocí a vlád v zahraničí)
- Kybernetické hrozby
- Proliferace ZHN (jen MI5)
- Organizovaný zločin (jen MI5 a jen v letech 1996-2006).

Je zde patrná jasná prioritizace a důraz kladený pouze na hrozby klíčového významu. Toto vymezení umožňuje britským zpravodajským službám soustředit se jen na skutečně důležité bezpečnostní výzvy. Díky tomu mohou být britské zpravodajské služby efektivní a ve výsledku i úspěšné. Problematika organizovaného zločinu byla v gesci domácí MI5 jen omezenou dobu (1996-2006) a s ohledem na potřebu využití všech kapacit zpravodajské služby v boji s terorismem byla tato gesce předána výhradně specializovaným policejním jednotkám (National Crime Agency).

Patrný je ale např. rozdíl v absenci hrozeb, které jsou akcentovány spíše v bezpečnostních doktrínách nových členských zemí NATO nebo EU, ČR nevyjímaje. Zde je důraz často kladen na obavy z možného ohrožení státního upořádání, ústavního pořádku, zahraničněpolitické orientace státu nebo jeho územní celistvosti. Hrozby tohoto typu tradiční demokracie jako je Velké Británie většinou neřeší. Aktuální popis bezpečnostních hrozeb ale i zde podléhá občasné

[124] The national security strategy-a strong Britain in an age of uncertainty. Dostupné z https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228539/7291.pdf [online, cit. 2021-01-07].

aktualizaci, kdy se do popředí zájmu britských zpravodajských služeb dostávají problémy, které dříve nebyly tak patrné. Řeč je nyní především o oblasti kybernetického světa, který se plně vyprofiloval v průběhu minulé dekády. Díky nástupu nových technologií, rychlých sítí typu 5G a tzv. umělé inteligenci (Artificial Intelligence) budou tyto oblasti hrát i v práci zpravodajských služeb stále významnější roli, neboť se všechny významné i nevýznamné aktivity lidské společnosti postupně přemisťují do tohoto virtuálního kybernetického světa.

Tabulka č. 3
Velká Británie: klíčové bezpečnostní hrozby vs. působnost civilních zpravodajských služeb

Klíčové bezpečnostní hrozby pro Velkou Británii *podle vládního Centra pro ochranu národní infrastruktury* ***https://www.cpni.gov.uk/national-security-threats***	**Působnost MI5 – vnitřní zpravodajská služba** ***https://www.mi5.gov.uk/what-we-do***	**Působnost MI6 (SIS) – vnější zpravodajská služba** ***https://www.sis.gov.uk/about-us.html***
1. Terorismus	**ANO**	**ANO**
2. Špionáž	**ANO** (domácí kontrašpionáž)	**ANO** (působení mimo území Velké Británie proti aktivitám cizích zemí a vlád směřujícím proti zájmům Velké Británie)
3. Kybernetické hrozby	**ANO**	**ANO**
4. Proliferace zbraní hromadného ničení	**ANO**	**NE** (zprostředkovaně v kontextu jiných aktivit)
5. Organizovaný zločin	**ANO** (pouze v letech 1996-2006[125])	**NE**

Z tabulky č. 3 vyplývá, že popis bezpečnostních hrozeb v kontextu aktivit zpravodajských služeb klade velký důraz na **stručnost, jasnost a transparentnost** deskripce bezpečnostního prostředí, na **exkluzivitu** využívání britských zpravodajských služeb a jejich cíleného úkolování. Britský model se neutápí v bezbřehém a často málo srozumitelném popisu různých druhů bezpečnostních hrozeb a komplikované působnosti zpravodajských služeb.[126]

[125] MI5 podporovala britské bezpečnostní složky v oblasti organizovaného zločinu jen v letech 1996-2006. Dostupné z (https://www.mi5.gov.uk/what-we-do [online, cit. 2021-01-07].
[126] Zde se pochopitelně jedná o informace dostupné v otevřených zdrojích, jako jsou např. oficiální stránky britských zpravodajských služeb. To nevylučuje skutečnost, že britské zpravodajské služby

Exkluzivní postavení britských zpravodajských služeb v národním bezpečnostních systému a jejich expertíza je velmi přesně a jasně zaměřena na potírání nejzávažnějších bezpečnostních hrozeb. Jejich výkonnost není plýtvána na aktivity, které nelze hodnotit jako prioritní. V českých strategických dokumentech často chybí prioritizace bezpečnostních hrozeb a kompetenční rozdělení úkolů.

Ačkoliv z mnoha důvodů nelze srovnávat tradice, kapacity nebo globální vliv britských a českých zpravodajských služeb, lze v britské hierarchizaci hrozeb, zákonné působnosti zpravodajských služeb, v jednoduchosti a transparentnosti přístupu spatřovat model, který by bylo možné za určitých podmínek implementovat i v ČR. Samozřejmě při zohlednění místních bezpečnostních specifik a potřeb. České a britské, resp. i ostatní euroatlantické zpravodajské služby spojuje stejný cíl a stejné ideály, tedy i v podstatě stejné bezpečnostní hrozby. Tato dizertační práce hledá jednu z cest, jak k podobně fungujícímu modelu v ČR dospět.

4. VÝZKUMNÁ A ANALYTICKÁ ČÁST

Projekt empirického výzkumu

Motto dizertace - *„Řecké slovo **méthodos** (μέθοδος) znamená **cesta**.“* - jako ústřední myšlenka této práce předurčuje, že popisovaná metoda nemá ambici být konečným a finálním řešením zkoumaného problému. Cílem dizertační práce je spíše ukázat a popsat jednu z cest, která by mohla k cíli vést. A tato cesta vede přes oslovení konkrétní exkluzivní skupiny bezpečnostních expertů ČR, kterých se zřejmě nikdo na podobné otázky v tomto kontextu a rozsahu neptal. Zkoumaná problematika vyžaduje i cyklické opakování empirického výzkumu rozloženého v čase, aby mohly být zjištěné závěry nadále upřesňovány. Výzkum proto nabízí metodu, která by mohla být využita při budoucím zkoumání, popisu a analýze klíčových bezpečnostních hrozeb a rizik naší země nejenom v prostředí BIS, ale i

mají i jiné veřejně nepřiznané aktivity. Zde se nejedná jen o šíři zpravodajského záběru, ale i o časovou osu, neboť se aktuální bezpečnostní hrozby objevují nebo rychle mění ve své prioritě.

v rámci jiných složek bezpečnostních sborů ČR a v podstatě celé české bezpečnostní komunity (včetně odborné akademické obce). Takto zjištěné výsledky by bylo možné využít i v kontextu přesnějšího zaměření práce českého národního zpravodajského aparátu – například ve stanovení bezpečnostních priorit nebo strategií či plánů (včetně techniky a lidských zdrojů).

Výzkumný problém

Významné negativní změny na poli bezpečnostní situace v České republice si v roce 2015 vynutily přijetí Bezpečnostní strategie ČR. S využitím stanovisek 100 expertů bylo vymezeno celkem 34 bezpečnostních hrozeb. Dané bezpečnostní hrozby odrážely změny ve vnitropolitickém a mezinárodně politickém kontextu. Za daného stavu se ukazuje jako potřebné pokusit se poodhalit názorové pohledy skutečných odborníků, expertů na relevanci stanovených hrozeb a přinést alespoň dílčí poznatky, založené na exaktním empirickém výzkumu. Na Policejní akademii České republiky v Praze proběhl v několika fázích empirický výzkum, snažící se o stanovení relevance (důležitosti) jednotlivých uvedených bezpečnostních hrozeb a vymezení jejich optimální faktorové skladby, s využitím faktorové analýzy. Výběrový soubor respondentů byl tvořen studenty bezpečnostních oborů, policisty, příslušníky HZS a celní správy, úředníky ministerstva vnitra a akademickými pracovníky PA ČR.

Je zřejmé, že daný výběrový soubor nelze označit jako soubor expertů v bezpečnostní problematice. Proto jeho výsledky při odhadech relevance 34 bezpečnostních hrozeb je třeba chápat jako vychýlené a vytvořenou faktorovou skladbu spíše jako pomocnou. Nový rozměr do zjišťování relevance daných bezpečnostních hrozeb přineslo zapojení expertů, analytiků BIS. Jejich účast v empirickém výzkumu přinesla do zjišťování relevance bezpečnostních hrozeb plně profesionální a naprosto kompetentní přístup. Navíc do skladby bezpečnostních hrozeb byly zařazeny tři doposud neuvedené hrozby, což si vynutily změny na poli mezinárodní situace. Nová zjištění získaná od výběrového souboru expertů BIS (57 expertů) lze považovat za zcela unikátní.

V této souvislosti vyvstávají dvě výzkumné otázky:

1) Jaká je relevance bezpečnostních hrozeb obsažených v českých národních bezpečnostních dokumentech pohledem analytické skupiny BIS jako významné autority v oblasti analýzy národní bezpečnosti?
2) Je aktuální zákonná působnost a organizace a koordinace činnosti českých zpravodajských služeb v souladu se stanovenou relevancí národních bezpečnostních hrozeb?

Objekt, předmět, cíl a úkoly empirického výzkumu

Objektem empirického výzkumu bylo pojetí a relevance bezpečnostních hrozeb vymezených Bezpečnostní strategií ČR z roku 2015.

Předmětem empirického výzkumu byla dosavadní zjištění relevance bezpečnostních hrozeb a posuzovací stanoviska expertů BIS hodnotících relevanci 34 bezpečnostních hrozeb, doplněné o 3 nové bezpečnostní hrozby (působení a vliv Ruska, působení a vliv Číny, působení a vliv Severní Koreje).

Cílem empirického výzkumu bylo shrnutí dosavadních zjištění relevance bezpečnostních hrozeb (za ČR i SR), jejich faktorové skladby a přednostní úsilí zjistit míru relevance 37 bezpečnostních hrozeb v podání expertů BIS. Dále postihnout, zda je působnost a případně organizace a koordinace práce českých zpravodajských služeb v souladu s aktuální relevancí nebo naléhavostí národních bezpečnostních hrozeb.

Empirický výzkum se zaměřil na splnění **základních výzkumných úkolů:**

1. Prostřednictvím dotazníku zjistit názory výběrového souboru expertů BIS na relevanci 37 bezpečnostních hrozeb pro Českou republiku.
2. Na základě analýzy dat kvantifikovat empirická zjištění o relevanci 37 bezpečnostních hrozeb v pojetí expertů BIS a prostřednictvím

pseudokvantifikace[127] setřídit jejich relevanci od nejvyšší po nejnižší úroveň. Daná zjištění věcně interpretovat.

3. Porovnat úroveň věcně významných rozdílů při stanovení relevance celkového průměrného skóre a u jednotlivých bezpečnostních hrozeb s ohledem na délku služební praxe expertů BIS.

4. Pokusit se ověřit 6 faktorovou skladbu zjištěnou u 34 bezpečnostních hrozeb v rámci výběrových souborů za ČR i SR a v pojetí stanovisek expertů BIS doplněných na 37 bezpečnostních hrozeb.

Výzkumné předpoklady

VP01: Mezi hodnotícími stanovisky expertů BIS na relevanci 37 bezpečnostních hrozeb nebude zjištěn věcně významný vliv jejich služební praxe.

VP02: Faktorová skladba, tvořená 6 společnými faktory, která byla získána se zjištěných relevancí u 34 bezpečnostních hrozeb, se po ověření na datových souborech bez chybějících hodnot nebude výrazně měnit.

VP03: Faktorové složení bezpečnostních hrozeb se u faktorové skladby vypočtené na základě hodnotících stanovisek expertů BIS (n = 57) nebude od původního zjištění výrazně odlišovat.

Metodický přístup k analýze dat

Výběrový soubor byl pořízen na základě dostupnosti, tudíž závěry nelze zobecňovat na základní soubor (budou mít platnost pouze pro daný výběrový soubor). Statistická významnost (p-value) tak pozbývá v tomto případě svůj hlavní význam, lze podle ní pouze odhadovat dostatečnost rozsahu výběrového souboru. Pro ověřování vztahů mezi proměnnými bude tudíž využito pojmu „**ověřování výzkumných předpokladů**“ (tento pojem není omezen podmínkami induktivní statistiky).

[127] Pseudokvantifikace znamená setřídění ordinálních dat (stupně relevance) prostřednictvím stanovení střední hodnoty (aritmetického průměru) a směrodatné odchylky.

Odbornou veřejností upřednostňované míry PRE (proporcionální redukce chyby) podávají odpověď na otázku, o kolik může být lepší odhad jedné proměnné (závislé), jestliže jsou známy hodnoty jiné proměnné (nezávislé). Jiný, více používaný způsob interpretace říká, kolik procent variability v závislé proměnné vysvětluje vliv nezávislé proměnné.

Odpověď je vždy vyjádřena jako proporce v rozsahu od nuly do jedné, či procento v rozsahu od 0 % do 100 %. K mírám PRE, o kterých pojednávají pod čarou uvedení autoři,[128] se řadí důležitá asymetrická míra, tzv. koeficient β, která sleduje vliv nominální proměnné na proměnnou ordinální. Autorem uvedené míry je dvojice českých statistiků Jana Řeháka a Blanky Řehákové. Jde o regresní koeficient ordinální statistické závislosti s přímou procentuální interpretací. [129]

Nyní několik slov k upřesnění pojmu – akceptovatelný věcně významný rozdíl mezi proměnnými. V praktické analýze, při hledání skutečně akceptovatelných efektů se stále více dostává do popředí tzv. analýza věcně významnosti (effect of size). K tomu Petr Soukup dodává: „*Věcná významnost výsledku znamená, že naměřený rozdíl či zjištěná souvislost je důležitá pro vědecké poznání či praktické účely. Na rozdíl od statistické významnosti, která zjišťuje, zda nalezený výsledek je zobecnitelný (tj. zda není způsobený náhodou ovlivňující výběr jednotek či experimentálních podmínek), nám věcná významnost sděluje, zda o výsledku má vůbec smysl hovořit a zda má praktické důsledky (vč. důsledků pro vědu samotnou)*“[130].

K tomu, abychom zjistili, zda je výsledek věcně významný, a pokud ano, pak nakolik, je třeba mít určité ukazatele, míry věcné významnosti.“[131]

---

[128] Viz: VOGT Paul W., VOGT Elaine R., GARDNER Dianne C., HAEFFELE Lynne M. Selecting the Right Analyses for Your Data. New York: The Guilford Press, 2014, s. 292. ISBN 78-1-4625-1602-5.

[129] ŘEHÁK, Jan; ŘEHÁKOVÁ Blanka. *Analýza kategorizovaných dat v sociologii*. Praha: Academia, 1986, s. 252.

[130] SOUKUP, Petr. Věcná významnost výsledků a její možnosti měření. Data a výzkum – SDA Info, 2013, roč. 7, č. 2, s. 128. ISSN 1802-8152. V této souvislosti dodává: Samozřejmě nezpochybňuji okřídlený výrok: „*I nula je ve vědě výsledek*.“

[131] Viz: SOUKUP, Petr. Věcná významnost výsledků a její možnosti měření. *Data a výzkum – SDA Info*. 2013, roč. 7, č. 2, s. 127. ISSN 1802-8152.

Při aplikacích vždy vzniká otázka, jaká hodnota koeficientů je vysoká. Význam číselné hodnoty závisí na věcném významu proměnných a na modelu, který používáme. Jestliže očekáváme, že *A* je jedinou příčinou *B,* pak význam budou mít hodnoty vyšší než 0.6 nebo 0.7. Je-li *A* jednou z několika málo paralelních příčin heterogenity vzhledem k *B,* pak koeficienty 0.3, 0.5 budou vysoké. Je-li však *A* jednou z mnoha drobných příčin, pak i koeficient 0.1 či 0.05 je interpretovatelný. Toto pojetí je vymezeno oběma uvedenými českými statistiky.

V odborné literatuře je již delší dobu přijata konvence, jaké hodnoty koeficientů asociace (PRE) jsou chápány jako akceptovatelné na úrovni tří věcně významných efektů asociace. Roger E. Kirk ve své monografii vymezil tyto uvedené bodové odhady akceptovatelného věcně významného efektu vysvětlujícího rozptyl ω^2 následovně 0,01 – malý efekt; 0,059 – střední efekt; 0,138 – velký efekt).[132]

Svými hodnotami 0,01 (malý efekt); 0,06 (střední efekt) a 0,14 (velký efekt) se nabízí určité srovnávací hranice i pro výše uvedené koeficienty asymetrické asociace PRE, které budou použity v naší analýze s ohledem na typ porovnávaných dat. K výpočtu je použit software SPSS V13.0 a jeho speciální utilita.

K provedení explorační faktorové analýzy (EFA) bude použit moderní softwarový freewarový produkt FACTOR V12.04.05 vyvinutý na Univerzitě Rovira i Virgili, v podání Dr. Urbano Lorenzo-Seva a Dr. Pere Joan Ferrando.[133]

---

[132] KIRK, Roger E. Statistics: an Introduction. Fift Edition. Belmont, CA: Thomson Wadsworth 2008, s. 419. ISBN 978-0-534-56478-0. Koeficient $\omega 2$, jako ukazatel relativní věcné významnosti nezávislé na různých rozsazích výběrů (N), má také zásadní význam pro srovnávání výsledků z různých výzkumných studií. Tedy také tam, kde jde o syntézu řady výsledků z mnoha výzkumů, článků atp., v tzv. meta-analytických studiích. Tam není možné jen konstatovat statistickou významnost anebo nevýznamnost, nebo porovnávat hodnoty t-testů aj., právě pro neporovnatelnost různých výzkumů s různými rozsahy výběrů N.

[133] Blíže viz: https://psico.fcep.urv.cat/utilitats/factor/Download.html

K provedení konfirmační faktorové analýzy bude použit komerční produkt – LISREL V8.80. O explorační a konfirmační faktorové analýze pojednává mnoho odborníků.[134]

Složení výběrového souboru

Empirického výzkumu se zúčastnilo 57 pracovníků centrální analytické skupiny Bezpečnostní informační služby (BIS).

Tabulka č. 4 – Služební praxe

Služební praxe

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	1	7	12,3	13,0	13,0
	2	5	8,8	9,3	22,2
	3	3	5,3	5,6	27,8
	4	3	5,3	5,6	33,3
	5	2	3,5	3,7	37,0
	6	2	3,5	3,7	40,7
	7	1	1,8	1,9	42,6
	8	1	1,8	1,9	44,4
	9	1	1,8	1,9	46,3
	10	4	7,0	7,4	53,7
	11	1	1,8	1,9	55,6
	12	2	3,5	3,7	59,3
	13	1	1,8	1,9	61,1
	14	1	1,8	1,9	63,0
	15	3	5,3	5,6	68,5
	17	1	1,8	1,9	70,4
	18	8	14,0	14,8	85,2
	21	1	1,8	1,9	87,0
	22	1	1,8	1,9	88,9
	23	2	3,5	3,7	92,6
	24	1	1,8	1,9	94,4
	27	1	1,8	1,9	96,3
	28	2	3,5	3,7	100,0
	Celkem	54	94,7	100,0	
Vynechaná	System	3	5,3		
Celkem		57	100,0		

I když se na první pohled jedná o relativně malý počet respondentů[135], oslovení analytici BIS jsou svou exkluzivitou a kompaktností unikátní v tom, že se

[134] Viz např: Amy E. Hurley, Terri A. Scandura, Chester A. Schriesheim, Michael T. Brannick, Anson Seers, Robert J. Vandenberg and Larry J. Williams: Exploratory and Confirmatory Factor Analysis: Guidelines, Issues, and Alternative. Journal of Organizational Behavior , Nov., 1997, Vol. 18, No. 6 (Nov., 1997), pp. 667-683 Published by: Wiley. Dostupné z: https://www.jstor.org/stable/3100253.
McDONALD Roderick, Peter. Faktorová analýza a příbuzné metody v psychologii. Praha: Academia, 1991, s. 252. ISBN 80-200-0081-X.

[135] Osloveno bylo celkem 60 respondentů, z čehož 3 z blíže nespecifikovaných důvodů tento výzkum ignorovali.

jedná o skupinu vysoce elitních bezpečnostních expertů, kteří v každodenní interakci pracují se zřejmě nejpestřejší škálou bezpečnostních informací dostupných v ČR.

Řeč je o expertech, kteří mají přístup ke kompletnímu spektru zpravodajských informací získaných z poznatků vlastní zpravodajské činnosti BIS, ale i k důležitým informacím ze zdrojů ostatních českých bezpečnostních sborů a zpravodajských služeb, zde mám především na mysli elitní části Policie ČR, české civilní rozvědky – Úřadu pro zahraniční styky a informace (ÚZSI) a Vojenského zpravodajství (VZ) nebo z informačních databází dalších institucí české státní správy, bankovního sektoru atd. Analytici BIS v neposlední řadě pracují i se zpravodajskými a bezpečnostními informacemi ze zahraničí, získané v rámci mezinárodní zpravodajské výměny informací vyplývající především z našeho členství v Organizaci Severoatlantické smlouvy (NATO) a Evropské unie (EU). Výběrový soubor není náhodným výběrovým souborem, ale získaným na základě dostupnosti. S ohledem na svůj specifický profil lze konstatovat, že empirický výzkum lze plně označit jako **expertní empirické šetření**, bez nároků na zobecňování výsledků.

Rozložení respondentů – analytiků centrální analytické skupiny BIS s ohledem na jejich kategorizovanou praxi ukazují následující tabulky:

Tabulka č. 5 – Rozložení kategorizované služební praxe respondentů

Kategorizovaná služební praxe

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Do 2 let	12	21,1	22,2	22,2
	Od 2 do 22 let	36	63,2	66,7	88,9
	Nad 22 let	6	10,5	11,1	100,0
	Celkem	54	94,7	100,0	
Vynechaná	System	3	5,3		
Celkem		57	100,0		

Tabulka č. 6 – Rozložení kategorizované služební praxe respondentů

Kategorizovaná služební praxe

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Do 3 let	15	26,3	27,8	27,8
	Nad 3 roky	39	68,4	72,2	100,0
	Celkem	54	94,7	100,0	
Vynechaná	System	3	5,3		
Celkem		57	100,0		

Na základě údajů z výše uvedených tabulek lze konstatovat, že je podíl oslovených respondentů v kategoriích seniorních a juniorních pozic téměř vyrovnaný, jen s lehnou převahou seniorních pracovníků centrální analytiky BIS. Celkové oslovené spektrum respondentů v rozmezí 1–28 let služební (pracovní) praxe je rovnoměrně rozloženo v čase, přičemž nejvyšší podíl je zastoupený u pracovníků s 18 lety (14 %) a 1 rokem (12 %) délky profesionální praxe. Délka praxe byla jediným použitým identifikátorem, který byl nakonec ve vztahu ke konkrétním respondentům použitý. Bylo tak rozhodnuto jednak z hlediska specifického pracovního zařazení analytických pracovníků BIS a v určitých případech i kvůli nezbytnosti utajení jejich příslušnosti ke zpravodajské službě. Nezanedbatelným důvodem však bylo i zajištění skutečné anonymity (a tedy i objektivity) předaných odpovědí. Původně však bylo zvažováno i využití jiných identifikátorů, např. konkrétního nebo obecného druhu nejvyššího dosaženého vzdělání nebo genderové identity, avšak tyto údaje by ve výsledku neměly žádný dopad na konkrétní výsledek a kvalitu hlavního zaměření výzkumu, tj. zjištění relevance konkrétních bezpečnostních hrozeb. Uvedené tabulky délky služební praxe však jednoznačně demonstrují, že v rámci centrální analytické skupiny BIS výrazně nepřevažuje žádná ze skupin seniorních nebo juniorních pracovníků, a že je s ohledem na profesionální vývoj této důležité zpravodajské složky minimálně zajištěna žádoucí profesionální kontinuita.

Pro úplnost je nutné konstatovat, že ve výzkumu bylo osloveno 60 analytiků BIS, avšak platný (resp. zcela jednoznačný) údaj o délce praxe odevzdalo jen 54 oslovených respondentů.

Empirický výzkum mohl být realizován jen díky pochopení a vstřícnosti vedení BIS a její centrální analytiky. Zpravodajští analytici jsou obvykle využíváni pro analýzu konkrétních informací a jevů v kontextu s konkrétními bezpečnostními hrozbami a celkovým zaměřením zpravodajské služby. Výsledkem jejich analýz jsou z pravidla syntetické informační výstupy zpracované s ohledem na kvalitní verifikaci pramenů pocházejících často z nejrůznějších zdrojů. Zpravodajské výstupy jsou exklusivně určeny pouze zákonem vymezeným adresátům, především ústavním činitelům státu.

Daný empirický výzkum je zaměřený na stanovení relevance bezpečnostních hrozeb pohledem zpravodajských analytiků s ohledem na hierarchizaci míry nebezpečí z hlediska českých národních zájmů. Zjištěné výsledky by mohly pomoci upřesnit prioritizaci bezpečnostních hrozeb, které by také mohly být (resp. měly být) cílem aktivit českých zpravodajských služeb. V extrémním případě si lze představit i ankety (s respektem k různému zaměření služeb) jako standardizovanou součást přípravy komplexních materiálů exekutivy (priorit, strategií apod.).

V kontextu řečeného je však důležité konstatovat, že není v možnostech žádné české zpravodajské služby efektivně a ve stejně vysoké kvalitě pokrýt celé spektrum bezpečnostních hrozeb, které jsou obsaženy a popsány v českých strategických dokumentech. Právě proto je nutná kvalifikovaná prioritizace.

Proto zjištěná relevance nabízí stanovení prioritizace bezpečnostních hrozeb během určitého období. Jinými slovy stejně tak, jako je důležité a nezbytné v pravidelných intervalech a s ohledem na daný čas a aktuální vývoj a změny bezpečnostní situace aktualizovat konkrétní popis bezpečnostního prostředí a konkrétních národních bezpečnostních hrozeb, je možné i s pomocí empirického výzkumu zjistit aktuální relevanci (prioritizaci) stanovených bezpečnostních hrozeb. Výsledky tokových výzkumů mohou především napomoci kvalitnějšímu plánování činnosti zpravodajského aparátu, ale i přesnějšímu stanovení skladby a výši jejich rozpočtů, dlouhodobějšího zacílení jednotlivých zpravodajských služeb a v neposlední řadě i omezení nežádoucích překryvů zpravodajské činnosti

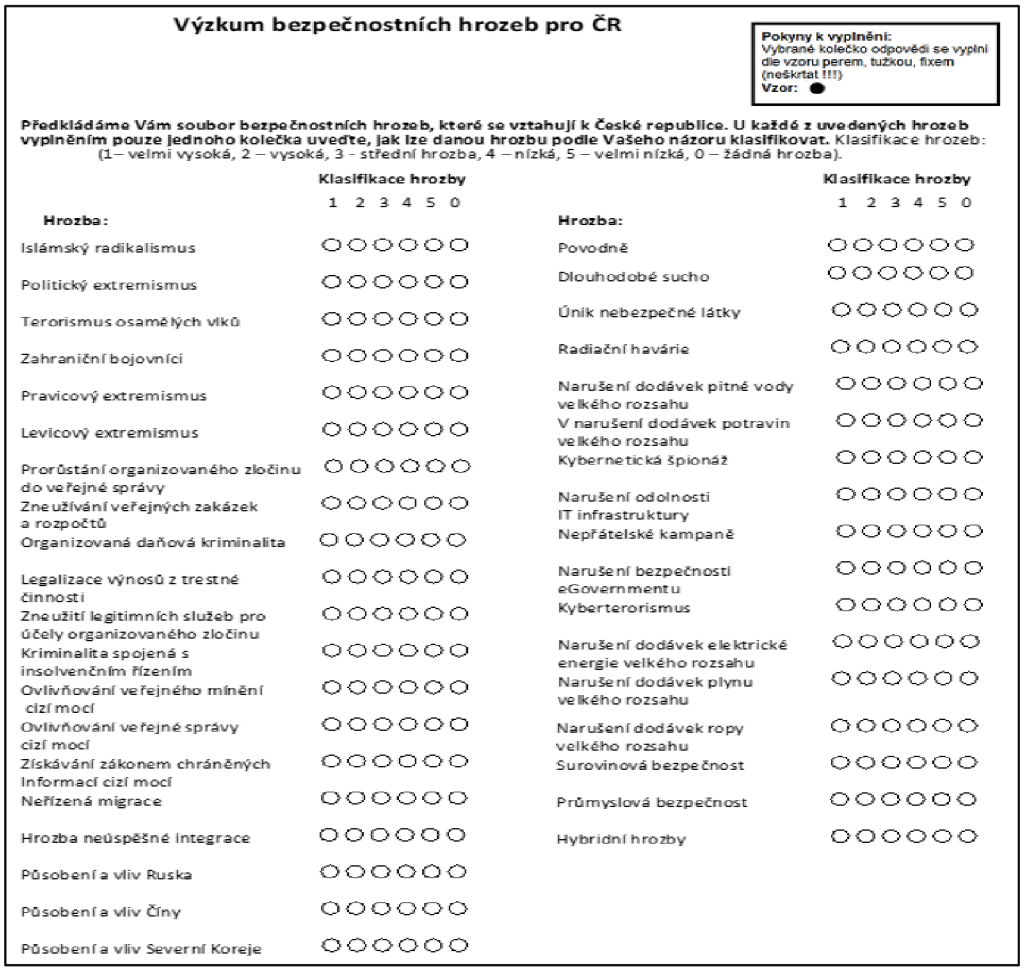
mezi jednotlivými službami. I tímto způsobem může dojít k minimalizaci eskalace zbytečných tenzí ve spolupráci konkrétních zpravodajských složek. Profesionální stanovení relevance bezpečnostních hrozeb rovněž může omezit nežádoucí veřejně prezentované rozdílné pohledy na národní bezpečnostní hrozby, které jsou mnohdy velmi protikladně komentovány bezpečnostní komunitou a některými českými ústavnímu činiteli[136].

Realizace empirického výzkumu

Empirický výzkum byl realizovaný v prostředí centrální analytiky BIS na jaře 2019. Pro potřeby této práce není důležité, že se již nejedná o zcela aktuální data, neboť cílem této dizertace není stanovit přesnou relevanci konkrétních bezpečnostních hrozeb v daném čase, jakož spíše ukázat metodu, jež by mohla být v budoucnosti použita při harmonizaci strategického pohledu různých částí komunity i při aktualizaci národního popisu bezpečnostních hrozeb a bezpečnostního prostředí.

[136] PAĎOUREK, Jan (2021), Rozdílné pohledy českých expertů a politiků na klíčové bezpečnostní hrozby, studie New Direction, Brusel, 19 s. Dostupné z https://newdirection.online/2018-publications-pdf/NDreportCZ-Rozdi%CC%81lnePohledy.pdf [online, cit. 2021-08-23].

Tabulka č. 7 dotazník použitý v empirickém výzkumu



Výzkum bezpečnostních hrozeb pro ČR

Pokyny k vyplnění:
Vybrané kolečko odpovědi se vyplní dle vzoru perem, tužkou, fixem (nešKrtat !!!)
Vzor: ●

Předkládáme Vám soubor bezpečnostních hrozeb, které se vztahují k České republice. U každé z uvedených hrozeb vyplněním pouze jednoho kolečka uveďte, jak lze danou hrozbu podle Vašeho názoru klasifikovat. Klasifikace hrozeb:
(1 – velmi vysoká, 2 – vysoká, 3 - střední hrozba, 4 – nízká, 5 – velmi nízká, 0 – žádná hrozba).

Hrozba:	Klasifikace hrozby 1 2 3 4 5 0
Islámský radikalismus	○ ○ ○ ○ ○ ○
Politický extremismus	○ ○ ○ ○ ○ ○
Terorismus osamělých vlků	○ ○ ○ ○ ○ ○
Zahraniční bojovníci	○ ○ ○ ○ ○ ○
Pravicový extremismus	○ ○ ○ ○ ○ ○
Levicový extremismus	○ ○ ○ ○ ○ ○
Prorůstání organizovaného zločinu do veřejné správy	○ ○ ○ ○ ○ ○
Zneužívání veřejných zakázek a rozpočtů	○ ○ ○ ○ ○ ○
Organizovaná daňová kriminalita	○ ○ ○ ○ ○ ○
Legalizace výnosů z trestné činnosti	○ ○ ○ ○ ○ ○
Zneužití legitimních služeb pro účely organizovaného zločinu	○ ○ ○ ○ ○ ○
Kriminalita spojená s insolvenčním řízením	○ ○ ○ ○ ○ ○
Ovlivňování veřejného mínění cizí mocí	○ ○ ○ ○ ○ ○
Ovlivňování veřejné správy cizí mocí	○ ○ ○ ○ ○ ○
Získávání zákonem chráněných informací cizí mocí	○ ○ ○ ○ ○ ○
Neřízená migrace	○ ○ ○ ○ ○ ○
Hrozba neúspěšné integrace	○ ○ ○ ○ ○ ○
Působení a vliv Ruska	○ ○ ○ ○ ○ ○
Působení a vliv Číny	○ ○ ○ ○ ○ ○
Působení a vliv Severní Koreje	○ ○ ○ ○ ○ ○

Hrozba:	Klasifikace hrozby 1 2 3 4 5 0
Povodně	○ ○ ○ ○ ○ ○
Dlouhodobé sucho	○ ○ ○ ○ ○ ○
Únik nebezpečné látky	○ ○ ○ ○ ○ ○
Radiační havárie	○ ○ ○ ○ ○ ○
Narušení dodávek pitné vody velkého rozsahu	○ ○ ○ ○ ○ ○
V narušení dodávek potravin velkého rozsahu	○ ○ ○ ○ ○ ○
Kybernetická špionáž	○ ○ ○ ○ ○ ○
Narušení odolnosti IT infrastruktury	○ ○ ○ ○ ○ ○
Nepřátelské kampaně	○ ○ ○ ○ ○ ○
Narušení bezpečnosti eGovernmentu	○ ○ ○ ○ ○ ○
Kyberterorismus	○ ○ ○ ○ ○ ○
Narušení dodávek elektrické energie velkého rozsahu	○ ○ ○ ○ ○ ○
Narušení dodávek plynu velkého rozsahu	○ ○ ○ ○ ○ ○
Narušení dodávek ropy velkého rozsahu	○ ○ ○ ○ ○ ○
Surovinová bezpečnost	○ ○ ○ ○ ○ ○
Průmyslová bezpečnost	○ ○ ○ ○ ○ ○
Hybridní hrozby	○ ○ ○ ○ ○ ○

Základem šetření bylo využití jednoduchého dotazníku, který obsahoval výčet konkrétních bezpečnostních hrozeb získaných z českých národních strategických dokumentů (Bezpečnostní strategie 2015, Audit národní bezpečnosti 2016, Obranná strategie ČR 2017 atd.). Respondentům bylo předloženo 34 přesně definovaných bezpečnostních hrozeb + tři hrozby geografické: působení a vliv Ruska, Číny a Severní Koreje s žádostí o vyznačení pouze jediné odpovědi u každé konkrétní hrozby v následujícím spektru:

1 – velmi vysoká, 2 – vysoká, 3 - střední, 4 – nízká, 5 – velmi nízká, 0 – žádná.

Vyplnění dotazníku proběhlo zcela anonymně a po schválení vedením BIS bylo realizováno počátkem roku 2019.

Setříděná relevance bezpečnostních hrozeb pro Českou republiku

Sebraná data byla vyhodnocena v tabulce třídění prvního stupně od nejnižšího aritmetického průměru (největší hrozby) po největší aritmetický průměr (nejnižší hrozby).

Tabulka setříděné relevance bezpečnostních hrozeb, která v sestupné tendenci (od nejvíce po nejméně nebezpečnou hrozbu) stanovila konkrétní a zřetelnou relevanci každé ze zkoumaných 37 bezpečnostních hrozeb. Sebraná data také mj. umožnila další analýzu každé z konkrétních bezpečnostních hrozeb již v kontextu jejich setříděné relevance i v kontextu aktuálních událostí a poskytla možnost, aby zjištěné výsledky byly komparovány s výsledky jiných výzkumů. Jedná se např. o průzkumy veřejného mínění na dané nebo podobné téma nebo v zákoně zveřejněném popis působnosti jednotlivých zpravodajských služeb ČR.

Tabulka č. 8 obsahuje vedle názvu bezpečnostní hrozby ve sloupci „N“ přesný a finální počet respondentů, kteří na konkrétní dotaz skutečně odpověděli. Ve sloupci „průměr“ uvádí hodnotu aritmetického průměru, která vyjádřená nižší hodnotou ve výsledku znamená vyšší relevanci zkoumané hrozby. Poslední údaj tabulky představuje tzv. „směrodatnou odchylku“, která určuje, jak moc jsou hodnoty uvedené jednotlivými respondenty odchýlené od aritmetického průměru. Nižší hodnota směrodatné odchylky znamená větší homogenitu (blízkost) v odpovědích respondentů.

Tabulka č. 8 - Setříděná relevance bezpečnostních hrozeb analytiky BIS (n = 57)

	N	Průměr	Směrodatná odchylka
Působení a vliv Ruska	57	1,60	,776
Kybernetická špionáž	57	1,68	,659
Ovlivňování veřejného mínění cizí mocí	57	1,74	,917
Působení a vliv Číny	57	1,79	,840
Ovlivňování veřejné správy cizí mocí	57	1,86	,895
Narušení odolnosti IT infrastruktury	57	1,91	,739
Zneužívání veřejných zakázek a rozpočtů	57	2,11	,724
Hybridní hrozby	56	2,11	,908
Nepřátelské kampaně	56	2,11	,985
Narušení bezpečnosti eGovemmentu	56	2,25	,879
Dlouhodobé sucho	57	2,28	,978
Prorůstání organizovaného zločinu do veřejné správy	56	2,41	,848
Získávání zákonem chráněných informací cizí mocí	57	2,46	,965
Kyberterorismus	56	2,50	1,079
Organizovaná daňová kriminalita	57	2,63	,816
Politický extremismus	57	2,63	1,029
Zneužití legitimních služeb pro účely organizovaného zločinu	57	2,68	,848
Legalizace výnosů z trestné činnosti	57	2,82	,735
Povodně	57	2,91	,950
Kriminalita spojená s insolvenčním řízením	57	3,11	,880
Terorismus osamělých vlků	57	3,19	1,043
Narušení dodávek plynu velkého rozsahu	57	3,25	1,106
Narušení dodávek pitné vody velkého rozsahu	56	3,25	1,254
Narušení dodávek elektrické energie velkého rozsahu	55	3,29	1,212
Narušení dodávek ropy velikého rozsahu	57	3,33	1,091
Surovinová bezpečnost	57	3,35	1,110
Průmyslová bezpečnost	56	3,38	,964
Islámský radikalismus	55	3,55	1,051
Hrozba neúspěšné integrace	57	3,58	1,017
Levicový extremismus	53	3,60	1,098
Pravicový extremismus	54	3,61	1,156
Únik nebezpečné látky	56	3,66	,769
Působení a vliv Severní Koreje	53	3,68	1,015
Zahraniční bojovníci	56	3,77	,894
Narušení dodávek potravin velkého rozsahu	53	3,89	1,171
Neřízená migrace	54	3,91	,917
Radiační havárie	54	4,15	,998

Oslovení respondenti měli možnost označit míru nebezpečí každé hrozby v uvedeném rozptylu „velmi vysoká – žádná hrozba“. V jistých případech se stalo, že některé z nabízených kritérií nebylo žádným z respondentů označeno, proto je detailní rozptyl každé konkrétní hodnocené hrozby velmi individuální. Tuto

skutečnost lze zaznamenat v níže komentovaných tabulkách, které vedle grafu každou bezpečnostní hrozbu uvádí.

Vedle komentářů a analýzy každé konkrétní bezpečnostní hrozby a následně provedené komparativní analýzy s jinými výzkumy se srovnatelným zaměřením (např. volně dostupných dat z některých tematicky podobných výzkumů veřejného mínění) tato výzkumná část prezentuje i jasnou názorovou neshodu v pohledu různých částí české bezpečnostní komunity (tj. zpravodajských služeb na straně jedné a odborné akademické veřejnosti a zástupců elitních policejních složek atd. na stran druhé) na konkrétní relevanci bezpečnostních hrozeb. Provedení této komparativní analýzy byla možná jen díky třem dříve realizovaným empirickým výzkumům o modelování faktorové skladby bezpečnostních hrozeb na Policejní akademii ČR v Praze, přičemž autor dizertace byl spoluřešitelem třetího a zatím posledního empirického výzkumu na toto téma.

4.3. RELEVANCE NÁRODNÍCH BEZPEČNOSTNÍCH HROZEB SETŘÍDĚNÁ ANALYTIKY BIS

4.3.1. A) BEZPEČNOSTNÍ HROZBY VYSOKÉ RELEVANCE

A1 PŮSOBENÍ A VLIV RUSKA
(intencionální bezpečnostní hrozba)

Anonymní empirický výzkum v prostředí centrální analytiky BIS zcela jasně označil „*působení a vliv Ruska*“ za absolutně největší bezpečnostní hrozbu pro Českou republiku. Jedná se však o hrozbu, která dlouhodobě způsobovala značné kontroverze ve veřejné diskusi expertní odborné bezpečnostní komunity a některých vrcholných ústavních činitelů České republiky[137]. Tato polemika byla ukončena (resp. dočasně umlčena) 24. únorem 2022, kdy došlo k otevřené ruské agresi proti Ukrajině. Následné události otevřeně eskalující v ruskou válku proti nezávislé Ukrajině svou razancí a brutalitou ze strany Ruska nejenom zaskočil

[137] PAĎOUREK, Jan (2022), Rozdílné pohledy českých expertů a politiků na klíčové bezpečnostní hrozby. Jedna středoevropská lekce, New Direction, 19 s., Brusel, Belgie

celý svět, ale dal za pravdu všem, kteří dlouhodobě v ruské politice spatřovali zásadní bezpečnostní ohrožené svobodného demokratického světa. Změnil se i celkový narativ této otázky v celé české společnosti. Skutečnost naléhavosti a závažnosti této bezpečnostní hrozby byla a je dlouhodobě zdůrazňována mnohými zcela konkrétními závěry, které prezentovaly a prezentují české zpravodajské služby ve veřejných částech výročních zpráv, s BIS[138] na čelné pozici. BIS nejenom konstatovala, ale často i s konkrétními příklady doložila, že jsou nejrůznější zpravodajské a jiné nepřátelské aktivity Ruské federace proti České republice a jejím spojencům závažným bezpečnostním problémem. Tento stav se netýkal pouze České republiky, ale dalších států euroatlantického hodnotového prostoru[139]. Závěry empirického výzkumu však významně podpořily mediálně známé stanovisko BIS v jejich zdůrazňovaném akcentu ohrožení našeho státu ze strany Ruska. Tím byla umocněna relevance této bezpečnostní hrozby a zároveň byly předloženy nové přesvědčivé argumenty a důkazy. Empirický výzkum byl realizován na jaře 2019, tj. téměř dva roky před zveřejněním kauzy Vrbětice[140] a tři roky před ruskou válkou proti Ukrajině. Bezprecedentní nepřátelský útok ruských zpravodajských služeb proti ČR ve Vrběticích medializovaný představiteli státu v dubnu 2021[141] potvrdil závažnost úsudku analytiků BIS a dal jejich jednoznačnému tvrzení nový a přesvědčivější obsah. Válka Ruska proti Ukrajině již jen naprosto přesvědčivě a tragicky ilustruje opodstatnění výše zmíněných závěrů. Ruská federace se nikdy nesmířila se ztrátou svého vlivu ve střední a východní Evropě, který Sovětská svaz a později Ruská federace ztratily po pádu komunismu na počátku 90. let minulého století. Aktuální aktivity Ruska v našem středoevropském prostoru mají za cíl jednak

---

[138] Podrobně dostupné z https://www.bis.cz/vyrocni-zpravy/ [online, cit. 2021-08-23].

[139] Např. USA – vyjádření šéfky amerických zpravodajců Avril Haines z dubna 2021, že Rusko a Čína jsou pro Ameriku největšími bezpečnostními hrozbami. Dostupné z https://www.npr.org/2021/04/14/987132385/intelligence-chiefs-say-china-russia-are-biggest-threats-to-u-s?t=1629733764639 [online, cit. 2021-08-23]

[140] Podrobněji např. „Do výbuchu ve Vrběticích byli podle zjištění BIS zapojeni příslušníci ruské tajné služby, oznámil Babiš". Dostupné z https://www.irozhlas.cz/zpravy-domov/andrej-babis-jan-hamacek-mimoradna-tiskova-konference-ministerstvo-zahranici_2104171945_kro [online, cit. 2021-07-29] nebo kompletní informace o průběhu akce dostupná z https://www.bellingcat.com/news/2021/04/20/senior-gru-leader-directly-involved-with-czech-arms-depot-explosion/ [online, cit. 2021-08-25]

[141] Např. Na výbuchu ve Vrběticích se podíleli ruští agenti, Česko vyhostí 18 diplomatů. Dostupné z https://zpravy.aktualne.cz/babis-a-hamacek-svolali-novinare-chystaji-na-ministerstvu-za/r~9e9059009fa411ebb0fa0cc47ab5f122/ [online, cit. 2022-02-14]

znovuobnovit ruský vliv ve střední a východní Evropě, ale i napomoci restaurovat ztracené velmocenské postavení, resp. pozice Ruska jako druhé globální supervelmoci. S tím jsou spojeny i ruské snahy rozmělnit jednotu a později samu existenci klíčových euroatlantických organizací (NATO, EU atd.) a dosáhnout stavu před pádem komunismu koncem 80. let minulého století. Ruská vojenská agrese proti Ukrajině však paradoxně způsobila pravý opak: členské státy NATO i EU se ještě více spojily a vytvořily silnou opoziční frontu ruské agresi. Jestliže Rusko před válkou na Ukrajině ke splnění svých cílů spíše používal různé metody a prostředky, velmi často spojené s tzv. hybridními způsoby soupeření, konfrontace nebo válčení (např. šíření dezinformací, falešných zpráv, pokusy o zasahování do kybernetické kritické infrastruktury státu nebo privátního sektoru, ovlivňování volebního procesu atd.), válka proti Ukrajině pak přerostla v kinetický konflikt bez jakékoliv tendence jeho skrývání. Vrbětický případ však také posunul ruské aktivity v České republice do fáze přímého konfliktu, při kterém také umírali lidé. Kreml má v prosazování svých cílů jistě celou motivační škálu, avšak často se zahraničními intervencemi hybridními nebo přímo válečnými jen snaží odvádět pozornost ruských voličů od krizových narativů domácí ekonomické, sociální nebo i politické reality[142]. Zohledňuje však i pozice nemalé části ruských občanů, kteří se s rozpadem Sovětského svazu nikdy nesmířili a skutečnost, že současná Ruské federace již nehraje roli druhého nejmocnějšího hegemona světa je stále velmi znepokojuje[143].

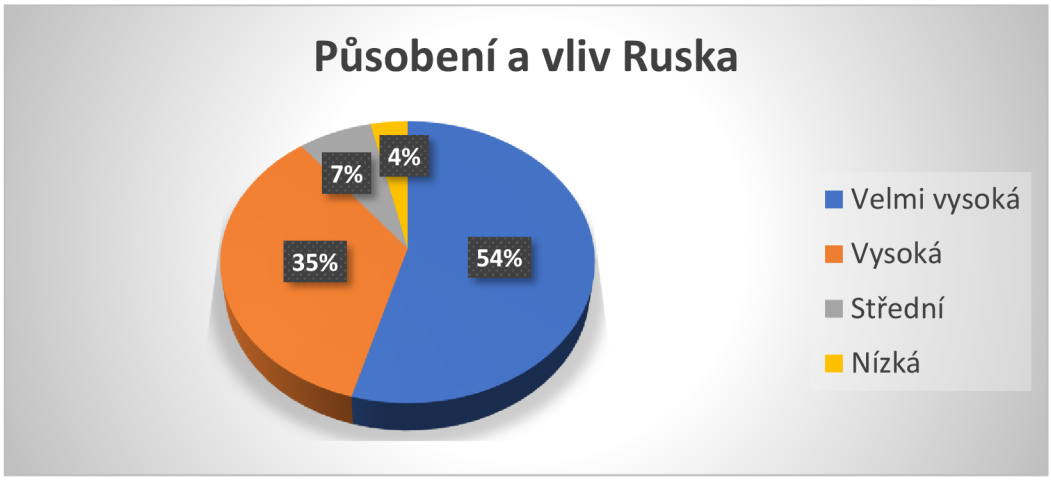
[142] PAĎOUREK, Jan (2021), Rozdílné pohledy českých expertů a politiků na klíčové bezpečnostní hrozby – jedna středoevropská lekce, 30 s., studie vydaná v edici nadace New Direction, CEVRO INSTITUT VŠ Praha

[143] Např. DEATH OF THE SOVIET UNION: Widespread nostalgia but no going back, IntelliNews, 12/2021. Dostupné z https://intellinews.com/death-of-the-soviet-union-widespread-nostalgia-but-no-going-back-228859/

Tabulka č. 9 a graf č. 2 Působení a vliv Ruska

Působení a vliv Ruska

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	31	54,4	54,4	54,4
	Vysoká	20	35,1	35,1	89,5
	Střední	4	7,0	7,0	96,5
	Nízká	2	3,5	3,5	100,0
	Celkem	57	100,0	100,0	



Z tabulky č. 9 a z grafu č. 2 vyplývá, že celkem 89,5 % procent respondentů ve škále „velmi vysoká a vysoká hrozba“ považuje působení a vliv Ruska za bezpečnostní hrozbu, pokud přidáme ještě hodnotu „střední hrozba“ je to celkově 96,5 %. Pouze 3,5 % oslovených analytiků BIS považuje ruskou hrozbu za nízkou. Žádný z respondentů nevyužil označení této bezpečnostní hrozby ve stupni „velmi nízká a žádná“. Průměr zkoumané hrozby vyjadřuje hodnotu 1,60. Směrodatná odchylka je 0,776, tzn., že se se jedná o nízkou hodnotu názorového rozptylu, resp., že se většina respondentů shoduje v názoru na finální hodnotu stanovené relevance. Ve zkoumaných hodnotách fakticky neexistuje žádný větší rozptyl reakcí jednotlivých skupin respondentů, neboť naprostá většina dotazovaných (téměř 90 %) označila hrozbu působení a vlivu Ruska v kategoriích velmi vysoká a vysoká relevance. Lze tedy konstatovat, že celkový pohled všech respondentů na bezpečnostní hrozbu působení a vliv Ruska vykazuje velmi vysokou shodu. Jedná se o bezprecedentně jednoznačné hodnocení, které v takto vyjádřených

hodnotách fakticky vylučuje zásadní statistickou chybu. Stanovený výsledek dále koresponduje s oficiálně zveřejněnými stanovisky některých domácích zpravodajských služeb, resp. odráží naléhavost hrozby popsané i v národních strategických dokumentech.

Veřejná část výroční zprávy BIS za rok 2019 (tj. ve shodné době v jakém byl realizovaný empirický výzkum, uvádí k hrozbě Působení a vliv Ruska mj. toto:

… V souladu se stanovenými prioritami, mírou ohrožení zájmů České republiky a vlastními kapacitami a možnostmi BIS byly v roce 2019 prioritními cíli zpravodajského rozpracování aktivity ruské a čínské státní moci ohrožující bezpečnost a další klíčové zájmy státu (s. 8) … Rusko usiluje o destabilizaci a rozklad svých protihráčů (s. 8) … byli na území Česka přítomni a vyvíjeli zpravodajskou činnost příslušníci a spolupracovníci všech ruských zpravodajských služeb: civilní rozvědky SVR, vojenské rozvědky GRU, vnitřní bezpečnostní služby FSB a Federální služby ochrany FSO (s. 9) …[144]

Vedle BIS se k tématu veřejně vyjadřují i další české bezpečnostní složky, jako je například Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Především v jejich oficiálních veřejně přístupných částech výročních zpráv[145] jsou jednoznačné indicie podporující zmíněné poznatky BIS.

Hrozbu působení a vliv Ruska zohledňují i některé české strategické bezpečnostní dokumenty. Bezpečnostní strategie 2015 sice ještě konkrétně Rusko jako hrozbu neuvádí, a i když tento trend popisuje zcela přesně, uchyluje se pouze k využití termínu *„**některé státy**“ usilují o revizi stávajícího mezinárodního uspořádání a jsou připraveny k dosažení svých mocenských cílů použít metod hybridního válčení, kombinujících konvenční i nekonvenční vojenské prostředky s nevojenskými nástroji (propaganda využívající tradiční i nová média,*

[144] Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf [online, cit. 2021-08-24].
[145] Dostupné z https://vzcr.cz/vyrocni-zpravy-o-cinnosti-vojenskeho-zpravodajstvi-41 nebo https://nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/ [online, cit. 2021-08-01].

zpravodajské dezinformační akce, kybernetické útoky, politický a ekonomický nátlak, vysílání neoznačených příslušníků ozbrojených sil). Tyto země posilují svůj vojenský potenciál a snaží se budovat si exkluzivní sféry vlivu prostřednictvím destabilizace sousedních zemí a využívání místních konfliktů a sporů (s.11) … [146] Audit národní bezpečnosti (2016) však hodnotí Rusko jako hrozbu zcela adresně: *… pro potřeby Auditu je třeba věnovat primární pozornost těm projevům cizí moci, které pro ČR mohou znamenat bezpečnostní hrozbu. V souladu se současnými poznatky vyplývajícími jak z informací poskytovaných zpravodajskými službami, tak z jiných zdrojů lze takto hodnotit působení ze strany Ruské federace* (s. 50) …[147] A v neposlední řadě i Obranná strategie ČR (2017) je vůči ruským nepřátelským aktivitám zcela adresná: *… Na východě Evropy Ruská federace otevřeně realizuje své mocenské ambice, a to i za použití vojenské síly. Přitom se nezdráhá porušovat normy mezinárodního práva, včetně narušení územní celistvosti okolních zemí. Vůči členským zemím NATO a EU používá řadu nástrojů hybridní kampaně včetně cílených dezinformačních aktivit a kybernetických útoků … Tyto nepříznivé trendy představují pro Českou republiku potenciální ohrožení. O to větší odpovědnost a zájem proto Česká republika má na výstavbě a připravenosti svých obranných schopností a na podpoře těch spojenců a partnerů, kteří nesou hlavní díl břemene (s. 1) …*[148]

Bezpečnostní hrozba působení a vliv Ruska **je intencionální hrozba s vysokou mírou rizika pro ČR a je součástí působnosti vše tří českých zpravodajských služeb.** Hrozba je zařazena do skupiny faktorové sklady **geopolitické hrozby.**

[146] Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf / [online, cit. 2021-08-24].
[147] Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2021-08-24].
[148] Dostupné z https://www.mocr.army.cz/images/id_40001_50000/46088/OS.pdf [online, cit. 2021-08-24].

A2 KYBERNETICKÁ ŠPIONÁŽ
(intencionální bezpečnostní hrozba)

Druhé místo tabulky setříděné relevance bezpečnostních hrozeb zaujala podle hodnocení analytiků BIS nepřekvapivě hrozba kybernetické špionáže. Jedná se o trend, který má společně s dalšími aktivitami v kybernetickém prostoru stále vzestupnou tendenci. S masivním nástupem tzv. umělé inteligence (Artificial Intelligence – AI)[149] nebo rychlých 5G sítí[150] se postupně přesouvá lidská činnost do kybernetického prostoru. S tím je spojena i otázka zabezpečení sítí, ale i robustní nástup nelegálních, nepřátelských nebo kriminálních aktivit. Kybernetické hrozby patří do kategorie rizik, které jsou dnes často velmi složitě odhalitelné. Klasickým příkladem je např. problematika zneužívání kybernetického prostoru pro nejrůznější anti společenské aktivity, počínaje terorismem a konče zásahy státních i nestátních aktérů vůči konkrétním zemím, jejich vládám a společnosti. ČR není výjimkou a je těmito riziky a hrozbami již dnes plně konfrontována. Není bez zajímavosti, že hrozba kybernetické špionáže je v českém, ale i v aliančním prostředí často spojována s aktivitami autoritativních a nepřátelských režimů jako je Ruská federace, Čínská lidová republika, Íránská islámská republika nebo Korejská lidově demokratická republika. České zpravodajské a bezpečnostní složky často a explicitně ukazují na prokazatelné nepřátelské aktivity především Ruska a Číny, a to jak přímo prostřednictvím státních, tak i nestátních aktérů[151].

---

[149] Z nekonečného množství definic vybírám definici AI od Johna McCarthyho: „*Je to věda a technika vytváření inteligentních strojů, zejména inteligentních počítačových programů. Souvisí s podobným úkolem využívání počítačů k porozumění lidské inteligenci, ale AI se nemusí omezovat na metody, které jsou biologicky pozorovatelné.* “ Dostupné z https://www.ibm.com/cloud/learn/what-is-artificial-intelligence [online, cit. 2021-08-24].

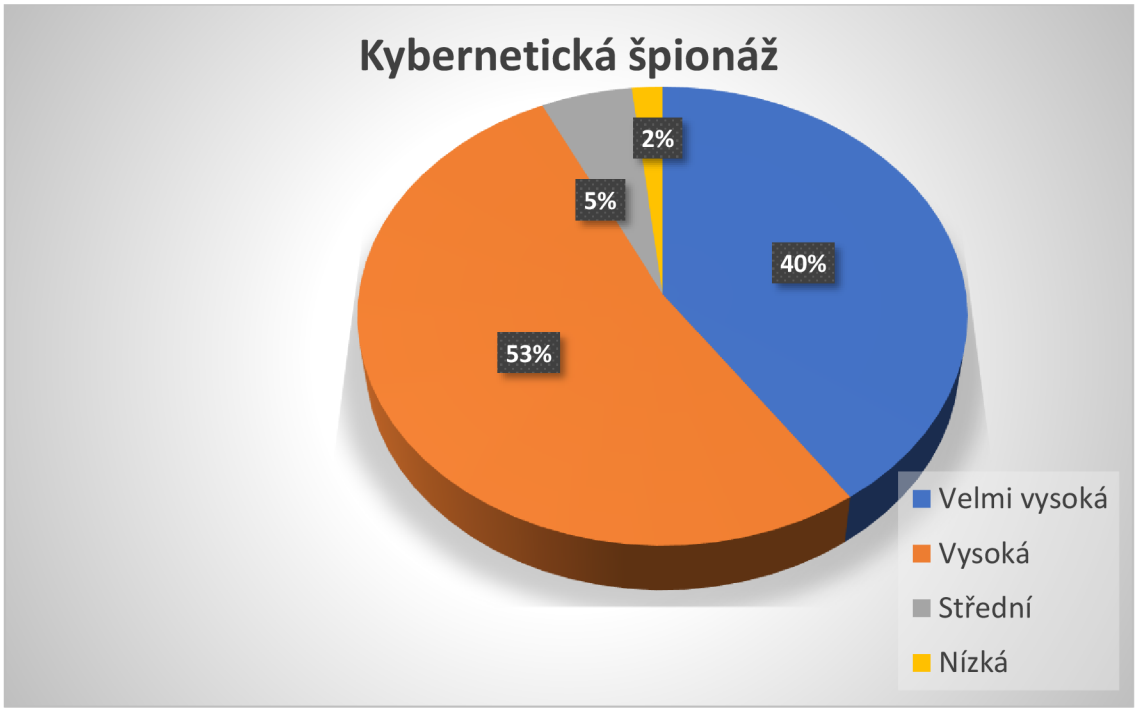
[150] „*5G je mobilní síť 5. generace. Jedná se o nový globální bezdrátový standard, který umožňuje nový druh sítě, která je navržena tak, aby spojovala prakticky všechny a všechno dohromady, včetně strojů, objektů a zařízení. Bezdrátová technologie 5G má zajistit vyšší špičkovou datovou rychlost (více Gbps), ultra nízkou latenci , větší spolehlivost, obrovskou kapacitu sítě, vyšší dostupnost a jednotnější uživatelské prostředí pro mnoho uživatelů. Vyšší výkon a vyšší účinnost posiluje nové uživatelské prostředí a spojují nová průmyslová odvětví ...*“ Dostupné z https://www.qualcomm.com/5g/what-is-5g [online, cit. 2021-08-24].

[151] Podle Národní strategie o kybernetické bezpečnosti 2020-2025 …“*Státní a nestátní aktéři mnohdy podporovaní nebo tolerovaní ze strany států, provádí cíleně škodlivé, ofenzivní kybernetické operace* (s. 5) …“ Dostupné z https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf [online, cit. 2021-08-24].

Tabulka č. 10 a graf č. 3 Spektrum relevance bezpečnostní hrozby Kybernetická špionáž

Kybernetická špionáž

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	23	40,4	40,4	40,4
	Vysoká	30	52,6	52,6	93,0
	Střední	3	5,3	5,3	98,2
	Nízká	1	1,8	1,8	100,0
	Celkem	57	100,0	100,0	



Tabulky č. 10 a graf č. 3 uvádí, že celkem 93 % procent respondentů ve škále „velmi vysoká a vysoká hrozba“ považuje kybernetickou špionáž za bezpečnostní hrozbu. Pokud přičteme ještě hodnotu „střední hrozby“ je to celkově 98 %. Pouze 2 % oslovených analytiků BIS považuje kybernetickou špionáž za nízkou hrozbu. Žádný z respondentů nevyužil označení zkoumané bezpečnostní hrozby ve stupni „velmi nízká a žádná“. Průměr zkoumané hrozby vyjadřuje hodnotu 1,68 a směrodatná odchylka je stanovena na 0,659. Hodnota směrodatné odchylky je v případě hrozby kybernetické špionáže zanedbatelná, neboť 93 %

respondentů označilo relevanci hrozby v kategoriích velmi vysoké a vysoké relevance. I z tohoto hlediska lze konstatovat, že se jedná o jednoznačný výsledek, který v takto vysoce vyjádřených hodnotách vylučuje zásadní statistickou chybu a také koresponduje s veřejně vyjadřovanými stanovisky bezpečnotsních složek, ale i závěrů národních strategických dokumentů.

Veřejná část výroční zprávy BIS za rok 2019 k bezpečnostní hrozbě kybernetické špionáže mj. uvádí: *„… Česká republika byla předmětem zájmu pro aktéry s vazbou na ruskou a čínskou státní moc i v kyberprostoru. V tomto kontextu zaznamenala BIS i v roce 2019 další bezpečnostní incidenty spojené s aktivitami státních či státem podporovaných kyberšpionážních skupin jako jsou Turla, Zebrocy, APT28 nebo APT15 (s. 9) … V roce 2019 navázala BIS na dřívější šetření kompromitace neutajované sítě Ministerstva zahraničních věcí (MZV) kyberšpionážní kampaní, za níž stála skupina pracující ve prospěch cizí moci, s vysokou pravděpodobností Ruské federace…"*[152]

Závěry BIS potvrzuje i veřejná část výroční zprávy Vojenského zpravodajství za rok 2019: *„…Rok 2019 v kybernetickém prostoru navázal na roky předchozí s tím, že byl opětovně zjištěn meziroční nárůst působení velkého množství aktérů, kteří se opětovně zaměřili zejména na kybernetickou špionáž a akty kybernetického zločinu… Byl opětovně zaznamenán zesilující trend prolínání nestátních a státních aktérů (s. 5) …"*[153] nebo závěry Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) publikované ve Zprávě o stavu kybernetické bezpečnosti České republiky za rok 2019: *… V roce 2019 zaznamenal NÚKIB spolu s partnery kybernetickou špionáž proti strategické instituci státní správy, téměř jistě ze strany státního aktéra. Na základě zjištění NÚKIB za útokem velmi pravděpodobně stála skupina Sofacy, kterou odborná*

[152] Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf [online, cit. 2021-08-24].
[153] Dostupné z https://vzcr.cz/uploads/41-Vyrocni-zprava-o-cinnosti-VZ-za-rok-2019.pdf [online, cit. 2021-08-24].

komunita, včetně partnerů NÚKIB, spojuje s vojenskou rozvědkou Ruské federace GU (též GRU) (s. 2) ...“[154]

Kybernetické bezpečnosti věnují národní strategické dokumenty patřičnou pozornost. Bezpečnostní strategie 2015 se velmi detailně věnuje otázce kybernetických útoků a tuto problematiku dále rozpracovává v Akčním plánu Národní strategii kybernetické bezpečnosti ČR na období let 2015–2020 a aktuálně v Národní strategii kybernetické bezpečnosti ČR 2020–2025. Bezpečnostní strategie 2015 k otázce kybernetické špionáže (resp. útoků) mj. konstatuje, že „…*v souvislosti s hrozbou kybernetických útoků patří k prioritám vlády zajištění bezpečnosti kritické informační infrastruktury a významných informačních systémů pomocí vládního koordinačního místa pro okamžitou reakci na kybernetické bezpečnostní incidenty. ČR podporuje budování takových systémů, které umožňují širokou spolupráci všech aktérů, tedy i těch, kteří nejsou součástí veřejné správy a přispívají k výměně zkušeností z řešení kybernetických incidentů na národní a mezinárodní úrovni* (s. 16) …“[155] Audit národní bezpečnosti 2016 je tradičně ještě konkrétnější. Kybernetickou špionáž označuje za samostatnou bezpečnostní hrozbu s vysokou mírou rizika (s. 96) a k problematice mj. konkrétně uvádí „… *Význam hrozby kybernetické špionáže se odráží na počtu případů i nárůstu rizika užití kybernetických nástrojů k útokům na veřejný i soukromý sektor. Za růstem tohoto trendu stojí snadnější dostupnost sofistikovaných nástrojů pro provádění kybernetické špionáže, profesionalizace útočníků, budování ofenzivních kapacit u státních a nestátních aktérů na poli kybernetické bezpečnosti, elektronizace mnoha činností ve společnosti i celková politická situace ve světě* (s. 97) ... *ČR a její instituce se opakovaně stávají cílem kybernetické špionáže a lze předpokládat, že v českém prostředí působí doposud nedetekované APT, které škodí národním zájmům. Vzhledem k četnosti kybernetické špionáže a jejím potenciálně závažným důsledkům pro národní bezpečnost pak lze tuto hrozbu hodnotit jako vysokou. Oběťmi se zpravidla stávají*

[154] Dostupné z https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf [online, cit. 2021-08-24].
[155] Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2021-08-24].

exponované státní úřady a jejich představitelé, ale také instituce zabývající se vzděláváním, výzkumem a vývojem, provozovatelé IS a KS KII, správci VIS, bezpečnostní složky a řada dalších organizací. Obdobně se kybernetická špionáž týká soukromého sektoru (s. 97) …"[156]

Bezpečnostní hrozba kybernetická špionáž **je intencionální hrozba s vysokou mírou rizika pro ČR a je součástí působnosti vše tří českých zpravodajských služeb.** Hrozba je zařazena do skupiny faktorové skladby **hrozby v kyberprostoru.**

A3 OVLIVŇOVÁNÍ VEŘEJNÉHO MÍNĚNÍ CIZÍ MOCÍ (intencionální bezpečnostní hrozba)

Bezpečnostní hrozba ovlivňování veřejného mínění cizí mocí (třetí místo tabulky) je společně s hrozbami ovlivňování veřejné správy cizí mocí (páté místo tabulky) a získávání zákonem chráněných informací cizí mocí (třináctém místo tabulky) již svou podstatou jednou z tradičních hrozeb, které byly a jsou po celá staletí dlouhodobě využívány v různých případech mezinárodního soupeření. Cílem těchto aktivit byly a jsou pokusy ovlivňovat situaci v klíčových oblastech protivníka se snahou zvýšit cizí vliv na jeho území. Moderním prvkem těchto hrozeb, které obecně řadíme do kategorie hybridních hrozeb, je větší důraz, který je dnes kladený na nové technologie využívané často, ale nikoliv výhradně v kybernetické oblasti. Tyto hrozby mají spíše charakter zpravodajských aktivit a vedle nelegálního působení v kybernetickém prostoru jsou často realizovány i klasickou nepřátelskou zpravodajskou činností cizí moci proti našemu státu. Spektrum těchto zpravodajských aktivit může být velmi pestré: od využívání korupčních mechanismů, přes rekrutování osob (agentů) v týlu nepřítele až po výrobu tzv. „fake news" a šíření dezinformací mající mj. za cíl měnit nebo alespoň zpochybňovat většinové názory ve společnosti a víru občanů ve svůj stát[157].

[156] Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2021-08-24].
[157] PAĎOUREK, Jan, KOVAŘÍK, Zdeněk (2021) Vnímání významu hybridních hrozeb českou (a slovenskou) bezpečnostní komunitou pohledem empirického výzkumu. 9. kapitola kolektivní

Především posledně jmenované metody mají v průběhu času stále intenzivnější charakter a jsou stále sofistikovanější a svým dopadem mohou mít na tvorbu veřejného mínění velmi destruktivní dopad. Podobné aktivity se mj. snaží výrazným způsobem ovlivnit tak důležité procesy jako jsou výsledky voleb, vztah veřejnosti k politické nebo zahraničněpolitické orientaci země atd. I tato bezpečnostní hrozba je často spojována s aktivitami některých státních i nestátních aktérů na našem území, mající původ v některých autoritativních režimech jako je např. Ruská federace nebo Čínské lidové republiky.

Tabulka č.11 a graf č. 4 Spektrum relevance bezpečnostní hrozby Ovlivňování veřejného mínění cizí mocí

Ovlivňování veřejného mínění cizí mocí

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	29	50,9	50,9	50,9
	Vysoká	17	29,8	29,8	80,7
	Střední	9	15,8	15,8	96,5
	Nízká	1	1,8	1,8	98,2
	Velmi nízká	1	1,8	1,8	100,0
	Celkem	57	100,0	100,0	

monografie KURFÜRST, Jaroslav, PAĎOUREK, Jan (eds.) Za zrcadlem: Hybridní válka jako staronový fenomén mezinárodních vztahů, nakladatelství Academia, 387 s.

Tabulky č. 11 a graf č. 4 uvádí, že celkem 80,7 % procent respondentů ve škále „velmi vysoká a vysoká hrozba“ považuje ovlivňování veřejného mínění cizí mocí za bezpečnostní hrozbu. Pokud přidáme ještě hodnotu „střední hrozba“ je to celkově 96,4 %. Pouze 3,6 % oslovených analytiků BIS považuje hrozbu za nízkou nebo velmi nízkou hrozbu. Žádný z respondentů nevyužil označení zkoumané bezpečnostní hrozby ve stupni „žádná hrozba“. Průměr zkoumané hrozby vyjadřuje hodnotu 1,74 a směrodatná odchylka je stanovena na 0,917, což vykazuje její malou hodnotu. I v případě hodnocení relevance hrozby ovlivňování veřejného mínění cizí mocí byl zaznamenán jen velmi malý názorový rozptyl v hodnocení relevance ze strany respondentů BIS. V tomto případě se jedná o vysoce průkazný výsledek, který vylučuje zásadní statistickou chybu. Odráží svůj charakter i ve veřejně sdílených textem národních bezpečnotsních složek a českých strategických dokumentů.

V kontextu sledované bezpečnostní hrozby ovlivňování veřejného mínění cizí mocí veřejná část výroční zprávy o činnosti BIS za rok 2019 například uvádí: „… *Čínští aktéři – zpravodajci, diplomaté, členové stranických organizací a další – hledali v ČR způsoby, jak ovlivňovat veřejné mínění, šířit čínskou propagandu a budovat pozitivní obraz ČLR prostřednictvím otevřeného i skrytého ovlivňování mediálního obsahu* (s. 10) ... *V roce 2019 pokračovalo šíření manipulativního zpravodajství a dezinformací, jehož důsledkem byla polarizace společnosti, podrývání důvěry v demokratický právní stát a jeho instituce a podpora zájmů cizí moci* (s. 11) … *Tyto aktivity lze interpretovat jako přirozenou součást širšího trendu, který lze popsat jako snahu posunout konspirační teorie, proruské narativy a protizápadní postoje z okraje mediálního spektra do jeho středu. V souvislosti s volbami do Evropského parlamentu v květnu 2019 monitorovala BIS možné snahy o nelegitimní ovlivňování výsledků voleb* (s. 11)“.[158]

[158] Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf [online, cit. 2021-08-24].

BS ČR (2015)[159] se problematiky bezpečnostní hrozby ovlivňování veřejného mínění cizí mocí dotýká jen okrajově, když mj. konstatuje, že „… *některé státy … jsou připraveny k dosažení svých mocenských cílů použít metod hybridního válčení, kombinujících konvenční i nekonvenční vojenské prostředky s nevojenskými nástroji (propaganda využívající tradiční i nová média, zpravodajské dezinformační akce, kybernetické útoky)* (s. 11) …“ Audit národní bezpečnosti ČR 2016 (ANB) však ovlivňování veřejného mínění cizí mocí vnímá jako konkrétní bezpečnostní hrozbu s vysokou relevancí. Důsledkem toho je podle ABN radikalizace veřejnosti (s. 52), což může mj. způsobit „… *snížení podpory pro ústavní uspořádání ČR a její začlenění do euroatlantických struktur, zvýšená podpora pro jeho revizi* (s. 51) … ANB také uvádí, že „… *hrozba ovlivňování veřejného mínění cílí primárně na následující životní zájmy: zajištění politické nezávislosti ČR, zachování všech náležitostí demokratického právního státu včetně záruky a ochrany základních lidských práv a svobod obyvatel* (s. 53-54) …“[160] Národní strategie kybernetické bezpečnosti 2020-2025 navíc konkretizuje cílovou skupinu těchto nepřátelských aktivit „… *Další významnou skupinu populace, která je vystavena negativním vlivům používání moderních technologií, jsou senioři. Na ně je zapotřebí edukativně působit zejména v oblastech schopností bezpečného používání digitálních technologií a rozeznávání dezinformací* (s. 20) …“[161]

Bezpečnostní hrozba ovlivňování veřejného mínění cizí mocí **je intencionální hrozba s vysokou mírou rizika pro ČR a je součástí působnosti vše tří českých zpravodajských služeb.** Hrozba je zařazena do skupiny faktorové skladby **ohrožení působnosti státu a jeho ekonomické stability.** Je třeba konstatovat, že tato hrozba trvá (ba s podporou energetické krize roste) i po

[159] Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2021-08-24].

[160] Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2021-08-24].

[161] Dostupné z https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf [online, cit. 2021-08-24].

odhalení přímého útoku Ruska na české občany ve Vrběticích nebo bez ohledu na válku RF vůči Ukrajině.

A4 PŮSOBENÍ A VLIV ČÍNY

(intencionální bezpečnostní hrozba)

Čínská lidová republika vedle Ruské federace patří k nejvýraznějším státním i nestátním aktérům nepřátelských aktivit širokého spektra různých aktivit nejen proti České republice, střední Evropě, ale v podstatě proti celému euroatlantickému prostoru. Čína tento svět v čele s USA považuje za svého úhlavního nepřítele. Bezpečnostní hrozba působení a vliv Číny (4. místo tabulky) náleží do skupiny závažných bezpečnostních hrozeb, které v aktuálním čase mohou mít a také mají velmi destruktivní charakter. Na rozdíl od Ruska má však Čína poněkud odlišnou motivaci, ideologický základ i metody, s kterými se snaží prosazovat některé své cíle. Čína na úkor Ruska dosáhla významného velmocenského postavení, neboť během posledních dekád v podstatě vystřídala Rusko na pozici druhé světové supervelmoci. Oficiální Peking se netají svými plány stát se během několika příštích desítek let první globální světovou mocností (ekonomickou i vojenskou) a má tento plán podrobně rozpracovaný v dlouhém časovém období.[162] Jestliže Rusko nejenom v regionu střední Evropy působí „tady a teď", Čína má své expanzivní plány rozloženy a plánovány v podstatně delším časovém úseku a na prostoru celého světa. Záměrem čínského středoevropského, resp. evropského působení je vybudovat si důležité expanzní body s důrazem na ovlivnění momentálně negativního evropského veřejného mínění ve vztahu k oficiální komunistické Číně. Čína rovněž aktivně působí celosvětově i v oblasti technologické a vědeckotechnické špionáže s patrnou snahou získat přístup ke všem důležitým technologiím a vědeckým objevům[163].

---

[162] K tématu podrobně např. studie o Velké čínské strategii, jak vystřídat USA v roli světového hegemona. Dostupné z https://www.brookings.edu/essay/the-long-game-chinas-grand-strategy-to-displace-american-order/ [online, cit. 2021-08-25].

[163] Pro ilustraci např. Survey of Chinese Espionage in the United States Since 2000. Dostupné z https://www.csis.org/programs/technology-policy-program/survey-chinese-linked-espionage-united-states-2000 [online, cit. 2021-08-01].

Čína se rovněž snaží využívat Českou republiku a některé další středoevropské a východoevropské státy jako vstupní bránu na evropský kontinent. K dosažené těchto cílů využívá nejrůznější metody, ať je to například vstřícnost některých významných politiků, nebo používání některých nelegálních metod jako je korupce, vydírání[164] atd. Zakládá i v našem regionu různé iniciativy, které sice mají deklarovaný ekonomických charakter, ale opět se spíše jedná o čínské vlivové akce (např. Pás a cesta, tzv. Belt and Road[165] nebo středoevropsko – východoevropská čínská iniciativa 17+1).[166]

Nebezpečím ruského a čínského vlivu v ČR se již v roce 2018 zabývala dokonce Poslanecké sněmovna PČR, která za tímto účelem zřídila vyšetřovací komisi pro vyhodnocení vlivu autoritářských režimů na vnitřní záležitosti českého politického systému. Návrh usnesení v souladu a s odkazem na výroční zprávu BIS kromě jiného konstatovala, že *„…růst intenzity a agresivity vlivových operací a nárůstu činnosti čínské špionáže na území ČR a proti českým zájmům a bezpečnosti"... Zvýšily se počty zpravodajců cestujících do ČR v rámci čínských oficiálních delegací, a především došlo ke zvýšení počtu, agresivity a intenzity čínských zpravodajských operací proti českým cílům a zájmům. Čínské zpravodajské služby při svých operacích na českém území využívají služeb a spolupráce čínské krajanské komunity v ČR ... Dominantním zájmem Číny a jejích zpravodajských služeb v ČR byla eliminace tibetské otázky a narušení česko-taiwanských vztahů…"*[167]

---

[164] PAĎOUREK, Jan, KOVAŘÍK, Zdeněk (2021) Vnímání významu hybridních hrozeb českou (a slovenskou) bezpečnostní komunitou pohledem empirického výzkumu. 9. kapitola kolektivní monografie KURFÜRST, Jaroslav, PAĎOUREK, Jan (eds.) Za zrcadlem: Hybridní válka jako staronový fenomén mezinárodních vztahů, nakladatelství Academia, 387 s.

[165] Podrobná informace o čínské iniciativě Belt and Road dostupná z https://www.scmp.com/news/china/diplomacy/article/3113231/what-chinas-belt-and-road-initiative-all-about [online, cit. 2021-08-25].

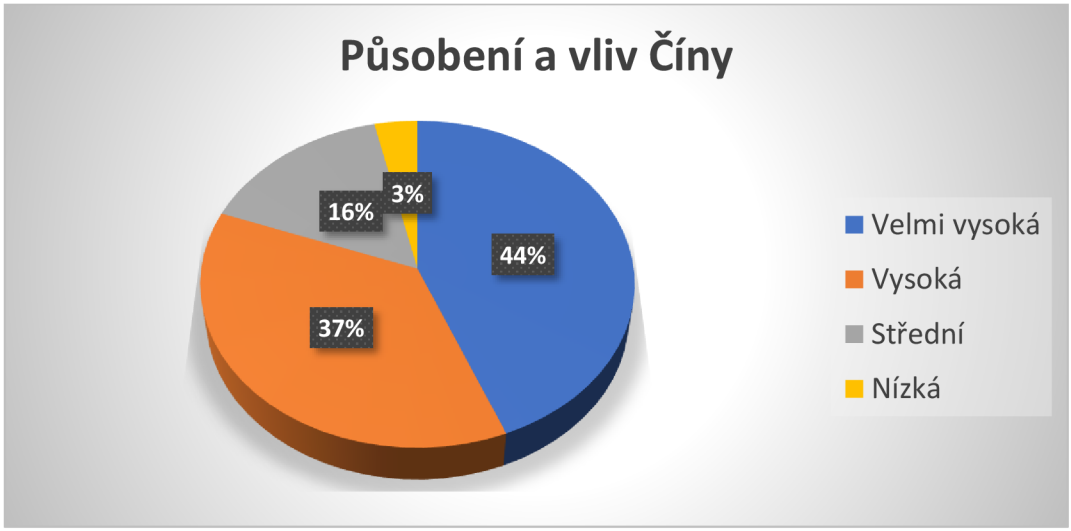
[166] Detailní audit čínské iniciativy 17+1 dostupný z http://www.amo.cz/wp-content/uploads/2020/06/AMO_Audit-vztah%C5%AF-%C4%8C%C3%ADny-se-zem%C4%9Bmi-st%C5%99edn%C3%AD-a-v%C3%BDchodn%C3%AD-Evropy_upraveno.pdf [online, cit. 2021-08-25].

[167] Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2015-vz-cz.pdf [online, cit. 2021-08-25] a také dostupné z https://www.psp.cz/sqw/sd.sqw?cd=1778&o=8 [online, cit. 2021-08-25].

Tabulka č. 12 a graf č. 5 Spektrum relevance bezpečnostní hrozby Působení a vliv Číny

Působení a vliv Číny

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	25	43,9	43,9	43,9
	Vysoká	21	36,8	36,8	80,7
	Střední	9	15,8	15,8	96,5
	Nízká	2	3,5	3,5	100,0
	Celkem	57	100,0	100,0	



Tabulka č. 12 a graf č. 5 konstatují, že celkem 80,7 % procent respondentů ve škále „velmi vysoká a vysoká hrozba“ považuje působení a vliv Číny za výraznou bezpečnostní hrozbu. Pokud přidáme ještě hodnotu „střední hrozba“ je to celkově 96,5 %. Pouze 3,5 % oslovených analytiků BIS považovalo hrozbu „působení a vliv Číny“ za nízkou hrozbu. Žádný z respondentů nevyužil označení zkoumané bezpečnostní hrozby ve stupni „velmi nízká a žádná hrozba“. Průměr zkoumané hrozby vyjadřuje hodnotu 1,79 a směrodatná odchylka je stanovena na 0,840, což prozrazuje její nízkou hodnotu. Rovněž rozptyl hodnocení respondentů je velmi malý, konstatující vysokou názorovou shodu. Výsledek je možno považovat za přesvědčivý, který navíc odráží realitu ve veřejně sdílených názorech národních zpravodajských složek, ale i některých klíčových strategických dokumentech.

Výroční zpráva BIS za rok 2019 ve veřejné části říká o čínském působení a jeho vlivových aktivitách mj. toto: *„…pro BIS byly v roce 2019 prioritními cíli zpravodajského rozpracování aktivity ruské a čínské státní moci ohrožující bezpečnost a další klíčové zájmy státu* (s. 8) *… Čínské zpravodajské služby při své činnosti využívaly tradiční krytí (diplomaté, novináři, akademici) i moderní metody zpravodajské práce (např. sociální sítě), zajímaly se o rozličné obory a využívaly otevřenosti českého prostředí k nabídce čínských investic. Jejich zájem cílil na široké spektrum oborů, ať se jednalo o technologická témata, vojenství, bezpečnost, infrastrukturní projekty, zdravotnictví, ekonomiku, životní prostředí, nebo témata mezinárodní i domácí politiky* (s. 10) …"[168]

Tak jako v jiných případech se i zde Bezpečnostní strategie ČR 2015 vyhýbá konkrétnímu označení Číny, a především čínských vlivových operací na území našeho státu a omezuje se pouze na obecné konstatování termínu *„některé státy".* Audit národní bezpečnosti ČR 2016 je však zcela jednoznačný, když mj. konstatuje, že: *„… pro potřeby Auditu je třeba věnovat primární pozornost těm projevům cizí moci, které pro ČR mohou znamenat bezpečnostní hrozbu. V souladu se současnými poznatky vyplývajícími jak z informací poskytovaných zpravodajskými službami, tak z jiných zdrojů lze takto hodnotit působení ze strany Ruské federace, Čínské lidové republiky, ale i některých nestátních aktérů jako je tzv. Islámský stát* (s.50) *…"*[169]

Bezpečnostní hrozba působení a vliv Číny **je intencionální hrozba s vysokou mírou rizika pro ČR a je součástí působnosti vše tří českých zpravodajských služeb.** Hrozba je zařazena do skupiny faktorové sklady **geopolitické hrozby.**

[168] Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf [online, cit. 2021-08-25].
[169] Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2021-08-25].

A5 OVLIVŇOVÁNÍ VEŘEJNÉ SPRÁVY CIZÍ MOCÍ
(intencionální bezpečnostní hrozba)

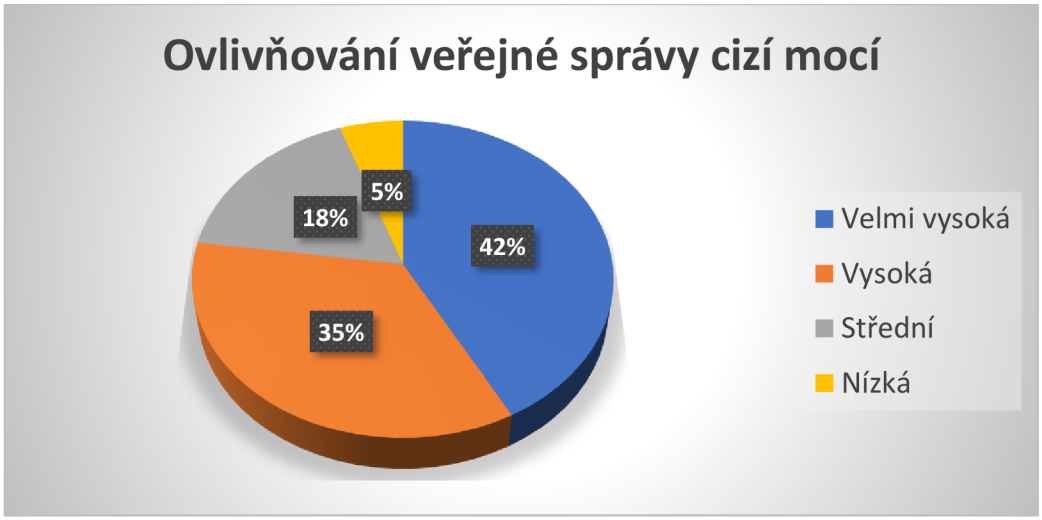
V tabulce pátá bezpečnostní hrozba ovlivňování veřejné správy cizí mocí řadí tuto proměnnou do skupiny faktorové skladby „Ohrožení působnosti státu a jeho ekonomické stability[170]“, která je naplněna některými dalšími (podobnými) bezpečnostními hrozbami, jako je např. hrozba ovlivňování veřejného mínění cizí mocí (třetí pozice v tabulce) nebo hrozba získávání zákonem chráněných informací cizí mocí (třináctá pozice v tabulce). Jedná se o problematiku zasahování cizí moci do citlivých oblastí státu, která je realizována jednak s využitím hybridních způsobů v aktivitách státních i nestátních aktérů, ale i prostřednictvím klasické špionáže s využitím moderních kybernetických technologií. V tomto případě se jedná o specifický prvek bezpečnostního ohrožení státu prostřednictvím zneužívání kybernetického prostoru a nezákonných aktivit v něm směrem ke státní správě a dalším jiným veřejným organizacím. Hrozba má rovněž charakter nepřátelských zahraničních zpravodajských aktivit, v tomto případě s cílem narušit bezproblémové fungování české veřejné správy. Může se např. jednat o snahy zahraničních zpravodajských služeb rekrutovat české úředníky pro práci ve prospěch cizí moci, za využívání celé škály tradičních nezákonných mechanismů, jako jsou korupční aktivity, vydírání, zastrašování atd.

[170] PAĎOUREK, Jan, KOVAŘÍK, Zdeněk (2021) Vnímání významu hybridních hrozeb českou (a slovenskou) bezpečnostní komunitou pohledem empirického výzkumu. 9. kapitola kolektivní monografie KURFÜRST, Jaroslav, PAĎOUREK, Jan (eds.) Za zrcadlem: Hybridní válka jako staronový fenomén mezinárodních vztahů, nakladatelství Academia, 387 s.

Tabulka č.13 a graf č. 6 Spektrum relevance bezpečnostní hrozby Ovlivňování veřejné správy cizí mocí

Ovlivňování veřejné správy cizí mocí

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	24	42,1	42,1	42,1
	Vysoká	20	35,1	35,1	77,2
	Střední	10	17,5	17,5	94,7
	Nízká	3	5,3	5,3	100,0
	Celkem	57	100,0	100,0	



Tabulka č. 13 a graf č. 6 ilustrují, že celkem 77,2 % procent respondentů ve škále „velmi vysoká a vysoká hrozba“ považuje hrozbu ovlivňování státní správy cizí mocí za výraznou bezpečnostní hrozbu. Pokud přidáme ještě hodnotu „střední hrozba“ je to celkově 94,7 %. Pouze 5,3 % oslovených analytiků BIS považuje hrozbu za nízkou hrozbu. Žádný z respondentů nevyužil označení zkoumané bezpečnostní hrozby ve stupni „velmi nízká a žádná hrozba“. Průměr zkoumané hrozby vyjadřuje hodnotu 1,86 a směrodatná odchylka je stanovena na 0,895, tzn. že je prokazatelně nízká. Názorový rozptyl respondentů je zde velmi malý a vyjadřuje velkou názorovou shodu v hodnocení relevance hrozby. Výsledek je možné považovat za přesvědčivý a řadí hrozbu do skupiny nejvyšší relevance, stejně jako veřejně publikované závěry českých zpravodajských složek, ale i národních strategických dokumentů.

BIS ve výroční zprávě (2019) o bezpečnostní hrozbě ovlivňování veřejné správy cizí mocí mj. uvádí: „… *scénář, kdy státní moc neprovádí vlastní činnost, zůstává v pozadí a různými cestami (PR, návodná prohlášení, propaganda atp.) volně inspiruje samostatné aktéry k možné akci, považuje BIS za rizikový, a to zvláště pokud by se počet takových iniciativních aktérů, jak z řad ruskojazyčné komunity, tak z řad českých občanů, v budoucnosti zvyšoval* (s.9) …“[171]

Bezpečnostní strategie ČR 2015 spíše obecně zmiňuje riziko této hrozby například v následujících intencích: „… *roste naopak schopnost nestátních aktérů ohrožovat zájmy států, nahrazovat prvky státního systému vlastními strukturami, realizovat územní ambice a s využitím extrémního násilí ohrožovat bezpečnost obyvatel a stabilitu a integritu zasažených států* (s. 9) …“[172] Audit národní bezpečnosti 2016 konkrétně zmiňuje „*Ovlivňování rozhodování na všech úrovních veřejné správy v rozporu se zájmy ČR*“ jako bezpečnostní hrozbu s vysokou mírou rizika (s.53). K hrozbě ANB 2015 dále uvádí „… *působení na pracovníky veřejné správy … působení na politické a ústavní představitele, a to jak stávající, tak využívání neformálního vlivu bývalých vrcholných představitelů státu. Na okraji pozornosti nestojí ani političtí představitelé v opozici, u kterých je spatřován potenciál do budoucna* (s. 53) …“[173]

Bezpečnostní hrozba ovlivňování veřejné správy cizí mocí **je intencionální hrozba s vysokou mírou rizika pro ČR a je součástí působnosti vše tří českých zpravodajských služeb.** Hrozba je zařazena do skupiny faktorové skladby **ohrožení působnosti státu a jeho ekonomické stability.**

[171] Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf [online, cit. 2021-08-25].
[172] Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2021-08-25].
[173] Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2021-08-25].

A6 NARUŠENÍ ODOLNOSTI INFRASTRUKTURY INFORMAČNÍCH TECHNOLOGIÍ[174]

(intencionální bezpečnostní hrozba)

Bezpečnostní hrozba narušení odolnosti IT infrastruktury zaujímá šestou pozici tabulky a patří do skupiny vysoce nebezpečných moderních bezpečnostních hrozeb se stále se zvyšující tendencí růstu jejího významu. Má potencionálně destruktivní dopad na život celé lidské společnosti. Potvrzením tohoto závěru, že se bude tato bezpečnostní hrozba v budoucnosti ještě více umocňovat je i skutečnost, že tento trend intenzivně sledují téměř všechny euroatlantické vlády. Severoatlantická aliance na svém summitu v Bruselu v roce 2018 zřídila nové operační středisko pro kyberprostor v rámci posílené struktury velení NATO[175]. Zajištění bezpečného provozu IT infrastruktury patří mezi jednu z nejvíce sofistikovaných výzev současnosti. Týká se jak zajištění bezproblémového provozu státní, tak i podnikové (soukromé) IT infrastruktury. Hrozba je součástí faktorové skladby „Hrozby v kyberprostoru"[176] společně s dalšími technologickými (resp. hybridními) hrozbami jako je např. kybernetická špionáž (druhá pozice tabulky), narušení bezpečnosti eGovermentu (desátá pozice tabulky) nebo kyberterorismus (čtrnáctá pozice tabulky). Obecně byly kybernetické hrozby, kam spadá posuzovaná hrozba narušení odolnosti IT infrastruktury, dlouhou dobu evropskými vládami zanedbávány především v otázkách aktivních národních opatření proti těmto anti společenským jevům. Až v posledních letech lze i v ČR spatřit některé konkrétní kroky české vlády v boji s touto hrozbou.[177] Nastupující

---

[174] Jednou z četných definic struktury informačních technologií (IT) je i tento výklad: „*IT infrastruktura se týká složeného hardwaru, softwaru, síťových zdrojů a služeb nezbytných pro existenci, provoz a správu podnikového IT prostředí. Infrastruktura IT umožňuje organizaci dodávat IT řešení a služby svým zaměstnancům, partnerům a/nebo zákazníkům a je obvykle interní v organizaci a nasazena v rámci vlastněných zařízení*". Dostupné z https://www.techopedia.com/definition/29199/it-infrastructure [online, cit. 2021-08-26].

[175] Podrobnosti dostupné z https://www.nato.int/nato_static_fl2014/assets/pdf/2020/8/pdf/2008-factsheet-cyber-defence-en.pdf [online, cit. 2021-08-26].

[176] PAĎOUREK, Jan, KOVAŘÍK, Zdeněk (2021) Vnímání významu hybridních hrozeb českou (a slovenskou) bezpečnostní komunitou pohledem empirického výzkumu. 9. kapitola kolektivní monografie KURFÜRST, Jaroslav, PAĎOUREK, Jan (eds.) Za zrcadlem: Hybridní válka jako staronový fenomén mezinárodních vztahů, nakladatelství Academia, 387 s.

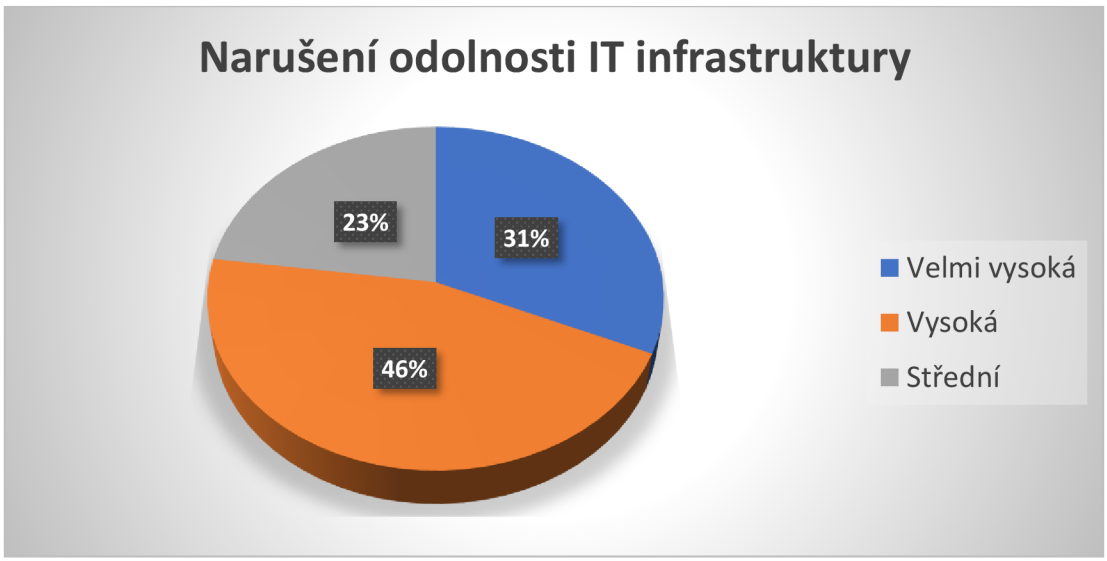
[177] Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) vznikl až k 1.8. 2017 na základě zákona č. 205/2017 Sb. Je ústředním orgánem státu pro kybernetickou bezpečnost se sídlem v Brně a vyčlenil se z Národního bezpečnostní úřadu, který dočasně za tuto problematiku zodpovídal.

problémy při řešení těchto otázek jsou dva: **a)** *schopnost provedení analýzy* a **b)** *schopnost obrany proti hrozbám*, které z části budou více kumulovány.[178]

Tabulka č. 14 a graf č. 7 Spektrum relevance bezpečnostní hrozby Narušení odolnosti IT infrastruktury

Narušení odolnosti IT infrastruktury

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	18	31,6	31,6	31,6
	Vysoká	26	45,6	45,6	77,2
	Střední	13	22,8	22,8	100,0
	Celkem	57	100,0	100,0	



Tabulka č. 14 a graf č. 7 dokumentují, že celkem 77,2 % procent respondentů ve škále „velmi vysoká a vysoká hrozba“ považuje hrozbu narušení odolnosti IT infrastruktury za hrozbu výraznou. Pokud přidáme ještě hodnotu „střední hrozba“ je to celkově 100 % respondentů, kteří stanovují takto vysokou relevanci zkoumané hrozby. V tomto případě žádný z respondentů nevyužil označení zkoumané bezpečnostní hrozby ve stupni „nízká, velmi nízká a žádná

[178] To je limitováno kapacitami především IT odborníků a v budoucnosti bude významné dělení států podle jejich schopnosti využít umělou inteligenci k obraně i útoku.

hrozba“. Průměr zkoumané hrozby vyjadřuje hodnotu 1,91 a směrodatná odchylka byla stanovena na 0,739, která vyjadřuje její nízkou hodnotu. Je zde zaznamenán jen velmi malý názorový rozptyl respondentů, kteří i v tomto případě vykazují vysokou názorovou shodu. Výsledek je možné považovat za zcela přesvědčivý a řadí hrozbu do skupiny nejvyšší relevance. Vše je také v souladu s veřejnými zprávami některých národních zpravodajských složek, ale i strategických dokumentů.

BIS ve veřejné části výroční zprávy (2019) k bezpečnostní hrozbě Narušení odolnosti IT infrastruktury konkrétně uvádí: *„… se ve druhé polovině roku BIS podílela také na prověřování napadení ICT infrastruktury jedné z českých diplomatických misí při mezinárodní organizaci. Nejméně jedno zařízení bylo na konci roku 2018 kompromitováno v rámci intenzivní celosvětové vlny útoků kyberšpionážní kampaně cizího státního aktéra, s vysokou pravděpodobností opět Ruské federace … v září 2019 získala BIS informaci o průniku pravděpodobně čínské kyberšpionážní skupiny do infrastruktury antivirové společnosti Avast. Na základě podnětu BIS začala firma extenzivně auditovat celou svou vnitřní síť a odhalila závažnou kompromitaci* (s. 11) *…“*[179] Vojenské zpravodajství jako garant kybernetické obrany státu poukazuje ve své výroční zprávě za rok 2019 i na zcela nové trendy, které jsou spojené se sledovanou problematikou ochrany IT infrastruktury: …“ *s masivním nasazením cloudových technologií úplně zaniká pojem bezpečnostní perimetr, který dříve definoval vnitřní zónu IT infrastruktury organizace a hranici s venkovním internetem. Přesouváním serverů z bezpečného umístění v organizaci (onpremise) do cloudů … z důvodu finanční výhodnosti a větší operability … se zásadně mění celková bezpečnost těchto zařízení. Roste možnost jejich napadení, jiné jsou způsoby správy a zálohování a přibývají nové hrozby např. možnost odcizení celých serverů a všech dat formou získání administrátorských přihlašovacích údajů do cloudu* (s.8) …“[180]

[179] Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf [online, cit. 2021-08-26].
[180] Dostupné z https://vzcr.cz/uploads/41-Vyrocni-zprava-o-cinnosti-VZ-za-rok-2019.pdf [online, cit. 2021-08-27].

Bezpečnostní strategie ČR 2015 k tématu uvádí, že „… *k negativním aspektům procesu globalizace patří zejména možnost zneužití provázanosti finančních trhů při absenci účinného systému mezinárodní regulace, zneužití informačních a komunikačních technologií a infrastruktury* (s.9) …“[181] Audit národní bezpečnosti ČR 2016 prezentuje narušení odolnosti IT infrastruktury jako samostatnou bezpečnostní hrozbu s vysokým stupněm její relevance. Jako důležité pro národní bezpečnost ANB ve sledovaném kontextu a s ohledem na nové trendy upozorňuje, že „… *kvůli vzrůstající robustnosti a komplexnosti celkové IT infrastruktury v ČR je nutné hodnotit hrozbu narušení odolnosti IT infrastruktury jako vysokou. Je tak zapotřebí neustále navyšovat jak organizační, tak i procesní a technické schopnosti a kapacity, a tudíž posilovat celkovou odolnost IT infrastruktury v ČR* (s. 98) …“[182]

Bezpečnostní hrozba narušení odolnosti IT infrastruktury **je intencionální hrozba s vysokou mírou rizika pro ČR a je součástí působnosti všech tří českých zpravodajských služeb.** Hrozba je zařazena do skupiny faktorové skladby **hrozby v kyberprostoru.**

A7 ZNEUŽÍVÁNÍ VEŘEJNÝCH ZAKÁZEK A ROZPOČTŮ

(intencionální bezpečnostní hrozba)

První bezpečnostní hrozba tabulky, která má spíše vnitrostátní dimenzi, i když existují i konkrétní případy analogických nelegálních aktivit se zahraničním přesahem. Hrozba zneužívání veřejných zakázek a rozpočtů je výrazným způsobem spojena s aktivitami organizovaného zločinu (domácího i zahraničního, aktivně působícího na území ČR). Tyto nelegální aktivity se významně vyprofilovaly především po pádu komunismu v bývalém Československu a později v samostatné České republice v 90. letech minulého století. Na počátku

[181] Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2021-08-27].
[182] Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2021-08-27].

devadesátých let hrozba představovala zásadní bezpečnostní riziko pro zdravý politický a ekonomický vývoj nově budované české demokracie. Tyto aktivity byly a jsou jednoznačně spojeny i s dalšími kriminálními jevy jako je korupce, vydírání, zastrašování, padělání veřejných listin nebo i únosy a vraždy. Zájem skupin organizovaného zločinu je v těchto případech vždy velmi podobný: nejrůznějšími nelegálními cestami vyvést finanční prostředky státu nebo soukromé organizace. Problematiku popisující stav v této oblasti na přelomu 20. a 21. století v ČR velmi detailně a profesionálně zpracovala česká odnož mezinárodní organizace Transparency International pod názvem Veřejné zakázky v České republice: korupce nebo transparentnost?[183]

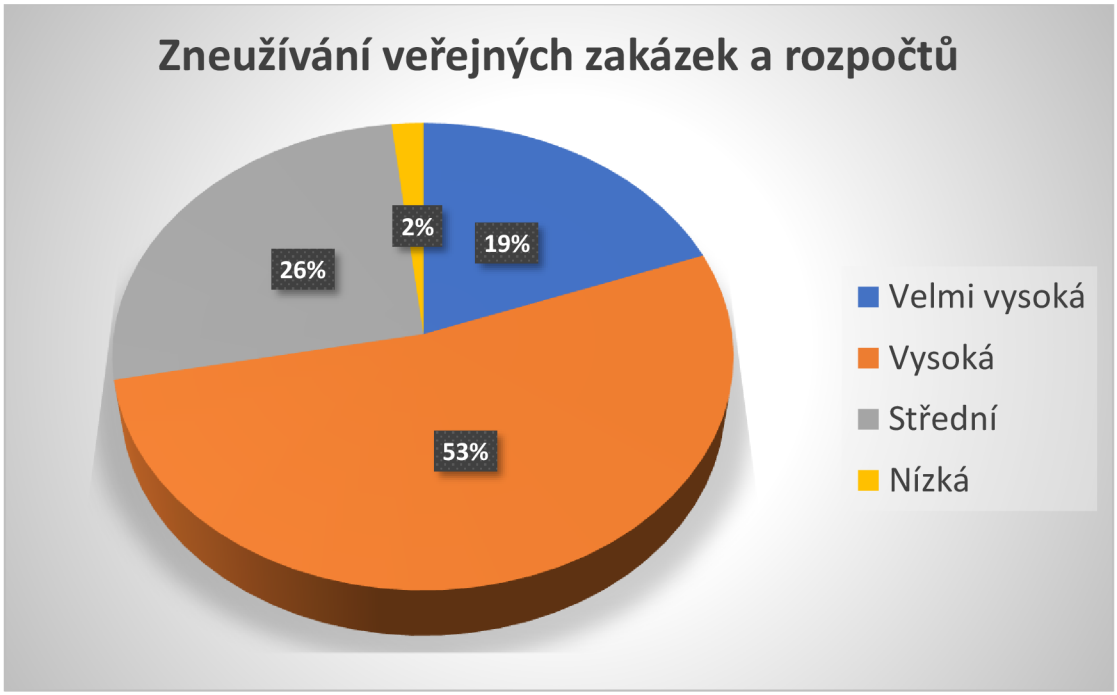
Ve shodě s empirickým výzkumem, který bezpečnostní hrozbu zneužívání veřejných zakázek a rozpočtů hodnotí jako vysoce závažnou a řadí jí do první desítky nejvyšší relevance zkoumaných bezpečnostních hrozeb, dochází ke stejným závěrům i Audit národní bezpečnosti ČR 2016 (viz níže).

Tabulka č.15 a graf č. 8 Spektrum relevance bezpečnostní hrozby Zneužívání veřejných zakázek a rozpočtů

Zneužívání veřejných zakázek a rozpočtů

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	11	19,3	19,3	19,3
	Vysoká	30	52,6	52,6	71,9
	Střední	15	26,3	26,3	98,2
	Nízká	1	1,8	1,8	100,0
	Celkem	57	100,0	100,0	

[183] Dostupné z https://www.transparency.cz/wp-content/uploads/vz_studie_text.pdf [online, cit. 2021-08-29].



Tabulka č. 15 a graf č. 8 demonstrují, že celkem 71,9 % respondentů řadí hrozbu do škály „velmi vysoká a vysoká hrozba“ a považuje ji za bezpečnostní hrozbu velmi vysoké relevance. Pokud přidáme ještě hodnotu „střední hrozba“ je to celkových 98,2 % respondentů, kteří stanovují takto vysokou relevanci zkoumané hrozby. Pouze 1,8 % respondentů hodnotilo hrozbu jako nízkou, přičemž žádný z respondentů nevyužil označení zkoumané bezpečnostní hrozby ve stupni „velmi nízká nebo žádná hrozba“. Průměr zkoumané hrozby vyjadřuje hodnotu 2,11 a směrodatná odchylka byla stanovena na 0,724, tj. velmi nízký názorový rozptyl dotazovaných respondentů. Výsledek je možné považovat za přesvědčivý a řadí hrozbu do skupiny nejvyšší relevance. Tento stav se plně odráží i ve veřejně přístupných textech českých zpravodajských i dalších národních složek.

Výroční zpráva BIS za rok 2019 je vůči této hrozbě velmi konkrétní: …“ *Trvajícím jevem, který dlouhodobě závažným způsobem ohrožuje ekonomické zájmy státu, byly v některých oblastech kartelové dohody mezi dodavateli při zadávání zakázek státními institucemi nebo státem ovládanými společnostmi. Zadavatel měl přitom často jen omezené možnosti jak i při povědomí o těchto*

dohodách negativní důsledky eliminovat. Jako problematická se v této souvislosti jevila především obtížná dokazatelnost kartelových dohod nebo závažné důsledky v případě vyřazení (s. 6-7) …"[184]

Bezpečnostní strategie ČR 2015 sice nezmiňuje hrozbu zneužívání veřejných zakázek a rozpočtů, ale k problematice se např. vyjadřuje takto: „… *prioritou vlády je boj proti korupci, daňovým únikům a závažné hospodářské kriminalitě, které jsou jedním z nástrojů pronikání organizovaného zločinu do veřejné správy a které ohrožují hospodářskou soutěž a základní principy demokratického zřízení. Vláda se v souladu se strategií boje proti korupci zaměřuje na efektivní předcházení korupci, snižování příležitostí korupčního jednání a zvýšení transparentnosti všech procesů k posílení možností státu při postihování korupčního jednání* (s. 17) …"[185] Audit národní bezpečnosti popisuje hrozbu zcela konkrétně, řadí jí do vysoké relevance a k tématice uvádí, že „… *zcela zásadní plýtvání rozpočtovými prostředky způsobené aktivitami organizovaného zločinu se odehrává v oblasti veřejných zakázek a veřejných dotací. Složité systémy zadávání a udělování dotací a veřejných zakázek spojené s absencí důsledného systému kontroly a individuální odpovědnosti u konkrétních rozhodnutí vedou k situaci, kdy je celá řada projektů manipulována ve prospěch zločineckých skupin. Ze strany kriminálních struktur se objevuje snaha řídit veřejné zakázky již od samého prvopočátku za účelem následného vyvádění finančních prostředků do soukromých rukou* (s. 41) ..."[186]

Bezpečnostní hrozba zneužívání veřejných zakázek a rozpočtů **je intencionální hrozba s vysokou mírou rizika pro ČR a je v oblasti působnosti českých zpravodajských služeb nejvíce součástí aktivit Bezpečnostní informační služby, která s potíráním hrozby bojuje v těsné spolupráci**

[184] Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf [online, cit. 2021-08-29].
[185] Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2021-08-29].
[186] Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2021-08-29].

s různými součástmi Policie České republiky a dalších orgánů činných v trestním řízení. Hrozba je zařazena do skupiny faktorové sklady **ohrožení působnosti státu a jeho ekonomické stability.**

A8 HYBRIDNÍ HROZBY

(intencionální bezpečnostní hrozba)

Akceptovaná česká definice hybridních hrozeb vychází např. z oficiálních webových stránek Centra proti terorismu a hybridním hrozbám Ministerstva vnitra ČR: „*To, co rozumíme pod hybridní hrozbou, je primárně metoda, způsob, jakým je vedena konfrontace, respektive konflikt. Tento způsob vedení konfliktu představuje širokou, komplexní, přizpůsobivou a integrovanou kombinaci konvenčních a nekonvenčních prostředků, otevřených a skrytých aktivit, majících primárně charakter nátlaku a podvratné činnosti, které jsou prováděny vojenskými, polovojenskými a různými civilními aktéry.*“ [187]

Zhruba osm z třiceti sedmi bezpečnotsních hrozeb z námi zkoumaného seznamu naplňuje svým obsahem charakter hybridní hrozby. To znamená, že tyto hrozby jsou v podstatě součástí jedné faktorové skladby[188]. Konkrétně se jedná o hrozby – ovlivňování veřejného mínění cizí mocí (třetí místo tabulky), ovlivňování veřejné správy cizí mocí (páté místo tabulky), získávání zákonem chráněných informací cizí mocí (třinácté místo tabulky), kybernetická špionáž (druhé místo tabulky), narušení odolnosti IT infrastruktury (šesté místo tabulky), nepřátelské kampaně (deváté místo tabulky), narušení bezpečnosti eGovernmentu (desáté místo tabulky) a kyberterorismus (čtrnácté místo tabulky). Již tento seznam a určená míra relevance každé hrozby dokazují, že se jedná o bezpečnostní riziko s vysokou mírou relevance, vyskytující se až na výjimky v první desítce zkoumaných bezpečnotsních hrozeb. V České republice se však vyprofilovala názorově velmi vyhrocená diskuse o existenci či neexistenci tzv. hybridních

[187] Dostupné z https://www.mvcr.cz/cthh/clanek/co-jsou-hybridni-hrozby.aspx [online, cit. 2021-08-29].

[188] PAĎOUREK, Jan, KOVAŘÍK, Zdeněk (2021) Vnímání významu hybridních hrozeb českou (a slovenskou) bezpečnostní komunitou pohledem empirického výzkumu. 9. kapitola kolektivní monografie KURFÜRST, Jaroslav, PAĎOUREK, Jan (eds.) Za zrcadlem: Hybridní válka jako staronový fenomén mezinárodních vztahů, nakladatelství Academia, 387 s.

hrozeb, resp. hybridního válčení. V ČR se k tématu vyjadřují jednoznační odpůrci, ale i zastánci existence tohoto druhu bezpečnostního ohrožení naší země [189].

Konkrétně se jedná o bezpečnostní hrozby patrné především v aktivitách zasahování cizí moci do citlivých oblastí státu (s pomocí hybridních hrozeb je řeč o aktivitách státních i nestátních aktérů, včetně aktivní role špionáže), které mají za cíl ovlivnit důležité oblasti života společnosti (např. nepřátelské a nelegální aktivity v oblasti veřejné správy, snahy o ovlivnění veřejného mínění nebo získávání státem utajovaných informací) až po jednoznačně kriminální aktivity velkého a organizovaného rozsahu, kde jejími aktéry mohou být domácí i zahraniční kriminální skupiny, ale i jejich kombinace (např. v otázkách zneužití legitimních služeb pro organizovaný zločin, prorůstání organizovaného zločinu do všech klíčových oblastí státu nebo daňová kriminalita, legalizace nelegálních výnosů či kriminalita spojená s insolvenčním řízením). Příkladem klasického hybridního válčení je především první fáze průběhu rusko – ukrajinského konfliktu na Donbase. Zde Rusko v prvních letech svých nepřiznaných aktivit v spíše proruské východo – ukrajinské oblasti učebnicově demonstrovalo všechny zásadní elementy hybridní války[190]. Hybridní hrozby nemusejí přicházet výhradně z kybernetického prostoru, i když zde pravděpodobně dominují. I tato skutečnost ilustruje, že mnohé tradiční lidské aktivity přenesly svou působnost do kybernetického prostoru. Z uvedeného je patrné, že jejich příští vývoj bude stále zřetelněji využívat moderní, více sofistikované metody nasazení.

---

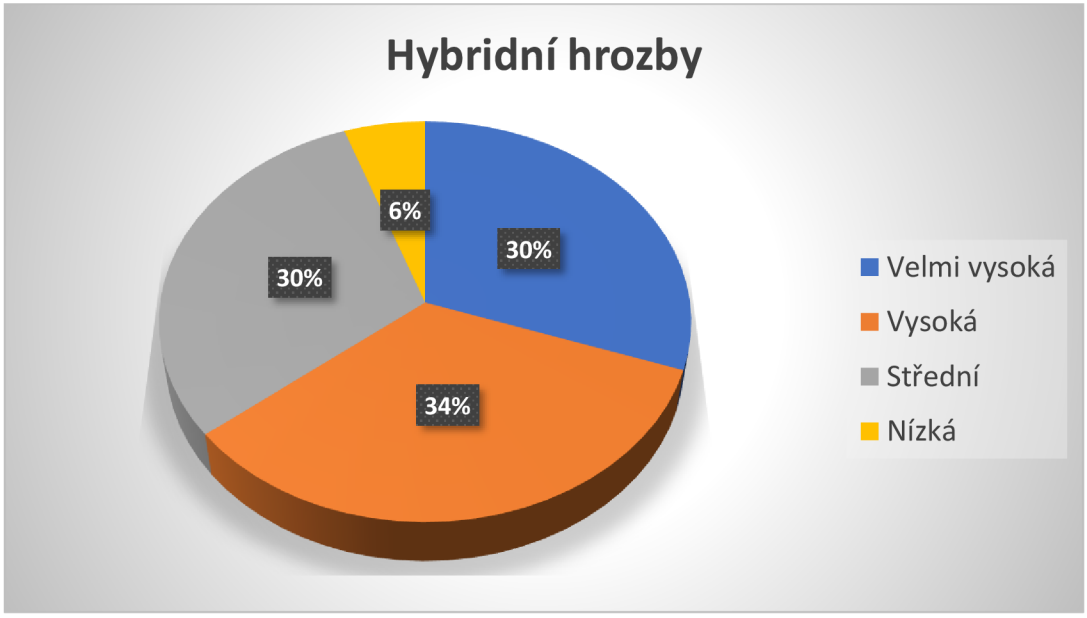
[189] Výrazným popíračem existence tzv. hybridního válčení je v ČR např. Ústav mezinárodních vztahů s protagonisty Janem DANIELEM a Jakubem EBERLEM, kteří publikovali např. konfrontační stať s názvem Jak se Česko začalo bát hybridní války a proč na slovech záleží (celý text dostupný z https://iir.cz/article/jak-se-cesko-zacalo-bat-hybridni-valky-a-proc-na-slovechzalezi [online, cit. 2019-11-17]. Na jejich článek zareagoval ve své stati Jak se diskutovalo o „českých hybridních válečnících“ a ztratila se podstata, diplomat a politický geograf Jaroslav KURFÜRST, který zde v podstatě shrnul argumentaci druhé názorové skupiny (celý text dostupný z http://blog.aktualne.cz/blogy/pohled-zblizka.php?itemid=33501 [online, cit. 2021-08-29]).

[190] Z mnoha studií např. DICKINSON, Peter (2020), All roads lead to Ukraine in Putin's global hybrid war, Atlantic Council, Ukraine Alert Service, 5.1. 2021. Dostupné z https://www.atlanticcouncil.org/blogs/ukrainealert/all-roads-lead-to-ukraine-in-putins-global-hybrid-war/ [online, cit. 2021-08-29].

Tabulka č.16 a graf č. 9 Spektrum relevance bezpečnostní hrozby Hybridní hrozby

Hybridní hrozby

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	17	29,8	30,4	30,4
	Vysoká	19	33,3	33,9	64,3
	Střední	17	29,8	30,4	94,6
	Nízká	3	5,3	5,4	100,0
	Celkem	56	98,2	100,0	
Vynechaná	System	1	1,8		
Celkem		57	100,0		



Tabulka č. 16 a graf č. 9 dokumentují, že celkem 64,3 % procent respondentů ve škále „velmi vysoká a vysoká hrozba“ považuje hrozbu „narušení odolnosti IT infrastruktury“ za výraznou bezpečnostní hrozbu. Pokud navíc přidáme hodnotu „střední hrozba“ je to celkových 94,7 % respondentů, kteří stanovují takto vysokou relevanci zkoumané hrozby. Pouze 5,4 % respondentů hodnotilo hrozbu jako nízkou, přičemž žádný z respondentů nevyužil označení zkoumané bezpečnostní hrozby ve stupni „velmi nízká nebo žádná hrozba“. Průměr zkoumané hrozby vyjadřuje hodnotu 2,11 a směrodatná odchylka byla stanovena na 0,908. Jedná se tedy o hodnotu nízkého názorového rozptylu nalezeného v odpovědích dotazovaných respondentů. Výsledek je možné

považovat za přesvědčivý. Řadí hrozbu do skupiny vysoké relevance, což koresponduje i s oficiálními názory českých zpravodajských složek.

Víceméně všechny české strategické dokumenty se vyjadřují v různé intenzitě a naléhavosti k Hybridním hrozbám. Bezpečnostní strategie ČR 2015, zdůrazňující především ruské angažmá na východní Ukrajině, vidí tuto hrozbu např. takto „… *ohrožení bezpečnosti spojenců může mít jak tradiční vojenskou povahu, tak i nejednoznačnou podobu metod takzvaného hybridního válčení. Základním nástrojem k eliminaci těchto rizik je členství ČR v NATO a EU a dobré vztahy se sousedními zeměmi* (s. 8) …"[191] Audit národní bezpečnosti 2016 se zprvu vyjadřuje spíše kriticky „… *zařazení tématu hybridních hrozeb mezi 10 nejzávažnějších bezpečnostních témat odhalilo nedostatek koordinace právě v případě aktivní hybridní kampaně vedené s úmyslem poškodit nejen ČR, ale i celou evropskou integraci, které se ČR účastní* (s. 4)…" a v samostatné kapitole „Hybridní hrozby a jejich vliv na bezpečnost občanů ČR" (s. 127) dále uvádí, že „… *řada státních i nestátních aktérů se snaží svých politických cílů dosáhnout pomocí otevřených i skrytých aktivit koordinovaných v rámci celé škály nástrojů moci, bez ohledu na případnou kolizi s mezinárodním řádem založeným na pravidlech. Právě v tomto kontextu se objevil pojem hybridní hrozby, respektive hybridního válčení* (s. 127) *…"*[192]

V internetu zveřejněná část výroční zprávy BIS za rok 2019 sice hybridní hrozby explicitně nezmiňuje, ale například v oblasti ruského vlivu popisuje aktivity, které lze označit za hybridní „… *navzdory častějšímu uplatňování nekonvenčních konceptů v prosazování ruských zájmů zastávají zpravodajské služby v ruských operacích a aktivitách nadále důležitou roli. Dohled a kontrolu ruských zpravodajských důstojníků lze totiž vysledovat nebo dovozovat i v případech, kdy nepřátelskou činnost samotnou vykonávají nestátní entity* (s.8) …"[193]

---

[191] Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2021-08-29].
[192] Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2021-08-29].
[193] Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf [online, cit. 2021-08-29].

Bezpečnostní hrozba hybridní hrozby **je intencionální hrozba s vysokou mírou rizika pro ČR v souladu se závěry ANB 2016 i empirického výzkumu v analytické skupině BIS. Je součástí působnosti všech tří českých zpravodajských služeb.** Hrozba je zařazena do skupiny faktorové skladby **hrozby v kyberprostoru.**

A9 NEPŘÁTELSKÉ KAMPANĚ
(intencionální bezpečnostní hrozba)

Hrozba nepřátelských kampaní jednoho státu proti druhému je stará jako lidstvo samo[194]. S rozvojem lidské společnosti má však stále sofistikovanější charakter. Nepřátelské kampaně plní mnoho cílů, přičemž jako hlavní lze uvést snahy nepřítele účinně šířit nepřátelskou propagandu a tím ovlivňovat veřejné mínění v prostředí protivníka.[195] Podle amerického badatele Johnsona-Cartee lze navíc vysledovat čtyři základní cíle nepřátelských propagandistických kampaní: mobilizace nenávisti proti nepříteli; uchování přízně spojenců; zajištění náklonnosti a případné spolupráce neutrálních a celková demoralizace protivníka[196] Dezinformace, polopravdy nebo vyloženě lživé informace jsou obsahovou náplní tohoto procesu. S ohledem na moderní společnost lze konstatovat, že jsou tyto aktivity realizovány především v prostředí kybernetického prostoru, a tak mají přímou návaznost na problematiku kybernetické bezpečnosti. Jsou nedílnou součástí hybridního nepřátelského působení a obecně tvoří jednu ze složek faktorové sklady hrozeb v kyberprostoru.

V unijním a v euroatlantickém prostředí lze především zaznamenat prokazatelně nepřátelské kampaně vedené proti ČR především ze strany Ruské

---

[194] TAYLOR, Philip M. (2003): Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Day. 3rd Edition. Manchester: Manchester University Press
[195] ŘEHKA, Karel (2017): Informační válka, Academia, 224 s.
[196] JOHNSON-CARTEE (2003), Karen S – Copeland, Gary A Strategic Political Communication – Rethinking Social Influence, Persuasion, & Propaganda

federace a Čínské lidové republiky, částečně i z jiných nedemokratických a totalitně řízených mocností (např. Irán, Severní Korea atd.)[197]

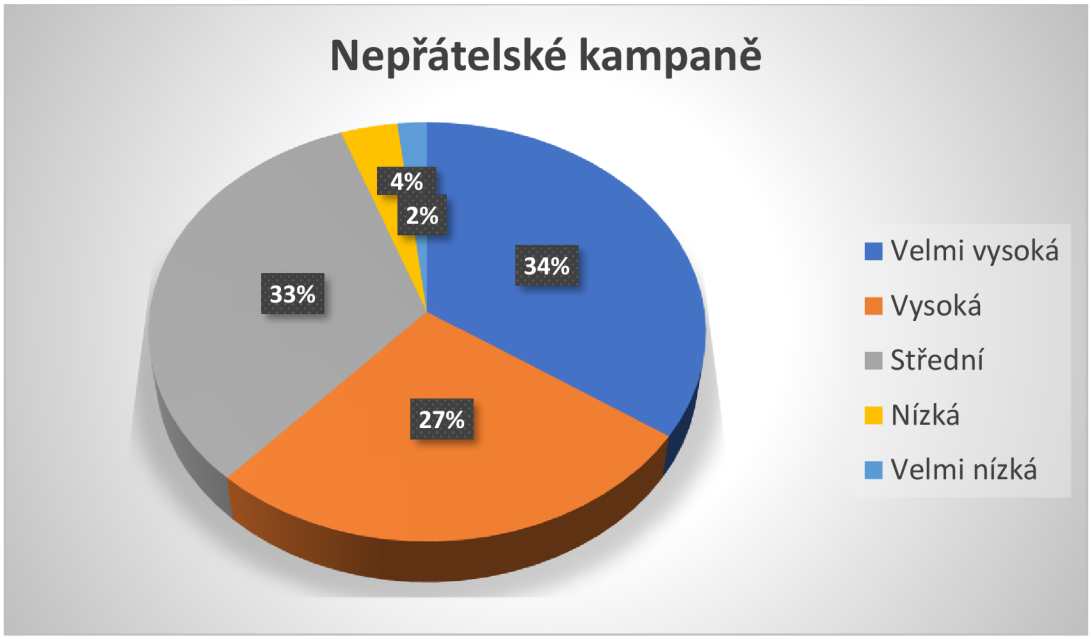
V domácích podmínkách lze konstatovat, že je česká společnost opakovaně a dlouhodobě zasažena silnými vlnami nepřátelských propagandistických kampaní především ze strany Ruské federace a z menší míry i ze strany ČLR. Cílem těchto aktivit je, ostatně jako v případě jiných druhů hybridního způsobu válčení, zpochybňování především národní zahraničněpolitické orientace s cílem narušit a rozmělnit euroatlantickou hodnotovou vazbu. Tento narativ je na území ČR, ale i v ostatních středoevropských státech šířen především aktivitami Kremlem zřízených nebo podporovaných dezinformačních webových portálů (např. Sputnik, Aeronet, OrgoNet atd.), cílenému rozesílání dezinformačních emailů, podporou uměle vyprovokovaných internetových diskusí nad nejrůznějšími aspekty národní zájmů atd. Jejich výstupy jsou zaměřeny převážně na představitele různých extremistických skupin nebo na zástupce starší a staré generace, kteří vyjadřují určitou míru nostalgie po bývalém zřízení vedeném komunistickou stranou.[198]

Tabulka č. 17 a graf č. 10 spektrum relevance bezpečnostní hrozby Nepřátelské kampaně

Nepřátelské kampaně

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	19	33,3	33,9	33,9
	Vysoká	16	28,1	28,6	62,5
	Střední	18	31,6	32,1	94,6
	Nízká	2	3,5	3,6	98,2
	Velmi nízká	1	1,8	1,8	100,0
	Celkem	56	98,2	100,0	
Vynechaná	System	1	1,8		
Celkem		57	100,0		

[197] MAZARR, Michael a kol. (2019): Hostile Social Manipulation, 303 s., Rand Corporation
[198] SYROVÁTKA Jonáš, PINKAS ŠIMON (2021), kapitola CZECHIA, War on People's Hearts and Minds. Societal vulnerabilities to the Kremlin's influence in Central and Eastern Europe & the Western Balkans, s. 11, GLOBSEC Bratislava



Výše uvedená tabulka č. 17 a graf č. 10 řadí hrozbu nepřátelských kampaní do závěru první desítky zkoumaných bezpečnostních hrozeb, čímž jí z hlediska české národní bezpečnosti přiřazuje relativně vysokou míru relevance. Celkových 62,5 % respondentů řadí nepřátelské kampaně do kategorií velmi vysoké a vysoké relevance, do střední kategorie dalších 31,6 % a pouze 5,4 % do kategorií nízké a velmi nízké relevance. Průměr zkoumané hrozby vyjadřuje hodnotu 2,11. Směrodatná odchylka je 0,985, tzn. že má střední hodnotu. Přiložený graf i tabulka navíc demonstrují, že je zde patrný větší názorový rozptyl, avšak přesvědčivě více jak 50 % respondentů hodnotí tuto hrozbu jako velmi závažnou. Z tohoto důvodu lze konstatovat, že hrozba nepřátelských kampaní je z hlediska národní bezpečnosti hrozbou s vysokou mírou relevance.

Bezpečnostní strategie ČR 2015 sice explicitně neuvádí nepřátelské kampaně jako přímou bezpečnostní hrozbu, ale vnímá je spíše jakou integrální součást nepřátelských hybridních operací. Velmi konkrétní je však Audit národní bezpečnosti 2016, který nepřátelské kampaně řadí do skupiny hrozeb v kyberprostoru a relevanci této hrozby hodnotí jako vysokou. ANB 2016 spatřuje v této kategorii především tyto rizikové aktivity a rizika: *vlivové a dezinformační mediální kampaně na internetu s cílem vyvolání společenského neklidu; vlivové a*

dezinformační mediální kampaně prováděné prostřednictvím internetu a organizované zájmovými skupinami, zločineckými strukturami, případně zpravodajskými službami jiných států; ve vyšší míře využívání kampaní … vůči určitým skupinám obyvatel, tak i státním orgánům, anebo samotnému zahraničněpolitickému směřování ČR za účelem dosažení vojenských, politických nebo ekonomických cílů atd. (s. 99)[199]

Výroční zpráva BIS za rok 2020 k nepřátelským kampaním na území ČR hovoří např. „*o zneužívání tzv. tzv. hack and leak scénáře, tj. postupnému selektovanému uvolňování exfiltrovaných informací a jejich využití v předpřipravené dezinformační kampani, která může být zacílena na diskreditaci kompromitované instituce, konkrétního státního představitele/zaměstnance či ČR jako takovou. Dalším stupněm … je zahrnutí zcela vyfabulované informace (falešný dokument, text e-mailu, fotografie) mezi skutečné uveřejňované dokumenty získané v rámci útoku. Oběť dezinformační (diskreditační) kampaně prakticky nemá reálnou možnost, jak se bránit a dopad na důvěryhodnost instituce či jednotlivce, vůči kterým je tato kampaň vedena, může být u veřejnosti enormní a v konečném důsledku již nevratný*“ (s.18).[200]

Bezpečnostní hrozba nepřátelské kampaně **je intencionální hrozba s vysokou mírou rizika pro ČR v souladu se závěry ANB 2016 i empirického výzkumu v analytické skupině BIS. Je součástí působnosti všech tří českých zpravodajských služeb.** Hrozba je zařazena do skupiny faktorové skladby **hrozby v kyberprostoru.**

[199] Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-01-17].
[200] Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf [online, cit. 2022-01-17].

A10 NARUŠENÍ BEZPEČNOSTI eGovernmentu
(intencionální bezpečnostní hrozba)

Pojem eGovernment byl pravděpodobně poprvé použit ve Velké Británii v roce 1999 s cílem zajistit efektivní státní veřejnou komunikaci s využitím moderních informačních technologií.[201] Postupem času tato moderní iniciativa přesáhla britské ostrovy a rozšířila se do celého světa, v prvé řadě do nejrozvinutějších demokratických států. Webový portál českého ministerstva vnitra popisuje eGovernment jako „*správu věcí veřejných za využití moderních elektronických nástrojů, díky kterým bude veřejná správa k občanům přátelštější, dostupnější, efektivnější, rychlejší a levnější. ... Díky nim může být většina agend veřejné správy pro svého zákazníka řešitelná elektronicky bez nutnosti chodit na úřad*“.[202] Každá pozitivní iniciativa a především ta, která je umístěna do kybernetického prostoru, má však řadu rizik.

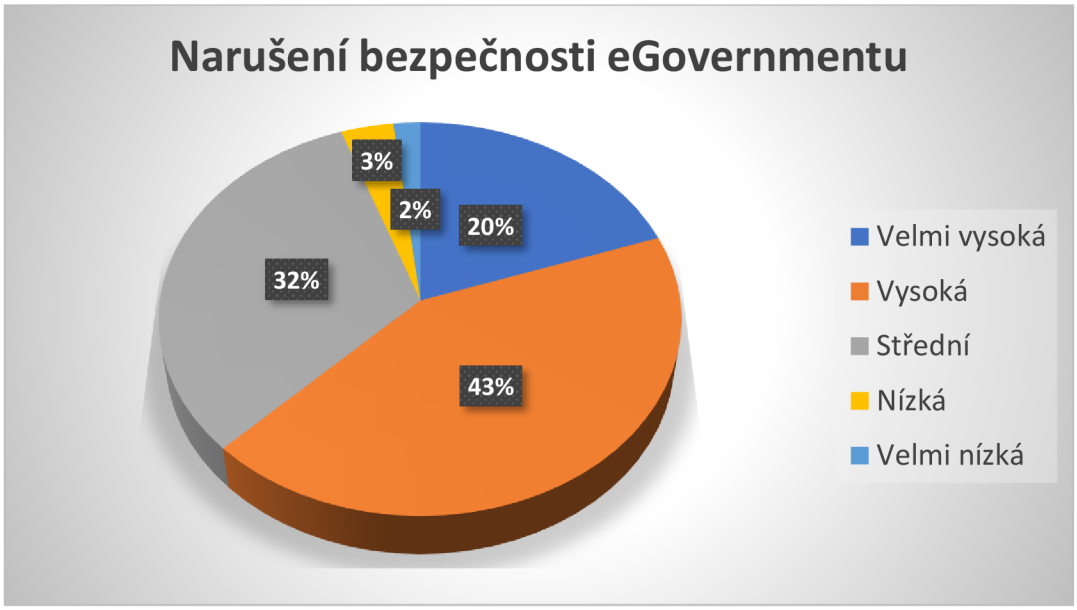
Nebezpečnost eGovernmentu je tedy z námi zkoumaného hlediska nejproblematičtější v oblasti jeho zranitelnosti vůči kybernetickým útokům. Z této perspektivy je bezpečnostní hrozba narušení bezpečnosti eGovernmentu integrální součástí kybernetické bezpečnosti a z námi zkoumaného hlediska patří do faktorové sklady hrozby v kyberprostoru. Míra spolehlivosti eGovernmentu je tedy závislá i na míře bezpečnostního zajištění, stejně jako v případ dalších aktivit v kybernetickém prostoru. Z tohoto hlediska je míra rizik eGovernmentu velmi vysoká, neboť právě tato oblast láká ke svým aktivitám nejenom národní a mezinárodní zločin, ale i cílem i nepřátelských útoků ze strany státních a nestátních aktérů širokého spektra nepřátelských režimů. Tyto systémy jsou pro útočníky zajímavé i proto, že obsahují informace prakticky o všech obyvatelích státu (regionu apod.) což umožňuje následné útoky ať na jednotlivce, nebo skupiny.

[201] Dostupné z https://topranker.cz/slovnik/co-je-to-e-government/ [online, cit. 2022-01-17].
[202] Dostupné z https://www.mvcr.cz/clanek/co-je-egovernment.aspx [online, cit. 2022-01-17].

Tabulka č. 18 a graf č. 11 Spektrum relevance bezpečnostní hrozby Narušení bezpečnosti eGovernmentu

Narušení bezpečnosti eGovernmentu

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	11	19,3	19,6	19,6
	Vysoká	24	42,1	42,9	62,5
	Střední	18	31,6	32,1	94,6
	Nízká	2	3,5	3,6	98,2
	Velmi nízká	1	1,8	1,8	100,0
	Celkem	56	98,2	100,0	
Vynechaná	System	1	1,8		
Celkem		57	100,0		



Tabulka č. 18 a graf č. 11 demonstrují, že je bezpečnostní hrozba narušení bezpečnosti eGovermentu další ze zásadních hrozeb ohrožující bezpečnost ČR. Podle výsledků empirického průzkumu považuje hrozbu za velmi vysokou a vysokou plných 61,5 % respondentů, za středně vysokou 31,5 % a za nízkou a velmi nízkou pouze 5,2 % dotazovaných. Díky těmto hodnotám se velmi přibližuje hodnocení např. v pořadí deváté bezpečnostní hrozby nepřátelských kampaní. Tato shoda je snad vysvětlitelná podobným změřením aktérů takového bezpečnostního ohrožení státu, především umístěním obou hrozeb do faktorové skladby hrozby v kyberprostoru. Průměr zkoumané hrozby vyjadřuje hodnotu

2,25. Směrodatná odchylka je 0,879, tzv., že má střední hodnotu. I názorový rozptyl dotazovaných respondentů vyjadřuje pestřejší spektrum, avšak stále největší počet dotazovaných hodnotí hrozbu jako vážnou (nad 50 %), ale téměř 32 % již jen jako střední a pouze 5,2 % jako nízkou. Lze proto konstatovat, že je tato hrozba z hlediska národní bezpečnosti součástí skupiny závažných bezpečnostních hrozeb.

Bezpečnostní strategie ČR 2015 sice hrozbu narušení bezpečnosti eGovernmentu explicitně nezmiňuje, ale stejně jako v případě nepřátelských kampaní je tato hrozba podrobně rozpracována v Auditu národní bezpečnosti ČR. Podle ANB 2016 je hrozba narušení bezpečnosti eGovernmentu součástí skupiny hrozby v kyberprostoru, ostatně jako v rámci našeho empirického výzkumu, který tuto hrozbu zařadil do stejné faktorové skladby. Má však na rozdíl od našeho empirického výzkumu, který ji přisuzuje vysokou míru relevance, relevanci střední. ANB 2016 mimo jiné konstatuje, kromě různých systémových chyb (např. malá míra financování kybernetické bezpečnosti), i „*slabé povědomí a edukaci obyvatelstva o kybernetické bezpečnosti a projektu eGovernmentu jako takovém*“ (s. 101).[203]

Výroční zpráva BIS za rok 2020 především akcentuje „*spolupráci BIS s odborem eGovernmentu MV při prověřování žadatelů o akreditaci pro správu kvalifikovaného systému elektronické identifikace podle zákona č. 250/2017 Sb., o elektronické identifikaci*“ (s. 29).[204]

Bezpečnostní hrozba narušení bezpečnosti eGovernmentu **je intencionální hrozba s vysokou mírou rizika pro ČR (empirický výzkum) a v souladu se závěry ANB 2016 střední relevance. Je součástí působnosti všech tří českých zpravodajských služeb v komplexní oblasti zajišťování**

[203] Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-01-17].
[204] Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf [online, cit. 2022-01-17].

kybernetické bezpečnosti ČR. Hrozba je zařazena do skupiny faktorové skladby **hrozby v kyberprostoru.**

A11 DLOUHODOBÉ SUCHO
(neintencionální bezpečnostní hrozba)

I když klimatické podmínky posledních let naznačují, že byla hrozba katastrofické predikce dlouhodobého nedostatku vody na území střední Evropy, a tedy i v ČR, částečně zažehnána, relevantní vědecké předpovědi zase tak optimistické nejsou. Podle některých odborných predikcí se frekvence velkého sucha v ČR do r. 2100 ještě výrazně zvýší.[205]

Jako jednu z reakcí na tyto negativní trendy je vládní strategický dokument, tzv. **Koncepce ochrany před následky sucha pro území ČR do r. 2030**,[206] kterou vláda v určitých cyklech a v rámci svých pozičních zpráv meziresortně vyhodnocuje.[207]

Bezpečnostní hrozba dlouhodobého sucha patří do skupiny neintencionálních bezpečnostních hrozeb, které nejsou v přímé náplni práce zpravodajských služeb. Přesto tato hrozba byla v rámci popisovaného empirického výzkumu experty BIS hodnocena jako zásadní.

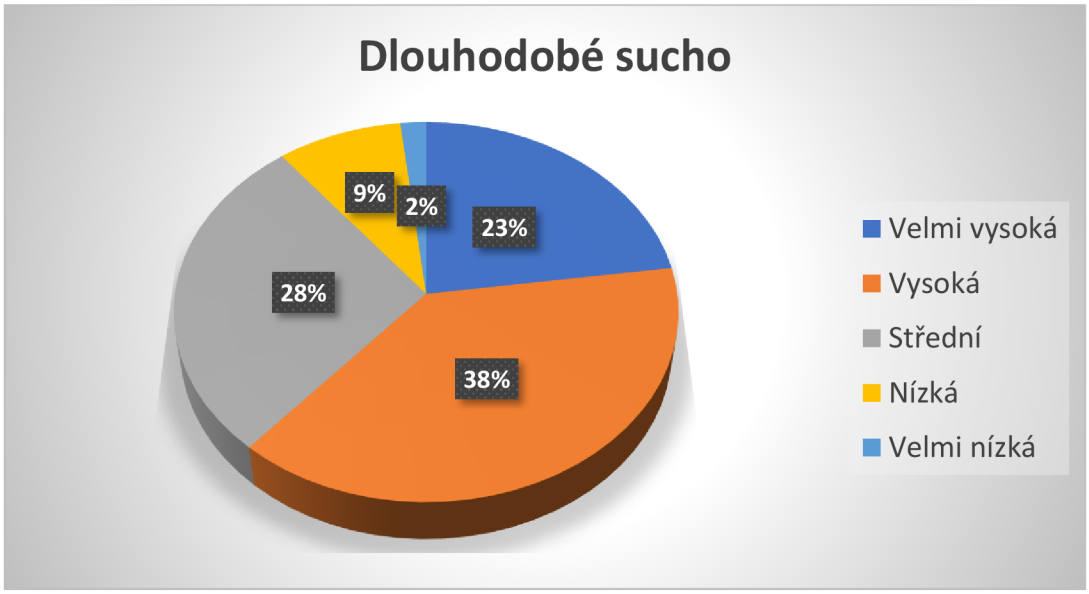
---

[205] Dostupné z https://www.climatechangepost.com/czech-republic/droughts/ [online, cit. 2022-01-17].
[206] Dostupné z https://eagri.cz/public/web/file/545860/Koncepce_ochrany_pred_nasledky_sucha_pro_uzemi_CR.pdf [online, cit. 2022-01-17].
[207] Dostupné z https://eagri.cz/public/web/file/650032/Pozicni_zprava_2019.pdf [online, cit. 2022-01-17].

Tabulka č. 19 a graf č. 12 Spektrum relevance bezpečnostní hrozby Dlouhodobé sucho

Dlouhodobé sucho

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	13	22,8	22,8	22,8
	Vysoká	22	38,6	38,6	61,4
	Střední	16	28,1	28,1	89,5
	Nízká	5	8,8	8,8	98,2
	Velmi nízká	1	1,8	1,8	100,0
	Celkem	57	100,0	100,0	



Empirický průzkum přiřadil hrozbě dlouhodobého sucha velmi vysokou relevanci. Celkově 61,4 % respondentů považuje problém sucha za velmi vysokou nebo vysokou relevanci této bezpečnostní hrozby, 28,1 % jako střední relevanci a jen 10,6 % jako relevanci nízkou a velmi nízkou. Průměr zkoumané hrozby vyjadřuje hodnotu 2,28. Směrodatná odchylka je 0,978, tzv., že má střední hodnotu. V názorovém rozptylu hodnocení respondentů přesvědčivá část hrozbu hodnotí jako závažnou, avšak téměř 30 % jen jako střední a téměř 11 % jako nízkou. Proto lze i tuto hrozbu zařadit do skupiny vysoké relevance ohrožení ČR. Tento výsledek byl mj. ovlivněn i skutečností, že v době dotazníkového šetření

trpěla kvůli nepříznivým klimatickým podmínkám ČR nebývalým obdobím sucha s velice negativní predikcí do střednědobé a dlouhodobé budoucnosti.[208]

Toto zjištění v podstatě koresponduje i se závěry učiněnými v Auditu národní bezpečnosti 2016, kde je hrozba dlouhodobého sucha zařazena v kategorii přírodních hrozeb. Je zde mimo jiné konstatováno, že „*legislativa neposkytuje dostatečnou oporu pro přijímání účinných opatření na zmírnění dopadů dlouhodobého sucha, s výjimkou omezení užívání pitné vody z veřejných vodovodů a náhradního zásobování a zajištění přídělů pitné vody*“. (s. 82).[209] Bezpečnostní strategie ČR 2015 sice o otázce dlouhodobého sucha explicitně nehovoří, ale problém v podstatě řeší v popisu bezpečnostní hrozby Pohromy přírodního a antropogenního původu a jiné mimořádné události. (s. 12).[210]

Bezpečnostní hrozba dlouhodobého sucha **je neintencionální hrozba s vysokou mírou rizika pro ČR (empirický výzkum i v souladu se závěry Auditu národní bezpečnosti). Hrozba však není součástí působnosti zpravodajských služeb.** Hrozba je zařazena do skupiny faktorové skladby **hrozby energetické, surovinové průmyslové a environmentální.**

A12 PRORŮSTÁNÍ ORGANIZOVANÉHO ZLOČINU DO VEŘEJNÉ SPRÁVY (intencionální bezpečnostní hrozba)

Bezpečnostní hrozba negativního ovlivňování veřejné správy organizovaným zločinem je hrozbou spíše domácího charakteru, i když díky působení četných mezinárodních zločineckých organizovaných skupin na území ČR má i svůj významný zahraniční přesah. Tato hrozba začala v ČR hrát důležitou roli počátkem 90. let minulého století, kdy po pádu železné opony v období

[208] Současný problém sucha v ČR (2019), Expertní stanovisko AV ČR 3/2019, 4 s. Dostupné z https://www.avcr.cz/export/sites/avcr.cz/cs/veda-a-vyzkum/avex/files/03-2019-AVEX-SUCHO-def.pdf [online, cit. 2022-03-07].
[209] Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-01-17].
[210] Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2022-01-17].

přechodu české (z počátku československé) plánované ekonomiky na ekonomiku tržní začala na našem území působit celá řada organizovaných zločineckých struktur, včetně zástupců mezinárodního organizovaného zločinu.[211] Snahou těchto kriminálních skupin mj. byla a je i jejich infiltrace do oblasti veřejné správy. Podle hodnocení oficiálního webového portálu českého ministerstva vnitra je tato hrozba dokonce „*v současné době nejzávažnější nevojenskou hrozbu pro českou společnost. Zločinecké skupiny skrze svou činnost podrývají společenské uspořádání, narušují stabilitu ekonomiky, podkopávají demokratické struktury a v konečné fázi tak způsobují zánik právního státu*“.[212] V roce 2018 přijala česká vláda dosud aktuální dokument podporující boj s touto bezpečnostní hrozbou – **Koncepci boje proti organizovanému zločinu do roku 2030**.[213]

Tabulka č.20 a graf č. 13 Spektrum relevance bezpečnostní hrozby Prorůstání organizovaného zločinu do veřejné správy

Prorůstání organizovaného zločinu do veřejné správy

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	9	15,8	16,1	16,1
	Vysoká	19	33,3	33,9	50,0
	Střední	24	42,1	42,9	92,9
	Nízká	4	7,0	7,1	100,0
	Celkem	56	98,2	100,0	
Vynechaná	System	1	1,8		
Celkem		57	100,0		

[211] Z velmi rozsáhlé literatury např. CEJP, Martin (2010): Vývoj organizovaného zločinu na území ČR, Institut pro kriminologii a sociální prevenci, 104 s.
[212] Dostupné z https://www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09Mg%3D%3D [online, cit. 2022-01-18].
[213] Dostupné z https://www.databaze-strategie.cz/cz/mv/strategie/koncepce-boje-proti-organizovanemu-zlocinu-do-roku-2023 [online, cit. 2022-01-18].

Experti BIS přiřadili této bezpečnostní hrozbě střední míru relevance, když celkově 49,7 % hodnotilo relevanci hrozby v kategorii velmi vysoká a vysoká relevance, 42,1 % jako střední a jen 7 % jako nízkou relevanci. Zkoumaná bezpečnostní hrozba má průměr 2,41 a směrodatnou odchylku 0,848. Směrodatná odchylka vyjadřuje středně vysoký charakter rozptylu, neboť je zde patrný celkem pestrý názorový rozptyl. Avšak přesně polovina dotázaných hodnotí hrozbu přesvědčivě jako vážnou, 43 % jako střední a pouze 7 % jako nízkou. Na základě těchto dat lze konstatovat, že je tato hrozba součástí závažného ohrožení bezpečnosti ČR.

Tento výsledek poněkud kontrastuje s hodnocením hrozby pronikání organizovaného zločinu oficiálními webovými stránkami českého ministerstva vnitra, které tuto hrozbu obecně považuje dokonce za „*nejzávažnější nevojenskou hrozbu pro českou společnost*“.[214] Rovněž Audit národní bezpečnosti 2016 hodnotí hrozbu prorůstání organizovaného zločinu do státní správy v pásmu vysoké relevance (s. 41).[215] Lze zde tedy konstatovat, že výsledky empirického výzkumu vykazují poněkud mírnější hodnocení v protikladu k některým národním strategickým dokumentům nebo oficiálním stanoviskům české vlády.

[214] Dostupné z https://www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09Mg%3D%3D [online, cit. 2022-01-18].
[215] Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-01-18].

Bezpečnostní strategie ČR 2015 klasifikuje otázku infiltrace státní správy organizovaným zločinem jako zásadní problém, když konstatuje, že „*narůstá schopnost kriminálních sítí narušovat instituce a hodnoty právního státu, infiltrovat orgány státní správy a ohrožovat bezpečnost občanů. Často se tak děje prostřednictvím korupce. Organizovaný zločin společně s korupčními praktikami může nabýt podoby vlivových, klientelistických, nebo korupčních sítí a vést k podkopání samotných základů společnosti*“ (s. 12).[216] Rovněž Audit národní bezpečnosti 2016 hodnotí tuto hrozbu jako vysoce relevantní, když konstatuje, že „*infiltrace organizovaného zločinu do struktur veřejné správy a orgánů činných v trestním řízení má zásadní negativní dopad na funkčnost a efektivitu veřejné správy…objevují se také kontakty organizovaného zločinu do prostředí orgánů činných v trestním řízení, dohledových a dozorových orgánů státní správy a průnik organizovaných skupin do legislativního procesu nejen na úrovni lokálních samospráv, ale i na vládní a parlamentní úrovni*“ (s.41).[217]

BIS má boj s organizovaným zločinem jako jediná česká zpravodajská služba v gesci i v rámci deklarativně přiznaného portfolia své činnosti (působnost „týkající se organizovaného zločinu a terorismu“[218]). V českých podmínkách se boji s organizovaným zločinem (včetně jeho infiltrace do státní správy) však primárně zabývají příslušné policejní složky PČR (především Národní centrála proti organizovanému zločinu - NCOZ) s významnou informační podporou BIS. BIS však v této souvislosti ve své výroční zprávě za rok 2019 jen lakonicky konstatuje, že „*…pravidelně spolupracovala s Národní centrálou proti organizovanému zločinu PČR*“ (s.14) a dále doplňuje, že se „*fenomén organizovaného zločinu … prolínal řadou jiných témat, jako je např. ochrana významných ekonomických zájmů nebo nepřátelské aktivity cizí moci*“ (s. 5).[219] Tyto letmé zmínky ve veřejné části výroční zprávy BIS za rok 2019 spíše podporují

[216] Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2022-01-18].
[217] Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-01-18].
[218] § 5/ 1e zákona č. 153/1994 Sb. – Působnost zpravodajských služeb
[219] Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf [online, cit. 2022-01-18].

v empirickém výzkumu vyjádřený názor analytiků BIS, že je relevance hrozby infiltrace státní správy organizovaným zločinem sice závažná, ale nikoliv kriticky významná. Lze také konstatovat, že se situace v této oblasti s porovnáním s devadesátými lety minulého století značně zlepšila. Příčinou rozdílu mezi hodnocením politiky a experty může být i rozdíl informovanosti – resp. závislosti politiků na médiích, kde je množství informací o kriminální korupci, zatímco média nemají tolik informací o řadě případů, které řeší zpravodajské služby, a o nichž se politici z výstupů služeb dovídají o několik řádů méně často.

Bezpečnostní hrozba prorůstání organizovaného zločinu do státní správy **je intencionální hrozba s vysokou mírou rizika pro ČR (empirický výzkum). Z hlediska zpravodajských služeb se problematikou systematicky zabývá BIS, zbylé zpravodajské služby nemají tuto gesci ve své prvoplánové činnosti a spíše ad hod podporují národní policejní složky v případě závažných důležitých zjištění.** Hrozba je zařazena skupiny faktorové skladby **ohrožení působnosti státu a jeho ekonomické stability.**

A13 ZÍSKÁVÁNÍ ZÁKONEM CHRÁNĚNÝCH INFORMACÍ CIZÍ MOCÍ (intencionální bezpečnostní hrozba)

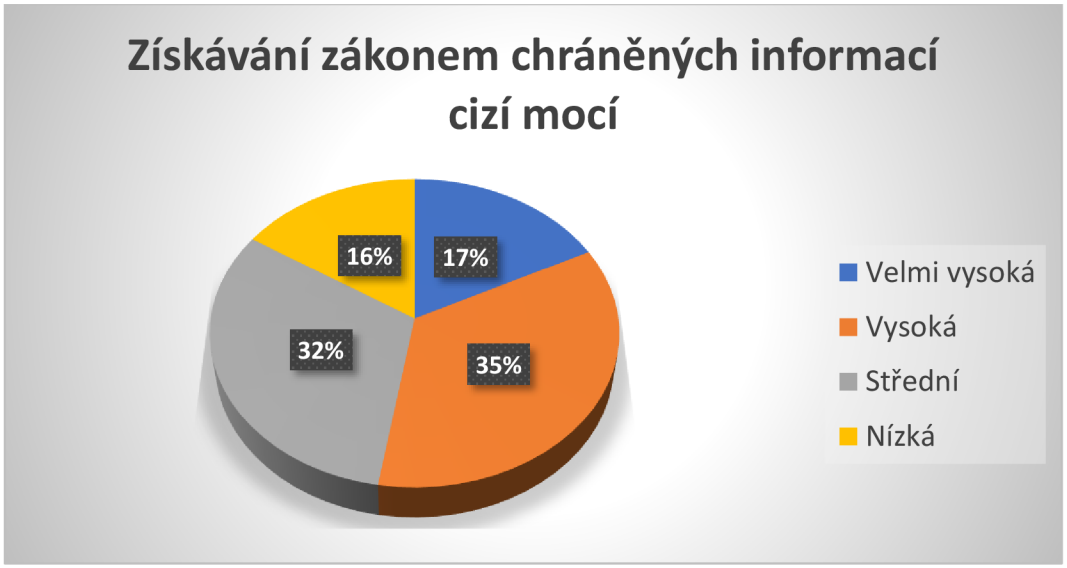
Bezpečnostní hrozba nezákonného získávání utajovaných informací cizí mocí náleží především do portfolia protišpionážních aktivit českých zpravodajských služeb realizovaných českými zpravodajci v čele s BIS. Ochrana chráněných informací má však své místo i v aktivitách orgánů činných v trestním řízení, neboť se o tyto nezákonné aktivity mohou pokusit i organizované zločinecké skupiny. Státem a zákonem chráněné informace, které mají obecně vysokou hodnotu pro cizí moc, vykazují především ekonomickou, politickou, vojenskou, zpravodajskou nebo i strategickou povahu atd. Úsilí získat takový druh informací vychází ze zájmu cizí moci dostat se k senzitivním informacím tohoto druhu. Tyto informace mohou protivníkovi přinést značnou výhodu nebo prospěch, a mohou z námi zkoumaného pohledu zásadně ohrozit bezpečnost státu nebo i bezpečnost euroatlantických spojenců. Zvláštní kapitolou této hrozby jsou

utajované informace[220], které mají z podstaty věci od ostatních chráněných informací nejvyšší stupeň ochrany.

Tabulka č. 21 a graf č. 14 Získávání zákonem chráněných informací cizí mocí

Získávání zákonem chráněných informací cizí mocí

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	10	17,5	17,5	17,5
	Vysoká	20	35,1	35,1	52,6
	Střední	18	31,6	31,6	84,2
	Nízká	9	15,8	15,8	100,0
	Celkem	57	100,0	100,0	



Respondenti BIS řadí tuto hrozbu do kategorie vysoké relevance, neboť 52,6 % dotazovaných řadí tuto hrozbu do kategorie velmi vysoké a vysoké relevance, avšak 32 % dotazovaných již hodnotí relevanci hrozby jako střední a 16 % jen jako nízkou. Průměr zkoumané hrozby je 2,46. Směrodatná odchylka vyjadřuje hodnotu 0,965, tedy středně vysokou míru měřeného rozptylu. Respondenti však nadpoloviční většinou označili i tuto hrozbu za závažnou a její relevanci za vysokou; tzn. „pouze" 30 % hodnotí hrozbu jako střední a 16 % ji

[220] Podrobněji např. DVOŘÁK Jan, CHROBÁK Jiří (2018): Zákon o ochraně utajovaných informací: Komentář. Wolters Kluwer, 480 s.

dokonce považuje za nízkou. Proto lze z hlediska české národní bezpečnosti i výzkumem stanovenou relevanci považovat za vysokou. Zde je patrný mírný rozpor s hodnocením hrozby v národních strategických textech, především s Auditem národní bezpečnosti, který hrozbě přiřadil střední stupeň relevance (viz níže).

Bezpečnostní strategie ČR sice této hrozbě nevěnuje explicitní pozornost, ale Audit národní bezpečnosti se již touto hrozbou podrobně zabývá v kapitole Působení cizí moci (s. 50)[221]. Přiřazuje jí střední míru relevance (s. 53)[222]. Je zde mj. konstatováno, že … „*získávání zákonem chráněných informací nebo jiných veřejně nepřístupných informací … může vést k ohrožení nebo poškození zájmů státu*." (s. 53).[223]

BIS ve své výroční zprávě za rok 2020 k státem připravovaném tendru na dostavbu nových bloků JE Dukovany např. konkrétně uvádí, že „*ve fázi před vyhlášením tendru spočívalo hlavní riziko v možném ovlivňování přípravy projektu a rozhodování o podstatných otázkách a parametrech tendru. BIS v této souvislosti zaznamenala např. snahu získávat interní informace z prostředí české státní správy a subjektů zapojených do přípravy projektu*" (s. 19)[224].

Bezpečnostní hrozba získávání zákonem chráněných informací cizí mocí **je intencionální hrozba s vysokou mírou rizika pro ČR (empirický výzkum). Audit národní bezpečnosti hrozbě přiřazuje střední hodnotu relevance. Z hlediska zpravodajských služeb se problematikou systematicky zabývají všechny tři české zpravodajské služby (BIS, ÚZSI a VZ) a jsou podporovány i národními policejními složkami v případě jejich závažných zjištění.** Hrozba je zařazena skupiny faktorové skladby **ohrožení působnosti státu a jeho ekonomické stability.**

---

[221] Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-03-07].
[222] Tamtéž
[223] Tamtéž
[224] Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf [online, cit. 2022-03-07].

A14 KYBERTERORISMUS
(intencionální bezpečnostní hrozba)

Oficiální webové stránky MV ČR definují kybernetický terorismus jako „souhrnný název pro teroristické aktivity, jejichž cílem útoku, použitým prostředkem nebo přenašečem je tzv. „kyberprostor“, neboli jde o teroristické aktivity zaměřené proti a prováděné prostřednictvím počítačové sítě a touto sítí řízených systémů („informační elektronické síťové struktury“)“[225]. Česká definice se však nezmiňuje o aktérech těchto nezákonných aktivit. Ve světě se často užívá definice kyberterorismu vypracována experty FBI, která kybernetický terorismus definuje jako „promyšlený, politicky motivovaný útok proti informacím, počítačovým systémům, počítačovým programům a datům, který vede k násilí proti nebojujícím cílům ze strany sub národních skupin nebo tajných agentů“[226]. Z kontextu vyplývá, že aktéry kybernetického terorismu jsou státní i nestátní aktéři a motivace kybernetických teroristických útoků může být různá (náboženská, sociální, politická nebo i vojenská atd.). Kybernetický terorismus je hrozba, která má stále aktuálnější potenciál a do budoucna může její nasazení převážit nad využitím klasických teroristických aktivit ve světě realizovaných do této doby. Její nespornou výhodou jsou relativně nízké náklady s velmi vysokou účinností možných následků těchto kybernetických teroristických útoků. I z tohoto důvodu jsou všechny vlády světa zainteresovány do boje s touto významově spíše budoucí bezpečnostní hrozbou. V českých podmínkách se těmito úkoly primárně zabývá Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), který však ve své koncepci rozvoje nepopisuje aktuální stav boje s těmito hrozbami zcela pozitivně: „*Nic z toho ovšem neznamená, že máme hotovo. Ve skutečnosti jsme teprve na začátku. Kybernetické hrozby ze strany států, kyberteroristů, kyberkriminálních skupin a dalších aktérů budou téměř jistě sílit. Dále lze očekávat příchod zcela nových a přelomových technologií, jako je umělá inteligence nebo*

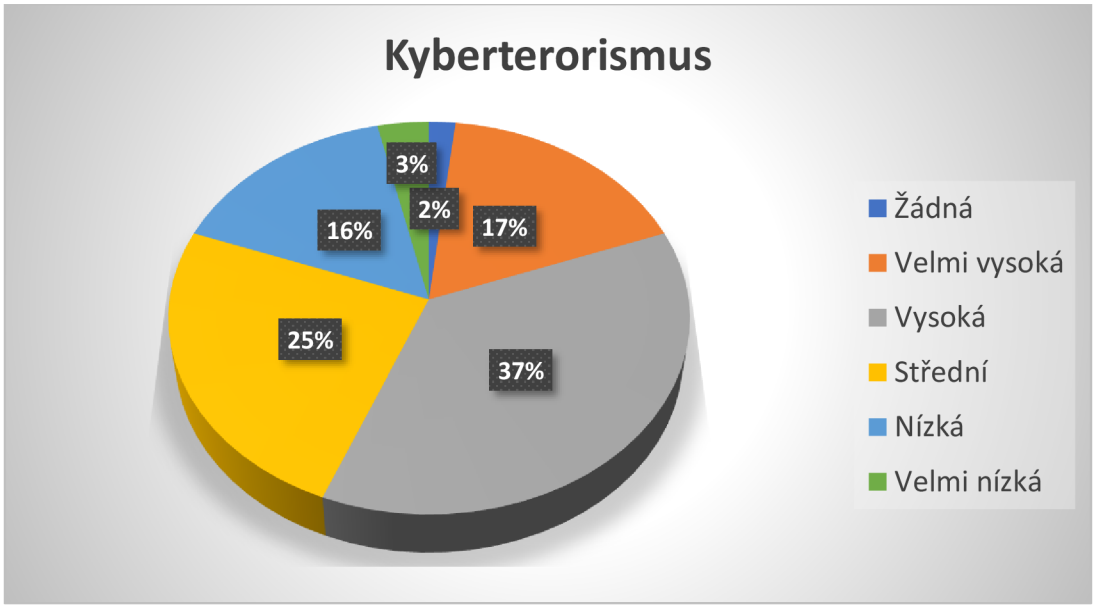
[225] Dostupné z https://www.mvcr.cz/clanek/kyberneticky-terorismus-kyberterorismus.aspx [online, cit. 2022-03-07].
[226] Dostupné z https://leb.fbi.gov/articles/featured-articles/cyber-terror [online, cit. 2022-03-07].

kvantové počítače, které zásadně ovlivní používanou kryptografii i další oblasti…“[227] Pozornost je této problematice stále intenzivněji věnována i na půdě NATO a EU. Kupříkladu Spojené státy otázku rozvíjejí především s ohledem na nepřátelské aktivity klíčových státních aktérů v čele s Ruskem, Severní Koreou nebo Íránem.[228]

Tabulka č. 22 a graf č. 15 Kyberterorismus

Kyberterorismus

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Žádná	1	1,8	1,8	1,8
	Velmi vysoká	10	17,5	17,5	19,3
	Vysoká	21	36,8	36,8	56,1
	Střední	14	24,6	24,6	80,7
	Nízká	9	15,8	15,8	96,5
	Velmi nízká	2	3,5	3,5	100,0
	Celkem	57	100,0	100,0	



[227] Koncepce rozvoje Národního úřadu pro kybernetickou a informační bezpečnost (2020), s. 4. Dostupné z https://www.nukib.cz/download/publikace/strategie_akcni_plany/Koncepce_rozvoje_NUKIB.pdf [online, cit. 2022-03-15].
[228] Annual Threat Assessment (2021), s. 8-16. Dostupné z https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf [online, cit. 2022-03-15].

Podle dotazovaných respondentů je hrozba kyberterorismu zařazena do kategorie vysoké relevance, neboť 54,3 % dotazovaných přiřadila této hrozbě kategorii velmi vysoké a vysoké relevance. Střední relevance byla označena 24,6 % dotazovaných, 15,8 % hrozbu hodnotí jako nízkou, 3,5 % jako velmi nízkou a dokonce 1,8 % jako žádnou. Průměr zkoumané hrozby je 2,5. Směrodatná odchylka vyjadřuje hodnotu 1,079, tedy vysoká míra měřeného rozptylu. Respondenti však nadpoloviční většinou označili i tuto hrozbu za závažnou a tím její relevanci za vysokou; avšak téměř 25 % respondentů hodnotilo hrozbu jako střední a téměř 16 % ji dokonce považuje za nízkou. Proto lze z hlediska české národní bezpečnosti i s odkazem na výsledky empirického výzkumu považovat relevanci této hrozby za vysokou, avšak s poměrně velkým názorovým rozptylem, který demonstruje nejednoznačnou shodu při stanovení konečné hodnoty relevance této bezpečnostní hrozby. V porovnání s hodnocením Auditu národní bezpečnosti (2016), který hrozbu kybernetického terorismu hodnotí ve střední škále, lze výsledek zjištěný empirickým výzkumem označit za ne zcela shodný, neboť ten tuto bezpečnostní hrozbu zařadil do kategorie vysoké relevance. Možný důvodem této skutečnosti může být i nestejný časový termín, kdy byly tyto hrozby hodnoceny. Mezi analýzou ANB (2016) a empirickým výzkumem uběhly minimálně 2,5 roky. Toto konstatování podporuje i naznačený trend ve stále se zvyšujícím nebezpečí jakéhokoliv ohrožení státu, které má svůj původ v kybernetické oblasti. A lze očekávat, že se tento trend bude nejenom zrychlovat, ale že i jeho intenzita bude výrazně stoupat.

Bezpečnostní strategie ČR (2015) věnuje obecně otázkám kybernetické bezpečnosti velkou pozornost a problematika kybernetické obrany státu se prolíná mnohými kapitolami textu. BS ČR (2015) se sice explicitně o kyberterorismu nezmiňuje; problém je ale řešen v popisu jedné z klíčových bezpečnostních hrozeb – Kybernetické útoky (s.11): „*Kybernetický prostor je velmi specifický neexistencí geografických hranic a relativizací vzdálenosti mezi zdroji hrozeb a potenciálním cílem. Díky své asymetričnosti pak umožňuje státním i nestátním*

aktérům poškodit strategické a významné zájmy ČR bez využití konvenčních prostředků (s. 11).“[229]

Zcela konkrétní je však Audit národní bezpečnosti (2016), který hrozbu kyberterorismu hodnotí jednak v otázkách možných útoků proti národní kritické infrastruktuře (s. 14), ale i jako samostatnou hrozbu v kapitole Hrozby v kyberprostoru, kde ji přiřazuje střední relevanci (s. 101). Zde je mj. konstatováno, že „*v užším pojetí lze za kyberterorismus považovat pouze takové teroristické aktivity v kyberprostoru, které způsobí rozsáhlé narušení počítačových sítí či zařízení se závažnými až fatálními dopady. Při těchto útocích může docházet ke ztrátám na životech či v případě kompromitace finančního systému k velmi závažným ekonomickým ztrátám s těžko předvídatelnými důsledky…kyberterorismus již nelze považovat za hypotetický fenomén a lze predikovat, že v blízké budoucnosti ke kyberteroristickým útokům bude docházet*…“ (s.101)[230].

BIS ve výroční zprávě za rok 2020 věnuje otázkám kybernetické bezpečnosti zvláštní pozornost, i když se o otázkám kyberterorismu explicitně nezmiňuje. V souladu s mezinárodními trendy však otázky kybernetické bezpečnosti akcentuje napříč celou veřejnou částí své výroční zprávy. Je zde zmiňována spolupráce s NCOZ, ale i s ostatními složkami spolupracujícími na platformách společné zpravodajské skupiny nebo Národního kontaktního bodu pro terorismus (s. 29).[231] Poslední výroční zprávy Vojenského zpravodajství a Národního úřadu pro kybernetickou bezpečnost se otázkami kyberterorismu explicitně nezabývají, i když je i tato problematika pokryta v jejich kompetenční gesci.

[229] Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2022-03-15].
[230] Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-03-15].
[231] Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf [online, cit. 2022-03-15].

Bezpečnostní hrozba kyberterorismus **je intencionální hrozba s vysokou mírou rizika pro ČR (empirický výzkum). Audit národní bezpečnosti hrozbě přiřazuje střední hodnotu relevance. Z hlediska zpravodajských služeb se problematikou systematicky zabývají všechny tři české zpravodajské služby (BIS, ÚZSI a VZ) a jsou podporovány i národními policejními a armádními složkami, a především aktivitami Národního úřadu pro kybernetickou a informační bezpečnost.** Hrozba je zařazena do skupiny faktorové skladby **hrozby v kyberprostoru.**

4.3.2. SOUHRNNÝ ROZBOR BEZPEČNOSTNÍCH HROZEB VYSOKÉ RELEVANCE

Výsledky empirického průzkumu přiřadily **čtrnácti zkoumaným bezpečnostním hrozbám vysokou míru relevance**. Téměř všechny bezpečnostní hrozby této skupiny jsou intencionálními hrozbami. Výjimku tvoří pouze hrozba dlouhodobého sucha, která je hrozbou neintencionální a není tudíž ze své podstaty obsahovou náplní práce českých zpravodajských služeb. Kromě dalších dvou hrozeb skupiny (zneužívání veřejných zakázek a rozpočtů a prorůstání organizovaného zločinu do veřejné správy) jsou všechny zbylé hrozby předmětem činnosti všech tří českých zpravodajských služeb. Bezpečnostní hrozby zneužívání veřejných zakázek a rozpočtů a prorůstání organizovaného zločinu do veřejné správy však náleží do působnosti domácí zpravodajské služby BIS. Lze konstatovat, že z hlediska zkoumané první skupiny vysoké relevance bezpečnostních hrozeb pokrývá činnost BIS celkově třináct položek ze čtrnácti (vyjma hrozby dlouhodobého sucha), a zbylé dvě služby (ÚZSI a VZ) jedenáct položek (vyjma hrozby dlouhodobého sucha, zneužívání veřejných zakázek a rozpočtů, prorůstání organizovaného zločinu do veřejné správy). Hrozba prorůstání organizovaného zločinu do veřejné správy však může mít i určitý mezinárodní přesah, rozhodně ale není prvoplánovou součástí aktivit ÚZSI a VZ. Znamená to tedy, že na sběr těchto informací nejsou z hlediska své působnosti ÚZSI a VZ zaměřeny a v případě, že na takové informace ve své činnosti narazí, většinou je předávají příslušným kompetentním, především policejním složkám.

Významné je však rozložení bezpečnostních hrozeb první skupiny stanovené nejvyšší relevance z hlediska jejich zařazení do konkrétních skupin faktorových skladeb[232].

Graf č. 16 Četnost hrozeb skupiny nejvyšší relevance do skupin faktorových skladeb

Z předem definovaných šesti faktorových skladeb zkoumaných bezpečnostních hrozeb[233] obsahuje první skupina vysoké relevance jen čtyři z nich (viz graf č. 16). Není zde zastoupena faktorová skladba skupin hrozeb spojených s hrozbami migrace a terorismu a hrozeb extremismu, tzn., že empirický výzkum nepřiřadil těmto hrozbám vysoký stupeň závažnosti.

Největší podíl stanovených hrozeb vysoké relevance (43 %) je z oblasti faktorové skladby **hrozby v kyberprostoru**. Konkrétně se jedná o hrozby

[232] Jak je uvedeno v kapitole 2, (2.4. Výzkum faktorové skladby bezpečnostních hrozeb na PAČR v Praze) jedná se o tyto faktorové skladby zkoumaných bezpečnostních hrozeb: 1. ohrožení působnosti státu a jeho ekonomické stability, 2. hrozby v kyberprostoru, 3. hrozby spojené s hrozbami migrace a terorismu, 4. hrozby extremismu, 5. hrozby energetické, surovinové, průmyslové a environmentální a 6. hrozby geopolitické.
[233] Poznámka č. 103

kybernetické špionáže, narušení odolnosti IT infrastruktury, hybridních hrozeb, nepřátelských kampaní, narušení bezpečnosti eGovernmentu a kyberterorismu. Výsledek je plně v souladu s aktuálními trendy, kdy se veškeré lidské aktivity přesunuly do kybernetického prostoru a tento hybridní způsob konfrontace nabírá stále na větším významu s tendencí postupné dominance.[234] Je však nutné zdůraznit, že tyto hybridní kybernetické hrozby mají stále více sofistikovaný a potencionálně velmi destruktivní charakter bezpečnostního ohrožení našeho státu. Hybridní hrozby jsou však chápány napříč českou bezpečnostní a expertní komunitou velmi odlišně. Obecně lze konstatovat, že vyšší míru relevance jim přiřazují zpravodajské služby a viditelně nižší míru relevance ostatní bezpečnostní složky, především z řad Policie ČR. Tento rozpor vysvětlitelný tím, že jsou české zpravodajské služby s těmito novými hrozbami konfrontovány podstatně intenzivněji, na rozdíl od některých policejních útvarů.[235] Zásadní podíl na aktivitách spojených s obranou kybernetického prostoru státu má od roku 2021 ve své gesci VZ, kterému novelou zákona o VZ byly značně rozšířeny pravomoci v této oblasti.

Druhý nejčastěji se vyskytující podíl hrozeb vysoké relevance (36 %) jsou hrozby obsažené ve faktorové skladbě **ohrožení působnosti státu a jeho ekonomické stability**. V tomto případě se jedná o hrozby ovlivňování veřejného mínění cizí mocí, ovlivňování veřejné správy cizí mocí, zneužívání veřejných zakázek a rozpočtů, prorůstání organizovaného zločinu do veřejné správy a získávání zákonem chráněných informací cizí mocí. BIS má v náplni své práce eliminaci všech pěti hrozeb. ÚZSI a VZ působí v oblasti tří z pěti uvedených hrozeb a nemají přímou působnost z hlediska boje s hrozbami zneužívání veřejných zakázek a rozpočtů a prorůstání organizovaného zločinu do veřejné správy. Hrozby z druhé skupiny faktorové sklady mají, s výjimkou již zmíněných hrozeb ekonomického charakteru, výraznou povahu nepřátelských aktivit cizí moci vůči našemu státu a projevují se v plném spektru kontrašpionážních aktivit

[234] KURFÜRST, PAĎOUREK (2021)
[235] Podrobně v 9. kapitole monografie KURFÜRST, PAĎOUREK (2021), PAĎOUREK Jan, KOVAŘÍK Zdeněk, Vnímání významu hybridních hrozeb českou (a slovenskou) bezpečnostní komunitou pohledem empirického výzkumu, s. 181–201.

českých zpravodajských služeb, ale i např. v odhalování nestátních aktivit nejrůznějších aktérů, kteří často v souladu s ideologií protivníka útočí na demokratickou podstatu ČR a její mezinárodní politické, ekonomické a bezpečnostní ukotvení. Často mají za cíl narušit jednak národní, ale i mezinárodní jednotu důležitou pro bezproblémové fungování českého státu.

4.4.3 B) BEZPEČNOSTNÍ HROZBY STŘEDNÍ RELEVANCE

B1 ORGANIZOVANÁ DAŇOVÁ KRIMINALITA
(intencionální bezpečnostní hrozba)

Daňová kriminalita je z hlediska národní bezpečnosti součástí nelegálních kriminální aktivit různých organizovaných kriminálních skupin, s kterými v českých podmínkách nejaktivněji bojují různé policejní složky (v čele s NCOZ), společně s pracovníky Generálního ředitelství cel (GŘC), Generálního finančního ředitelství (GFŘ), ale i s významnou informační podporou BIS. Ostatní české zpravodajské služby sledují tuto problematiku spíše okrajově, zda – li vůbec. V rámci boje s organizovanou daňovou kriminalitou byl v ČR zřízen společný tým NCOZ, GŘC a GFŘ tzv. Daňová kobra[236]

O tom, že má tato problematika i výrazný mezinárodní přesah vypovídají např. různé aktivity významných mezinárodních platforem, které věnují boji s organizovanou daňovou kriminalitou zásadní pozornost. Jako příklad lze uvést aktivity Organizace pro hospodářskou spolupráci a rozvoj (OECD), která v roce 2021 vydala zprávu věnovanou právě boji s daňovou kriminalitou. Ve zprávě „Ending the Shell Game: Cracking down on the Professionals that aktivs Tax and White Collar Crimes“[237] vybízí všechny národní státy, aby zvážily přijetí národních

[236] Tým Daňová kobra složený z pracovníků NCOZ, GŘC a GFŘ od svého vzniku již zachránil státnímu rozpočtu desítky miliard korun. Dostupné z https://www.danovakobra.cz/ [online, cit. 2022-03-15].
[237] Dostupné z https://www.oecd.org/tax/crime/ending-the-shell-game-cracking-down-on-the-professionals-who-enable-tax-and-white-collar-crime.pdf [online, cit. 2022-03-15].

koncepcí v boji s organizovanou daňovou kriminalitou[238]. Toto konstatování jen potvrzuje, že je tento problém přítomný ve všech zemích světa, a že je obecně vnímán jako zásadní bezpečnostní hrozba.

Daňová kriminalita je často úzce spojena i s dalšími nezákonnými aktivitami, jako je praní špinavých peněz, korupce, vydírání atd.

Tabulka č.23 a graf č. 17 Organizovaná daňová kriminalita

Organizovaná daňová kriminalita

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	4	7,0	7,0	7,0
	Vysoká	20	35,1	35,1	42,1
	Střední	27	47,4	47,4	89,5
	Nízká	5	8,8	8,8	98,2
	Velmi nízká	1	1,8	1,8	100,0
	Celkem	57	100,0	100,0	

[238] Podrobnosti dostupné z https://www.oecd.org/ctp/crime/about-tax-and-crime.htm [online, cit. 2022-03-15].

Respondenti přiřadili této hrozbě středně vysokou relevanci. Celkově 42,1 % dotazovaných považuje hrozbu za velmi vysokou a vysokou relevanci. Střední relevance byla označena 24,6 % dotazovaných, 15,8 % hrozbu hodnotí jako nízkou, 3,5 % jako velmi nízkou a dokonce 1,8 % jako žádnou. Průměr zkoumané hrozby je 2,5. Směrodatná odchylka vyjadřuje hodnotu 1,079, tedy vysoká míra měřeného rozptylu. Respondenti však nadpoloviční většinou označili i tuto hrozbu za závažnou a tím její relevanci za vysokou; avšak téměř 25 % respondentů hodnotilo hrozbu jako střední a téměř 16 % ji dokonce považuje za nízkou. Proto lze z hlediska české národní bezpečnosti i s odkazem na výsledky empirického výzkumu považovat relevanci této hrozby za vysokou, avšak s poměrně velkým názorovým rozptylem, který demonstruje nejednoznačnou shodu při stanovení relevance této bezpečnostní hrozby. V porovnání s hodnocením Auditu národní bezpečnosti (2016), který hrozbu organizované daňové kriminality hodnotí ve střední škále, lze výsledek zjištěný empirickým výzkumem označit za ne zcela shodný, neboť ten tuto bezpečnostní hrozbu zařadil do kategorie vysoké relevance. Možný důvodem této skutečnosti může být i nestejný časový termín, kdy byly tyto hrozby hodnoceny. Mezi analýzou ANB (2016) a empirickým výzkumem uběhly minimálně 2,5 roky. Toto konstatování podporuje i naznačený trend ve stále se zvyšujícím nebezpečí ohrožení státu z různých hledisek, které má svůj původ v kybernetické oblasti. A lze očekávat, že se tento trend bude nejenom zrychlovat, ale že i jeho intenzita bude výrazně zvyšovat.

Konstatování o aktivitách BIS v této oblasti a její spolupráci s příslušnými orgány činnými v trestním řízení potvrzují např. i informace z výroční zprávy BIS za rok 2020. Konkrétně je zde mimo jiné konstatováno, že „*…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* (s.38).“[239]

[239] Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf [online, cit. 2022-05-05].

Bezpečnostní hrozba organizovaná daňová kriminalita **je intencionální hrozba se středně vysokou mírou rizika pro ČR (empirický výzkum s velkým názorovým rozptylem). Audit národní bezpečnosti hrozbě přiřazuje střední hodnotu relevance. Z hlediska zpravodajských služeb se problematikou systematicky zabývá především BIS, která svými aktivitami a informacemi podporuje policejní složky činné v trestním řízení, ale i Generální finanční ředitelství nebo Úřad pro ochranu hospodářské soutěže, Generální ředitelství cel** atd. Hrozba je zařazena do skupiny faktorové skladby **ohrožení působnosti státu a jeho ekonomické stability.**

B2 POLITICKÝ EXTREMISMUS
(intencionální bezpečnostní hrozba)

Ministerstvo vnitra ČR a konkrétně Národní centrála proti organizovanému zločinu definuje extremismus jako **pojem, kterým jsou označovány „vyhraněné ideologické postoje, které vybočují z ústavních, zákonných norem, vyznačují se prvky netolerance, a útočí proti základním demokratickým ústavním principům, jak jsou definovány v českém ústavním pořádku.“**[240] Tato definice extremismu v podstatě obsahuje vyčerpávající popis i zkoumané bezpečnostní hrozby politického extremismu. V českých podmínkách rozlišujeme v podstatě dva druhy politického extremismu: politický extremismu **pravicový** a politický extremismus **levicový**. Levicový i pravicový extremismus jsou však v tomto empirickém výzkumu vnímány jako samostatné bezpečnostní hrozby, které budou níže dále analyzovány odděleně. Český pravicový extremismus čerpá především z ideologie rasové nesnášenlivosti a hledá inspiraci ve fašistických nebo nacistických ideologiích. Levicový extremismus naopak akcentuje otázky sociální rovnosti a jeho inspirací jsou často komunistické nebo přímo anarchistické ideologie.[241] Podle oficiálního webového portálu MV ČR však není obecný pojem

[240] Dostupné z https://www.policie.cz/clanek/ncoz-extremismus-co-je-extremismus.aspx [online, cit. 2022-05-05].
[241] Podrobněji viz oficiální webový portál MV ČR. Dostupné z https://www.mvcr.cz/clanek/co-je-extremismus.aspx [online, cit. 2022-05-05].

extremismu v českém právu nikterak definován a české složky činné v trestním řízení spíše používají jiné užší verze tohoto pojmu, resp. trestné činnosti, jako je například extremistická trestná činnost nebo trestný čin s extremistickým podtextem.[242]

Z hlediska činnosti českých zpravodajských služeb má hlavní a v podstatě exkluzivní působnost v této oblasti BIS, která je v odhalování a předcházení těmto nezákonným aktivitám přímo úkolována v zákoně O zpravodajských službách ČR č. 153/1994 Sb. Neboť jsou podstatou těchto nelegálních aktivit především snahy narušit nejrůznějšími způsoby ústavní pořádek země, je činnost BIS v otázkách boje s politickým extremismu i jeho jinými druhy[243] obsažena v konkrétním popisu jedné z působností dané zákonem: „*zabezpečuje informace o záměrech a činnostech namířených proti demokratickým základům, svrchovanosti a územní celistvosti České republiky*.“[244]

MV ČR rovněž publikuje a veřejně zpřístupňuje řadu přehledových zpráv, akčních plánů nebo koncepcí o problematice extremismu a boje s ním.[245] I tato hrozba má významný mezinárodní přesah a je akcentována v mnohých zprávách nebo rezolucích mezinárodních organizací.[246]

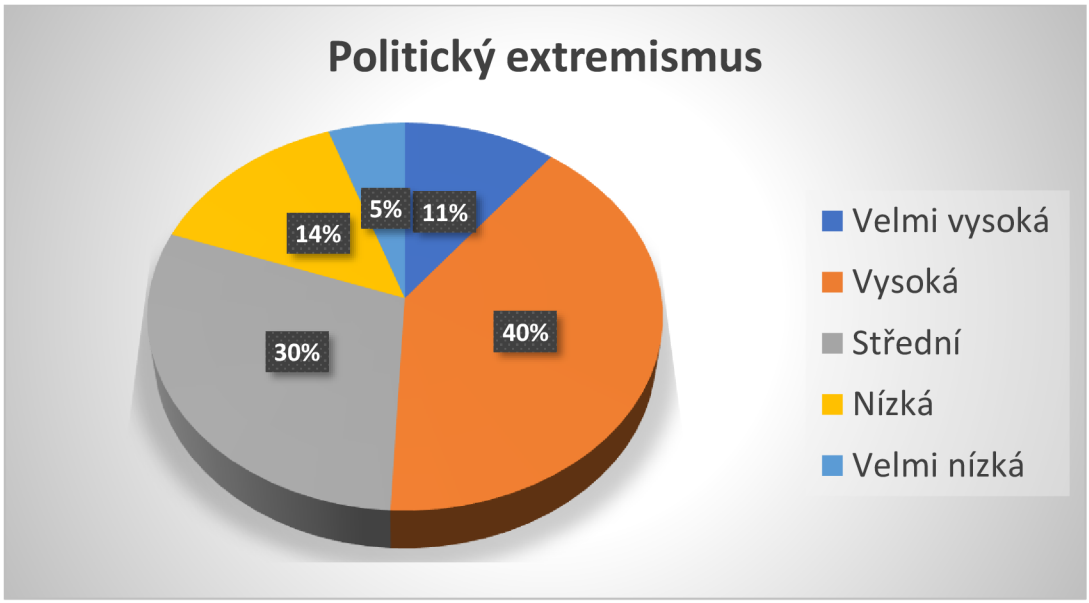
---

[242] Dostupné z https://www.mvcr.cz/clanek/co-je-extremismus.aspx [online, cit. 2022-05-05].
[243] Např. extremismus národnostní, radikální, náboženský atd.
[244] Zákon č. 153/1994 Sb., §5, odst. a). Dostupné z https://www.zakonyprolidi.cz/cs/1994-153 [online, cit. 2022-05-05].
[245] Např. Zpráva o extremismu a předsudečné nenávisti na území ČR v roce 2020, Akční plán proti projevům extremismu a předsudečné nenávisti 2021-2022, Koncepce boje proti projevům extremismu a předsudečné nenávisti 2021-2026. Dostupné z https://www.mvcr.cz/clanek/extremismus-vyrocni-zpravy-o-extremismu-a-strategie-boje-proti-extremismu.aspx [online, cit. 2022-05-05].
[246] Např. nejrůznější rezoluce Parlamentního shromáždění Rady Evropy (PACE), viz. např. Fight against Extremism: Achievements, Deficiencies and Failures. Dostupné z http://www.assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=17898&lang=en [online, cit. 2022-05-05].

Tabulka č. 24 a graf č. 18 Politický extremismus

Politický extremismus

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	6	10,5	10,5	10,5
	Vysoká	23	40,4	40,4	50,9
	Střední	17	29,8	29,8	80,7
	Nízká	8	14,0	14,0	94,7
	Velmi nízká	3	5,3	5,3	100,0
	Celkem	57	100,0	100,0	



Ačkoliv více jak polovina respondentů označila hrozbu politického extremismu v ČR za velmi vysokou a vysokou (50,9 %), je tato hrozba řazena již do horní části středně vysoké relevance. Důvodem je jednak vysoký názorový rozptyl respondentů (směrová odchylka 1,029), ale naměřený i průměr 2,63, shodný např. s bezpečnostní hrozbou organizované daňové kriminality. Jako středně vysokou relevanci hodnotí hrozbu 29.8 % respondentů, nízkou relevanci 14 % a velmi nízkou relevanci 5,5 %. Audit národní bezpečnosti analyzující i tuto hrozbu však stanovil pouze nízkou hodnotu relevance. Z této komparace lze dovodit, že zpravodajská služba hodnotí nebezpečí politického extremismu pro českou národní bezpečnost poněkud vážněji, ale zároveň nepřisuzuje této hrozbě nejvyšší relevanci. To je doloženo i informacemi obsaženými ve veřejně sdílených

informacích publikovaných touto zpravodajskou službou ve veřejných částech výročních zpráv. V roce 2019 zde BIS konstatuje, že „*tradiční pravicově i levicově extremistická scéna se již několik let nachází v krizi. Existující skupiny štěpí a oslabuje vnitřní názorová roztříštěnost i řada osobních animozit a v důsledku nejsou schopny získávat nové členy ani podporovatele. Aktivity extremistických uskupení stagnují nebo upadají i proto, že extremistům dlouhodobě chybí témata, která by scénu aktivizovala a mobilizovala její příznivce*“ (s.12).[247] V zatím poslední publikované výroční zprávě z roku 2020 BIS uvádí, že „*Pandemie covid-19 pouze akcelerovala dlouholetý vývoj extremistické scény, který potvrdil, že scéna prošla výraznou transformací. Byť je činnost některých extremistů mediálně atraktivní a jejich případné excesy přitahují pozornost, reálný mobilizační potenciál i kompetence členů organizovaných extrémistických skupin zůstávají malé a tyto subjekty víceméně stagnují. Ve vztahu k ochraně demokratických základů státu nejsou organizované extremistické skupiny již několik let v ČR závažným bezpečnostním rizikem* (s.21).[248]

Bezpečnotsní strategie ČR (2015) vidí důvody extremismu v ČR především z hlediska problémů s chudobou a sociálním vyloučením. Konkrétně uvádí: „*Problémy spojené s chudobou, dlouhodobým sociálním vyloučením a nedostatkem základních potřeb a služeb mohou výrazně zvýšit pravděpodobnost výskytu extremismu…* (s.9)“[249] Audit národní bezpečnosti pak popis extremistické scény v ČR doplňuje těmito slovy a konstatuje i jeho mezinárodní přesah: „*V ČR působí množství skupin, které je možné označit za extremistické, přičemž některé z nich mají mezinárodní vazby. Členové těchto skupin se dopouští trestné činnosti, v některých případech i násilného charakteru*“ (s. 12).[250]

[247] Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf [online, cit. 2022-05-05].
[248] Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf [online, cit. 2022-05-05].
[249] Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2022-05-05].
[250] Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-05-05].

Bezpečnostní hrozba politický extremismus **je intencionální hrozba se středně vysokou mírou rizika pro ČR (výsledek empirického výzkumu s velkým názorovým rozptylem). Audit národní bezpečnosti hrozbě přiřazuje nízkou hodnotu relevance. Z hlediska zpravodajských služeb se problematikou systematicky zabývá především BIS, která svými aktivitami a informacemi podporuje policejní složky činné v trestním řízení, v konkrétních případech však zahraniční přesah hrozby sledují i ostatní zpravodajské služby, především ÚZSI.** Hrozba je zařazena do skupiny faktorové skladby **hrozby extremismu.**

B3 ZNEUŽÍVÁNÍ LEGITIMNÍCH SLUŽEB ORGANIZOVANÝM ZLOČINEM (intencionální bezpečnostní hrozba)

Zneužití legitimních služeb organizovaným zločinem patří mezi velmi komplikované a bezpečnostními složkami často velmi složitě odhalitelné aktivity podsvětí, které nejrůznějšími způsoby zneužívají legální služby pro maskování nebo legalizaci nezákonně nabitých zisků nebo transferů nejrůznějších komodit. Jedná se zde především o celý systém služeb, které jsou prvoplánově určeny pro užití jednak běžného občana nebo firem a různých obchodních společností. Jako příklad lze uvést např. poštovní nebo kurýrní služby, jejichž prostřednictvím mohou být distribuovány nezákonné komodity (např. drogy, zbraně). Daleko závažnějším problém je však zneužívání bankovních služeb, kde je akcent kladen především na problematiku praní špinavých peněž nebo jiné formy peněžních podvodů majících původ v nezákonné organizované kriminalitě. Své místo zde hrají i pokusy korumpovat státní správu a její představitele. Tyto formy kriminality jsou často spojovány s tzv. „zločinem bílých límečků“ tedy osob, které zneužívají svého postavení a s tím spojených možností k páchání závažné trestné činnosti. Často působí organizovaně. Na tento druh organizovaného zločinu „vyšší společenské třídy“ upozornil již ve 40.letech minulého století americký sociolog Edwin H. Sutherland,[251] který poprvé komplexněji definoval stále intenzivnější zapojování těchto struktur do aktivit organizovaného zločinu. Tento problém v průběhu 90. let

[251] SUTHERLAND, Edwin H. (1940), White-Coller Criminality, American Sociological Review 5, číslo 1, s. 1-12.

minulého století vyeskaloval i v ČR. Podle mediálně prezentovaného sdělení ředitele Institutu pro kriminologii a sociální prevenci M. Scheinosta se značně změnil i charakter trestné činnosti různých zahraničních nebo mezinárodních mafiánských struktur působících na území ČR (ruské, ukrajinské, vietnamské nebo albánské mafie), které postupně přešly od svých „klasických" aktivit (krádeže aut, výpalné, prostituce, prodej drog, pašování a prodej zbraní atd.) k ekonomické kriminalitě.[252] Toto konstatování svědčí o tom, že se popisovaný problém netýká pouze domácí kriminality, ale má i velký zahraniční přesah, i když se v našem prostředí primárně týká nezákonných aktivit cizinců dlouhodobě působcích na území ČR. Toto konstatování znamená, že z hlediska zpravodajských služeb je působnost v této oblasti zaměřena především na působnost BIS, která v úzké součinnosti s policejními složkami čelí těmto nezákonným aktivitám. Kvůli zahraničním přesahům však svou roli hraje i činnost ÚZSI a v případě obchodu s vojenským materiálem i VZ.

Tabulka č. 25 a graf č. 19 Zneužívání legitimních služeb pro účely organizovaného zločinu

Zneužití legitimních služeb pro účely organizovaného zločinu

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	3	5,3	5,3	5,3
	Vysoká	22	38,6	38,6	43,9
	Střední	23	40,4	40,4	84,2
	Nízká	8	14,0	14,0	98,2
	Velmi nízká	1	1,8	1,8	100,0
	Celkem	57	100,0	100,0	

[252] Od krádeží aut k daňovým podvodům, studie popsala, jak se v Česku od roku 1989 změnila mafie, Seznam zprávy, 21.9. 2019. Dostupné z https://www.seznamzpravy.cz/clanek/od-kradezi-aut-k-ekonomicke-kriminalite-studie-popsala-jak-se-v-cesku-od-roku-1989-zmenila-mafie-79260 [online, cit. 2022-05-31].

Hrozba zneužití legitimních služeb pro účely organizovaného zločinu je respondenty empirického průzkumu hodnocena jako hrozba střední relevance. Vykazuje relativně velký názorový rozptyl. Byl zde dosažen průměr 2,68 se směrodatnou odchylkou 0,848. Pouze 5,3 % respondentů vnímá tuto hrozbu jako velmi vysokou, ale již celých 38,6 % jako vysokou. Největší počet respondentů označilo hrobu v pásmu střední relevance (40,4 %), 14 % za nízkou a jen 1,8 % za velmi nízkou. Tyto výsledky víceméně korespondují i se závěry učiněnými v Auditu národní bezpečnosti (2016), který hrozbu také zařadil do střední relevance.[253]

Audit národní bezpečnosti k problematice mj. konstatuje, že „*zneužití legitimních služeb a oprávnění není přímou novou hrozbou, ale „pouze" napomáhá úspěšnému páchání organizované trestné činnosti*"[254]. Z tohoto kontextu je patrné, že je hrozba i v ČR přítomna dlouhodobě, ale v posledních dekádách zaznamenává vyšší nárůst. To potvrzují i informace z oficiální webové stránky MV ČR, kde je mj. konstatováno, že „[skupiny organizovaného zločinu] *prostřednictvím svých kontaktů nepřímo ovlivňují politiku, justici, obchod a výrobu,*

[253] ANB (2016), s. 44. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-05-31].
[254] ANB (2016), s. 44. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-05-31].

mediální a zábavní průmysl a občanskou společnost takovým způsobem, že je i pro bezpečnostní sbory velmi často obtížné rozlišovat mezi legitimní a nelegitimní činností. V České republice dosáhl pokročilého stadia proces, kdy nejnebezpečnější organizované zločinecké skupiny využívají k získání moci a prospěchu nikoliv násilí, ale finančních machinací".[255]

Z hlediska působnosti zpravodajských služeb je patrné, že největší díl odpovědnosti za boj s touto hrozbou nese BIS, jako zásadní podporovatel aktivit speciálních policejních jednotek (především NCOZ). BIS ve své výroční zprávě za rok 2019 mj. uvádí, že problémem je „*fenomén organizovaného zločinu, který se prolínal řadou jiných témat, jako je např. ochrana významných ekonomických zájmů nebo nepřátelské aktivity cizí moci*."[256] I když ÚZSI ani VZ ve svých veřejných výstupech aktivity spojené s touto hrozbou explicitně neuvádí je zřejmé, že minimálně díky mezinárodnímu přesahu různých zločineckých aktivit spojených s organizovaným zločinem v této oblasti rovněž informačně přispívají. Hlavní zátěž v národních podmínkách však v této otázce leží na bedrech BIS.

Bezpečnostní hrozba zneužití legitimních služeb pro účely organizovaného zločinu **je intencionální hrozba se střední mírou rizika pro ČR (výsledek empirického výzkumu s relativně velkým názorovým rozptylem). Audit národní bezpečnosti rovněž hrozbě přiřazuje střední hodnotu relevance. Z hlediska zpravodajských služeb se problematikou systematicky zabývá především BIS, která svými aktivitami a informacemi podporuje policejní složky činné v trestním řízení (především NCOZ). V konkrétních případech však zahraniční přesah hrozby sledují i ostatní zpravodajské služby, především ÚZSI.** Hrozba je zařazena do skupiny faktorové skladby **ohrožení působnosti státu a jeho ekonomické stability.**

---

[255] Dostupné z https://www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09Mg%3D%3D [online, cit. 2022-05-31].
[256] Výroční zpráva BIS (2019) s. 5. Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf. [online, cit. 2022-05-31].

B4 LEGALIZACE VÝNOSŮ Z TRESTNÉ ČINNOSTI
(intencionální bezpečnostní hrozba)

Legalizace výnosů z trestné činnosti je klasickou bezpečnostní hrozbou, která je nedílnou součástí nezákonných aktivit jedinců, ale především nelegálních aktivit různých skupin organizovaného zločinu. Z tohoto hlediska lze tvrdit, že je téměř jakákoliv nezákonná aktivita organizovaného zločinu ve finále zvršena legalizací nezákonných výnosů. I proto se jedná o mimořádně nebezpečnou hrozbu, narušující politické, právní, ekonomické i sociální prostředí společnosti. Jan Ondřej Wilsdorf z advokátní kanceláře Brož & Sokol & Novák ve studii Praní peněz optikou trestního zákoníku (2020)[257] mj. tvrdí, že i když český trestní zákoník postihuje tento trestný čin již od počátku devadesátých let minulého století, prvním skutečně odsouzeným člověkem za tuto trestnou činnost byl pachatel odsouzený až v roce 2005. Navíc novela trestního zákona z roku 2018, s účinností od roku 2019, přinesla v trestání těchto zločinů zásadní změny[258]. Podle této právní úpravy je legalizace výnosů z trestní činnosti obecně definována takto: Legalizací výnosů z trestné činnosti se rozumí *„jednání sledující zakrytí nezákonného původu jakékoliv ekonomické výhody vyplývající z trestné činnosti s cílem vzbudit zdání, že jde o majetkový prospěch nabytý v souladu se zákonem“*.[259] Tato forma kriminality má svoji domácí i zahraniční působnost.

---

[257] WILSDORF, Jan Ondřej (2020), Praní peněz optikou trestního zákoníku, portál epravo.cz. Dostupné z https://www.epravo.cz/top/clanky/prani-penez-optikou-trestniho-zakoniku-110566.html#_ftn1 [online, cit. 2022-05-31].

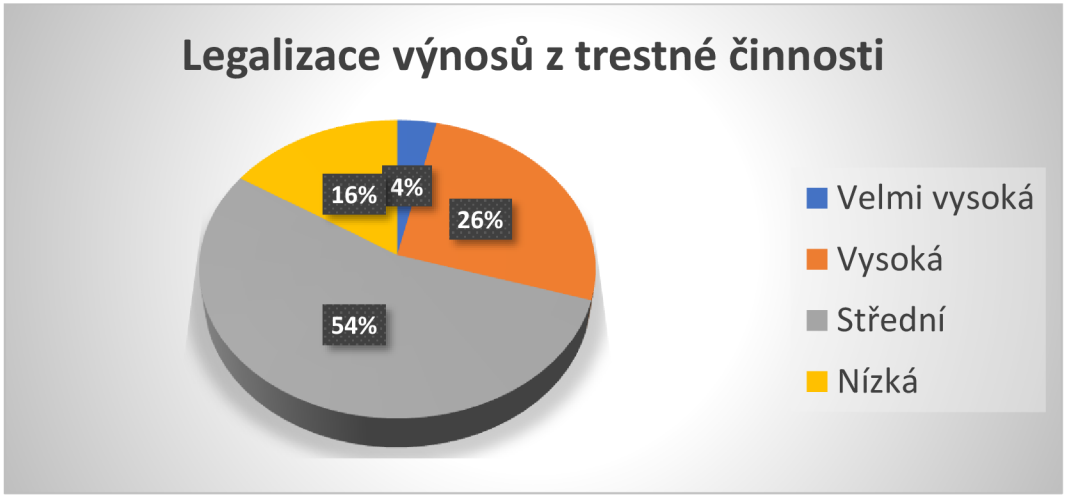
[258] WILSDORF, Jan Ondřej (2020), Praní peněz optikou trestního zákoníku, portál epravo.cz. Dostupné z https://www.epravo.cz/top/clanky/prani-penez-optikou-trestniho-zakoniku-110566.html#_ftn1 [online, cit. 2022-05-31].

[259] WILSDORF, Jan Ondřej (2020), Praní peněz optikou trestního zákoníku, portál epravo.cz. Dostupné z https://www.epravo.cz/top/clanky/prani-penez-optikou-trestniho-zakoniku-110566.html#_ftn1 [online, cit. 2022-05-31] a dále Trestní zákoník, ČÁST DRUHÁ, HLAVA V, § 216, odst. 1. Dostupné z http://zakony.centrum.cz/trestni-zakonik/cast-2-hlava-5-paragraf-216 [online, cit. 2022-05-31].

Tabulka č. 26 a graf č. 20 Legalizace výnosů z trestné činnosti

Legalizace výnosů z trestné činnosti

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	2	3,5	3,5	3,5
	Vysoká	15	26,3	26,3	29,8
	Střední	31	54,4	54,4	84,2
	Nízká	9	15,8	15,8	100,0
	Celkem	57	100,0	100,0	



Z hlediska respondentů empirického výzkumu byla bezpečnostní hrozba legalizace výnosů z trestné činnosti zařazena do střední relevance s relativně velkým názorovým rozptylem. Pouze 3,5 % respondentů hodnotí hrozbu jako velmi vysokou; 26,3 % však jako vysokou; 54,4 % jako střední a celých 15,8 % jako nízkou. Empirický výzkum naměřil průměr této hrozby 2,82 a směrodatnou odchylku 0,735. I když zde jednoznačně převažuje shoda na střední relevanci hrozby, přesto více jak 30 % hodnotí hrozbu jako velmi vysokou a vysokou. Proto lze konstatovat, že je tato hrozba jednou z velmi vážných rizik ohrožující národně bezpečnostní zájmy. Je proto zcela legitimní, že se aktivity bezpečnostních složek, včetně některých zpravodajských služeb (primárně BIS), tímto směrem zaměřují. Stejně tak je hrozba akcentována i v některých národních strategických dokumentech, především v ANB 2016.

ANB 2016 přiřazuje hrozbě legalizace výnosů z trestné činnosti shodně s empirickým výzkumem střední relevanci. Ve zdůvodnění mj. uvádí, že „*aktivity organizovaných zločinecký struktur generují vysoké zisky, které se logicky jejich příslušníci snaží opětovně využít ve svůj prospěch a pokud možno je zlegalizovat investicí do legálních statků (obchodních společností a nemovitostí). Významným problémem v této oblasti je vytváření vysoce sofistikovaných struktur obchodních společností s cílem legalizovat v nich prostředky pocházející z trestné činnosti*."[260] Rovněž Bezpečnostní strategie ČR (2015) věnuje tomuto jevu pozornost v oddíle popisující jednotlivé prvky organizovaného zločinu. BS ČR 2015 zde akcentuje především důraz na posilování kapacit státních institucí v boji s touto hrozbou: „*Klíčová je podpora vyhledávání a zajišťování výnosů z trestné činnosti. Zásadním problémem boje s organizovaným zločinem a korupcí zůstává případná zranitelnost státu. Proto je v první řadě nezbytné posilovat kapacity státních institucí k ochraně společnosti před organizovanou kriminalitou a korupcí*."[261]

Důležitým vedlejším problémem této hrozby je účast jednotlivců nebo i běžných institucí z důvodu obchodního zájmu (banky, realitní instituce apod.). Nejde jen o domácí kriminalitu, příkladem je například účast některých velkých evropských bank při mezinárodním praní peněz z Ruska.[262] V posledních letech proto zesílil i mezinárodní tlak na transparentnost finančních operací.

Bezpečnostní hrozba legalizace výnosů z trestné činnosti **je intencionální hrozba se středně vysokou mírou rizika pro ČR (výsledek empirického výzkumu s relativně velkým názorovým rozptylem). Ve shodě se závěry empirického výzkumu i Audit národní bezpečnosti přiřazuje hrozbě střední hodnotu relevance. Z hlediska zpravodajských služeb se problematikou**

[260] Audit národní bezpečnosti (2016), s. 43. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-06-07].
[261] BS ČR (2015), s. 17, odst. 71. Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2022-06-07].
[262] Např. vyšetřování Deutsche Bank kvůli podezření praní peněž z Ruska. Dostupné z https://www.cnbc.com/2022/04/29/prosecutors-search-deutsche-bank-hq-in-money-laundering-investigation.html [online, cit. 2022-10-13].

systematicky zabývá především BIS, která i v tomto případě významně podporuje policejní složky činné v trestním řízení (především NCOZ). Zahraniční přesah hrozby sledují i ostatní zpravodajské služby, především ÚZSI. Hrozba je zařazena do skupiny faktorové skladby **ohrožení působnosti státu a jeho ekonomické stability.**

B5 POVODNĚ
(neintencionální bezpečnostní hrozba)

Bezpečnostní ohrožení země povodněmi je druhou neintencionální bezpečnostní hrozbou (vedle již popsané hrozby dlouhodobého sucha), která má své místo v pestré paletě bezpečnostních hrozeb ČR. Tato hrozba je zde především vnímána zásadně jako důsledek přírodních jevů, na které má člověk pouze druhotný, resp. zanedbatelný vliv. Povodeň však může být i důsledkem technické katastrofy, ale i v tomto případě (pokud se nejedná o konkrétní formu terorismu nebo sabotáže) není tato hrozba předmětem aktivit zpravodajských služeb. Obecně termín „povodeň" definují oficiální stránky MV ČR jako „*přechodné výrazné zvýšení hladiny vodních toků nebo jiných povrchových vod, při kterém voda již zaplavuje území mimo koryto vodního toku. Přechodné výrazné stoupnutí vodní hladiny konkrétního vodního toku, při kterém se voda z koryta vylévá, způsobuje následné zaplavení bezprostředního i blízkého okolí vodního toku, ohrožuje životy a majetek, devastuje životní prostředí a působí značné materiální škody...*".[263]

Zásadním mementem a důvodem, proč se problematika povodní dostala do zorného úhlu i českých strategických bezpečnostních dokumentů, byly dvě vlny povodní z let 1997 a 2002. Podle vládních odhadů napáchaly povodně v ČR v roce 1997 celkové škody za 62,7 miliard korun a v roce 2002 již za téměř 80 miliard korun. Mezi oběma povodněmi však byl jeden zásadní rozdíl. Jestliže v roce 1997 zcela selhal národní integrovaný záchranný systém (IZS), což způsobilo smrt 50 lidí, v roce 2002 během povodní zemřelo 17 občanů ČR, a to

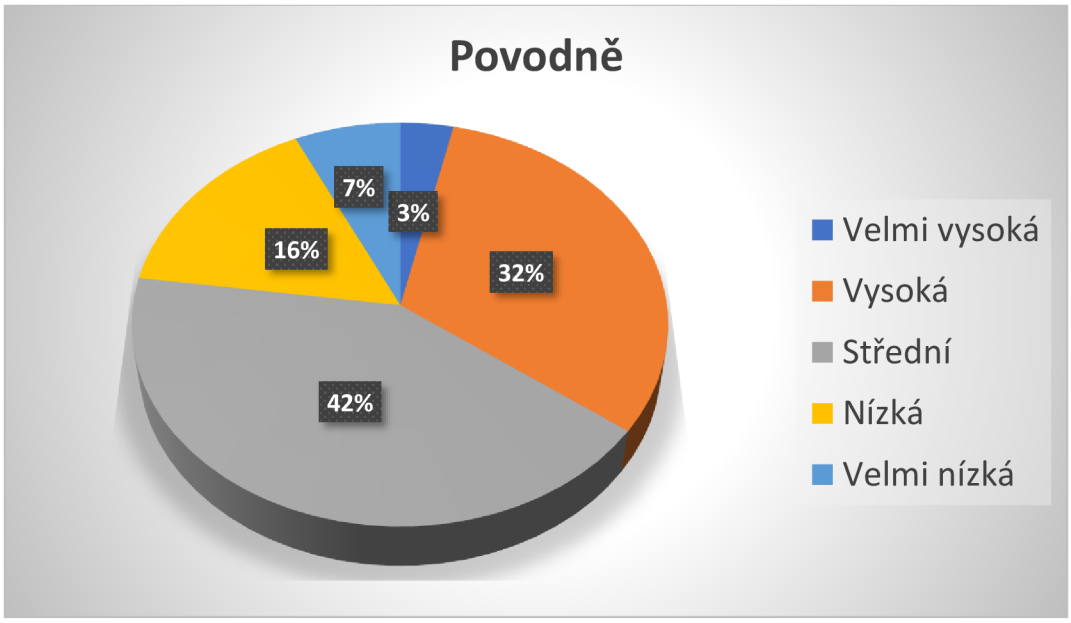
[263] Dostupné z https://www.mvcr.cz/clanek/povoden.aspx [online, cit. 2022-06-07].

především z řad neukázněných jedinců. Tento stav je výsledkem práce profesionálně poučeného a nyní již připraveného IZS.[264]

Tabulka č.27 a graf č. 21 Povodně

Povodně

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	2	3,5	3,5	3,5
	Vysoká	18	31,6	31,6	35,1
	Střední	24	42,1	42,1	77,2
	Nízká	9	15,8	15,8	93,0
	Velmi nízká	4	7,0	7,0	100,0
	Celkem	57	100,0	100,0	



Ačkoliv je bezpečnostní hrozba povodní mimo působnost zpravodajských služeb, přesto respondenti empirického výzkumu zařadili hrozbu do významné střední relevance. Byl naměřen průměr 2,91 a směrodatnou odchylkou 0,950. Je

[264] ZEMAN, Jan (2003) Povodeň 2002 v ČR – fakta, úspěchy a prohry. Dostupné z https://www.bezpecnostpotravin.cz/povoden-2002-v-cr-fakta-uspechy-a-prohry.aspx [online, cit. 2022-06-07].

zde však patrný velký názorový rozptyl, neboť jen 3,5 % dotazovaných hodnotí hrozbu jako velmi vysokou; již ale 31,6 % jako vysokou; 42,1 % jako střední; 15,8 % jako nízkou a jen 7 % jako velmi nízkou. Vysoký rozptyl v názorech respondentů zřejmě dokazuje, že se v tomto případě nejedná o názory podpořené exaktními zpravodajskými informacemi, a jde spíše o pocitové hodnocení hrozby podpořené zkušenostmi ČR z nedávných rozsáhlých povodní.

Na podobné zkušenosti s povodněmi 1997 a 2002 logicky reagují i české národní strategické dokumenty. Je zde nutné konstatovat, že ČR poučena z kolapsu IZS v 1997 udělala velký kus práce, neboť je nyní na podobné přírodní katastrofy podstatně lépe připravena. BS ČR (2015) nicméně konstatuje, že „*vláda bude zlepšovat podmínky pro … akceschopnost a efektivní spolupráci včetně posílení součinnosti s Armádou ČR a bude podporovat vybavení základních složek integrovaného záchranného systému a sborů dobrovolných hasičů za účelem jejich většího zapojení do řešení mimořádných událostí*“.[265]

ANB (2016) dělí hrozbu povodní do dvou hlavních skupin: na povodně přívalové[266], tj. způsobené přírodními vlivy a povodně zvláštní[267], tj. povodně způsobené jako následek poruchy nebo havárie.

Bezpečnostní hrozba povodní **je neintencionální hrozba s naměřenou středně vysokou mírou rizika. Hrozba není součástí klasické působnosti zpravodajských služeb, avšak i tak ji respondenti z BIS přiřadili významnou střední relevanci.** Hrozba je zařazena do skupiny faktorové skladby **hrozby energetické, surovinové, průmyslové a environmentální.**

[265] BS ČR (2015), s. 19, odst. 81. Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2022-06-08].
[266] ANB (2016) s. 76, 2/I. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-06-08].
[267] ANB (2016) s. 86, 2/I. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-06-08].

B6 KRIMINALITA SPOJENÁ S INSOLVENČNÍM ŘÍZENÍM (intencionální bezpečnostní hrozba)

Budeme – li na počátku charakterizovat insolvenční řízení, potom lze konstatovat, že je to „*druh soudního řízení, ve kterém je projednáván* **úpadek dlužníka** *a možnosti jeho řešení dle insolvenčního zákona. Insolvenční řízení může být zahájeno na základě* **podaného insolvenčního návrhu** *samotným dlužníkem nebo jeho věřitelem. … V rámci insolvenčního řízení pak soud následně rozhoduje o způsobu řešení úpadku a pokud soud nerozhodne jinak, je dlužník povinen zdržet se nakládání s majetkovou podstatou a majetkem, který do ní může náležet*“.[268]

Podle mnohých veřejně přístupných informací je kriminalita spojená s insolvenčním řízením velmi častým a důmyslným kriminálním jevem, kdy se často do tohoto druhu trestné činnosti zapojují i samotní insolvenční správci.[269] Opakovaně se jedná o sofistikovaně organizovanou trestnou činnost, proto je tento druh hrozby také součástí boje s organizovaným zločinem. Nejvyšší státní zastupitelství ve své výroční zprávě za rok 2020 mj. uvádí, že „*insolvenční řízení může být zneužíváno propracovaným způsobem a může být i nástrojem legalizace protiprávního jednání s trestněprávním přesahem.“*[270]

Z uvedeného vyplývá, že hlavní gesci při odhalování těchto trestných činů má Policie ČR, v tomto případě však i Finanční analytický úřad, ovšem s informační podporou i národních zpravodajských služeb, zejména BIS.

---

[268] Definice dostupná z https://azlegal.cz/pravni-slovnik/insolvencni-rizeni/ [online, cit. 2022-06-08].

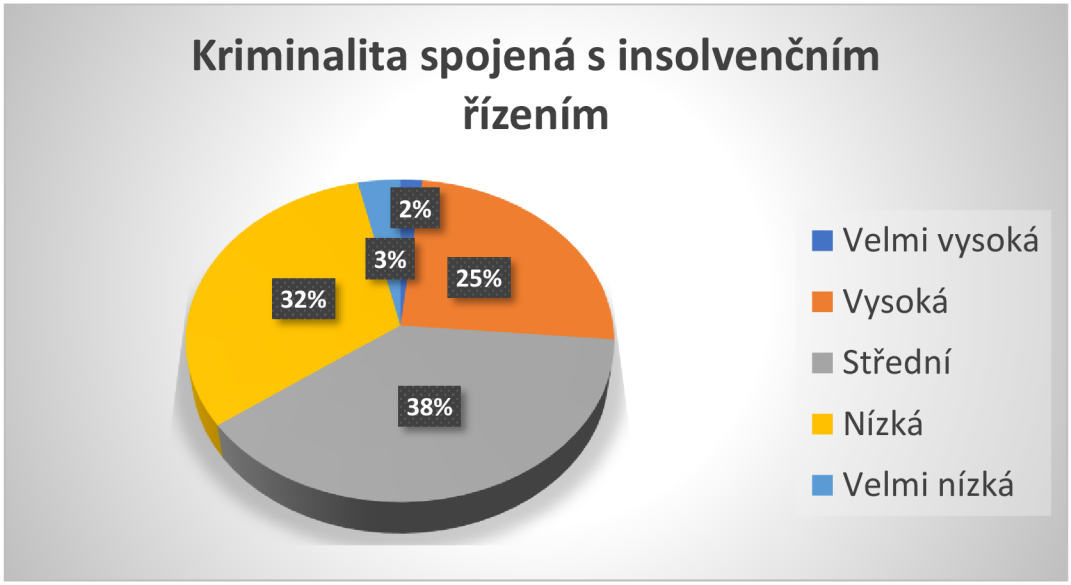
[269] GREIF, Václav (2018), Na insolvence navázaná kriminalita pokračuje, specializované orgány jsou zahlceny. Dostupné z https://www.ceska-justice.cz/2018/06/insolvence-navazana-kriminalita-pokracuje-specializovane-organy-jsou-zahlceny/ [online, cit. 2022-06-08].

[270] Zpráva o činnosti Státního zastupitelství za rok 2020 (2021), Textová část, s. 85. Dostupné z https://verejnazaloba.cz/wp-content/uploads/2021/06/Zpr%C3%A1va_o_%C4%8Dinnosti_SZ_za_rok_2020_textov%C3%A1_%C4%8D%C3%A1st.pdf [online, cit. 2022-06-08].

Tabulka č. 28 a graf č. 22 Kriminalita spojená s insolvenčním řízením

Kriminalita spojená s insolvenčním řízením

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	1	1,8	1,8	1,8
	Vysoká	14	24,6	24,6	26,3
	Střední	22	38,6	38,6	64,9
	Nízká	18	31,6	31,6	96,5
	Velmi nízká	2	3,5	3,5	100,0
	Celkem	57	100,0	100,0	



Respondenti z analytické skupiny BIS přiřadili této bezpečnostní hrozbě střední relevanci s naměřeným průměrem 3,11 a se směrodatnou odchylkou 0,880. Lze tedy konstatovat, že je zde patrný velmi vysoký názorový rozptyl, neboť sice jen 1,8 % respondentů hodnotí hrozbu jako velmi vysokou, ale již 24,6 % jako vysokou; 38,6 % jako střední; 31,6 % jako nízkou a jen 3,5 % jako velmi nízkou. Uvedené hodnoty dokazují velký názorový nesoulad, i tak získaná data opravňují zařazení hrozby do skupiny střední závažnosti. To ne zcela koresponduje se závěry SWOT analýzy učiněné ANB (2016), který navzdory konstatování nárůstu

této kriminální činnosti od roku 2014, přiřazuje hrozbě pouze nízkou hodnotu relevance. ANB (2016) rovněž konstatuje, že existuje „*možnost koluze insolvenčního soudce nebo správce s některými z účastníků řízení a následné účelové zvýhodnění těchto účastníků oproti ostatním*.“ [271]

Bezpečnostní hrozba kriminalita spojená s insolvenčním řízením **je intencionální hrozba se střední relevancí. Hrozba je součástí klasické působnosti především policejních složek. Z hlediska zpravodajských služeb je nejvíce součástí působnosti BIS, která při odhalování této nezákonné činnosti aktivně spolupracuje s PČR (NCOZ).** Hrozba je zařazena do skupiny faktorové skladby **ohrožení působnosti státu a jeho ekonomické stability.**

B7 TERORISMUS OSAMĚLÝCH VLKŮ
(intencionální bezpečnostní hrozba)

Terorismus se za poslední dekády stal v celém světě výraznou bezpečnostní hrozbou a boj proti němu je jednou z nejdůležitějších působností všech zpravodajských služeb a ostatních bezpečnostních složek státu. Toto konstatování platí bezvýhradně i v našich národních podmínkách. ČR však zatím jako jedna z mála vyspělých demokratických zemí nebyla terčem teroristického útoku velkého rozsahu. Přesto domácí bezpečnostní složky odpovědné za boj s terorismem neposuzují nebezpečí možného teroristického útoku proti ČR v logice zda „ano nebo ne“, jako spíše „kdy a kde“. S tím korespondují i závěry národních bezpečnostních dokumentů (především ABN 2016), které jednotlivým oblastem možného teroristického ohrožení českých národních zájmů přiřazují ve většině případů významnou střední míru relevance[272]. Děje se tak navzdory tomu, že je aktuální riziko teroristického útoku v ČR dlouhodobě vyhodnocováno jako

[271] ABN (2016), s. 45. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-06-08].
[272] ANB (2016), kapitola Terorismus, s. 10–17, Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-06-08].

nízké. Z rozhodnutí vlády a s ohledem na aktuální míru rizika teroristického útoku funguje v ČR čtyřstupňový sytém, který v případě potřeby aktivuje ministr vnitra.[273]

Hrozba terorismu osamělých vlků je v Evropě jednou z nejčastějších forem teroristických útoků. Z tohoto hlediska je popisovaná hrozba terorismu osamělých vlků analyzována v empirickém výzkumu v podstatě jako příklad komplexní hrozby terorismu, i když lze připustit, že se jedná jen o jeden segment tohoto bezpečnostního rizika. Formy politického terorismu mohou být velmi rozmanité, vedle nejznámějšího náboženského terorismu existují i příklady krajně levicového nebo krajně pravicového terorismu, etnického nebo enviromentálního terorismu atd.[274]

Přehlednou, jasnou a shrnující definici terorismu překládá např. profesor Ganor z Mezinárodního institutu boje s terorismem (ICT) v izraelské Herzliyi: „*Terorismus je záměrné použití násilí namířené proti civilním cílům za účelem dosažení politických cílů; nacionalistických, socioekonomických, ideologických, náboženssko-politických*.“[275] Naproti tomu definování hrozby terorismu osamělých vlků lze zúžit na výstižný popis termínu definovaném americkými badateli Hammem a Spaajem jako „*politické násilí páchané jednotlivci, kteří jednají sami; kteří nepatří k organizované teroristické skupině nebo síti; kteří jednají bez*

---

[273] **Nulový stav** je dle schváleného systému situace, při níž není známa žádná konkrétní, ani obecná hrozba teroristického či obdobného útoku na území ČR. **První stupeň** ohrožení terorismem upozorňuje na existenci obecného ohrožení terorismem, vyplývající ze situace v zahraničí a z příslušnosti České republiky k euroatlantickým strukturám i z mezinárodních aktivit České republiky, zároveň ale není známa konkrétní hrozba teroristických aktivit na území ČR. **Druhý stupeň ohrožení terorismem** upozorňuje na existenci zvýšené pravděpodobnosti ohrožení terorismem, přičemž bližší okolnosti hrozby, včetně přesnějšího načasování, nelze předpovědět. **Třetí stupeň ohrožení terorismem** zavádí vysoký stupeň bdělosti a pohotovosti, kdy je teroristický útok na český cíl (v na českém území či v zahraničí) očekáván s vysokou pravděpodobností nebo již proběhl. MV ČR. Stupně ohrožen í terorismem.
Dostupné z https://www.mvcr.cz/cthh/clanek/stupne-ohrozeni-terorismem.aspx [online, cit. 2022-06-08].

[274] MV ČR. Typologie terorismu. Dostupné z https://www.mvcr.cz/clanek/typologie-terorismu.aspx [online, cit. 2022-06-08].

[275] GANOR, Boaz (2005) The Counter-Terrorism Puzzle: A Guide for Decision Makers. New Brunswick, Transaction Publishers, s. 17.

přímého vlivu vůdce nebo hierarchie; a jejichž taktiky a metody jsou vytvořené a řízené jednotlivcem bez jakéhokoli přímého vnějšího příkazu nebo vedení."[276]

Jak již bylo řečeno ČR prozatím nebyla terčem teroristického útoku zásadního rozsahu. Na počátku devadesátých let však bylo bývalé Československo konfrontováno nevyšetřeným teroristickým útokem pravděpodobně osamělého vlka – krajně levicového aktivisty. V roce 1990 bylo na následky použití trubkové bomby zraněno na Staroměstském náměstí v Praze 18 osob.[277] Za teroristický čin byl poprvé v ČR odsouzen v roce 2017 důchodce Jaromír Balda, který plánoval iniciovat železniční neštěstí s cílem eskalovat protimuslimské nálady v české společnosti.[278] Jako příklad tzv. státního terorismu poslouží nepřátelský útok ruských zpravodajských služeb (resp. ruského státu) ve vojenských skladech ve Vrběticích z roku 2014, avšak usvědčeného až v roce 2021, který byl doprovázen úmrtím dvou nevinných obětí.[279]

Důkazem, že se v případě bezpečnostní hrozby terorismu osamělých vlků nejedná jen o planý poplach je i varování BIS, které důrazně zaznělo ve veřejné části výroční zprávy BIS za rok 2020. K tématu mimo jiné uvádí: „*velkou výzvu bude i nadále představovat nebezpečí teroristického útoku osamělého aktéra, zejména pak s přihlédnutím k zvyšující se úloze internetu při radikalizaci potenciálních útočníků a změněné bezpečnostní situaci po odchodu spojeneckých sil z Afghánistánu, která se vedle terorismu dotýká i migrace.*"[280]

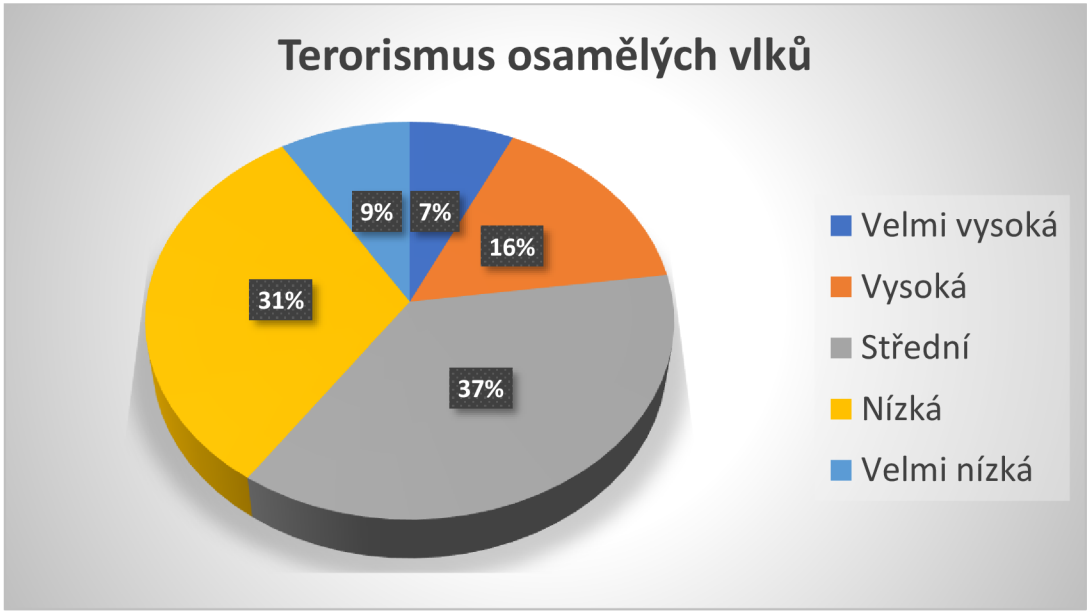
---

[276] HAMM, Mark a SPAAJ, Ramon (2015), Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies, s. 4. Dostupné z https://www.ojp.gov/pdffiles1/nij/grants/248691.pdf [online, cit. 2022-06-08].
[277] Dostupné z https://ct24.ceskatelevize.cz/specialy/30-let-zpet/3107405-30-let-zpet-vybuch-na-staromestskem-namesti [online, cit. 2022-06-08].
[278] Dostupné z https://www.seznamzpravy.cz/clanek/jsem-vlastenec-ne-terorista-jaromir-balda-je-z-vezeni-doma-a-promluvil-169016 [online, cit. 2022-06-08].
[279] Dostupné z https://www.idnes.cz/zpravy/domaci/bellingat-vrbetice-vybuch-sest-clenu-velitel-komanda-general-gru-averjanov.A210420_142835_domaci_lre [online, cit. 2022-06-08].
[280] BIS. Výroční zpráva 2020. s. 9. Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf [online, cit. 2022-06-08].

Tabulka č. 29 a graf č. 23 Terorismus osamělých vlků

Terorismus osamělých vlků

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	4	7,0	7,0	7,0
	Vysoká	9	15,8	15,8	22,8
	Střední	21	36,8	36,8	59,6
	Nízká	18	31,6	31,6	91,2
	Velmi nízká	5	8,8	8,8	100,0
	Celkem	57	100,0	100,0	



Oslovení analytici BIS hodnotí hrozbu terorismu osamělých vlků jako střední bezpečnostní hrozbu s výrazným názorovým rozptylem. Pouze 7% s dotazovaných respondentů hodnotí hrozbu jako velmi vysokou, 16% jako vysokou, 37% jako střední a 31% dokonce jako nízkou nebo v 9% jako velmi nízkou. V kontextu toho lze konstatovat, že byl naměřený průměr 3,19 se směrodatnou odchylkou 1,043, což potvrzuje výrazný názorový rozptyl respondentů.

Hodnocení hrozby ve středním pásmu relevance se víceméně shoduje se závěry učiněnými v Auditu národní bezpečnosti[281]. ANB (2016) tuto formu terorismu v domácích podmínkách spíše přiřazuje aktivitám levicových nebo pravicových extremismů, když konstatuje, že *„jako u pravicových extremistů se i u krajní levice lze obávat výskytu tzv. osamělých vlků neboli militantních radikálů, kteří se nezapojují do veřejných aktivit a čekají na vhodnou příležitost k provedení násilného aktu*“[282]. Bezpečnostní strategie ČR (2015) podrobněji otázku terorismu osamělých vlků nerozpracovává, termín pouze zmiňuje jako příklad v samostatné kapitole věnované terorismu (Lone Wolves).[283]

Bezpečnostní hrozba terorismus osamělých vlků **je intencionální hrozba se střední relevancí** (shoda empirického výzkumu se SWOT analýzou ANB 2016)**. Hrozba je součástí působnosti všech bezpečnostních složek v čele se zpravodajskými službami a PČR. Z hlediska zpravodajských je tato hrozba v domácích podmínkách součástí působnosti především BIS, ale svou významnou úlohu zde plní i zbylé zpravodajské složky.** Hrozba je zařazena do skupiny faktorové skladby **hrozby spojené s hrozbami migrace a terorismu.**

B8 NARUŠENÍ DODÁVEK PLYNU VELKÉHO ROZSAHU
B9 NARUŠENÍ DODÁVEK PITNÉ VODY VELKÉHO ROZSAHU
B10 NARUŠENÍ DODÁVEK ELEKTRICKÉ ENERGIE VELKÉHO ROZAHU
B11 NARUŠENÍ DODÁVEK ROPY VELKÉHO ROZSAHU
(intencionální bezpečnostní hrozby)

Celkem čtyři významné energetické hrozby byly hodnoceny respondenty empirického výzkumu v posloupnosti, což umožňuje vyhodnotit tyto závěry

[281] ANB (2016), s. 12. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-07-12].
[282] ANB (2016) s. 30. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf
[283] BS ČR (2015), s. 11. Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2022-07-12].

komplexně. Jedná se o hrozby narušení dodávek velkého rozsahu **plynu, vody, elektrické energie a ropy.** V úvodu je však nutné konstatovat, že se přinejmenším v některých komoditách (především plyn a ropa) situace od doby realizace výzkumu k dnešku zásadně změnila. Ruská válka proti Ukrajině nezasáhla jenom tuto napadenou zemi, ale v podstatě bezprecedentním způsobem rozkolísala všechny trhy světa a zpochybnila všechny dosavadní modely víceméně bezproblémových dodávek energií z východu do Evropy. Situace nutí evropské vlády zásadním způsobem přehodnocovat své energetické strategie, a dokonce dočasně rezignovat i na využívání zdrojů, které byly označeny na překonané a ohrožující životní prostředí planety. Nejzásadnějším jevem současnosti je v první řadě reálné nebezpečí zastavení dodávek ruského plynu a možná i dalších komodit do Evropy. Tato realita ovlivňuje celkovou ekonomiku všech evropských států, ale i sociální stabilitu celého světa.

Navzdory řečenému lze však konstatovat, že tyto hrozby byly vnímány jako velký bezpečnostní problém dlouhou dobu před vypuknutím války na Ukrajině, i když ne s takovou intenzitou, jak situaci hodnotíme dnes. Všechny české strategické dokumenty na tyto okolnosti důrazně reagují. Tato oblast je však příkladem jistého rozporu v závěrech učiněnými bezpečnostními složkami a některých reakcí politických vlád. Energetika a s tím spojené dodávky surovin má důležitou strategickou povahu a dopad na kvalitu života všech obyvatel. Proto ne všechny vlády včas dbají varování bezpečnostních složek a v některých přepadech rozhodují ve prospěch ekonomických, resp. rozpočtových dopadů na úkor bezpečnostních faktorů.

Výše uvedené čtyři strategické komodity (plyn, voda, elektrické energie a ropa) lze obecně rozdělit na dvou skupin. V první skupině jsou komodity plyn, ropa a částečně elektrická energie, tj. zdroje, které ČR dováží a jejich dovoz je závislý na mnohých faktorech a okolnostech (politických, ekonomických, technických, technologických atd.). Bezproblémový dovoz těchto komodit je často mimo kompletní vliv ČR. Vláda ČR je v dodávkách energetických surovin plně závislá na zahraničních zdrojích a na dalších různých faktorech a v mnoha ohledech není schopna sama aktivně situaci usměrňovat. Existuje však jedna oblast, kde lze

z pozice české vlády aktivně konat. Je to důležitá snaha o diverzifikaci dodávek strategických surovin z různých zdrojů s cílem nebýt plně závislý na jediném dodavateli (jedné zemi). Tato politika však v ČR nebyla vždy uspokojivě řešena. Pokud se v oblasti dovozu ropy podařila diverzifikace dodávek např. realizací ropovodu Ingolstadt, díky čemuž není ČR plně závislá na ruských zdrojích (i tak dováží ČR z Ruska téměř 50% všech zásob ropy[284]), potom situace v dovozu plynu je značně komplikovanější. V roce 2017 nebyly prodlouženy dřívější kontrakty na dodávky norského plynu, proto veškerý plynový import byl zaměřen jen na dodávky plynu z Ruska. ČR je kvůli této skutečnosti v oblasti dovozu plynu jednou z nejzávislejších zemí EU na ruských dodávkách. Tato závislost je téměř 100%.[285] Tím se ČR, stejně jako některé další evropské státy, dostala do nebezpečně krizové situace, jejíž následné řešení si vyžádá nejen značné úsilí a vysoké náklady, ale i velké oběti nejen ze strany státu, ale i všech jeho občanů.

V oblasti dodávek elektrické energie je situace v ČR také poněkud komplikovaná. ČR elektrickou energii dováží, ale je i jejím významným vývozcem. Elektrická energie se však v ČR vyrábí z různých zdrojů, tedy i dováženého plynu. Např. v roce 2021 ČR vyrobila 33,6% elektřiny z jaderných zdrojů, 32,2% z hnědého uhlí, 11,1% z plynu, 5% ze solárních zdrojů[286] atd. Tento výrobní mix má pochopitelně zásadní vliv i na konečnou cenu prodávané elektrické energie a tím na celkový stav ekonomické situace v ČR.

Druhá skupina zahrnuje poslední zbylou komoditu, tj. vodu. Případné narušení dodávek pitné vody velkého rozsahu je v českém prostředí spojováno především s domácí produkcí, která je jednak ovlivňována enviromentálními vlivy, ale i celou další řadou možných ohrožení (viz kapitola dlouhodobé sucho). Vedle nebezpečí možných teroristických útoků zásobárnám vody, jakož i proti celé

---

[284] Český statistický úřad, dostupné z https://www.czso.cz/documents/10180/20562265/8105110503.pdf/feb15a14-1b43-4465-a9b0-4a6987428754?version=1.0 [online, cit. 2022-07-13].
[285] ONERGETICE.CZ. Na ruském plynu jsou v EU nejvíc závislé Česká republika a Lotyšsko. Dostupné z https://oenergetice.cz/plynarenstvi/na-ruskem-plynu-jsou-v-eu-nejvic-zavisle-ceska-republika-a-lotyssko. [online, cit. 2022-07-13].
[286] ONERGETICE.CZ. Více než třetina elektřiny vyrobené v Česku pochází i v létě stále z uhlí. Dostupné z https://oenergetice.cz/energetika-v-cr/vice-nez-tretina-elektriny-vyrobene-v-cesku-pochazi-i-v-lete-stale-z-uhli

kritické infrastruktuře státu, jsou v případě vody dalšími riziky především nejrůznější poruchy, havárie, ale i další nepředvídatelné události jako jsou přírodní pohromy atd.

Audit národní bezpečnosti (2016) věnuje problematice zajištění dodávek strategických energetických surovin značnou pozornost. V otázkách možného narušení dodávek plynu velkého rozsahu mj. konstatuje, že „*nejpravděpodobnější příčinou výpadku dodávek plynu jsou přírodní pohromy, technologické havárie, terorismus nebo obchodně-politické spory*“[287]. Stejně jako v otázkách dodávek plynu kritizuje ANB (2016) i jednostrannou závislost na jednom ruském dodavateli ropy. ANB (2016) celkem vizionářsky prorokuje, že „*závislost vytváří riziko vzniku situace, kdy dojde k přerušení dodávek ropy do ČR. Přerušení může být krátkodobé či dlouhodobé*“[288].

Bezpečnostní strategie ČR (2015) rovněž velmi přesně předvídá možné důsledky narušení dodávek strategických energetických surovin a mnoho let před vypuknutím ruské války na Ukrajině upozorňuje na některé výrazné trendy, které se nakonec staly realitou. Jde např. o varování možného přerušení dodávek strategických surovin, ale i o varování, že *„zneužívání pozice výhradního dodavatele těchto surovin či tranzitní země k prosazení vlastních politických a bezpečnostních zájmů má dopad i na zajištění základních potřeb ČR a jejích spojenců, ohrožuje politickou soudržnost NATO a EU a lze jej označit za asymetrickou hrozbu strategické povahy…“*[289]

Otázky energetické bezpečnosti jako důležité strategické oblasti při zajištění národní bezpečnosti jsou jednou z důležitých priorit v působnosti i českých zpravodajských služeb. Vedle aktivit namířených proti možným teroristickým útokům nebo záškodnickým aktivitám proti kritickým energetickým

[287] ANB (2016), s. 114. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-07-12].
[288] ANB (2016) s. 117. Dostupné z Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-07-12].
[289] BS ČR (2015), s. 9. Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2022-07-13].

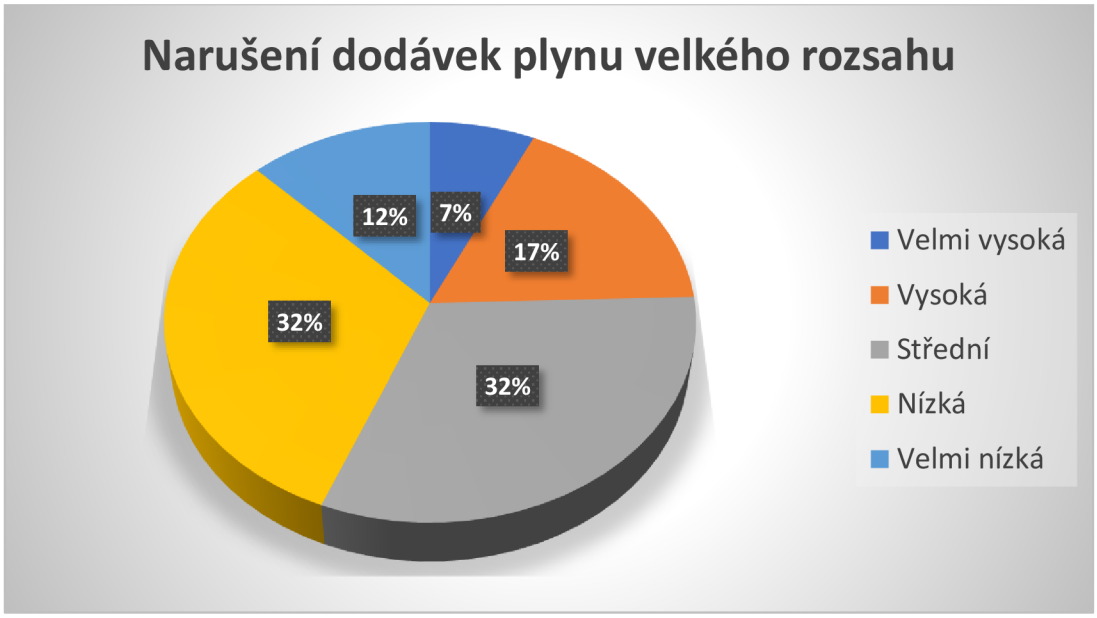
cílům jde především o dlouhodobou analýzu možných trendů, které mají za cíl včas upozornit na možná rizika a hrozby. Zpravodajské služby se zahraniční působností získávají, vyhodnocují a analyzují všechny nezbytné informace důležité v procesu předvídání možných problémů. Služby s vnitřní působností pak reagují na skutečnosti, která mají především domácí původ. BIS ve veřejné části své výroční zprávy za rok 2019 sice akcentuje především zajištění bezpečnosti v oblasti jaderné energetiky (s důrazem na ochranu klíčových jaderných tendrů před možnou problematickou účastí některých autoritativních mocností), zároveň však přiznává realizaci různých bezpečnostních projektů, které jsou často zaměřeny i na oblast energetiky.[290]

Tabulka č. 30 a graf č. 24 Narušení dodávek plynu velkého rozsahu

Narušení dodávek plynu velkého rozsahu

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	4	7,0	7,0	7,0
	Vysoká	10	17,5	17,5	24,6
	Střední	18	31,6	31,6	56,1
	Nízká	18	31,6	31,6	87,7
	Velmi nízká	7	12,3	12,3	100,0
	Celkem	57	100,0	100,0	

[290] Výroční zpráva BIS za rok 2019. Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf [online, cit. 2022-07-13].



Možné narušení dodávek plynu velkého rozsahu hodnotí respondenti empirického průzkumu v pásmu střední relevance hrozby s velkým názorovým rozptylem. U této hrozby byl naměřený průměr 3,25 a směrodatná odchylka 1,106. Tento výsledek prezentuje ne zcela jednotný názor, neboť pouze 7% dotázaných hodnotí hrozbu jako velmi vysokou, 17 % jako vysokou, 32 % jako střední, 32 % jako nízkou a 12 % jako velmi nízkou. Je zřejmé, že by v současné době byly pravděpodobně tyto hodnoty jiné, avšak prezentovaný výsledek se odráží v aktuální době, kdy byl průzkum realizován. Ostatně výsledek střední relevance je shodný i se závěry ANB (2016). V roce 2016 však ABN ještě konstatuje, že ČR diverzifikuje dodávku plynu a konstatuje, že *„63,44% plynu dodávaného do ČR pochází z Ruska, 2,95% z Norského království a 33,59% z EU“*[291] V roce 2022 je však ČR již závislá na ruských dodávkách téměř ze 100 %.

Bezpečnostní hrozba narušení dodávek plynu velkého rozsahu **je intencionální hrozba se střední relevancí. Hrozba je součástí působnosti všech zpravodajských služeb ČR, případně i některých policejních složek. Vedle odhalování případných teroristických útoků proti kritické infrastruktuře v oblasti energetiky se zde především jedná o sběr a analýzu**

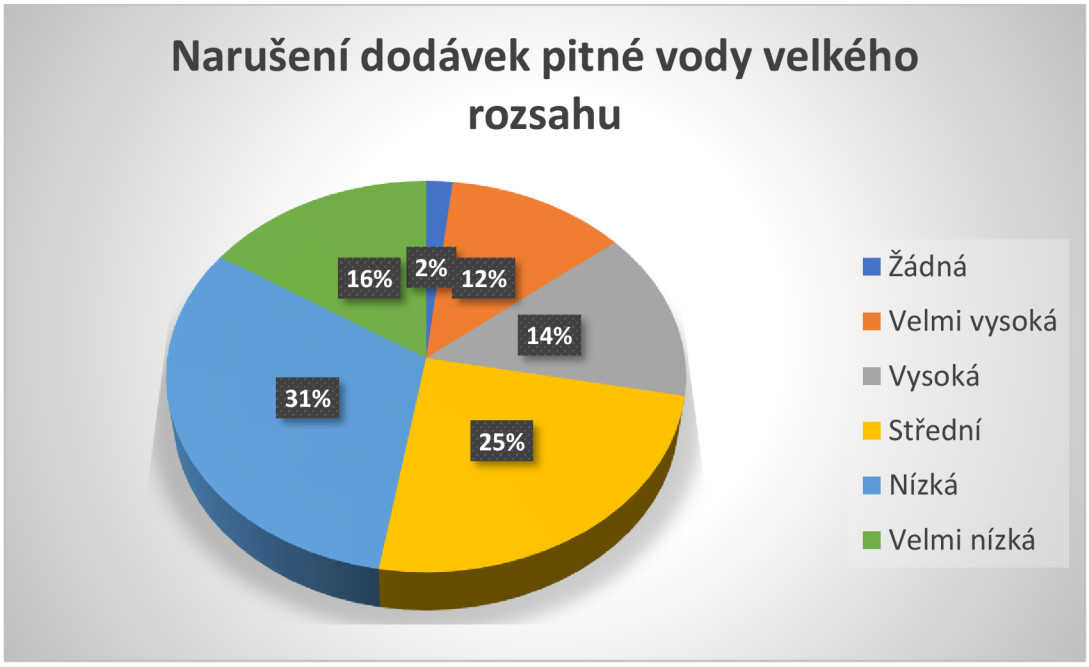
[291] ANB (2016), s. 115. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-07-20].

informací předvídající potencionální problémy s dodávkami této strategické komodity. Hrozba je zařazena do skupiny faktorové skladby **hrozby energetické, surovinové, průmyslové a environmentální.**

Tabulka č. 31 a graf č. 25 Narušení dodávek pitné vody velkého rozsahu

Narušení dodávek pitné vody velkého rozsahu

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Žádná	1	1,8	1,8	1,8
	Velmi vysoká	7	12,3	12,3	14,0
	Vysoká	8	14,0	14,0	28,1
	Střední	14	24,6	24,6	52,6
	Nízká	18	31,6	31,6	84,2
	Velmi nízká	9	15,8	15,8	100,0
	Celkem	57	100,0	100,0	



Hodnocení respondentů v případě narušení dodávek pitné vody velkého rozsahu vykazuje velmi vysoký názorový rozptyl, i když celkově lze hrozbu zařadit do střední relevance. Tato hrozba má průměr 3,25 a směrodatnou odchylku 1,254. Takto vysoký názorový rozptyl je pravděpodobně důsledkem skutečnosti, že se

jedná o hrozbu, která není v přímé, resp. každodenní gesci analytiků BIS, i když je součástí skupiny kriticky významných komodit. Jako velmi vysokou hrozbu ji hodnotí pouze 12 % respondentů, 2 % dokonce jako žádnou, 25 % jako střední, 31 % jako nízkou a 16% jako velmi nízkou. ANB (2016) ve své analýze predikuje možné narušení dodávek pitné vody z důvodu mimořádných a krizových situací, ale připouští i možnost úmyslného narušení systému dodávek pitné vody.[292]

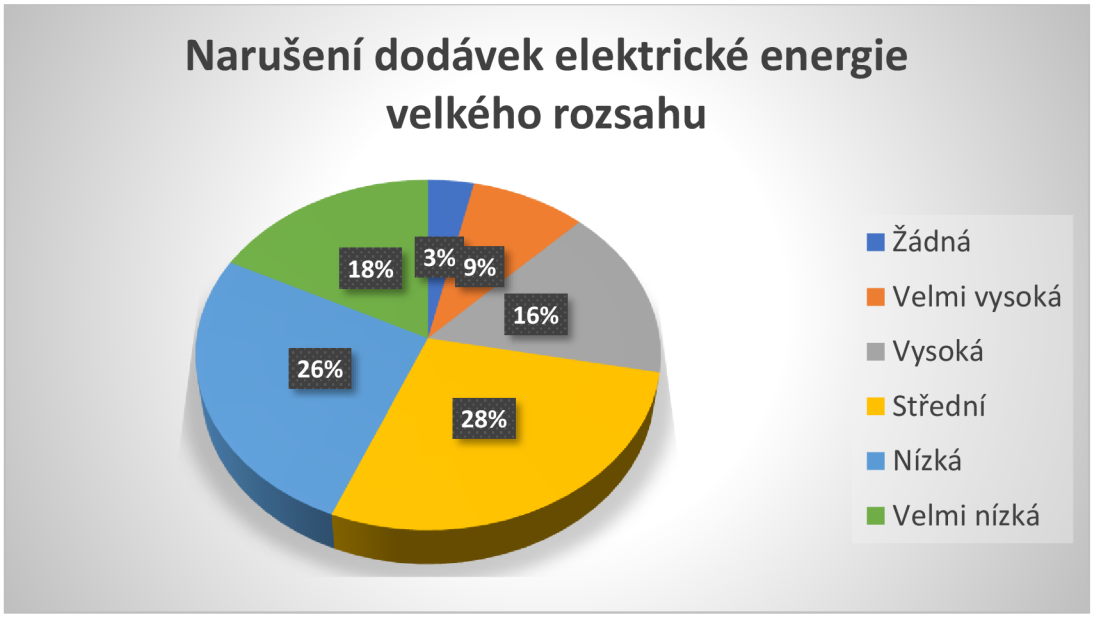
Bezpečnostní hrozba narušení dodávek pitné vody velkého rozsahu **je intencionální hrozba se střední relevancí. Hrozba není typickou součástí působnosti všech zpravodajských služeb ČR, případně i některých policejních složek. Bezpečnotsní složky včetně zpravodajských služeb působí proti této hrozbě především v situacích, kdy mě mělo dojít nebo již došlo k úmyslnému narušení těchto dodávek.** Hrozba je zařazena do skupiny faktorové skladby **hrozby energetické, surovinové, průmyslové a environmentální.**

Tabulka č. 32 a graf č. 26 Narušení dodávek elektrické energie velkého rozsahu

Narušení dodávek elektrické energie velkého rozsahu

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Žádná	2	3,5	3,5	3,5
	Velmi vysoká	5	8,8	8,8	12,3
	Vysoká	9	15,8	15,8	28,1
	Střední	16	28,1	28,1	56,1
	Nízká	15	26,3	26,3	82,5
	Velmi nízká	10	17,5	17,5	100,0
	Celkem	57	100,0	100,0	

[292] ANB (2016) s. 88. Dostupné z z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-07-20].



Potencionální narušení dodávek elektrické energie velkého rozsahu hodnotí analytici BIS nejednoznačně, neboť byl i v tomto případě zjištěný výrazný názorový rozptyl s průměrem 3,29 a směrodatnou odchylkou 1,212. Pouze 9 % respondentů hodnotí hrozbu jako velmi vysokou, 16 % jako vysokou, 28% jako střední, 26 % jako nízkou, 18 % jako velmi nízkou a dokonce 3 % jako žádnou. Tyto výsledky víceméně akcentují jen určitý výsek aktivit zpravodajských služeb v této oblasti, které se spíše zaměřují na případnou eliminaci hrozeb možného napadení kritické infrastruktury, ale i na nezastupitelnou lustraci zahraničních kandidátů na vstup do české energetické soustavy. Dalším příkladem náplně bezpečnostních složek je eliminace klasických kriminálních aktivit, které nejrůznějšími způsoby (korupce, uplácení, zpronevěra atd.) mohou ohrožovat bezproblémový chod české energetické soustavy, včetně výroby elektrické energie. Podle Státní energetické koncepce[293] z roku 2015, která by měla být v příštích letech zásadně aktualizována, je cílem soběstačnost v dodávkách elektřiny ve výši 90%.[294]

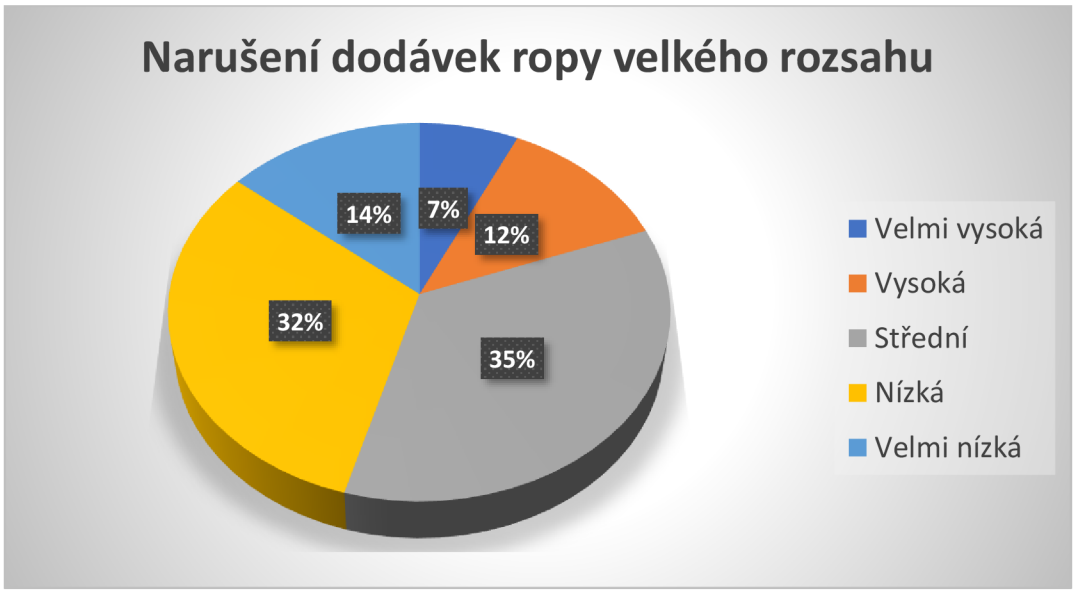
[293] Dostupné z https://www.mpo.cz/assets/cz/energetika/statni-energeticka-politika/2016/12/Statni-energeticka-koncepce-_2015_.pdf [online, cit. 2022-07-20].
[294] Státní energetická koncepce (2015), s. 35. Dostupné z https://www.mpo.cz/assets/cz/energetika/statni-energeticka-politika/2016/12/Statni-energeticka-koncepce-_2015_.pdf [online, cit. 2022-07-20].

Bezpečnostní hrozba narušení dodávek elektrické energie velkého rozsahu **je intencionální hrozba se střední relevancí. Hrozba není typickou součástí působnosti zpravodajských služeb ČR. V případě gesce bezpečnostních složek je akcent kladen na situace, kdy mě mohlo dojít nebo již došlo k úmyslnému narušení těchto dodávek, resp. kritické infrastruktury.** Hrozba je zařazena do skupiny faktorové skladby **hrozby energetické, surovinové, průmyslové a environmentální.**

Tabulka č. 33 a graf č. 27 Narušení dodávek elektrické energie velkého rozsahu

Narušení dodávek ropy velikého rozsahu

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	4	7,0	7,0	7,0
	Vysoká	7	12,3	12,3	19,3
	Střední	20	35,1	35,1	54,4
	Nízká	18	31,6	31,6	86,0
	Velmi nízká	8	14,0	14,0	100,0
	Celkem	57	100,0	100,0	



Potencionální narušení dodávek ropy velkého rozsahu hodnotí respondenti ve středním pásmu relevance s relativně pestrým názorových rozptylem. Empirickým výzkumem byl naměřený průměr 3,33 a směrodatná odchylka 1,091.

Jako velmi vysokou relevanci hrozbu hodnotilo 7 % dotazovaných, jako vysokou 12 %, jako střední 35 %, jako nízkou 32 % a jako velmi nízkou 14% respondentů. Větší optimismus je zde dán podstatně kvalitnější diverzifikací dodávek ropy do ČR, neboť země není na těchto dodávkách tak závislá jako je tomu například v případě plynu. I tak však aktuální závislost ČR na dodávkách z Ruska vykazuje téměř 50 %. Tyto hodnoty se však v budoucnosti mohou měnit v souvislosti s ruskou válkou proti Ukrajině.

Bezpečnostní hrozba narušení dodávek ropy velkého rozsahu **je intencionální hrozba se střední relevancí. Hrozba není typickou součástí působnosti zpravodajských služeb ČR, i když je zde kladen důraz na situace, kdy by mohlo dojít nebo již došlo k úmyslnému narušení těchto dodávek. Zpravodajské služby však analyzují všechna rizika spojená s dodávkami strategických komodit v oblasti energetické bezpečnosti.** Hrozba je zařazena do skupiny faktorové skladby **hrozby energetické, surovinové, průmyslové a environmentální.**

B12 SUROVINOVÁ BEZPEČNOST
B13 PRŮMYSLOVÁ BEZPEČNOST
(intencionální bezpečnostní hrozby)

Surovinová a průmyslová bezpečnost a hrozby s tím spojené jsou v jisté symbióze, neboť dodávky strategických, kritických i jinak důležitých surovin zásadním způsobem ovlivňují bezproblémový chod a světovou konkurenceschopnost českého průmyslového sektoru. Česká republika patří již od Rakouska – Uherska k nejvíce průmyslovým zemím v Evropě, což má dnes své pozitivní i stinné stránky. V ČR je kladným rysem tohoto stavu například nízká nezaměstnanost, avšak se zápornými důsledky jako jsou v porovnání s vyspělými evropskými zeměmi nižší mzdy. ČR je v rámci EU společně s Irskem nejvíce průmyslovou zemí Unie, což klade značný důraz i na otázky spojené se surovinovou a průmyslovou bezpečností. I tyto bezproblémové dodávky jsou nezbytností pro zajištění práce velké části národní populace. Podle ČSÚ z roku

2019 procovalo v českém průmyslu 1,3 miliónů lidí, přičemž nejvíce tak bylo ve zpracovatelském průmyslu a v jeho rámci především v automobilovém odvětví.[295]

ČR je součástí zemí rozvíjejících tzv. Průmysl 4.0, který je spojený s vyšším nasazením digitalizace a automatizace výroby. Tyto trendy s sebou nesou nasazení nejmodernějších technologií, které s příchodem superrychlých počítačových sítí a umělé inteligence předznamenávají revoluční změny. Jednotlivé elementy tohoto procesu jsou cílem nelegálního získávání informací ze strany cizích mocností. ČR je v otázce dodávek surovin částečně soběstačná, částečně tyto suroviny dováží a také je získává formou recyklace z jiných již použitých materiálů.[296] Podle vládní surovinové strategie *Surovinová politika ČR v oblasti nerostných surovin a jejich zdrojů* z roku 2019 s výhledem na příštích 15 let byl stanoven mj. cíl udržet přijatelnou míru dovozní závislosti těchto komodit, a především klást důraz na vyšší diverzifikaci těchto dodávek z více zdrojů.[297] ČR má díky nedostatku vlastních zdrojů např. totální závislost na dovozu železné rudy, kterou dováží především z Ruska a stále více i z Ukrajiny.[298] Rusko – ukrajinská válka je jedním z hmatatelných příkladů problematičnosti dovozu těchto komodit z jednoho, dvou zdrojů a slouží jako příklad pro urychlení nalezení nových dodavatelů ze stabilnějších oblastí a především s akcentem na potřebnou diverzifikaci těchto dodávek.

Oblast nových technologií, vědeckých výzkumů, výrobních postupů a vynálezů atd. je předmětem zájmu cizích států, které prostřednictvím průmyslové špionáže kradou strategicky důležité informace. Na tuto tendenci upozorňuje i

---

[295] ČSÚ (2019). Dostupné z https://www.czso.cz/csu/czso/v-prumyslu-pracuje-13-milionu-osob [online, cit. 2022-07-25].
[296] MPO (2017) Surovinová politika ČR v oblasti nerostných surovin a jejich zdrojů, s. 5. Dostupné z https://www.mpo.cz/cz/stavebnictvi-a-suroviny/surovinova-politika/statni-surovinova-politika-nerostne-suroviny-v-cr/nova-surovinova-politika-v-oblasti-nerostnych-surovin-a-jejich-zdroju---mpo-2017--229820/ [online, cit. 2022-07-25].
[297] MPO (2017) Surovinová politika ČR v oblasti nerostných surovin a jejich zdrojů, s. 10. Dostupné z https://www.mpo.cz/cz/stavebnictvi-a-suroviny/surovinova-politika/statni-surovinova-politika-nerostne-suroviny-v-cr/nova-surovinova-politika-v-oblasti-nerostnych-surovin-a-jejich-zdroju---mpo-2017--229820/ [online, cit. 2022-07-25].
[298] MPO (2017) Surovinová politika ČR v oblasti nerostných surovin a jejich zdrojů, s. 42. Dostupné z https://www.mpo.cz/cz/stavebnictvi-a-suroviny/surovinova-politika/statni-surovinova-politika-nerostne-suroviny-v-cr/nova-surovinova-politika-v-oblasti-nerostnych-surovin-a-jejich-zdroju---mpo-2017--229820/ [online, cit. 2022-07-25].

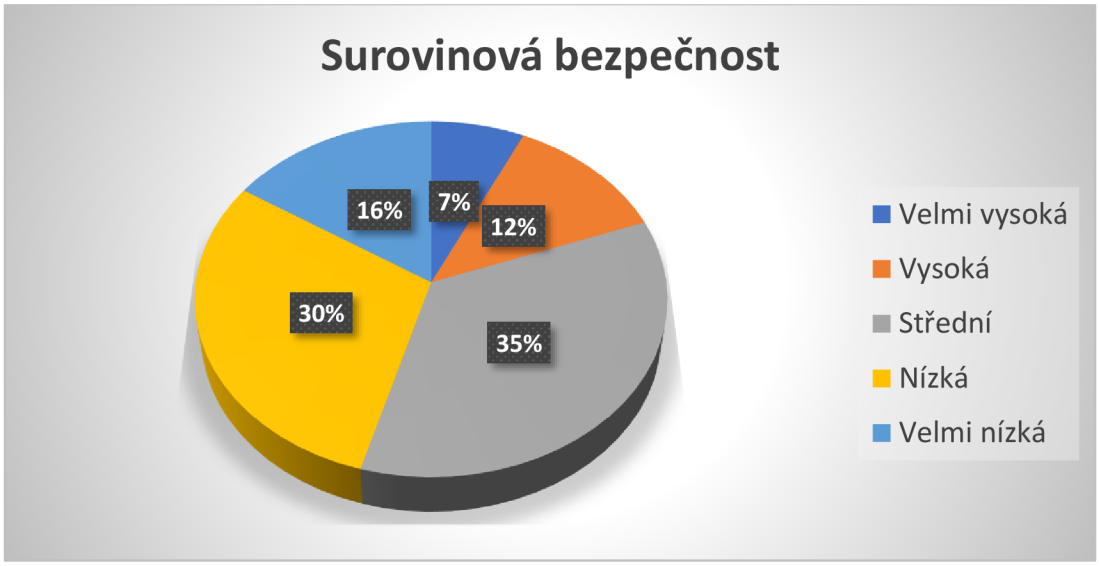
ANB (2016), který mj. konstatuje, že „*významné riziko pro český průmysl pak mohou představovat vlivové a infiltrační operace zpravodajských služeb cizí moci namířené proti strategickým hospodářským zájmům ČR, průmyslová a vědecko-technická špionáž. V případě státem vlastněných či spoluvlastněných společností se obrana proti takovému jednání odvíjí především od náležitého výkonu jeho vlastnických práv.“*[299] Konkrétní rizika spojená s průmyslovou špionáží připouští např. i veřejná část výroční zprávy BIS za rok 2019, která tyto trendy spojuje především s aktivitami čínských zpravodajských služeb.[300] BIS hovoří rovněž o spolupráci s NBÚ v oblasti zajišťování průmyslové bezpečnosti státu.[301]

Tabulka č. 34 a graf č. 28 Surovinová bezpečnost

Surovinová bezpečnost

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Velmi vysoká	4	7,0	7,0	7,0
	Vysoká	7	12,3	12,3	19,3
	Střední	20	35,1	35,1	54,4
	Nízká	17	29,8	29,8	84,2
	Velmi nízká	9	15,8	15,8	100,0
	Celkem	57	100,0	100,0	

[299] ANB (2016), s. 123. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-07-25].
[300] Výroční zpráva BIS za rok 2019, s. 10. Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf [online, cit. 2022-07-25].
[301] Výroční zpráva BIS za rok 2019, s. 17. Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf [online, cit. 2022-07-25].



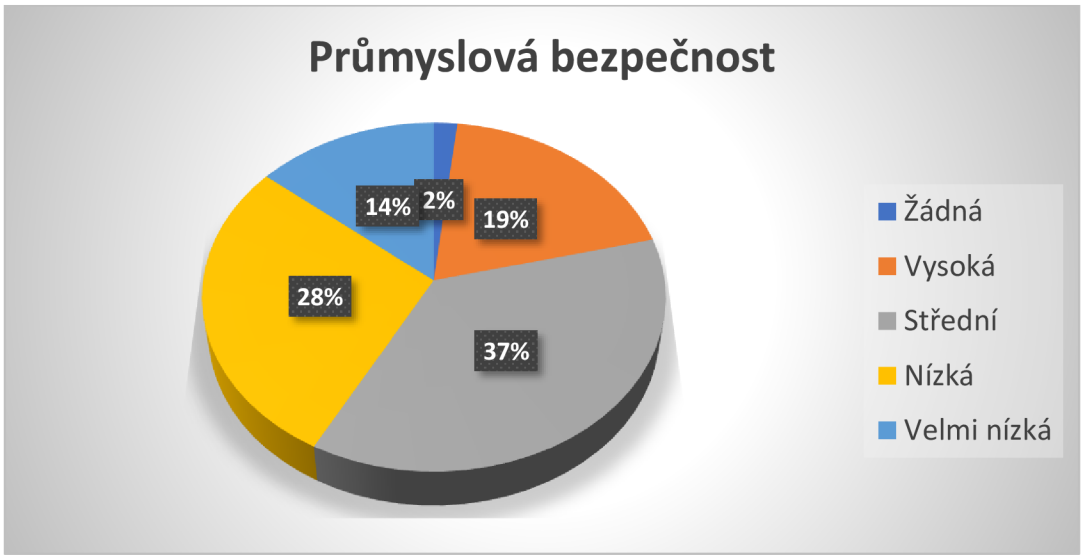
Respondenti empirického výzkumu přisoudili otázkám spojených s možnými hrozbami v oblasti surovinové bezpečnosti střední míru relevance s relativně velmi vysokým názorovým rozptylem. Výzkum naměřil průměr 3,35 a směrodatnou odchylku 1,110. Pouze 7 % dotazovaných přiřazuje hrozbě velmi vysokou relevanci, 12 % vysokou, 35 % střední, 30 % nízkou a 16 % velmi nízkou.

Bezpečnostní hrozba surovinová bezpečnost **je intencionální hrozba se střední mírou relevance. Hrozba je součástí působnosti zpravodajských služeb ČR a je zde kladen důraz na situace, kdy by mohlo dojít nebo již došlo k úmyslnému narušení těchto dodávek, včetně analýzy s tím souvisejících tendencí.** Hrozba je zařazena do skupiny faktorové skladby **hrozby energetické, surovinové, průmyslové a environmentální.**

Tabulka č. 35 a graf č. 29 Průmyslová bezpečnost

Průmyslová bezpečnost

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Žádná	1	1,8	1,8	1,8
	Vysoká	11	19,3	19,3	21,1
	Střední	21	36,8	36,8	57,9
	Nízká	16	28,1	28,1	86,0
	Velmi nízká	8	14,0	14,0	100,0
	Celkem	57	100,0	100,0	



Respondenti z analytického úseku BIS přiřadili hrozbám spojených s průmyslovou bezpečností ČR střední míru relevance opět s naměřeným vysokým názorovým rozptylem. Průměr byl naměřený hodnotou 3,38 se směrodatnou odchylkou 0,964. Celkem 19 % respondentů spatřuje v hrozbě vysokou relevanci, 37 % střední, 28% nízkou, 14 % velmi nízkou a 2 % žádnou. Vyšší počet respondentů spatřující v hrozbě vysokou nebo střední relevanci lze vysvětlit již odhalenými pokusy především čínských zpravodajských složek tradičně velmi aktivních především v oblasti průmyslové špionáže ve vyspělých zemích světa, včetně ČR.

Bezpečnostní hrozba průmyslová bezpečnost **je intencionální hrozba se střední mírou relevance. Hrozba je součástí působnosti všech**

zpravodajských služeb ČR, přičemž v domácích podmínkách především v gesci BIS. Průmyslová špionáž je tradiční aktivitou a cílem některých světově významných velmocí, které zvyšují technický a technologický potenciál svých zemí právě těmito nelegálními špionážními aktivitami. Hrozba je zařazena do skupiny faktorové skladby **hrozby energetické, surovinové, průmyslové a environmentální.**

B14 ISLÁMSKÝ RADIKALISMUS
(intencionální bezpečnostní hrozba)

Dr. Said Hassan z Sultan Qaboos University v Ománu popisuje islámský radikalismus nebo radikální islám jako „*historické, socioekonomické, politické a kulturní hnutí, které vnímá islám jako komplexní náboženství, revoluční politickou ideologii a stát. Znamená to postoj mysli přizpůsobující jednání, jehož cílem je z jakéhokoli důvodu násilně podkopat a transformovat status quo nebo řád nevíry a nespravedlnosti na utopický stav víry (iman) a rovnosti.“*[302] Jedná se o výborně popsaný mediálně často skloňovaný výraz, který se po desetiletí objevuje i v západním politickém diskursu. Situace v ČR je však poněkud odlišná. ČR prozatím není cílovou destinací radikálně orientovaných muslimů, tzn., že tento element prozatím nezpůsobuje zásadní hrozbu české národní bezpečnosti. Podle Daniela Topinky, editora sborníku „Muslimové v Česku“, je naopak česká muslimská komunita (podle některých odhadů cca 21 tisíc osob) mnohotvárná a etnicky pestrá[303] a nevykazuje nebezpečné prvky radikalismu. Zkušenosti ČR s muslimskou komunitou jsou tak zásadně odlišné od negativních zkušeností mnohých evropských západních zemí, která mají bohatější zkušenosti s podstatně větší a často i radikálnější muslimskou komunitou . Dá se v podstatě konstatovat, že v ČR je prozatím hrozba islámského radikalismu spíše potencionálním nebezpečím. Toto tvrzení podporuje i jeden ze závěrů ANB

[302] HASSAN SAID Gubara (2015), Radical Islam/ Islamic Radicalism: Towards a Theoretical Framing, Canadian Journal of Sociology. Dostupné z https://www.researchgate.net/publication/266030514_Radical_Islam_Islamic_Radicalism_Towards_a_Theoretical_Framing [online, cit. 2022-07-25].
[303] TOPINKA Daniel (Ed.) (2016). Muslimové v Česku. Etablování muslimů a islámu na veřejnosti. Brno, Barrister a Principal, 472 s.

(2016), že je „*relevance a struktura této hrozby v jednotlivých regionech i státech odlišná – západní Evropa je např. radikálním islamismem ohrožena z historických i demografických důvodů daleko více než Evropa střední*.“[304]

Ve stejném duchu mluví i BIS, která ve veřejná části výroční zprávy za rok 2020 mj. konstatuje: „*…navzdory vyššímu počtu úspěšných útoků v Evropě zůstala míra ohrožení nábožensky motivovaným terorismem v ČR na nízké úrovni. BIS sice zaznamenala známky příklonu k radikálnímu výkladu islámu u několika jednotlivců původem zejména ze severní Afriky, kteří měli různě silnou vazbu na ČR (pobytový status, dočasný tranzit v rámci svého pohybu po Evropě), ale bezprostřední ohrožení bezpečnosti dle poznatků BIS nehrozilo*“.[305] Tato víceméně optimistická konstatování však neznamenají, že by problematika islámského radikalismu, jako zdroje nábožensky motivovaného terorismu ve světě, stála na okraji zájmu českých zpravodajských služeb. Navzdory aktuálně klidnému stavu je povinností zpravodajských služeb s těmito hrozbami počítat, předvídat se, analyzovat a včas eliminovat.

Tabulka č. 36 a graf č. 30 Islámský radikalismus

Islámský radikalismus

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Žádná	2	3,5	3,5	3,5
	Velmi vysoká	2	3,5	3,5	7,0
	Vysoká	6	10,5	10,5	17,5
	Střední	18	31,6	31,6	49,1
	Nízká	18	31,6	31,6	80,7
	Velmi nízká	11	19,3	19,3	100,0
	Celkem	57	100,0	100,0	

[304] ANB (2016), s. 10. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-07-25].
[305] Výroční zpráva BIS (2020), s. 22. Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf [online, cit. 2022-07-25].

Bezpečnostní hrozba islámského radikalismu je hodnocena respondenty průzkumu ve střední relevanci s relativně velkým názorovým rozptylem. Tento výsledek nekoresponduje se závěry učiněné ANB (2016), který hrozbu islámského radikalismu vnímá jako nízkou.[306] Byl zjištěn průměr 3,55 se směrodatnou odchylkou 1,051. Stejný počet respondentů (shodně 3 %) se domnívá, že islámský radikalismus není žádnou hrozbou, jakož i velmi vysokou hrozbou, 11 % hrozbu vnímá jako vysokou, 32 % jako střední, shodně 32 % jako nízkou a 19 % jako velmi nízkou. Tento výsledek víceméně ilustruje aktuální stav, kdy české zpravodajské služby nevnímají hrozbu jako kriticky aktuální, avšak v potencionální rovině se jedná o možné vysoké riziko.

Bezpečnostní hrozba islámský radikalismus **je intencionální hrozba se střední mírou relevance.** ANB (2016) však hrozbě přiřazuje nízkou relevanci. **Hrozba je součástí působnosti všech zpravodajských služeb ČR, neboť je úzce spjata s hrozbami mezinárodního islámského terorismu, který sice není aktuálně v ČR přítomný, ale objevuje se relativně často v těsném sousedství ČR. Jeho výskyt je i v ČR v budoucnosti potencionálně možný.** Hrozba je zařazena do skupiny faktorové skladby **hrozby spojené s hrozbami migrace a terorismu.**

[306] ANB (2016), s. 11. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-07-25]

4.4.4. SOUHRNNÝ ROZBOR BEZPEČNOSTNÍCH HROZEB STŘEDNÍ RELEVANCE

Výsledky empirického průzkumu přiřadily **čtrnácti zkoumaným bezpečnostním hrozbám střední míru relevance**. Téměř všechny bezpečnostní hrozby této skupiny jsou intencionálními hrozbami. Výjimku tvoří pouze hrozba povodní, která je neintencionální a není tudíž předmětem zájmů českých zpravodajských služeb. Kromě již zmíněné hrozby povodní je působnost BIS zastoupena ve všech třinácti zbývajících hrozbách. Samostatnou zpravodajskou působnost má BIS v eliminaci hrozeb organizované daňové kriminality a kriminality spojení s insolvenčním řízením. Zbylé bezpečnostní hrozby střední relevance jsou víceméně náplní činnosti všech tří českých zpravodajských služeb. Konktrétně se jedná o politický extremismus, zneužití legitimních služeb pro potřeby organizovaného zločinu a legalizaci výnosů z trestné činnosti (v obou posledně jmenovaných případech má BIS dominující působnost), terorismus osamělých vlků, narušení dodávek plynu, pitné vody, elektrické energie a ropy velkého rozsahu (zde hraje klíčovou roli především zpravodajská analytická činnost předvídající negativní tendence směřující proti zájmům ČR), surovinová a průmyslová bezpečnost a v neposlední řadě i islámský radikalismus jako víceméně potencionální bezpečnostní hrozba, která se prozatím ČR spíše vyhýbá.

Z hlediska zařazení konkrétních bezpečnostních hrozeb střední relevance do skupin faktorové skladby bezpečnostních hrozeb skupina střední relevance zahrnuje čtyři ze šesti skupin faktorových skladeb. Fakticky se jedná o faktorovou skladu ohrožení působnosti státu a jeho ekonomické stability, hrozby energetické, surovinové, průmyslové a enviromentální, hrozby spojené s migrací a terorismem a hrozby extremismu. Konkrétní četnost bezpečnostních hrozeb střední relevance ukazuje následující graf č.31.

Graf č. 31 Četnost bezpečnostních hrozeb střední relevance řazených podle faktorové skladby

Nejpočetněji jsou ve skupině střední relevance zastoupeny hrozby energetické, surovinové, průmyslové a enviromentální (50%). Konkrétně se jedná o pestrou paletu bezpečnotsních hrozeb, které jsou spojeny především s otázkami dodávek strategických energetických surovin z domácí, ale především zahraniční produkce. Kromě **hrozby povodní**, jako jediné neintencionální hrozby skupiny, jde o **dodávky plynu, ropy, elektrické energie a vody, ale i o surovinovou a průmyslovou bezpečnost** státu. V těchto oblastech je působnost českých zpravodajských služeb (vyjma eliminace pokusů terorismem nebo sabotáží narušit kritickou infrastrukturu státu) zaměřena především na analytické sledování a vyhodnocování všech hrozeb, které jsou s těmito dodávkami spojeny. Zpravodajské služby v těchto otázkách plní funkci včasného varování státu před možnými energetickými a surovinovými problémy. Sehrávají svou roli i jako bezpečnostní garant při výběru zahraničních, ale i domácích společností, které v různých tendrech projevují zájem kapitálově nebo technicky do těchto oblastí vstoupit. Druhou nejpočetnější faktorovou skupinou jsou hrozby ohrožující působnost státu a jeho ekonomické stability (29%). Jde zejména o **daňovou**

kriminalitu, zneužívání systému služeb organizovaným zločinem nebo legalizaci výnosů získanou trestnou činností. Zde mají klíčovou působnost hlavně domácí zpravodajské služby, v českém případě především BIS, které v interakci s policejními útvary zajišťují nezbytnou informační zpravodajskou podporu. Skupina střední relevance rovněž obsahuje dvě hrozby z faktorové skupiny hrozeb spojených s hrozbami migrace a terorismu (14%). Konkrétně se jedná o tzv. **terorismus osamělých vlků a islámský radikalismus.** Tato skupina hrozeb je součástí působnosti všech tří českých zpravodajských služeb, neboť tyto hrozby mají výrazný domácí i zahraniční přesah. I když je hrozba terorismu jednou z hlavních působností zpravodajských služeb, zastoupená v empirickém výzkumu právě těmito dvěma hrozbami, nejedná se z pohledu ČR prozatím o nejvýznamnější bezpečnostní hrozby. Střední relevance těchto hrozeb však upozorňují na jejich významný potenciál, které nelze podceňovat. Poslední skupina hrozeb je v oblasti střední relevance spojena s riziky extremismu (7%), zastoupena konkrétně s hrozbou **politického extremismu**. I když byla hrozbě politického extremismu přiřazena hodnota střední relevance, dva konkrétní projevy extremismu – levicový a pravicový, byly zařazeny do skupiny nízké relevance. Skupina hrozeb střední relevance neobsahuje ani jednu položku z faktorových skladeb hrozeb v kyberprostoru a geopolitických hrozeb, neboť těmto hrozbám byla ve všech případech přiřazena výhradně vysoká relevance, tzn., že tyto hrozby jsou z hlediska národní bezpečnosti nejvíce nebezpečné. Hrozby střední relevance však navazují na některé hrozby faktorových skupin z vysoké relevance, jako je skupina hrozeb faktorové sklady ohrožení působnosti státu a jeho ekonomické stability a hrozby energetické, surovinové, průmyslové a enviromentální. Obecně patří tyto faktorové skupiny do kategorie nejnebezpečnějších hrozeb pro ČR, jen v některých případech jim byla naměřena střední relevance.

4.4.5 C) BEZPEČNOSTNÍ HROZBY NÍZKÉ RELEVANCE

C1 HROZBA NEÚSPĚŠNÉ INTEGRACE
(intencionální bezpečnostní hrozba)

I když v posledních dekádách až do počátku ruské války proti Ukrajině zahájené 24. 2. 2022 nebyla ČR tradičním cílem světových migračních proudů. ČR (resp. Československo) však má své zkušenosti s integračními procesy relativně masových migračních proudů. Již od 50. let minulého století šlo především o víceméně řízenou vietnamskou migraci, v 70. letech o příchod nevelkých vln muslimské migrace především z Iráku, Súdánu, Sýrie, Libanonu nebo Palestiny,[307] až po poslední dekády, kdy se v ČR usazovaly nebo jen pracovaly relativně velké počty migračních skupin ze zemí bývalého SSSR, především z Ukrajiny. Ruská válka proti Ukrajině však otevřela cestu k historicky nejmasovější migraci prchajících ukrajinských válečných uprchlíků do ČR, kde bylo integrováno téměř 460 tisíc běženců z Ukrajiny.

Velká evropská migrační krize z roku 2015 se ČR v podstatě vyhnula, avšak způsobila určité neshody mezi starými a novými členskými zeměmi EU. Nové členské země EU ve střední Evropě odmítly masové přijímání miliónových počtů uprchlíků, což způsobilo rozkol ve vzájemných vztazích se starou Evropou, která nové členské státy obviňovala z nedostatku solidarity. Tato dosud největší migrační krize však eskalovala zahájení příprav na zvládnutí potencionálně další migrační krize v rámci celého evropského kontinentu. Tento proces zahrnoval především důraz na bezpečnostní aspekty migrace, které mohou migraci provázet nebo které se již v reálné podobě objevily. Z iniciativy ministerstva vnitra byla vypracována Strategie migrační politiky[308] (2015), která nově vzniklou evropskou migrační situaci nově posoudila z hlediska krátkodobých i dlouhodobých cílů ČR. Oficiální webový portál českého ministerstva vnitra ve sledované souvislosti mj.

[307] FELČER Petr (2019). Tváře migrace. MÝTY VERSUS REALITA: Imigrace z Blízkého východu a severní Afriky do České republiky, s. 4. Dostupné z https://tvaremigrace.cz/res/archive/001/000208.pdf?seek=1582901302 [online, cit. 2022-07-26].
[308] Dostupné z https://www.mvcr.cz/migrace/clanek/strategie-migracni-politiky-ceske-republiky.aspx [online, cit. 2022-07-26].

konstatuje, že migrace může být doprovázena rizikem „*terorismu, organizovaného zločinu, ale i šíření infekční nákazy, kulturních zvyklostí neslučitelných s naším právním pořádkem nebo snížené ochoty k integraci.*“[309] Ve stejném duchu reagovaly a některé národní strategické texty. Např. Bezpečnostní strategie (2015) přímo konstatuje, že nekontrolovaná migrace do zemí Evropy může vést k „*nežádoucí radikalizaci členů těchto přistěhovaleckých komunit*“,[310] v podstatě právě jako důsledek neúspěšné integrace migrantů do české společnosti. Audit národní bezpečnosti (2016) pak problematiku hrozby neúspěšné integrace migrantů rozpracovává ještě podrobněji. Mj. konstatuje, že „*nedostatečná integrace přináší riziko vytváření uzavřených komunit cizinců. Jejich společenská izolace či sociální vyloučení vedou nejen k osobní frustraci, ale i ke vzniku konfliktů mezi cizinci a majoritou či komunitami cizinců navzájem. Nedostatečná či neúspěšná integrace přináší riziko nárůstu xenofobie, netolerance a extremismu ve společnosti*.“[311] S odkazem na uvedené bezpečnostní hrozby, které by mohly neúspěšnou integraci migrantů doprovázet byly aktivovány i nové kapacity českého bezpečnostního aparátu, včetně zpravodajských služeb, které jsou všechny tři (BIS, ÚZSI i VZ) v této otázce plně kompetenčně příslušné. Např. BIS ve veřejné části své výroční zprávy z roku 2019 upozorňuje, že mezi některými sunnitskými muslimy žijícími v ČR se projevují negativní postoje vůči české společnosti a „…*mezi faktory, které přispívaly k přijímání radikálních postojů, patřily zejména nedostatečná integrace*…“[312] Hrozby plynoucí z neúspěšné integrace migrantů mají své konkrétní příklady i v ČR, i když je tato intenzita v porovnání s některými jinými evropskými státy s velkou přítomností muslimského obyvatelstva, podstatně menší.

---

[309] MV ČR (www.mvcr.cz). Bezpečnostní aspekty migrace. Dostupné z https://www.mvcr.cz/chh/clanek/bezpecnostni-aspekty-migrace.aspx [online, cit. 2022-07-26]

[310] BS ČR ČR (2015), s. 11. Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2022-07-26].

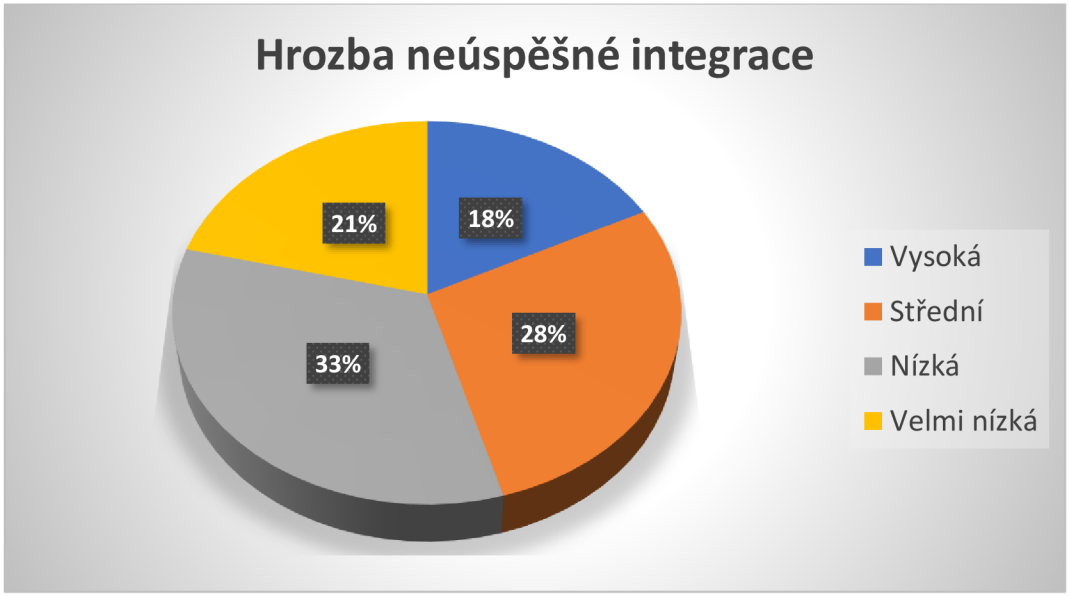
[311] ANB (2016), s. 66. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf

[312] Výroční zpráva BIS za rok 2019, s. 13. Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf [online, cit. 2022-07-26].

Tabulka č. 37 a graf č. 32 Hrozba neúspěšné integrace

Hrozba neúspěšné integrace

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Vysoká	10	17,5	17,5	17,5
	Střední	16	28,1	28,1	45,6
	Nízká	19	33,3	33,3	78,9
	Velmi nízká	12	21,1	21,1	100,0
	Celkem	57	100,0	100,0	



Respondenti empirického průzkumu přiřadili hrozbě neúspěšné integrace cizinců na našem území nízkou míru relevance, i když byl zaznamenán relativně velký názorový rozptyl. Byl naměřený průměr 3,58 a směrodatná odchylka 1,017. Celkem 18 % dotazovaných však hrozbu hodnotí jako velmi vysokou, 28 % jako střední, 33 % jako nízkou a 21 % jako velmi nízkou. Tento názorový rozptyl, který z bezpečnostního hlediska ve většině zohledňuje spíše uspokojivý stav relevance této hrozby však zároveň připouští, že by tato hrozba mohla při určitém vývoji událostí (např. novým masovým migračním vlnám) rychle změnit svou nízkou relevanci. Lze konstatovat, že s odkazem na tyto důvody je nezbytná aktivita všech českých bezpečnostních složek v čele se zpravodajskými službami, neboť

tato reálná hrozba je provázána i s dalšími bezpečnostními riziky, které ohrožují bezpečnostní zájmy ČR, ale i jejích spojenců.

Bezpečnostní hrozba neúspěšné integrace **je intencionální hrozba s nízkou mírou relevance. Hrozba je součástí působnosti všech tří zpravodajských služeb ČR. Je navíc úzce spjata s hrozbami terorismu, organizovaného zločinu atd. Navzdory skutečnosti, že hrozba neúspěšné integrace cizinců do české společnosti má aktuálně spíše okrajový charakter, může být v budoucnosti zásadním bezpečnostním problémem i pro ČR.** Hrozba je zařazena do skupiny faktorové skladby **hrozby spojené s hrozbami migrace a terorismu.**

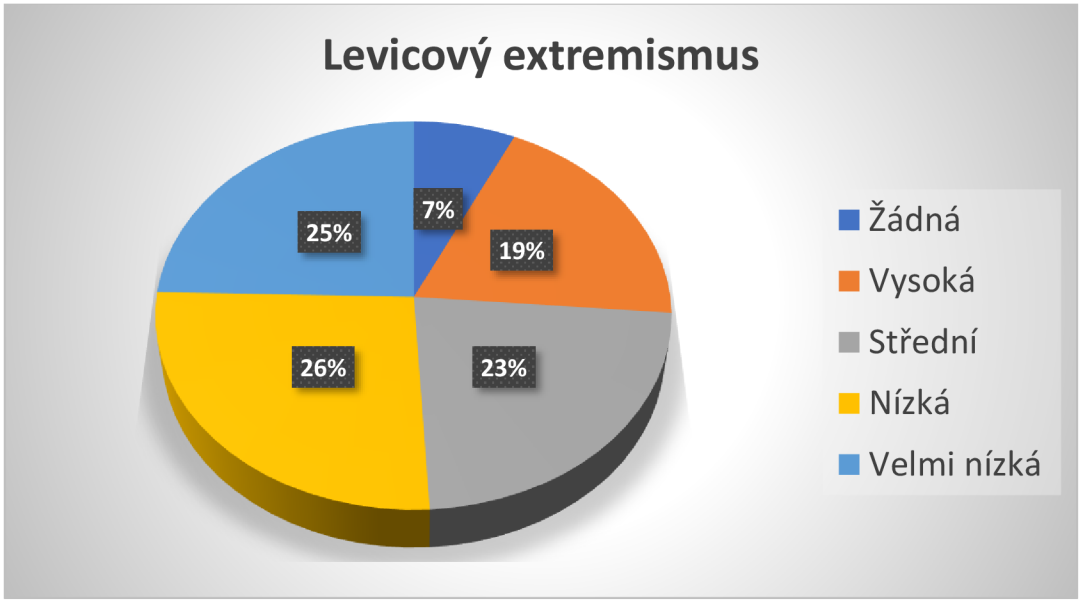
C2 LEVICOVÝ EXTREMISMUS
C3 PRAVICOVÝ EXTREMISMUS (intencionální bezpečnostní hrozby)

Hrozby levicového a pravicového extremismu jsou již popsány a komentovány v kapitole **4.4.3.2 B2 POLITICKÝ EXTREMISMUS**. Respondenti empirického výzkumu přiřadili hrozbám politického extremismu jako takovému střední míru relevance, avšak jeho dvěma nejčastějším podobám v ČR – levicovému a pravicovému extremismu „pouze“ nízkou míru relevance. To je sice z určitého hlediska v mírném rozporu, avšak u všech zkoumaných proměnných (politický, levicový a pravicový extremismus) lze konstatovat výskyt relativně velkého názorového rozptylu, což vede k závěru, že se jedná o hrozby, které mohou při určitém vývoji situace svou relevanci velmi rychle měnit.

Tabulka č. 38 a graf č. 33 Levicový extremismus

Levicový extremismus

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Žádná	4	7,0	7,0	7,0
	Vysoká	11	19,3	19,3	26,3
	Střední	13	22,8	22,8	49,1
	Nízká	15	26,3	26,3	75,4
	Velmi nízká	14	24,6	24,6	100,0
	Celkem	57	100,0	100,0	



Pracovníci analytické skupiny BIS přiřadili hrozbě levicového extremismu v ČR nízkou míru relevance s poněkud pestrým názorovým rozptylem. Celkově lze ale konstatovat, že dominantně převládá názor nízké relevance zkoumané bezpečnostní hrozby. Byl zjištěný průměr 3,60 a směrodatná odchylka 1,098. Pouze 19 % dotazovaných hodnotí hrozbu jako vysokou, 23 % jako střední, 26 % jako nízkou, 25 % jako velmi nízkou a dokonce 7 % jako žádnou.

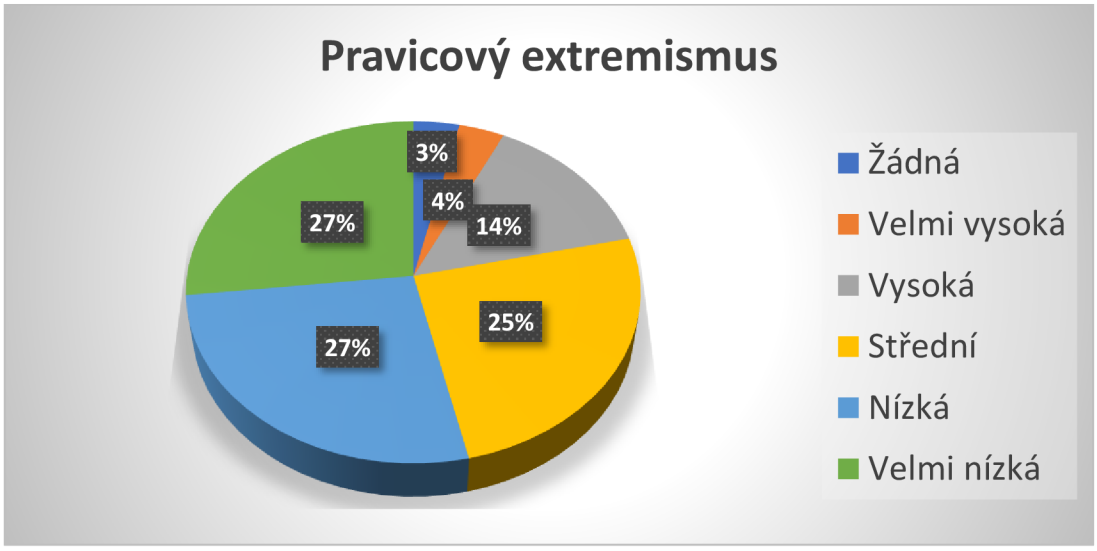
Bezpečnostní hrozba levicového extremismu **je intencionální hrozba s nízkou mírou relevance. Hrozba je součástí působnosti především policejních orgánů a vnitřní BIS, s určitými přesahy do militární oblasti i VZ.**

I když v současnosti není výraznou bezpečnostní hrozbou má při určitém vývoji situace velký potenciál relevanci změnit. Proto je odhalování všech souvislostí spojených s touto hrozbou důležitou působností českého bezpečnostního aparátu v čele s BIS. Hrozba je zařazena do skupiny faktorové skladby **hrozby spojené s hrozbami migrace a terorismu.** Hrozba je zařazena do skupiny faktorové skladby **hrozby extremismu.**

Tabulka č. 39 a graf č. 34 Pravicový extremismus

Pravicový extremismus

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Žádná	2	3,5	3,6	3,6
	Velmi vysoká	2	3,5	3,6	7,1
	Vysoká	8	14,0	14,3	21,4
	Střední	14	24,6	25,0	46,4
	Nízká	15	26,3	26,8	73,2
	Velmi nízká	15	26,3	26,8	100,0
	Celkem	56	98,2	100,0	
Vynechaná	System	1	1,8		
Celkem		57	100,0		



Respondenti průzkumu hrozbu pravicového extremismu zařadili do nízké relevance, avšak opět s relativně pestrým názorovým rozptylem. Byl zjištěný průměr 3,61 a směrodatná odchylka 1,156. Názorový nesoulad je zde velmi

podobný hodnocení respondentů hrozby levicového extremismu. Jeden 4 % dotázaných označili hrozba za velmi vysokou, 14 % za vysokou, 25 % za střední, 27 % za nízkou, 27 % za velmi nízkou a 3 % za žádnou. Platí zde stejný závěr jako u hrozby levicového extremismu, neboť aktuální stav může být s nepříznivým vývojem událostí ve společnosti rychle nahrazen zcela jinými hodnotami.

Bezpečnostní hrozba pravicového extremismu **je intencionální hrozba s nízkou mírou relevance. Hrozba je** stejně jako v případě levicového extremismu **součástí působnosti především policejních orgánů a vnitřní BIS, a v případě přesahů do militární oblasti i VZ. Aktivity pravicového extremismu však často mají přeshraniční charakter, proto je tento jev v zájmu i zahraniční zpravodajské služby ÚZSI. I když pravicový extremismus není v současnosti pro českou společnost výraznou bezpečnostní hrozbou, má při určitém vývoji situace velký potenciál svou relevanci změnit. Proto je odhalování všech souvislostí spojených s touto hrozbou důležitou působností českého bezpečnostního aparátu v čele s BIS, ale i ostatních zpravodajských služeb.** Hrozba je zařazena do skupiny faktorové skladby **hrozby spojené s hrozbami migrace a terorismu.**

C4 ÚNIK NEBEZPEČNÉ LÁTKY
(intencionální bezpečnostní hrozba)

Podle informací ze Znalostního systému prevence rizik[313] jsou v ČR nebezpečné látky definovány a stanovovány zákonem č. 350/2011 Sb. (Chemický zákon) jako „***výbušné, oxidující, extrémně hořlavé, vysoce hořlavé, hořlavé, vysoce toxické, toxické, zdraví škodlivé, žíravé, dráždivé, senzibilizující, karcinogenní, mutagenní, toxické pro reprodukci, nebezpečné pro životní prostředí.***“[314] S výčtu vyplývá, že jedná především o antropogenní hrozby

[313] Znalostní systém prevence rizik v BOZP. Dostupné z https://zsbozp.vubp.cz/ [online, cit. 2022-07-26].
[314] Znalostní systém prevence rizik v BOZP. Mimořádné události. Únik nebezpečných látek. Dostupné z https://zsbozp.vubp.cz/unik-nebezpecnych-latek https://zsbozp.vubp.cz/ [online, cit. 2022-07-26].

způsobené sice činností člověka, ale ve většině vzniklých v důsledku nejrůznějších havárií, technickým a technologickým selhání atd. Vyjma případů, kdyby k úniku nebezpečných látek došlo cestou teroristického útoku nebo sabotáže není tato problematika součástí působnosti zpravodajských služeb. Jedinou výjimkou by mohl být únik nebezpečné látky z prostředků zbraní hromadného ničení nebo z jiných vojenských materiálů. Takové případy jsou z hlediska proliferace zbraní hromadného důležitou součástí práce všech tří českých zpravodajských služeb.

Tabulka č. 40 a graf č. 35 Únik nebezpečné látky

Únik nebezpečné látky

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Žádná	1	1,8	1,8	1,8
	Vysoká	3	5,3	5,3	7,0
	Střední	20	35,1	35,1	42,1
	Nízká	26	45,6	45,6	87,7
	Velmi nízká	7	12,3	12,3	100,0
	Celkem	57	100,0	100,0	

Respondenti z BIS hodnotili hrozbu možného úniku nebezpečné látky v pásmu nízké relevance. Byl zde však zaznamenán určitý názorový rozptyl, i když zařazení do kategorie nízké relevance přesvědčivě převažuje. Byl naměřený

průměr 3,66 se směrodatnou odchylkou 0,769. Pouze 5 % respondentů hodnotí hrozbu jako vysokou, ale již 35 % jako střední, 46 % jako nízkou, 12 % jako velmi nízkou a 2 % jako žádnou.

Bezpečnostní hrozba úniku nebezpečné látky **je intencionální hrozba s nízkou mírou relevance. Hrozba v podstatě není v přímé působnosti žádné z českých zpravodajských služeb. Jedinou výjimkou jsou případy úniku nebezpečné látky v důsledku terorismu nebo sabotáže nebo jakou součást zpravodajských aktivit v oblasti proliferace zbraní hromadného ničení, kde jsou obsaženy i chemické zbraně.** Hrozba je zařazena do skupiny faktorové skladby **hrozby energetické, surovinové, průmyslové a environmentální.**

C5 PŮSOBENÍ A VLIV SEVERNÍ KOREJE
(intencionální bezpečnostní hrozba)

Severní Korea se svým totalitním režimem představuje závažné bezpečnostní riziko celému civilizovanému světu, avšak nejvíce asi sousední Jižní Koreji a Japonsku. Toto riziko se ještě zvětšilo, když Severní Korea v roce 2003 odstoupila od Smlouvy o nešíření jaderných zbraní a v roce 2009 oficiálně oznámila vlastnictví jaderné bomby.[315] I když je Severní Korea jednou z nejzaostalejších zemí světa, severokorejský diktátorský režim s pomocí jaderného arsenálu, a především s podporou některých jiných autoritativních režimů (Čína, Rusko) doma nejen přežívá, ale stále stupňuje míru agrese vůči okolnímu světu.

ČR je jednou z mála vyspělých zemí, která v severokorejském hlavním městě Pchjongjangu provozuje zastupitelský úřad a v některých případech dokonce zastupuje i zájmy jiných spřátelených států. Tato skutečnost díky

[315] CARREL-BILLIARD Francois, WING Christine (2010), North Korea and the NPT, Nuclear Energy, Nonproliferation, and Disarmament: Briefing Notes for the 2010 NPT Review Conference, International Peace Institute New York, s. 28–33.

reciprocitě umožňuje severokorejskému režimu provozovat svou ambasádu v Praze, která vedle oficiálních diplomatických aktivit provozuje i špionážní činnost nejenom vůči českému státu, ale i proti jiným západním zemím. Severokorejská špionáž je více něž na politickou výzvědnou činnost zaměřena především na získávání hospodářských, technologických, technických nebo vědeckých informací z nejrůznějších výzkumných aktivit. Cílem jsou často i informace z vojenské oblasti. Důvodem tohoto zaměření je především všeobecná severokorejská chudoba a snaha těmito prostředky nelegálně získat vše, co by mohlo severokorejskému režimu přinést profit. Aktivity vedoucí k odhalování těchto nepřátelských aktivit mj. přiznává i veřejná část výroční zprávy BIS, kde je špionáž Severní Koreje v ČR explicitně zmíněna.[316]

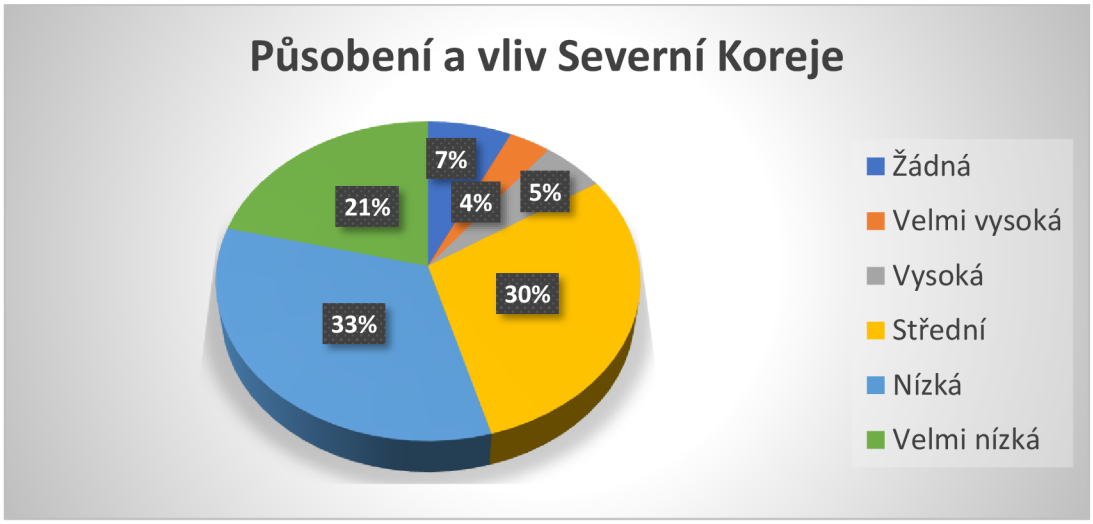
Podle redakčního článku Revue Politika z roku 2006 je „*ČR pro KLDR v současnosti spíše zajímavá z hlediska hospodářské špionáže, která může být využita pro další rozvoj vojenských programů*.“[317] I tato informace napovídá, že je severokorejská špionáž proti našemu státu předmětem zájmu všech tří českých zpravodajských služeb, především BIS a VZ, ale v mnoha souvislostech i ÚZSI. Vzhledem k relativně omezeným severokorejským kapacitám však lze tvrdit, že tyto nepřátelské aktivity aktuálně neznamenají pro českou národní bezpečnost skutečně závažný problém.

[316] Výroční zpráva BIS za rok 2019, s. 3. Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf [online, cit. 2022-07-26].
[317] Revue Politika 9/2006. Severokorejský jaderný pokus a bezpečnost ČR. Dostupné z https://www.cdk.cz/severokorejsky-jaderny-pokus-bezpecnost-cr [online, cit. 2022-07-26].

Tabulka č. 41 a graf č. 36 Působení a vliv Severní Koreje

Působení a vliv Severní Koreje

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Žádná	4	7,0	7,0	7,0
	Velmi vysoká	2	3,5	3,5	10,5
	Vysoká	3	5,3	5,3	15,8
	Střední	17	29,8	29,8	45,6
	Nízká	19	33,3	33,3	78,9
	Velmi nízká	12	21,1	21,1	100,0
	Celkem	57	100,0	100,0	



Respondenti empirického výzkumu přiřadili hrozbě působení a vlivu Severní Koreje nízkou míru relevance. Byl však zaznamenán relativně velký názorový rozptyl což ve výsledku znamená, že tato hrozba nepatří mezi největší zpravodajské výzvy českých bezpečnostních složek, ale nelze ji brán jen na lehkou váhu. Byl zjištěný průměr 3,68 a směrodatná odchylka 1,015. Sice pouze 3 % respondentů hodnotí hrozbu jako velmi vysokou, jen 5 % jako vysokou, ale již 30% hrozbu označuje za střední, 33 % za nízkou, 21 % za velmi nízkou a 7 % za žádnou.

Bezpečnostní hrozba působení a vliv Severní Koreje **je intencionální hrozba s nízkou mírou relevance. Hrozba je v přímé působnosti všech českých zpravodajských služeb. Jedná se především o odhalování a eliminaci severokorejských špionážních aktivit (především hospodářských,**

vědeckých nebo vojenských atd.), ale i o odhalování pokusů porušování sankčních programů s cílem vyvézt do Severní Koreje sankcemi zakázané zboží nebo materiál. Hrozba je zařazena do skupiny faktorové skladby **geopolitické hrozby.**

C6 ZAHRANIČNÍ BOBJOVNÍCI
(intencionální bezpečnostní hrozba)

Zahraniční bojovníci (nebo foreign fighters) jsou fenoménem nejen dnešní doby v podobě dobrodruhů, ale i jinak narušených osobností (někdy i teroristů, avšak ne výhradně), kteří se pod různými příčinami účastní nebezpečných, často válečných operací a bojů pod cizí vlajkou v různých koutech světa. Podle analýzy Vlády ČR o zhodnocení možností trestního postihu těchto lidí[318] lze zahraniční bojovníky definovat jako „*osoby, které jsou zapojeny do ozbrojeného konfliktu mimo území jejich domovského státu a nestojí na straně tohoto státu*.“ [319] Tito lidé mohou i po svém návratu do domovské země představovat významné bezpečností riziko. Podle webového portálu českého ministerstva vnitra může mj. jít o rizika další radikalizace těchto, ale i jiných osob, šíření radikálních ideologií nebo propagandy nebo možnosti zneužití migračních vln k bezproblémovému přesunu do Evropy.[320]

Fenomén zahraničních bojovníků byl během poslední dekády spojován především s radikálními muslimy z různých evropských států, kteří přecházeli na stranu tzv. Islámského státu, kde páchali nejrůznější zvěrstva. V českém prostředí se spíše jednalo o ideologicky pomatené jedince, kteří např. bojovali na straně separatistů na ukrajinském Donbase atd. Čeští zahraniční bojovníci, kteří mj. v domovské zemi nesou trestní odpovědnost za své činy však po případném

[318] Vláda ČR (2019), Analýza zhodnocení možností trestního postihu činnosti zahraničních (teroristických) bojovníků, 17 s. Dostupné z https://www.vlada.cz/assets/urad-vlady/poskytovani-informaci/poskytnute-informace-na-zadost/Priloha-c--1---mat--42-19.pdf [online, cit. 2022-07-27].
[319] Vláda ČR (2019), Analýza zhodnocení možností trestního postihu činnosti zahraničních (teroristických) bojovníků, s. 1. Dostupné z https://www.vlada.cz/assets/urad-vlady/poskytovani-informaci/poskytnute-informace-na-zadost/Priloha-c--1---mat--42-19.pdf [online, cit. 2022-07-27].
[320] www.mvcr.cz Přístup vybraných zemí k návratu zahraničních bojovníků ze Sýrie a Iráku. Dostupné z https://www.mvcr.cz/chh/clanek/pristup-vybranych-zemi-k-navratu-zahranicnich-bojovniku-ze-syrie-a-iraku.aspx [online, cit. 2022-07-27].

návratu mohou představovat rizika nejenom ve formě šíření nepřátelské ideologie, ale často mohou být i tajnými spolupracovníky cizích mocí a jednat v jejich zájmu. Problémem pro ČR však nemusejí být jen čeští státní občané v řadách zahraničních bojovníků, ale i cizí státní příslušníci, kteří do ČR cestují buď cíleně nebo ČR využívají jako tranzitní prostor k dalšímu přemístění do jiných zemí.

ANB (2016) věnuje problematice zahraničních bojovníků významný prostor a přiřazuje této hrozbě střední míru relevance, i když zároveň konstatuje, že ČR není zemí s vysokým výskytem těchto osob.[321] Jako východisko především pro české zahraniční bojovníky nabízí „*věnovat pozornost boji proti radikalizaci a náboru bojovníků, zneužívání internetu včetně sociálních médií, formování paramilitárních skupin a zahraničnímu vlivovému působení*."[322]

Hrozba přítomnosti tzv. zahraničních bojovníků na území ČR, resp. jejich návratu nebo příjezdu do ČR je náplní práce všech tří českých zpravodajských služeb. Cílem těchto aktivit je nejenom monitorovat tento proces, ale také mu účinně předcházet. V souvislosti s válkou Sýrii BIS ve veřejné části své výroční zprávy za rok 2019 sděluje, že „*…získala během roku 2019 informace o smrti dalšího z dobrovolníků, kteří mezi lety 2012–2017 opustili ČR a vydali se bojovat do válečných oblastí na Blízkém východě. Je-li tato informace pravdivá, jedná se již o pátého zabitého bojovníka, který vycestoval z ČR. Další dva stále na území konfliktu v Sýrii zůstávali, o několika zbylých nezískala BIS aktuální informace. Riziko ve vztahu k radikalizaci muslimské komunity dlouhodobě představuje možnost návratu dobrovolníků z bojových zón zpět do ČR. V roce 2019 však BIS nezískala žádné informace o návratech bojovníků na území ČR a zároveň podle dostupných informací nikdo další z ČR do válečných zón neodcestoval*."[323] Citace prakticky ilustruje, že je tento problém nejenom pod přísným dohledem českých bezpečnostních složek, ale zároveň, že se jedná o nikterak častou bezpečnostní

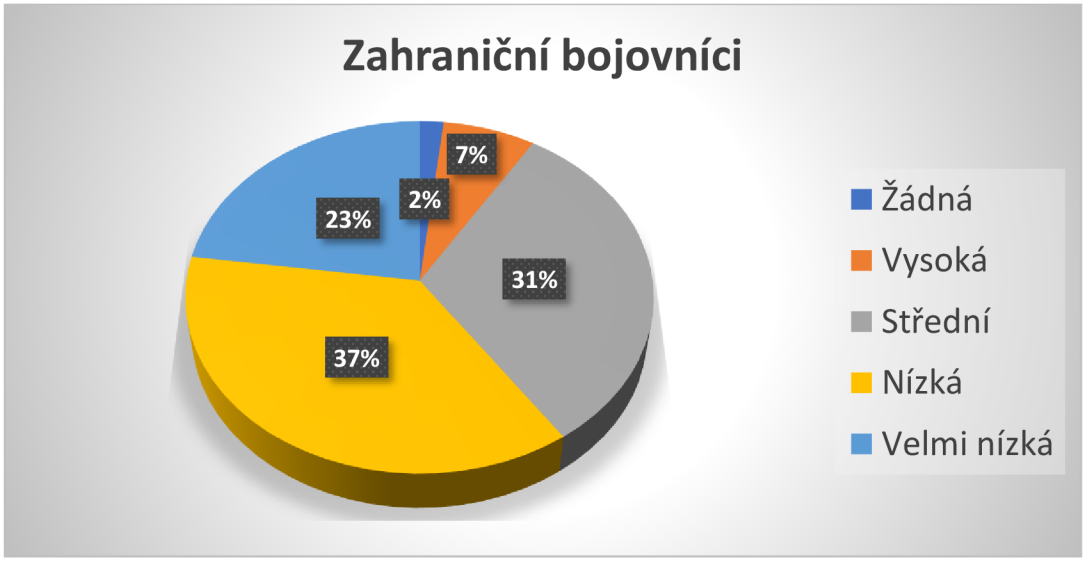
[321] ANB (2016), s. 13. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-07-27].
[322] ANB (2016), s. 14. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-07-27].
[323] Výroční zpráva BIS za rok 2019, s. 13. Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf [online, cit. 2022-07-20].

hrozbu, neboť zahraniční bojovníci českého původu se dají počítat jen v jednotkách.[324] Poněkud odlišná je otázka možného výskytu cizích státních občanů – zahraničních bojovníků, kteří mohou na území ČR pronikat nelegálně a významně ohrožovat české národní bezpečnostní zájmy. V úzké spolupráci s našimi aliančními partnery je však i tento proces podrobně monitorován českými zpravodajskými službami.

Tabulka č. 42 a graf č. 37 Zahraniční bojovníci

Zahraniční bojovníci

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Žádná	1	1,8	1,8	1,8
	Vysoká	4	7,0	7,0	8,8
	Střední	18	31,6	31,6	40,4
	Nízká	21	36,8	36,8	77,2
	Velmi nízká	13	22,8	22,8	100,0
	Celkem	57	100,0	100,0	



[324] Poněkud novým fenoménem je fakt, že v souvislosti s ruskou válkou na Ukrajině udělil prezident republiky souhlas více jak stovce českých občanů, aby mohli legálně bojovat na straně Ukrajiny bránící se ruské agresi. Dostupné z https://www.irozhlas.cz/zpravy-domov/zeman-ukrajinske-ozbrojene-sily-fiala_2205111415_ind [online, cit. 2022-07-20].

I když respondenti empirického výzkumu zařadili bezpečnostní hrozbu zcela přesvědčivě do nízkého pásma relevance, lze však konstatovat určitý názorový rozptyl. Byl naměřený průměr 3,77 a směrodatná odchylka 0,894. V podstatě pouze 7 % dotazovaných hodnotí hrozbu jako vysokou, 31 % jako střední, 37 % jako nízkou, 23 % jako velmi nízkou a 2 % jako žádnou. Názorový rozptyl zde ilustruje kromě konstatování stávající stavu rovněž určitý potenciál, který by hrozba mohla v budoucnu představovat. Závěry empirického výzkum jsou v tomto případě i v rozporu s analýzou ANB (2016), který hrozbě přiřazuje střední míru relevance a vidí tak tuto skutečnost podstatně pesimističtěji, než je tomu i analytiků BIS.

Bezpečnostní hrozba zahraniční bojovníci **je intencionální hrozba s nízkou mírou relevance. Hrozba je v přímé působnosti všech českých zpravodajských služeb. Kromě monitorování identit a pohybu z bezpečnostního hlediska závadných osob, jde rovněž o analýzu a eliminaci všech rizik, která jsou s touto hrozbou spojena.** Hrozba je zařazena do skupiny faktorové skladby **hrozby spojené s hrozbami migrace a terorismu.**

C7 NARUŠENÍ DODÁVEK POTRAVIN VELKÉHO ROZSAHU (intencionální bezpečnostní hrozba)

Bezpečnostní hrozba narušení dodávek potravin velkého rozsahu a plány na její eliminaci je součástí krizových plánů nejenom na celostátní, ale i krajské nebo místní úrovni. Např. internetový portál KRIZPORT, který je veřejným portálem krizového řízení jihomoravského kraje definuje tuto hrozbu jako „*krizovou situaci, která zasáhne celou ČR. Lze předpokládat, že příčinou bude výhradně jiná krizová situace, která způsobí nemožnost pravidelné distribuce potravin koncovým odběratelům. Samostatný výskyt této krizové situace se nepředpokládá.*“[325] V podobném duchu hrozbu hodnotí i ANB (2016), který rovněž nepředpokládá

[325] Dostupné z https://www.krizport.cz/ohrozeni/hrozby-v-jmk/krizove-situace#k14 [online, cit. 2022-08-01].

velkou pravděpodobnost výskytu této hrozby a připouští, že pokud by se tak stalo, bude se jednat o sekundární jev.[326]

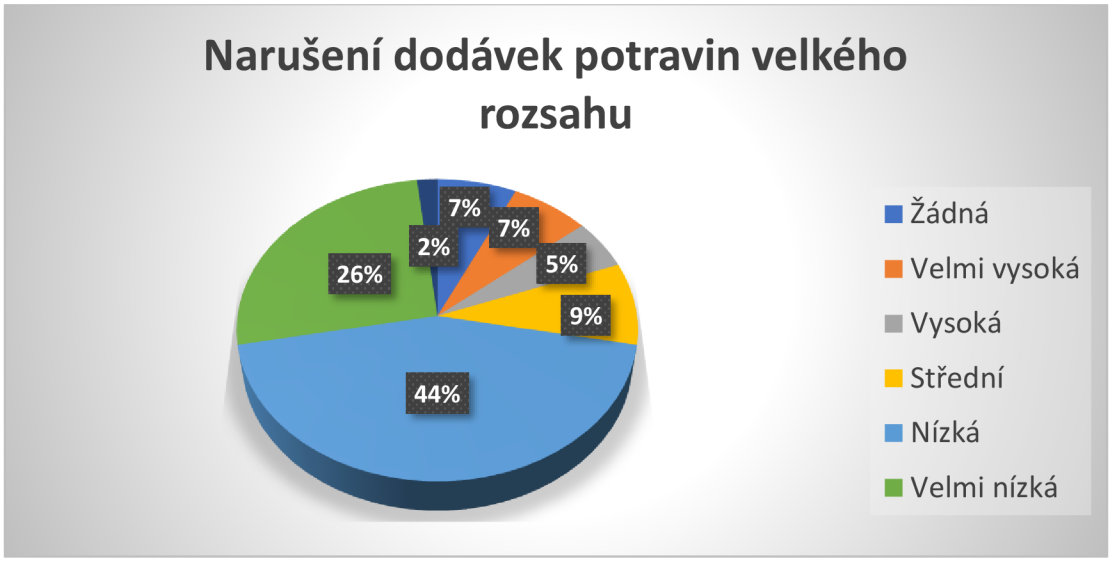
Aktuální situace, s ohledem na ruskou válku na Ukrajině, však v jiných částech světa takovou krizi připouští. Rusko aktivně blokuje vývoz ukrajinského obilí do některých částí světa, což ve finále může např. na africkém kontinentu vyvolat hladomor, s následnými lidovými bouřemi a velkými migračními vlnami. Vznikla by tak uměle vyprovokovaná situace, kdy na počátku je narušení dodávek potravin velkého rozsahu ve velkých světových regionech. I když se tato krize prvoplánově netýká bohaté a potravinově soběstačné Evropy a celého západního světa, následné migrační vlny, uměle vyvolané hrozbou narušení dodávek potravin do některých závislých a chudých regionů, budou mířit právě do bohatých západních států. Jedná se o další velmi konkrétní příklad pestré palety ruské agrese proti svobodnému světu, která ve finále může způsobit zásadní migrační krizi. Hovoříme – li však pouze o hrozbě narušení potravin velkého rozsahu nejedná se o typickou gesci ani jedné z českých zpravodajských služeb.

Tabulka č. 43 a graf č. 38 Narušení dodávek potravin velkého rozsahu

Narušení dodávek potravin velkého rozsahu

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Žádná	4	7,0	7,0	7,0
	Velmi vysoká	4	7,0	7,0	14,0
	Vysoká	3	5,3	5,3	19,3
	Střední	5	8,8	8,8	28,1
	Nízká	25	43,9	43,9	71,9
	Velmi nízká	15	26,3	26,3	98,2
	6	1	1,8	1,8	100,0
	Celkem	57	100,0	100,0	

[326] ANB (2016), s. 88. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-08-01].



Respondenti empirického výzkumu přiřadili hrozbě narušení dodávek potravin velkého rozsahu přesvědčivě nízkou relevanci, i když je jejich názorové spektrum celkem bohaté. Byl naměřen průměr 3,89 a směrodatná odchylka 1,171. Překvapivě 7 % dotázaných hodnotí hrozbu jako velmi vysokou, 5 % jako vysokou, 9 % jako střední, ale 44 % jako nízkou, 26 % jako velmi nízkou a 2 % jako žádnou. I když naprostá většina respondentů (celkem 72%) hodnotí hrozbu v pásmu nízké relevance, je zde zastoupeno je plné spektrum podstatně odlišných názorů.

Bezpečnostní hrozba narušení dodávek potravin velkého rozsahu **je intencionální hrozba s nízkou mírou relevance. Hrozba není v přímé působnosti českých zpravodajských služeb.** Hrozba je zařazena do skupiny faktorové skladby **hrozby energetické, surovinové, průmyslové a environmentální.**

C8 NEŘÍZENÁ MIGRACE
(intencionální bezpečnostní hrozba)

Druhy a migrační vlny do bývalého Československa, resp. ČR byly popsány již v kapitole 4.4.4.1 C1 HROZBA NEÚSPĚŠNÉ INTEGRACE. Bezpečnostní hrozba neřízené migrace, její popis a výskyt v českých národních strategických dokumentech však reaguje na rozsáhlé migrační vlny z roku 2015. Evropská

migrační krize 2015, která jako následek tzv. arabského jara 2010/11 (prodemokratických protestů a povstání, které se konaly na Blízkém východě a v severní Africe)[327] přivedla víceméně živelně do bohatých států Evropy několik milionů migrantů, skutečných válečných uprchlíků z oblasti válečného konfliktu v Sýrii atd., ale i mnoho ekonomických migrantů především ze států severní Afriky. Migrační krize způsobila v Evropě nejenom potíže s dopady na ekonomiku a sociální politiku, ale i vážný rozkol mezi tzv. starými a novými členskými státy EU. Některé velké Evropské státy (především Německo) se rozhodly statisícové skupiny migrantů integrovat a žádaly i ostatní unijní země o solidaritu formou přerozdělování běženců. Tato politika narazila na vážný odpor některých středoevropských států v čele se státy V4, které politiku přerozdělování odmítly.[328]

ČR, kromě nesouhlasu s masivním umisťováním muslimských uprchlíků v EU, se sice pokusila převzít na své území malé skupiny válečných migrantů z blízkovýchodních zemí, avšak tato integrace nebyla úspěšná i díky rozdílné výši sociálních dávek, které poskytla české vláda, a které vyplácely některé bohaté evropské státy. Podobný trend jen utvrdil odpírače přijímání migrantů v přesvědčení, že spíše něž o válečné uprchlíky jde o ekonomické migranty. Na rozdíl od starých členských států byla v ČR, ale i dalších V4 státech, podstatně úspěšnější antimigrační rétorika silně rezonující v mediálním prostoru ze strany některých opozičních politických proudů (v českém případě např. předseda SPD T. Okamura, který úspěšně do české veřejnosti umístil dezinformační narativ o spojení migrace s hrozbou terorismu,[329] i když tato teorie nebyla prozatím v praxi prokázána).

BS ČR2015 obecně vnímá migraci jako nevojenskou bezpečnostní hrozbu[330] a důvody neřízené migrace dává do souvislosti s chudobou, výskytem

---

[327] Podrobněji dostupné z https://www.britannica.com/event/Arab-Spring [online, cit. 2022-08-03].
[328] Asylum and migration into the EU in 2015, European Union Agency for Fundamental Rights, Luxembourg 2016, 44 s. Dostupné z https://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-fundamental-rights-report-2016-focus-0_en.pdf [online, cit. 2022-08-03].
[329] Tomio Okamura: Migrace – trojský kůň terorismu, dostupné z https://www.spd.cz/tomio-okamura-migrace-trojsky-kun-terorismu/ [online, cit. 2022-08-03]
[330] BS ČR (2015), s. 9. Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2022-08-03].

extremismu, kriminality nebo lokálních ozbrojených konfliktů v některých částech světa.[331] ANB (2016) neřízenou migraci vnímá jako hrozbu, která může ve výsledku způsobit nepokoje a radikalismus na straně minority i majority[332] a radí spíše *„předcházet problémům, než čelit následkům neřízené migrace a nezvládnuté integrace.*“[333]

Hrozba neřízené migrace je součástí aktivit všech tří českých zpravodajských služeb především v oblasti prevence a předcházení těmto jevům, ale i ve sféře analytického vyhodnocování tendencí spojených s touto hrozbou. BIS ve veřejné části výroční zprávy 2015, jako reakci na evropskou migrační krizi 2015 mj. konstatuje, že *„Česká republika leží v dopravně exponované centrální části Evropy a ohrožují ji v zásadě stejné migrační a na migraci navazující hrozby jako Francii, Belgii a SRN. Riziko jejich naplnění je však zatím řádově nižší, což odpovídá průběhu migrační vlny a jejím dopadům na ČR v roce 2015.*“[334] BIS v téže zprávě mj. konkrétně upozorňuje na *„hrozby, které vyplývají z toho, že je fakticky nemožné organizovaně integrovat velké množství cizinců z kulturně odlišného prostředí do evropské společnosti. Následně dochází ke vzniku uzavřených komunit, které mohou být vůči evropskému kulturnímu prostředí nepřátelské. Tyto komunity pak mohou vytvářet ideové či logistické zázemí pro kriminální aktivity rozličného charakteru*“.[335] Z výše uvedeného vyplývá, že i když ČR nepatří mezi velké příjemce nelegálních migrantů jako důsledku neřízených migračních vln nedávné minulosti a slouží spíše jako tranzitní země, přesto se cítí být díky otevřenému evropskému prostoru těmito trendy ohrožena.

---

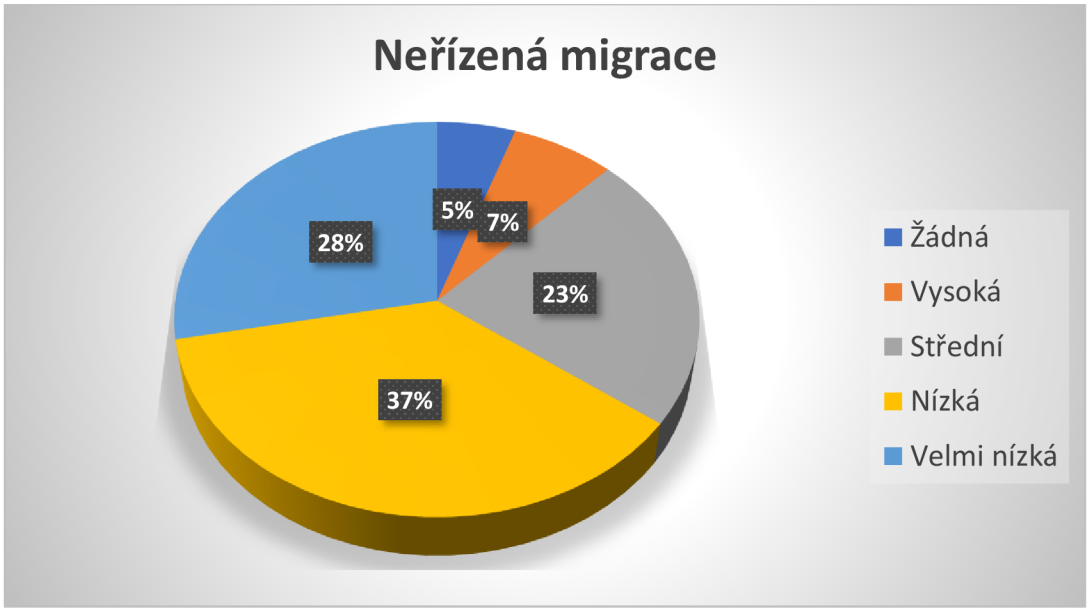
[331] BS ČR (2015), s. 9 a s. 11. Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2022-08-03].
[332] ANB (2016), s. 62. Dostupné z https://www.vlada.cz/assetsmedia-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-08-03].
[333] ANB (2016), s. 67. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-08-03].
[334] Výroční zpráva BIS za rok 2015, s.7. Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2015-vz-cz.pdf [online, cit. 2022-08-03].
[335] Výroční zpráva BIS za rok 2015, s. 7. Dostupné z https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2015-vz-cz.pdf [online, cit. 2022-08-03].

Samostatnou migrační kapitolou je masivní vlna humanitární migrace z Ukrajiny, která částečně změnila názor veřejnosti a některých politiků na riziko migrace. Tato humanitární pomoc ČR však není součástí neřízených migračních vln, neboť právě naopak vykazuje všechny prvky velmi dobře zvládnuté, státem koordinované akce.

Tabulka č. 44 a graf č. 39 Neřízená migrace

Neřízená migrace

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Žádná	3	5,3	5,3	5,3
	Vysoká	4	7,0	7,0	12,3
	Střední	13	22,8	22,8	35,1
	Nízká	21	36,8	36,8	71,9
	Velmi nízká	16	28,1	28,1	100,0
	Celkem	57	100,0	100,0	



Respondenti empirického průzkumu výraznou většinou (70%) přiřadili bezpečnostní hrozbě neřízené, živelné migrace nízkou míru relevance. Žádný z nich neoznačil hrozbu jako velmi vysokou, avšak 7 % dotazovaných hodnotí hrozbu jako vysokou, 23 % jako střední, 37 % jako nízkou, 28 % jako velmi nízkou

a 5 % jako žádnou. Byl zjištěný průměr 3,91 a směrodatná odchylka 0,917. I když se situace ve světě za poslední roky radikálně změnila lze předpokládat, že tento trend je pro ČR stále platný. V důsledku ruské agrese proti Ukrajině ČR sice přijala téměř 400 tisíc ukrajinských válečných běženců, ale tento proces nelze označit za neřízenou migraci. Jiná situace však může nastat díky ruskému tlaku na omezení dodávek ukrajinského obilí do Afriky, čímž může být vyprovokována nová masivní vlna neřízené migrace, která by mohla postihnout i ČR.

Bezpečnostní hrozba neřízená migrace **je intencionální hrozba s nízkou mírou relevance. Hrozba je v přímé působnosti všech tří českých zpravodajských služeb, které jsou velmi zainteresovány v eliminaci, ale i analytické prognóze tohoto rizika .** Hrozba je zařazena do skupiny faktorové skladby **hrozby spojené s hrozbami migrace a terorismu.**

C9 RADIAČNÍ HAVÁRIE
(intencionální bezpečnostní hrozba)

Oficiální webový portál českého ministerstva vnitra definuje radiační havárii jako *„událost, která má za následek nepřípustné uvolnění radioaktivních látek nebo ionizujícího záření nebo nepřípustné ozáření fyzických osob*“.[336] Historie jaderné energetiky, která, jak se původně zdálo měla velmi slibnou budoucnost, byla poznamenána několika jadernými haváriemi (v moderní historii především v roce 1986 ukrajinský, resp. sovětský Černobyl a v roce 2011 japonská Fukušima), které zásadním způsobem přehodnotily dosud projadernou politiku mnohých vlád Evropy a světa. V sousedství ČR to bylo nejprve Rakousko, které po černobylské jaderné havárii zcela odstoupilo od jaderného energetického konceptu a v nedávné minulosti i Německo, které se po havárii ve Fukušimě rovněž rozhodlo k ukončení činnosti svých jaderných elektráren. I když ruská válka proti Ukrajině pravděpodobně prodlouží německou jadernou agónii, vše nasvědčuje tomu, že z dlouhodobé perspektivy je rozhodnuto v neprospěch německých jaderných elektráren. Navzdory řečenému lze konstatovat, že i tak je

[336] Dostupné z https://www.mvcr.cz/clanek/radiacni-nehoda.aspx [online, cit. 2022-08-03].

jaderná energie vyráběná v moderních jaderných elektrárnách jednou z nejbezpečnějších metod získávání relativně čisté energie.[337] ČR je jednou z nemnoha evropských zemí, která nejen zachovává stávající systém svých jaderných elektráren (JE Temelín a JE Dukovany), ale ve své národní energetické koncepci z roku 2014 plánuje jejich další rozvoj[338].

BS ČR (2015) se explicitně hlásí k nutnosti zajištění ochrany energetické infrastruktury, tj. včetně jaderných elektráren.[339] ANB (2016) však věnuje otázce ochrany proti radiační havárii širší pozornost. Vedle výkonu státní správy v oblasti zajištění jaderné bezpečnosti (zde má hlavní působnost Státní úřad jaderné bezpečnosti) se zmiňuje i o monitorování radiační situace na území ČR[340], která je pravidelně vykonávána díky novele Atomového zákona z roku 2016.[341] Z hlediska působnosti zpravodajských služeb ČR není výkon odborných aktivit zajišťujících radiační bezpečnost ČR náplní jejich práce. Jedinou výjimkou jsou potencionální snahy narušit bezpečnost těchto zařízení ze strany jednak cizí moci, ale i cestou kriminálních (sabotážních) aktivit doma. Tato tendence se ale nedávno projevila v bezprecedentním mediálním prohlášení bývalého ruského prezidenta Medveděva, který evropské státy vydíral vyhrožováním o možných haváriích evropských jaderných elektráren.[342] Moderní jaderné elektrárny mj. podléhají speciálnímu systému ochrany čtyř bariér, které musejí odolat i nejrůznějším živelním katastrofám, pádu letadla, teroristickým útokům nebo i selhání obsluhy atd.[343]

---

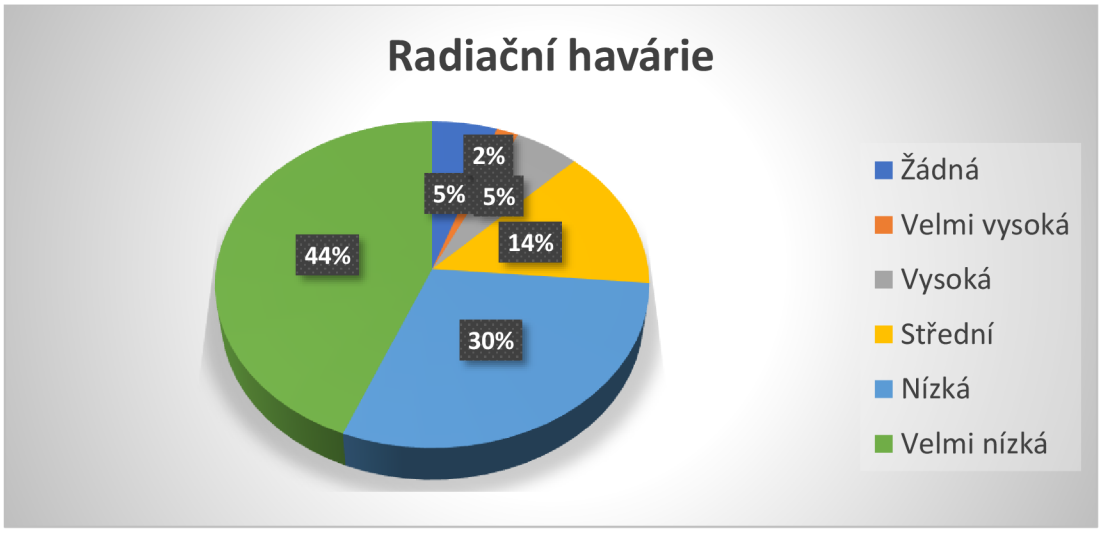
[337] International Atomic Energy Agency. Dostupné z https://www.iaea.org/topics/nuclear-power-plant-safety [online, cit. 2022-08-08].
[338] Státní energetická koncepce ČR (2014). Dostupné z https://www.mpo.cz/assets/dokumenty/52841/60959/636207/priloha006.pdf [online, cit. 2022-08-08].
[339] BS ČR (2015), s. 18. Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [online, cit. 2022-08-08].

[340] ANB (2016), s. 87. Dostupné z https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf [online, cit. 2022-08-08].
[341] Zákon č. 263/2016 Sb. Atomový zákon. Dostupné z https://www.zakonyprolidi.cz/cs/2016-263 [online, cit. 2022-08-08].
[342] Dostupné z https://www.seznam.cz/komentare/17432887-v-jadernych-elektrarnach-po-evrope-se-muzou-stat-nehody-vyhrozuje-medvedev [online, cit. 2022-08-15].
[343] ČEZ: Bezpečnost jaderných elektráren. Dostupné z https://www.cez.cz/edee/content/file/static/encyklopedie/encyklopedie-energetiky/03/bezpecnost_2.html [online, cit. 2022-08-15].

Tabulka č. 45 a graf č. 40 Radiační havárie

Radiační havárie

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Žádná	3	5,3	5,3	5,3
	Velmi vysoká	1	1,8	1,8	7,0
	Vysoká	3	5,3	5,3	12,3
	Střední	8	14,0	14,0	26,3
	Nízká	17	29,8	29,8	56,1
	Velmi nízká	25	43,9	43,9	100,0
	Celkem	57	100,0	100,0	



Respondenti empirického průzkumu zařadili hrozbu radiační havárie celkem jednoznačně do pásma nízké relevance. Byl naměřen vysoký průměr 4,15 a směrodatná odchylka 0,998. Zjištění hodnoty sice řadí hrozbu radiační havárie na poslední místo, tedy nejméně nebezpečnou, avšak názory nejsou u všech zcela totožné. Výzkum i v této otázce odhalil celkem vysoký názorový rozptyl. Jako velmi vysokou hodnotí hrozbu 2 % respondentů, jako vysokou 5,3 %, jako střední 14 %, jako nízkou 30 %, jako velmi nízkou 44 % a jako žádnou 5,5 %. Vzhledem ke skutečnosti, že se radiační ochrana ČR zpravodajských služeb prvoplánově netýká lze usuzovat, že reakce respondentů byly spíše odhadem nezaloženým na exaktních informacích jako u jiných bezpečnostních hrozeb.

Bezpečnostní hrozba radiační havárie **je intencionální hrozba s nízkou mírou relevance. Hrozba není v přímé působnosti českých zpravodajských služeb. Zájmovým tématem zpravodajských služeb se může potencionálně stát pouze v případě teroristického, resp. sabotážního ohrožení, včetně veřejně publikovaných agresivních útoků představitelů nepřátelských mocností vůči bezpečnosti jaderné energetiky, neboť již tyto hrozby mohou být chápana jako předpoklad vedoucí k teroristickému útoku.** Hrozba je zařazena do skupiny faktorové skladby **hrozby energetické, surovinové, průmyslové a environmentální.**

4.4.6. SOUHRNNÝ ROZBOR BEZPEČNOSTNÍCH HROZEB NÍZKÉ RELEVANCE

Empirický výzkum přiřadil **devíti bezpečnostním hrozbám nízkou míru relevance.** Ve všech případech se jedná o intencionální hrozby. Z hlediska působnosti českých zpravodajských služeb pokrývají BIS, ÚZSI a VZ v podstatě všechny bezpečnostní hrozby skupiny, s jistou rezervou v případě bezpečnostní hrozby úniku nebezpečné látky a narušení dodávek potravin velkého rozsahu. Zcela přesvědčivě však zpravodajské služby působí v oblasti eliminace hrozeb neúspěšné integrace, levicového a pravicového extremismu, působení a vlivu Severní Koreje, zahraničních bojovníků a neřízené migrace. Jejich gesce je dána domácím i zahraničním přesahem a v podstatě ve všech uvedených případech se rovněž jedná o oblasti, kde je vyvíjena intenzivní a rozsáhlá mezinárodní zpravodajská spolupráce realizovaná napříč euroatlantickým spektrem. Pouze dvě hrozby, narušení dodávek potravin velkého rozsahu a radiační havárie nejsou v přímé působnosti žádné z českých zpravodajských služeb vyjma případných domácích a zahraničních pokusů teroristických nebo sabotážních aktivit.

Z pohledu šesti stanovených skupin faktorové skladby zkoumaných bezpečnostních hrozeb skupina nízké relevance obsahuje pouze čtyři faktorové skupiny, tj. hrozby spojené s hrozbami migrace a terorismu, hrozby extremismu, hrozby energetické, surovinové, průmyslové a enviromentální a jedna hrozba geopolitická. Nejsou zde zastoupeny žádné hrozby ze skupin faktorových skladeb

ohrožení působnosti státu a jeho ekonomické stability a hrozeb v kyberprostoru, které mají ve všech konkrétních případech spíše vysokou míru relevance bezpečnostního ohrožení ČR. Konkrétní četnost bezpečnostních hrozeb nízké relevance s ohledem na jejich zařazení do jednotlivých skupin nízké relevance je zobrazena grafu č. 41.

Graf č. 41 Četnost hrozeb skupiny nízké relevance řazených do skupin faktorových skladeb

Největší podíl bezpečnostních hrozeb nízké relevance byl přiřazen hrozbám ve faktorové skupině hrozeb spojených s hrozbami migrace a terorismu (34%). Konkrétně se jedná o **hrozbu neúspěšné integrace, zahraničních bojovníků a neřízené migrace**. Následují hrozby z faktorové skupiny hrozeb energetických, surovinových, průmyslových a enviromentálních (33%), konkrétně **únik nebezpečné látky, narušení dodávek potravin velkého rozsahu a radiační havárie**. Skupina nízká relevance dále obsahuje hrozby z faktorové skladby hrozeb extremismu (22%), konkrétně **levicový a pravicový extremismus**. Faktorová skladba geopolitických hrozeb je zde zastoupena hrozbou **působení a vlivu Severní Koreje** (11%).

Výsledky ověřování výzkumných předpokladů[344]

Autorská poznámka: *Tato část dizertační práce – „Výsledky ověřování výzkumných předpokladů“ (výzkumné předpoklady VP01, VP02 a VP03) byla zpracována na základě materiálu, který vypracoval a autorovi dizertační práce předal Dr. Zdeněk Kovařík, CSc., který provedl softwarové zpracování tohoto empirického výzkumu. Znamená to, že níže uvedené výsledky výzkumných předpokladů VP01, VP02 a VP03 v této části dizertace (strany dizertační práce 195–202) jsou z podstatné míry autorským dílem Dr. Zdeňka Kovaříka, CSc. a autorovi dizertace přísluší autorství v oblasti interpretace zjištěných výsledků.*

VP01: Prvním výzkumným předpokladem bylo očekávání, že hodnotící stanoviska expertů BIS na relevanci 37 bezpečnostních hrozeb, nebude věcně významné ovlivněno délkou jejich služební praxe.

Po zevrubném hledání věcně významných závislostí byl zjištěn vliv dvou skupin kategorizovaných hodnot služební praxe. V prvním případě byl zjištěn věcně významný vliv kategorizované služební praxe (praxe do 2 let, praxe od 2 do 22 let, praxe nad 22 let) na bezpečnostní hrozbu „kybernetická špionáž“.

Tabulka č. 46 Kategorizovaná služební praxe

Kategorizovaná služební praxe

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Do 2 let	12	21,1	22,2	22,2
	Od 2 do 22 let	36	63,2	66,7	88,9
	Nad 22 let	6	10,5	11,1	100,0
	Celkem	54	94,7	100,0	
Vynechaná	System	3	5,3		
Celkem		57	100,0		

Výsledek vlivu tří skupin služební praxe na „kybernetickou špionáž“ obsahuje následující kontingenční tabulka s uvedením znaménkového schématu a hodnotou asymetrického koeficientu β.

[344] KOVAŘÍK Zdeněk (2024), Projekt empirického výzkumu. Výsledky ověřování výzkumných předpokladů, archiv autora dizertační práce.

Tabulka č. 47 Kategorizovaná služební praxe „Kybernetická špionáž“

Kategorizovaná služební praxe * Kybernetická špionáž

			Kybernetická špionáž				Celkem
			Velmi vysoká	Vysoká	Střední	Nízká	
Četnost	Kategorizovaná služební praxe	Do 2 let	9	3	0	0	12
		Od 2 do 22 let	8	24	3	1	36
		Nad 22 let	4	2	0	0	6
	Celkem		21	29	3	1	54
Řádková procenta	Kategorizovaná služební praxe	Do 2 let	75,0%	25,0%	,0%	,0%	100,0%
		Od 2 do 22 let	22,2%	66,7%	8,3%	2,8%	100,0%
		Nad 22 let	66,7%	33,3%	,0%	,0%	100,0%
	Celkem		38,9%	53,7%	5,6%	1,9%	100,0%

Kategorizovaná služební praxe	Kybernetická špionáž						
	Velmi vysoká	Vysoká	Střední	Nízká	celkem	medián	dorvar
Do 2 let	++	-	o	o	12	1,167	,375
Od 2 do 22 let	---	++	o	o	36	1,917	,597
Nad 22 let	o	o	o	o	6	1,250	,444
celkem	21	29	3	1	54	1,707	,649

Hodnota koeficientu beta je 0,182 s 95% intervalem spolehlivosti (0,01; 0,354).

Hodnota asymetrického koeficientu β ukazuje, že variabilita odpovědí na relevanci u této bezpečnostní hrozby je z 18,2 % ovlivněna třemi skupinami délky služební praxe. Jde o „velký“ věcně významný efekt.

Bezpečnostní hrozba „Kybernetická špionáž“ byla v naměřené míře závažnosti zařazena na druhé místo nejvyšší relevance zkoumaných hrozeb. Toto zjištění zcela potvrzuje aktuální stav, kdy bezpečnostní hrozby v kybernetickém prostoru představují stále se zvyšující hrozbu bezpečnosti dnešního světa a kybernetický prostor je stále častěji konfrontován nepřátelskými aktivitami protivníka. Zjištěný „velký“ věcně významný efekt ve třech skupinách délky služební praxe lze interpretovat tak, že nejmladší a generace (do dvou let služební praxe) je zastoupena mladými odborníky již s vysokým IT vzděláním nebo IT zkušenostmi, což vysvětluje velmi vysoký a vysoký akcent na relevanci této bezpečnostní hrozby. Praktická zkušenost těchto lidí je však velmi malá, takže tito experti přistupují k této problematice více intuitivně, než je tomu s ohledem na délku jejich. Druhá skupina dotazovaných (služební praxe od 2 do 22 let) je skupinou s největšími praktickými zkušenostmi a je zde zároveň zastoupena jak nemladší generace expertů s vysokou IT profesionalitou, tak i experti, kteří ještě nekladli ve svém klasickém vzdělání tak vysoký důraz na IT vzdělanost, ale mají

bohaté profesní i životní zkušenosti. Z tohoto důvodu považuji tuto skupinu za skupinu, jejíž názory jsou nejvíce relevantní. Třetí skupina bezpečnostních analytiků (praxe nad 22 let) jednoznačně těží z dlouholeté praxe, čímž se ve výsledku přibližují nejmladší generaci, avšak nikoliv pouze intuitivně, ale na základě četných a dlouhodobých zkušeností.

V druhém případě byl zjištěn věcně významný efekt ve vlivu dvou skupin délky služební praxe (praxe do 3 let, praxe nad 3 roky) na bezpečnostní hrozbu „kyberterorismus“.

Tabulka č. 48 Kategorizovaná služební praxe

Kategorizovaná služební praxe

		Četnost	Procenta	Procenta z platných	Kumulativní procenta
Platná	Do 3 let	15	26,3	27,8	27,8
	Nad 3 roky	39	68,4	72,2	100,0
	Celkem	54	94,7	100,0	
Vynechaná	System	3	5,3		
Celkem		57	100,0		

Výsledek vlivu dvou skupin služební praxe na „kyberterorismus“ obsahuje následující kontingenční tabulka s uvedením znaménkového schématu a hodnotou asymetrického koeficientu β.

Tabulka č. 49 Kategorizovaná služební praxe „Kyberterorismus“

Kategorizovaná služební praxe * Kyberterorismus

			Kyberterorismus						Celkem
			Žádná	Velmi vysoká	Vysoká	Střední	Nízká	Velmi nízká	
Četnost	Kategorizovaná služební praxe	Do 3 let	1	4	9	1	0	0	15
		Nad 3 roky	0	6	12	12	7	2	39
	Celkem		1	10	21	13	7	2	54
Řádková procenta	Kategorizovaná služební praxe	Do 3 let	6,7%	26,7%	60,0%	6,7%	,0%	,0%	100,0%
		Nad 3 roky	,0%	15,4%	30,8%	30,8%	17,9%	5,1%	100,0%
	Celkem		1,9%	18,5%	38,9%	24,1%	13,0%	3,7%	100,0%

Kategorizovaná služební praxe	Kyberterorismus								
	Žádná	Velmi vysoká	Vysoká	Střední	Nízká	Velmi nízká	celkem	medián	dorvar
Do 3 let	o	o	+	o	o	o	15	2,778	,693
Nad 3 roky	o	o	-	o	o	o	39	3,625	1,210
celkem	1	10	21	13	7	2	54	3,262	1,193

Hodnota koeficientu beta je 0,106 s 95% intervalem spolehlivosti (0,02; 0,192).

Hodnota asymetrického koeficientu β ukazuje v tomto případě, že variabilita odpovědí na relevanci u této bezpečnostní hrozby je z 10,6 % ovlivněna dvěma skupinami délky služební praxe. Jde o více než „střední“ věcně významný efekt.

Stejně jako u v přechozím případě hrozby kybernetické špionáže je hrozba kybernetického terorismu součástí skupiny hrozeb v kybernetickém prostoru. Na rozdíl od hrozby kybernetické špionáže, která obsadila druhou nejvyšší příčku relevance se hrozba kybernetického terorismu umístila „až“ na čtrnácté pozici a byl zde zaznamenán více než „střední“ věcně významný efekt naměřený ve dvou skupinách. První skupina expertů (služební praxe do tří let) řadí hrozbu zřetelněji do pásma velmi vysoké a vysoké relevance. Tento výsledek lze interpretovat podobně jako v předchozím případě, kdy se experti s vysokým IT vzděláním vyjadřují spíše intuitivně s ohledem na všeobecně vnímané trendy bez dlouholetých praktických zkušeností. Druhá skupina (služební praxe nad tři roky) rozložila své hodnocení do celého spektra od velmi vysoké do velmi nízké relevance, kdy nejvyšší akcent byl koncentrován ve skupinách vysoká a střední relevance (téměř shodně po 30%). Domnívám se však, že jsou všechny naměřené hodnoty poněkud ovlivněny skutečností, že ČR nebyla dosud konfrontována přímým kybernetickým teroristickým útokem velkého rozsahu. Proto je hodnocení expertů zatíženo tímto aspektem. Jinými slovy si všichni oslovení experti uvědomují naléhavost i aktuálnost této hrozby, avšak praktické zkušenosti chybí.

VP02: Druhý výzkumný předpoklad byl zaměřen na ověření šesti faktorové skladby bezpečnostních hrozeb na datech bez chybějících hodnot. A) Faktorová skladba, tvořená 6 společnými faktory, která byla získána se zjištěných relevancí u 34 bezpečnostních hrozeb, se po ověření na datových souborech bez chybějících hodnot nebude výrazně měnit. B) Faktorové složení bezpečnostních hrozeb se u faktorové skladby vypočtené na základě hodnotících stanovisek expertů BIS (n = 57) nebude od původního zjištění výrazně odlišovat.

Pro jeho naplnění bylo nutné učinit tři analytické kroky.

1) Redukovat spojený datový soubor původního rozsahu (n = 731) na datový soubor bez chybějících hodnot na rozsah (**n = 432**) a provést explorační faktorovou analýzu (EFA) u daného výběrového souboru.

2) Redukovat datový soubor za českou republiku (n = 324, součástí je i podsoubor BIS, n = 57) na datový soubor bez chybějících hodnot (**n = 174**) a provést explorační faktorovou analýzu (EFA) u daného výběrového souboru.

3) V případě korekcí v obsahu faktorového modelu použít pro ověření předem připraveného modelu u obou výběrových souborů konfirmační faktorovou analýzu (CFA).

4) Provést faktorovou analýzu bezpečnostních hrozeb u datového souboru expertů BIS (**n = 57**).

Nově uvedený postup pouze doplňuje zjištění, uvedená v jiných částech textu. Jde o pokus zjistit nové skutečnosti na tzv. čistých datech (chybějící data v tomto případě neexistují a nemohou tak negativně ovlivnit výsledky analýzy. U explorační faktorové analýzy je známo, že nepotřebuje testovat teoretický model (jako je tomu u faktorové analýzy konfirmační). Nicméně nemůže být na škodu věci, připustit si určitá omezení, vyplývající z logiky obsahové skladby bezpečnostních hrozeb začleněných do určitých faktorů. Lze předpokládat, že pokud jsou bezpečnostní hrozby spíše přírodního charakteru, měly by být sdruženy do jednoho faktoru. Jiná možnost spočívá v tom, že bezpečnostní hrozby nezáměrného charakteru (určitá nechtěná nebo náhodná selhání) by taktéž mohly být obsahem jednoho nebo více faktorů dle typu bezpečnostní hrozby. Poslední možností je očekávání faktorové příbuznosti u bezpečnostních hrozeb záměrného charakteru. Tyto skutečnosti by mohly napomoci při korekci výsledků faktorové analýzy, které lze označit za problémové.

Výsledkem optimální faktorové skladby u výběrového souboru n = 432 je faktorový model tvořený sedmi faktory (jeho složení, faktorové zátěže a indexy vhodnosti modelu jsou obsahem Přílohy č. 1). Daný model vysvětluje 0,68 % rozptylu na základě vlastních čísel. Není zde splněna podmínka mnohorozměrné variability (Mardiův test).

První faktor je složen z bezpečnostních hrozeb – Kybernetická špionáž; Narušení odolnosti IT infrastruktury; Kyberterorismus; Narušení bezpečnosti eGovernmentu; Nepřátelské kampaně; Hybridní hrozby. Z hlediska obsahu je uvedený faktor obsahově homogenní.

Druhý faktor je složen z bezpečnostní hrozeb – Pravicový extremismus; Levicový extremismus a Politický extremismus. Dané složení lze akceptovat.

Třetí faktor je složen z bezpečnostních hrozeb – Organizovaná daňová kriminalita; Zneužívání veřejných zakázek a rozpočtů; Legalizace výnosů z trestné činnosti; Zneužití legitimních služeb pro účely organizovaného zločinu; Kriminalita spojená s insolvenčním řízením a Prorůstání organizovaného zločinu do veřejné správy. S ohledem na obsah lze skladbu daného faktoru přijmout.

Čtvrtý faktor lze opět akceptovat. Tvoří jej – Narušení dodávek elektrické energie velkého rozsahu; Narušení dodávek plynu velkého rozsahu; Narušení dodávek ropy velikého rozsahu; Surovinová bezpečnost; Průmyslová bezpečnost; Narušení dodávek potravin velkého rozsahu a Narušení dodávek pitné vody velkého rozsahu.

Pátý faktor je složen z bezpečnostních hrozeb – Únik nebezpečné látky; Povodně; Radiační havárie a Dlouhodobé sucho. Z obsahového hlediska by umístění bezpečnostní hrozby – radiační havárie přináleželo spíše do skladby čtvrtého faktoru.

Šestý faktor lze s ohledem na obsah považovat za akceptovatelný. Tvoří jej bezpečnostní hrozby – Neřízená migrace; Islámský radikalismus; Zahraniční bojovníci; Terorismus osamělých vlků a hrozba neúspěšné integrace.

Poslední sedmý faktor je taktéž obsahově homogenní. Tvoří jej – Ovlivňování veřejné správy cizí mocí; Ovlivňování veřejného mínění cizí mocí a Získávání zákonem chráněných informací cizí mocí.

Dílčí závěr: Výše uvedená skladba sedmi faktorového modelu je téměř přijatelná. Všechny uvedené indexy vhodnosti modelu jsou akceptovatelné. Pouze se ukazuje nutnost korekce faktorového zařazení u bezpečnostní hrozby radiační havárie.

Nyní je třeba se podívat na faktorovou skladbu vytvořenou z dat výběrového souboru n = 174. I v tomto případě se jako optimální ukázal model tvořený sedmí faktory (jeho složení, faktorové zátěže a indexy vhodnosti modelu jsou obsahem Přílohy č. 2). Daný model taktéž vysvětluje 0,68 % rozptylu na základě vlastních čísel. V tomto případě je splněna podmínka mnohorozměrné variability (Mardiův test). Skladba jednotlivých faktorů je v naprosté většině shodná jako u modelu na rozsahu výběru n = 432, pouze se zde mění číslo faktoru.

První faktor má stejnou skladbu jako je tomu u modelu v případě rozsahu výběru n = 432. Proto není třeba ho znovu uvádět.

Zajímavé je složení druhého faktoru – Povodně a Únik nebezpečné látky. Zajímavost spočívá v tom, že zde alespoň jedna bezpečnostní hrozba chybí (např. Dlouhodobé sucho).

Třetí faktor má takřka shodnou skladbu bezpečnostních hrozeb jako faktor č. 4 v případě rozsahu výběru n = 432. Pozitivní je zde však to, že je zde zahrnuta i bezpečnostní hrozba – Radiační havárie.

Čtvrtý faktor má stejnou skladbu jako sedmý faktor u výběru n = 432. Pátý faktor má stejnou skladbu jako šestý faktor u výběru n = 432. Šestý faktor má obdobnou skladbu jako třetí faktor u výběru n = 432, je zde však navíc nesprávně umístěna bezpečnostní hrozba – Dlouhodobé sucho. Tato skutečnost si vyžaduje korekci. Poslední sedmý faktor odpovídá složení druhého faktoru u výběru n = 432.

Dílčí závěr: Výše uvedená skladba sedmi faktorového modelu je téměř přijatelná. Všechny uvedené indexy vhodnosti modelu v Příloze č. 2 jsou akceptovatelné. Pouze se ukazuje nutnost korekce faktorového zařazení u bezpečnostní hrozby dlouhodobé sucho. V případě výběrového souboru českých dat (n = 174) je dobře si uvědomit skladbu daného výběrového souboru. Největší zastoupení zde mají experti BIS – 55 osob; dále akademičtí pracovníci PA ČR – 33 osob; příslušníci HZS ČR – 33 osob; příslušníci Policie ČR – 26 osob; úředníci ministerstva vnitra – 18 osob a příslušníci celní správy – 8 osob. Z těchto údajů je zřejmé, že dominantní zastoupení zde mají pracovníci BIS.

Cestou k vyřešení u vedených problémů je použití konfirmační faktorové analýzy (CFA) do které bude vložen tzv. faktorový optimální model řešící potřebné korekce. K výpočtu bude použit komerční software LISREL 8.80. Ověřované faktorové modely se skladbou sedmi faktorů budou cestou CFA vypočteny u obou výběrových souborů. Výsledky CFA obsahují Příloha č. 3 – model pro data n = 432 a Příloha č. 4 – model pro data n = 174. Obě přílohy obsahují sedmi faktorovou skladbu pro každý výběrový soubor dat, faktorové zátěže – regresní koeficienty a t-testy, které ukazují na statistickou významnost jednotlivých regresních koeficientů. Je třeba uvést, že oba faktorové modely jsou téměř totožné, pouze u bezpečnostní hrozby H33 – průmyslová bezpečnost jsou u obou modelů t-testy statisticky nevýznamné (n = 432, regresní koeficient 0,022 a t-test 0,38; n = 174, regresní koeficient 0,13 a t-test 1,43).

Při zvažování této skutečnosti se nabízí otázka, zdali pojem „průmyslová bezpečnost“ je dostatečně konkrétní, aby při hodnocení vyvolával podobnou míru relevance u respondentů. Tento problém se ukazuje jako vhodný pro hlubší posouzení bezpečnostní hrozby – průmyslová bezpečnost.

VP02: S oporou o výsledky konfirmační faktorové analýzy (CFA) lze uvedený, **sedmi faktorový model** bezpečnostních hrozeb dočasně přijmout.[345] V tomto případě lze zamítnou existenci faktorového modelu o šesti faktorech.

Provedení faktorové analýzy 37 bezpečnostních hrozeb u expertů BIS nebylo možné uskutečnit. Podařilo se sice vytvořit polychorickou korelační matici, ale její charakter je pozitivně definitní a neumožňuje provedení faktorové analýzy. V takovém případě použitý software ukončí analytickou činnost.

VP03: Ověření faktorové skladby na datech u výběrového souboru expertů BIS (n = 57) není s použitím programu FACTOR 12. 04. 05, IBM SPSS V26.0 a programu LISREL V8.80 možné. Vzhledem k této skutečnosti budou zjištění učiněná u výběrového souboru n = 174 považována za osvědčená (i s ohledem na převahu v zastoupení expertů BIS u daného výběrového souboru). Relevance

---

[345] Karl Popper mluví o koroboraci teorie jako o jejím osvědčení. Hypotézy nemůžeme prohlašovat za pravdivé, ale můžeme jim dát určité ocenění, tedy můžeme je prohlásit za dočasné domněnky. Viz: POPPER, Karl Raimund. Logika vědeckého bádání. Praha: OIKOYMENH 1997, s. 276
ISBN 80–86005-45-3.

nově zařazených 3 bezpečnostních hrozeb v podání expertů BIS si na své začlenění do faktorové skladby bude muset ještě počkat.

5.KOMPARATIVNÍ ČÁST

5.1. SROVNÁNÍ VÝSKYTU BEZPEČNOSTNÍCH HROZEB ŘAZENÝCH PODLE SKUPIN FAKTOROVÝCH SKLADEB VYSOKÉ RELEVANCE V KONTEXTU PŮSOBNISTI ZPRAVODAJSKÝCH SLUŽEB

Výsledky zjištěné empirickým výzkumem umožňují srovnat relevanci bezpečnostních hrozeb, resp. skupin těchto hrozeb řazených podle zjištěných faktorových skladeb i podle jejich konkrétního zařazení do skupin v pásmu vysoké relevance. Tímto způsobem lze vyvodit první dílčí závěry při pokusech stanovit finální relevanci nejvýznamnějších bezpečnotsních hrozeb ve vztahu k působnosti zpravodajských služeb. K tomuto srovnání byla použita jednoduchá metoda součtu hodnot pouze kladných odpovědí respondentů (tzn. byly sečteny odpovědi hodnot „velmi vysoká“ a „vysoká“ relevance)

5.1.1 Skupiny faktorových skladeb hrozeb zařazené výhradně do pásma vysoké relevance

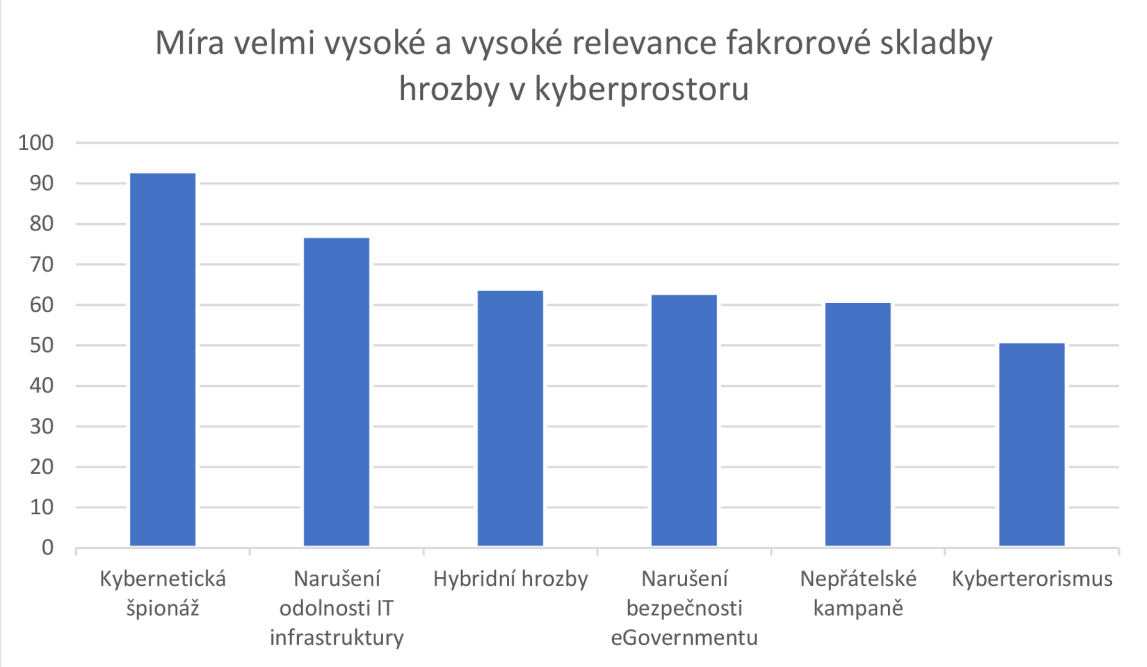
Pouze jedna skupina ze šesti zkoumaných faktorových skladeb hrozeb byla umístěna kompletně do pásma **vysoké** relevance. Jedná se o faktorovou skladbu **hrozeb v kyberprostoru** (*hybridní hrozby, kybernetická špionáž, kyberterorismus, narušení bezpečnosti eGovernmentu, narušení odolnosti IT infrastruktury a nepřátelské kampaně*[346]). Tento výsledek řadí tuto skupinu hrozeb v kybernetickém prostoru z hlediska jejich relevance na čelné místo. Pořadí závažnosti hrozeb této skupiny je následující:

1. Kybernetická špionáž (velmi vysoká relevance 40%, vysoká relevance 53%) **93%**
2. Narušení odolnosti IT infrastruktury (vv 31%, v 46%) **77%**

[346] Řazeno abecedně.

3. Hybridní hrozby (vv 30%, v 34%) **64%**
4. Narušení bezpečnosti eGovernmentu (vv 20%, v 43%) **63%**
5. Nepřátelské kampaně (vv 34%, v 27%) **61%**
6. Kyberterorismus (vv 17%, v 34%) **51%**

Graf č. 42 Míra velmi vysoké a vysoké relevance hrozeb v kyberprostoru



Skutečnost, že naměřený výsledek empirického výzkumu nepřipouští jinou variantu, než je vysoká míra relevance, koresponduje již s výše uvedenými argumenty. Kybernetické hrozby jsou jedny z nejzávažnějších hrozeb bezpečnosti státu. Jsou citelně přítomné jak v současnosti, ale mají velmi vysoký potencionál i v budoucím masivním rozvoji a širokopásmovém nasazení ze strany nepřátelských aktivit cizí moci proti ČR a euroatlantickým spojencům. V boji s těmito hrozbami jsou aktivní všechny tři české zpravodajské služby, i když vedoucí úlohu zde hraje Vojenské zpravodajství. To má ve své nové působnosti z července 2021 zásadní podíl na zajištění kybernetické obrany státu.[347] Klíčovou roli v boji s těmito hrozbami hraje i mezinárodní zpravodajská spolupráce, jako nezbytný předpoklad úspěšnému čelení kybernetickým hrozbám. Výhoda

[347] Zákon č. 150/221 Sb. Dostupné z https://www.zakonyprolidi.cz/cs/2021-150 [online, cit. 2022-09-01] nebo https://www.vzcr.cz/novela-zakona-o-vojenskem-zpravodajstvi-151 [online, cit. 2022-09-01]

mezinárodní spojenecké spolupráce a nezastupitelnost výměny detailních informací (identifikujících např. identitu útočníka podle ustanovených a ztotožněných IP adres) zde netkví pouze v podpůrném benefitu velkých a technologicky mocných států poskytovaným menším spojencům, ale i v podpoře našich kapacit spojencům. Navzdory konstatovanému je nutné poznamenat, že pokud chce ČR těmto hrozbám čelit efektivně, neobejde se to bez velkých finančních investic spojených s náborem a vyškolením nových expertů a nákupem moderní techniky a technologií.

Nejvyšší shoda v pásmu vysoké relevance faktorové skladby hrozeb v kyberprostoru byla zjištěna v případě **kybernetické špionáže** (93%). Nepřátelské kybernetické kampaně formou špionáže, jak již bylo zargumentováno výše, často přicházejí z několika „tradičních" oblastí. Konkrétně je jedná o Ruskou federaci, Čínskou lidovou republiku nebo Íránskou islámskou republiku. Řeč je o vysoce sofistikovaných a často složitě predikovatelných aktivitách protivníka, které mají za cíl nejen získat senzitivní a státem chráněné informace, ale i poškodit ČR jako takovou. Lze rovněž tvrdit, že se především ruské a čínské nepřátelské aktivity táhnou jako červená nit v podstatě všemi bezpečnostními hrozbami této skupiny, ale často i v jiných dalších oblastech. Tato skutečnost znovu potvrzuje, že je Rusko s Čínou nejvýznamnější bezpečnost výzvou z hlediska českých národních zájmů, která nemá v posledních dekádách našeho státu obdoby. Vedle VZ zde hraje aktivní roli i práce obou civilních zpravodajských služeb (BIS a ÚZSI), avšak stávající kapacity zřejmě nebudou pro bezproblémové zvládnutí těchto výzev zcela dostatečné.

Druhou pozici skupiny faktorové sklady hrozeb v kybernetickém prostoru zaujala hrozba **narušení odolnosti IT infrastruktury** (77%). Tato hrozba je pupeční šňůrou spojena s předchozí hrozbou kybernetické špionáže, neboť kromě jiného otevírá cestu k její realizaci. I v tomto případě lze na základě publikovaných částí výročních zpráv českých zpravodajských služeb konstatovat, že hlavní roli v nepřátelských aktivitách proti ČR opět hraje Rusko, Čína nebo Írán.

Třetí pozice je zastoupena skupinou tzv. **hybridních hrozeb** (64%), která je zde sice vnímána jako samostatná hrozba, ale v podstatě v sobě koncentruje mnoho dalších hrozeb a rizik, které se dají označit jako hybridní. I když se nejedná o zcela nový fenomén, má využití hybridních hrozeb velmi vysoký budoucí potenciál. Nejrůznější formy hybridního válčení jsou našimi protivníky nasazovány stále častěji a mnohdy velmi efektivně. Důvodem je nejenom záludnost a často problematická odhalitelností protivníka, ale mnohdy, v porovnání s konvenčním bojem, i podstatně nižší náklady a jejich vysoká efektivita. Hrozba hybridního působení proti bezpečnosti našeho státu je často zneužívána opět našimi tradičními protivníky, v tomto případě především z Ruska za přispění státních i nestátních aktérů.

Jako čtvrtá byla ve skupině kybernetických hrozeb zařazena hrozba **narušení bezpečnosti eGovernmentu** (63%). Jedná se o aktivity, jejichž cílem je poškodit nebo přímo zdecimovat kapacity a schopnosti státu v oblasti výkonu státní správy vůči občanovi. Přechod těchto aktivit do kybernetického prostoru nejenom zjednodušuje, urychluje a zefektivňuje výkon státní moci na úrovni stát – občan, ale díky zranitelnosti těchto systémů vytváří i předpoklad možného zneužití a následné možné paralyzaci celého systému. V katastrofické variantě může způsobit až zhroucení výkonu státní správy.

Páté místo skupiny hrozeb v kybernetickém prostoru zaujala hrozba **nepřátelských kampaní** (61%), která má rovněž významné místo ve využívání kybernetických nástrojů. Jedná se především o zneužití vlivu nejrůznějších sociálních sítí, internetových diskusních platforem nebo o elektronickou poštu, kde lze poměrně levně, ale i rychle a vysoce efektivně rozšířit v mediálním prostoru nejrůznější informace různých podob. Řeč je například o tzv. falešných zprávách nebo přímo dezinformacích, které mají za cíl změnit většinový názor populace ve prospěch protivníka a poškodit vnitrostátní, zahraničněpolitickou nebo bezpečnostní orientaci země. Nepřátelské kampaně tohoto druhu mají velký potenciál a jsou stále sofistikovanější. Na základě zveřejněných informací českých zpravodajských služeb vyvíjejí tuto aktivitu proti bezpečnosti ČR především Rusko a Čína.

Poslední místo ve skupině kybernetických hrozeb představují hrozby **kybernetického terorismu** (51%). ČR společně s dalšími spojeneckými zeměmi vyvíjí značnou aktivitu s maximální snahou těmto hrozbám předcházet. Zde jako nikde jinde platí konstatování, že zneužití těchto prostředků nejrůznějšími teroristickými skupinami světa (ale i nepřátelskými totalitními státy využívající i teroristické aktivity proti svým protivníkům) může způsobit katastrofu fatálních rozměrů. Realizace takových útoků může být pro teroristy nebo jejich skupiny velmi levná a technicky rychle proveditelná. Hrozba spadá do oblasti boje s terorismem, kde je zajištěna působnost celého českého zpravodajského aparátu.

5.1.2. SKUPINY FAKTOROVÝCH SKLADEB ŘAZENÝCH DO PÁSMA VYSOKÉ A STŘEDNÍ RELEVANCE

Na základě posuzovaných kritérií byly bezpečnostní hrozby skupiny faktorové skladby **ohrožení působnosti státu a jeho ekonomické stability** (tj. *kriminalita spojená s insolvenčním řízením, legalizace výnosů z trestné činnosti, organizovaná daňová kriminalita, ovlivňování veřejné správy cizí mocí, prorůstání organizovaného zločinu do veřejné správy, získávání zákonem chráněných informací cizí mocí, zneužití legitimních služeb pro účely organizovaného zločinu a zneužívání veřejných zakázek a rozpočtů*[348]) umístěny výhradně do pásem **vysoké a střední relevance.** Z tohoto důvodu lze konstatovat, že je tato skupina hrozeb z hledika své relevance druhou nejvíce nebezpečnou sérií hrozeb pro českou národní bezpečnost a zcela navazuje na předchozí skupiny hrozeb vysoké relevance.

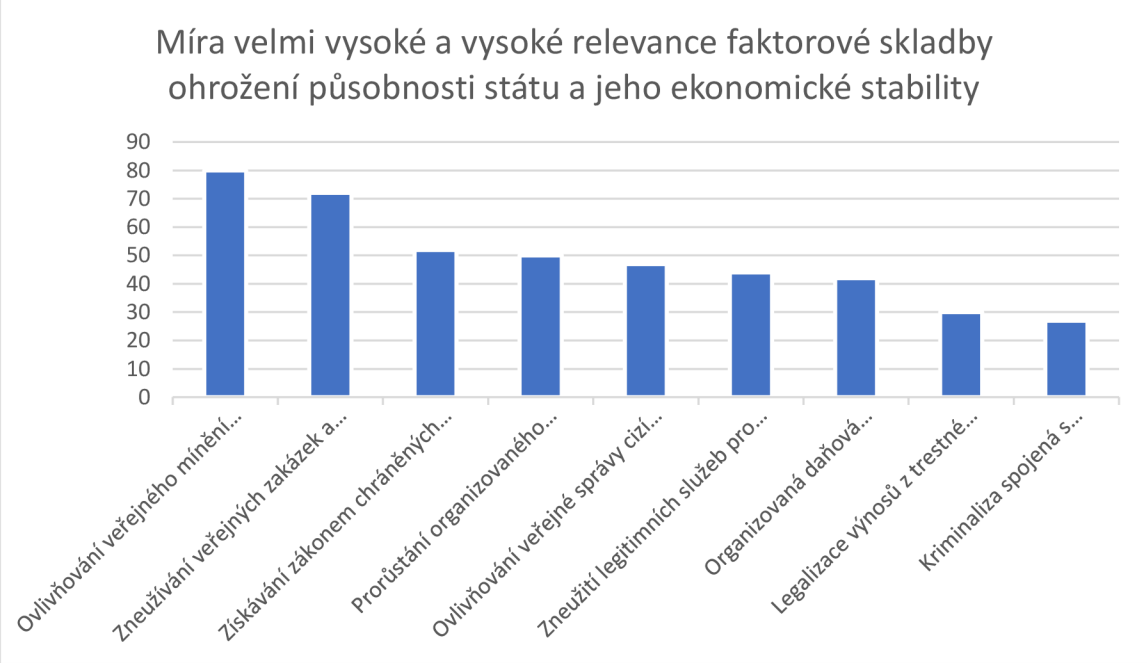
Hrozby obsažené ve skupině faktorové skladby ohrožení působnosti státu a jeho ekonomické stability lze v podstatě rozdělit do dvou základních podskupin. Na hrozby, které mají charakter ohrožení bezpečnosti státu v oblasti **špionážních aktivit a konkrétních nepřátelských zpravodajských aktivit cizí moci proti ČR**

[348] Řazeno abecedně.

(*ovlivňování veřejné správy cizí mocí, ovlivňování veřejného mínění cizí mocí, získávání zákonem chráněných informací cizí moci*) a na hrozby, které obsahují **aktivity organizovaného zločinu, korupce, ekonomické a daňové kriminality** atd. (*kriminalita spojená s insolv*enčním *řízením, legalizace výnosů z trestné činnosti, organizovaná daňová kriminalita, prorůstání organizovaného zločinu do veřejné správy, zneužití legitimních služeb pro účely organizovaného zločinu a zneužívání veřejných zakázek a rozpočtů*). Pořadí závažnosti hrozeb této skupiny je následující:

1. Ovlivňování veřejného mínění cizí mocí (vv 51% a v 29%) **80%**
2. Zneužití veřejných zakázek a rozpočtů (vv 19% + v 53%) **72%**
3. Získávání zákonem chráněných informací cizí mocí (vv 17% + v 35%) **52%**
4. Prorůstání organizovaného zločinu do veřejné správy (vv 16% a v 34%) **50%**
5. Ovlivňování veřejné správy cizí mocí (vv 5% + v 42%) **47%**
6. Zneužití legitimních služeb pro účely OZ (vv 5% + v 39%) **44%**
7. Organizovaná daňová kriminalita (vv 7% + v 35%) **42%**
8. Legalizace výnosů z trestné činnosti (vv 4% + v 26%) **30%**
9. Kriminalita spojená s insolvenčním řízením (vv 2% + v 25%) **27%**

Graf č. 43 Míra velmi vysoké a vysoké relevance ohrožení působnosti státu a jeho ekonomické stability



Graf mj. ilustruje, že z devíti bezpečnostních hrozeb jsou zařazeny v prvních pěti pozicích hrozby z oblasti špionáže a zpravodajských aktivních opatření (*ovlivňovaní veřejného mínění cizí mocí, získávání zákonem chráněných informací cizí mocí a ovlivňování veřejného mínění cizí mocí*) přičemž všechny tyto hrozby se nacházejí pouze v pásmu vysoké relevance. Zbylých šest hrozeb je ze skupiny aktivit organizovaného zločinu, korupce nebo ekonomické a daňové kriminality, přičemž dvě z nich byly zařazeny do pásma vysoké relevance (*zneužívání veřejných zakázek a rozpočtů a prorůstání organizovaného zločinu do veřejné správy)* čtyři v pásmu střední relevance (*zneužití legitimních služeb pro účely OZ, organizovaná daňová kriminalita, legalizace výnosů z trestné činnosti a kriminalita spojená s insolvenčním řízením)*.

Z hlediska působnosti zpravodajských služeb lze konstatovat, že je skupina hrozeb špionážních aktivit a zpravodajských operací proti ČR pokryta aktivitami všech tří českých zpravodajských služeb. Tato skupina hrozeb z oblasti aktivit organizovaného zločinu, korupce a daňové kriminality je z jejich hlediska působnosti vyhrazena především BIS a příslušným policejním útvarům. Svou speciální gesci zde však má i VZ, které se orientuje na aktivity spojené s vojenskou částí tohoto druhu kriminality.

S ohledem na hodnotící metodu lze konstatovat, že je skupina hrozeb faktorové skladby ohrožení působnosti státu a jeho ekonomické stability druhou největší bezpečnostní výzvou nejen pro národní zpravodajské služby. Z určitého hlediska navazuje nebo se prolíná s hrozbami, které byly popsány v první skupině s výhradně vysokou mírou relevance. To platí především pro hrozby se špionážním a zpravodajským charakterem, které jako samostatné položky dominují první desítce nejvíce nebezpečných hrozeb.

5.1.3. SKUPINY FAKTOROVÝCH SKLADEB ŘAZENÉ DO PÁSMA VYSOKÉ, STŘEDNÍ A NÍZKÉ RELEVANCE

Pouze jediná skupina hrozeb seřazených podle faktorové sklady **hrozeb energetických, surovinových, průmyslových a enviromentálních** obsahuje konkrétní bezpečnostní hrozby, které našly své umístění ve všech stanovených pásmech (vysoká, střední i nízká relevance). Důvodem je jednak velké množství konkrétních hrozeb (celkem jedenáct), ale i různorodost jejich obsahu, a proto i byly naměřeny rozdílné hodnoty relevance bezpečnostního ohrožení státu. Skupina zahrnuje intencionální (celkem dvě) i neintencionální hrozby (celkem devět).

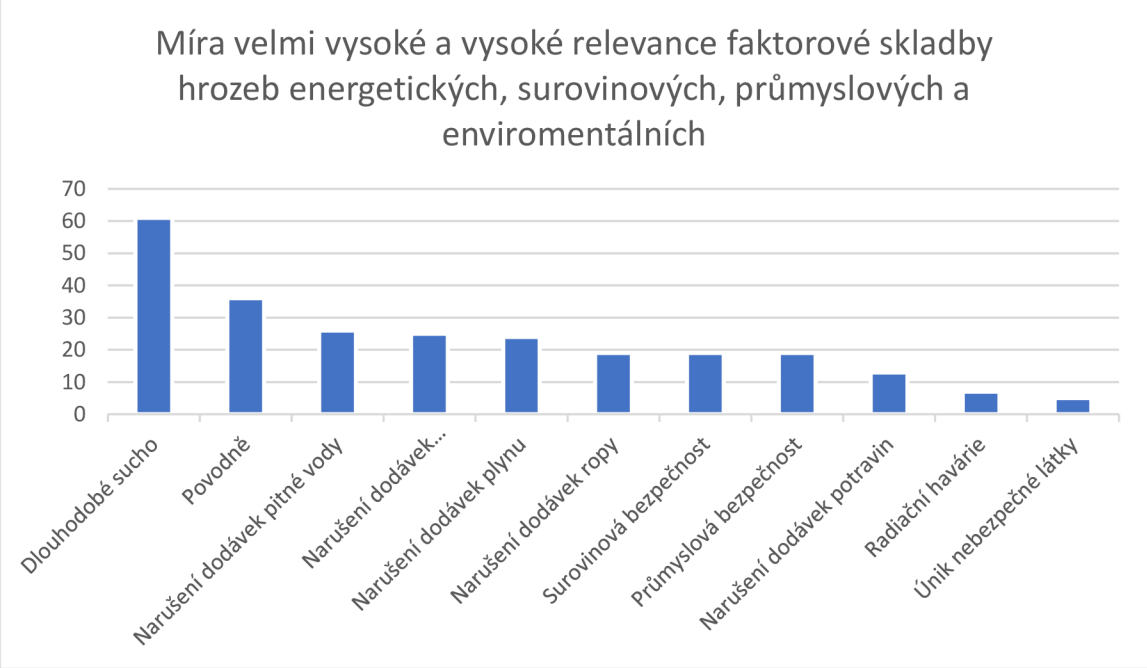
Mezi bezpečnostní hrozby skupiny, které se zařadily do pásma **vysoké** relevance patří pouze jediná (*hrozba dlouhodobého sucha)*, která mj. patří do skupiny neintencionálních hrozeb. Skupina hrozeb **střední** relevance je zastoupena celkem sedmi hrozbami (*narušení dodávek elektrické energie velkého rozsahu, narušení dodávek pitné vody velkého rozsahu, narušení dodávek plynu velkého rozsahu, narušení dodávek ropy velkého rozsahu, povodně, průmyslová bezpečnost a surovinová bezpečnost)*[349]. Hrozby **nízké** relevance zde reprezentují dvě hrozby – hrozba *radiační havárie a únik nebezpečné látky*. Pořadí závažnosti hrozeb této skupiny je následující:

1. Dlouhodobé sucho (vv 23% + v 38%) **61%**
2. Povodně (vv 4% + v 32%) **36%**
3. Narušení dodávek pitné vody velkého rozsahu (vv 12% + v 14%) **26%**
4. Narušení dodávek elektrické energie velkého rozsahu (vv 9% + v 16%) **25%**
5. Narušení dodávek plynu velkého rozsahu (vv 7% + v 17%) **24%**
6. Narušení dodávek ropy velkého rozsahu (vv 7% + v 12%) **19%**
7. Surovinová bezpečnost (vv 7% + v 12%) **19%**
8. Průmyslová bezpečnost (v 19%) **19%**

[349] Vzhledem k tomu, že byl empirický výzkum realizován dávno před vypuknutím ruské války na Ukrajině lze namítnout, že dnes by byly tyto hodnoty zcela jiné a minimálně v energetických otázkách by se řadily na první místo nejvyšší relevance. Výzkum byl však organizován na počátku roku 2019, a tak zohledňuje tento stav.

9. Narušení dodávek potravin velkého rozsahu (vv 7% + v 5%) **13%**
10. Radiační havárie (vv 2% + v 5%) **7%**
11. Únik nebezpečné látky (v 5%) **5%**

Graf č. 44 Míra velmi vysoké a vysoké relevance hrozeb energetických, surovinových, průmyslových a enviromentálních



Zjištěné výsledky empirického průzkumu z roku 2019 naměřené relevance bezpečnostních hrozeb energetické a surovinové skupiny nekorespondují se současnou realitou druhé poloviny roku 2022. Ruská válka na Ukrajině zásadním způsobem změnila význam a akcent některých bezpečnostních hrozeb v čele s hrozbami spojenými s energetickou bezpečností. Putinův režim efektivně využil energetiku jako nástroj nátlaku, ale i boje proti svobodnému světu. Energetika se pro Putinův režim stala klíčovým nástrojem nátlaku na euroatlantickou civilizaci s cílem přimět ji k zastavení pomoci napadené Ukrajině. Jedná se fakticky o další konkrétní příklad hybridního válčení, kdy forma nátlaku nepůsobí prvoplánově jako válka, ale přesto se jedná o jednu z jejích mnoha variant. Tento rozpor v minulé a současné relevanci hrozeb dokumentují na konkrétních příkladech rychlé změny hodnot relevance i dalších bezpečnostních hrozeb, což je průvodním jevem současného stavu světa s rychle se měnící bezpečnostní situací. Na základě

konstatovaného lze opět upozornit na nezbytnost častější aktualizace národních i aliančních strategických bezpečnostních dokumentů (v domácím případě Bezpečnostní a obranné strategie ČR).

Energetické, surovinové, průmyslové a enviromentální hrozby leží z hledika působnosti zpravodajských služeb spíše v oblasti analytické predikce konkrétních rizik nebo kvalifikovaného odhadu možného vývoje realizovaného na základě sběru zpravodajských informací. Zde jsou aktivitní především české civilní zpravodajské služby. Výjimkou jsou teroristické nebo sabotážní aktivity, které by mohly fatálně narušit národní energetickou nebo průmyslovou kritickou infrastrukturu. Vedle zpravodajských služeb jsou zde aktivní především specializované policejní složky. Enviromentální hrozby pak leží zcela mimo působnost zpravodajských služeb.

5.1.4. SKUPINY FAKTOROVÝCH SKLADEB ŘAZENÉ DO PÁSMA VYSOKÉ A NÍZKÉ RELEVANCE

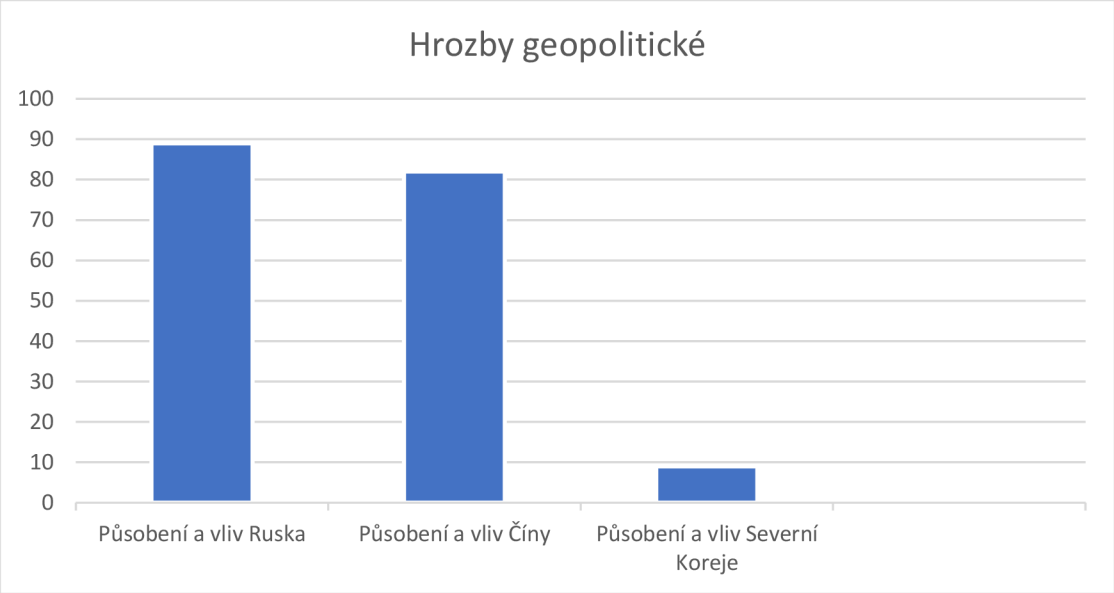
Jedinou skupinou bezpečnostních hrozeb řazených podle faktorové skladby s výskytem konkrétních hrozeb zařazených současně do pásma vysoké a nízké relevance jsou **hrozby geopolitické** (*nebezpečí čínského vlivu, nebezpečí ruského vlivu a nebezpečí severokorejského vlivu)*[350]. Tyto tři bezpečnostní hrozby byly přidány do seznamu hrozeb jako příklady nejčastěji zmiňovaných státních aktérů citovaných ve veřejných částech výročních zpráv českých zpravodajských služeb, dalších bezpečnostních složek, ale i v mediálním prostředí. Jak již vyplývá z celkového seznamu setříděné relevance bezpečnostních hrozeb zaujímá hrozba *působení a vlivu Ruska* bezprecedentní první místo nejvyšší relevance hrozeb, dále hrozba *působení a vlivu Číny* čtvrtou pozici. Výjimkou je hrozba *působení a vlivu Severní Koreje*, která byla zařazena do nízkého pásma relevance. Pořadí závažnosti hrozeb této skupiny je následující:

1. Působení a vliv Ruska (vv 54% + v 35%) **89%**

[350] Řazeno v abecedním pořadí.

2. Působení a vliv Číny (vv 45% + v 37%) **82%**
3. Působení a vliv Severní Koreje (vv 4% + v 5%) **9%**

Graf č. 45 Hrozby geopolitické



Hrozby **působení a vlivu Ruska** a **působení a vlivu Číny** se v podstatě prolínají většinovým spektrem všech zkoumaných bezpečnostních hrozeb. V případě skupiny hrozeb setříděné do faktorové skladby geopolitických hrozeb jsou tyto hrozby sice posuzovány odděleně, ale jejich obsah je přítomný i v mnohých konkrétních hrozbách, které realizují Rusko a Čína jako státní aktéři s nejnebezpečnějším potenciálem ohrožení české a euroatlantické bezpečnosti, státní suverenity a našich národních zájmů. Nízká hodnota relevance v případě bezpečnostní hrozby působení a **vlivu Severní Koreje** však neznamená, že by nebyl severokorejský despotický režim nebezpečný. Zásadním bezpečnostním ohrožením světa severokorejským režimem je jeho jaderný status a ochota použít jaderné zbraně i v rámci tzv. preventivních opatření. Tato politika byla severokorejskými úřady oficiálně ohlášena v září 2022.[351] Možný negativní dopad pravděpodobných severokorejských aktivit na světovou bezpečnost má tudíž

[351] REUTERS, New N.Korea law outlines nuclear weapons use, including preemptive strikes Dostupné z https://www.reuters.com/world/asia-pacific/nkorea-passes-law-declaring-itself-nuclear-weapons-state-kcna-2022-09-08/ [online, cit. 2022_09_09].

velmi vysoký potenciál. Možnosti severokorejského režimu aktivně ovlivňovat bezpečnost přímo v ČR a v dalších evropských zemí jsou však zatím aktuálně nízké. Trojice státních aktérů zařazených do skupiny geografických hrozeb má však i zvláštní úzkou vazbu tím, že tyto nedemokratické režimy pracují často ve shodě. Severokorejský režim by nemohl být takto negativně aktivní bez přímé podpory právě ze strany Ruska a Číny. I když je Severní Korea technologicky velmi zaostalým státem, nemohla by destruktivně působit např. v oblasti kybernetických hrozeb, kdyby nezískala možnost propojení do globálních internetových sítí právě s aktivní podporou Moskvy a Pekingu.

Geografické ohrožení ze strany Ruska, Číny, Severní Koreje, ale i např. Íránu, jsou z hlediska působnosti českých zpravodajských služeb nejhlavnější náplní jejich aktivit. Všechny národní zpravodajské služby vnímají míru rizika bezpečnostního ohrožení ČR ze strany těchto zemí jako vysoce aktuální. I když byl tento stav stejně naléhavý i před zahájením ruské invaze na Ukrajinu v únoru 2022, tato skutečnost relevanci českých zpravodajských aktivit zvýšila na maximum. Ve stínu války na Ukrajině sice také existují hrozby pramenící z nepřátelských aktivit a rozdílných národních zájmů Číny, avšak i tyto hrozby mají vysoký potenciál. Jak bylo již v této dizertaci argumentováno[352], jsou čínské aktivity v pokusech získání vlivu a nadvlády nad demokratickým světem od těch ruských sice poněkud rozdílné, svými možnými důsledky ale mají stejně vysokou destruktivní kapacitu.

5.1.5. SKUPINY FAKTOROVÝCH SKLADEB ŘAZENÉ DO PÁSMA STŘEDNÍ A NÍZKÉ RELEVANCE

Hrozby zařazené výhradně do pásma střední a nízké relevance obsahují dvě skupiny faktorových skladeb hrozeb, tj. **hrozby spojené s migrací a terorismem** a **hrozby extremismu.** Z určitého hlediska se jedná o dvě odlišné skupiny bezpečnostních hrozeb, které však v jistém slova smyslu na sebe

[352] Kapitola 3.4.1.4 A4. PŮSOBENÍ A VLIV ČÍNY

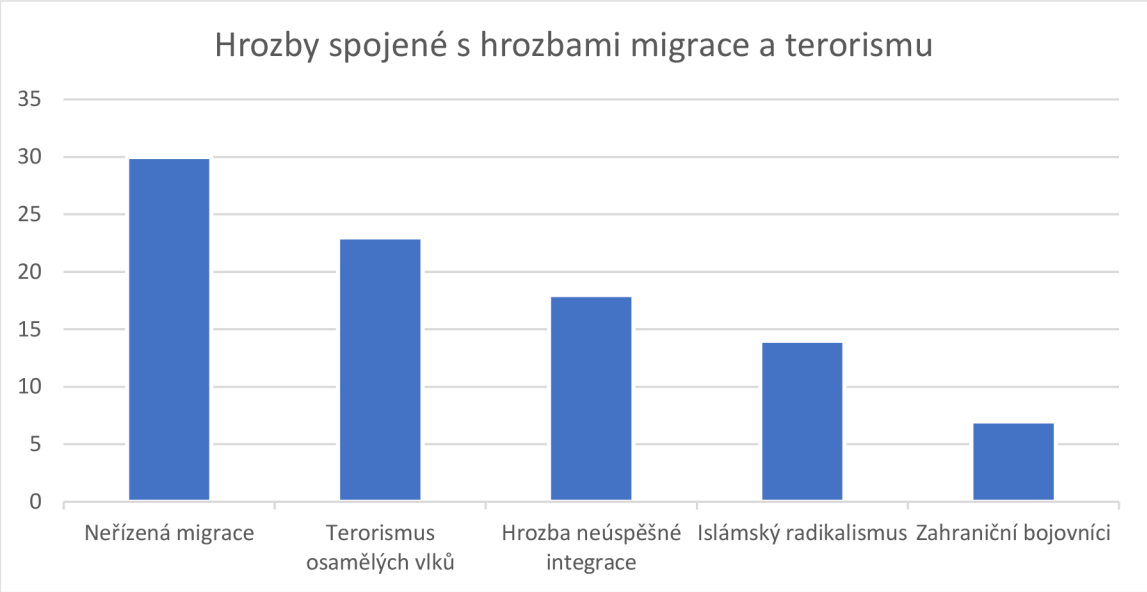
navazují. Řeč je především o otázkách migrace, které jsou častým námětem, resp. obsahem ideologie, reakcí a akcí některých extremistických skupin.

Hrozby spojené s migrací a terorismem sice byly v rámci empirického výzkumu zařazeny do jedné skupiny hrozeb řazených podle zjištěné faktorové skladby, avšak tyto dvě skupiny nelze bez kritického vyhodnocení a priori propojovat. I když možnost zneužití migračních vln teroristickými skupinami je potencionálně pravděpodobná, nejedná se zcela jistě o systémovou záležitost. Cílená a opakovaná přítomnost teroristů v nedávných migračních vlnách nebyla zatím nikým explicitně prokázána. Z tohoto hlediska se jedná spíše o problém implicitní[353]. V opačném případě v určitých částech světa však může velká přítomnost terorismu a tím vyvolaná nestabilita, destrukce a strach nastartovat velké migrační vlny. Z tohoto hlediska je pak propojení hrozeb migrace a terorismu do jedné skupiny zcela legitimní. Pořadí závažnosti hrozeb této skupiny je následující:

1. Neřízená migrace (vv 7% + v 23%) **30%**
2. Terorismus osamělých vlků (vv 7% + v 16%) **23%**
3. Hrozba neúspěšné integrace (v 18%) **18%**
4. Islámský radikalismus (vv 3% + v 11%) **14%**
5. Zahraniční bojovníci (v 7%) **7%**

[353] Oficiální stránky MV ČR v článku Bezpečnostní aspekty migrace ve vazbě migrace a přítomnost teroristů připouštějí pouze „specifické případy“, ovšem bez jejich konkretizace. Dostupné z https://www.mvcr.cz/chh/clanek/bezpecnostni-aspekty-migrace.aspx [online, cit. 2022_09_09].

Graf č. 46 Hrozby spojené s hrozbami migrace a terorismu



Hrozby faktorové skupiny spojené s hrozbami migrace a terorismu mají v působnosti českých zpravodajských služeb zvláštní význam. Především boj s terorismem je jednou z nejdůležitějších aktivit zpravodajských služeb všech států demokratického, západního světa.

Použitá data z empirického výzkumu z r. 2019, odrážejí hrozby *nelegální migrace* především ze zkušeností z velké migrační krize z oblastí Blízkého Východu do Evropy v roce 2015. Další neřízené vlny masové migrace z nestabilních částí světa však mají stále vysoký potencionál a mohou být kdykoliv zopakovány. ČR v současné době čelila vysokému počtu ukrajinských migrantů, kteří byli nuceni uprchnout před ruskou válkou na Ukrajině. V tomto kontextu se však nejednalo o neřízenou migraci, neboť tato vlna uprchlíků byla českými úřady dobře koordinována a velmi kvalitně zvládnuta. Experti BIS hodnotili v roce 2019 neřízenou migraci z hlediska českých bezpečnostních zájmů a její relevance jako relativně nízkou, neboť žádná z masivních migračních vln r. 2015 nemířila finálně do ČR, ale ČR posloužila pouze jako tranzitní země do konečných destinací v bohatých západoevropských státech. Hrozba neřízené migrace však může i v ČR v relativně blízké době znovu silně udeřit.[354]

[354] Dostupné z https://www.seznamzpravy.cz/clanek/domaci-zivot-v-cesku-cesko-zaziva-rekordni-narust-nelegalni-migrace-213597 [online, cit. 2022_09_12].

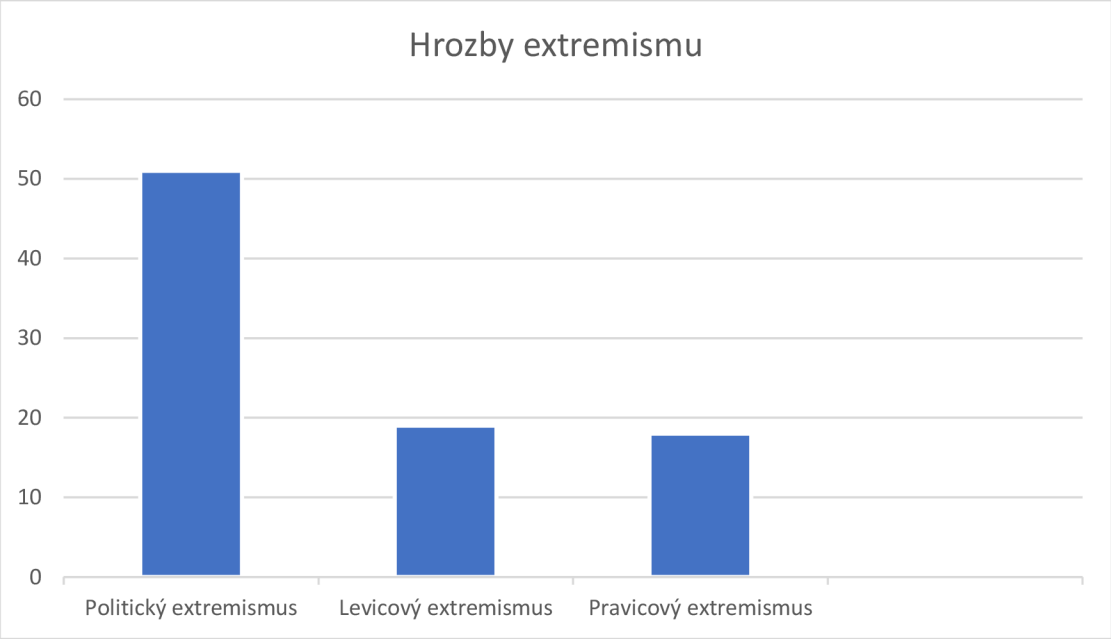
Další pozice z hlediska relevance zaujaly hrozby *terorismu osamělých vlků*, *neúspěšné integrace, islámského radikalismu a zahraničních bojovníků* . Tyto hrozby mají určitou souvislost a bývají často propojeny. Radikálně orientovaní jedinci se mohou díky své neschopnosti integrovat se do většinové evropské společnosti začít aktivně angažovat v rámci nejrůznějších teroristických aktivit. Především hrozba teroristických akcí tzv. osamělých vlků je noční můrou všech zpravodajských služeb, neboť působí nezávisle, přísně utajeně a mohou udeřit kdekoliv a kdykoliv bez možnosti jejich včasného odhalení. I když stále platí, že je ČR z hlediska teroristických útoků spíše bezpečným státem, nebezpečí potencionálních teroristických hrozeb ze strany radikalizovaných jedinců je stále častěji součástí varování v rámci veřejných částí výročních zpráv BIS. Otázkami neřízené migrace a terorismu se však aktivně zabývají všechny české zpravodajské služby.

Druhou skupinou hrozeb zařazených výhradně do pásma střední a nízké relevance jsou **hrozby extremismu** (*levicový extremismus, politický extremismus a pravicový extremismus*[355]*).* Tyto hrozby sice byly v roce 2019 zařazeny do relativně nízkého pásma relevance, avšak jejich potenciál stoupá s ohledem na měnící se kvalitu ekonomické úrovně státu a životních podmínek jejich obyvatel. Platí úměra, že čím je větší ekonomická a společenská krize, tím větší prostor vyplňují aktivity extremistických skupin a politických proudů. Pořadí závažnosti hrozeb této skupiny je následující:

1. Politický extremismus (vv 11% + v 40%) **51%**
2. Levicový extremismus (v 19%) **19%**
3. Pravicový extremismus (vv 4% + v 14%) **18%**

[355] Seřazeno v abecedním pořadí.

Graf č. 47 Hrozby extremismu



Respondenti empirického výzkumu překvapivě zařadili politický extremismus a jeho dvě nejčastější formy (levicový a pravicový extremismus) do celkem rozdílných skupin i z hlediska naměřené relevance. Pokud podle tohoto zjištění představuje politický extremismus vážné ohrožení, potom jeho levicová a pravicová varianta v obou případech vykazuje téměř poloviční hodnotu naměřené relevance, a tudíž podstatně nižší hodnotu. Možným vysvětlením je, že respondenti ve svých reakcích zohlednili vedle levicové a pravicové formy i další varianty této hrozby (např. náboženský, etnický, rasový charakter atd.), které považují za více nebezpečné, než je tomu v případě exaktně chápaných forem levicového a pravicového spektra.

Z hlediska působnosti zpravodajských služeb jsou hrozby extremismu v náplni práce především domácích zpravodajských služeb, i když i zde může hrát svou roli zahraniční přesah hrozby. Největší podíl na eliminaci těchto hrozeb leží na BIS a ve vojenské oblasti na VZ, konkrétně na jeho kontrarozvědné (domácí) části.

5.1.6. POŘADÍ SKUPIN HROZEB SETŘÍDĚNÝCH VE FAKTOROVÝCH SKLADBÁCH A SEŘAZENÝCH PODLE NAMĚŘENÉ RELEVANCE V KONTEXTU PŮSOBNOSTI ČESKÝCH ZPRAVODAJSKÝCH SLUŽEB

Komparace skupin hrozeb řazených podle faktorových skladeb v pásmech vysoké, střední a nízké umožňuje předložit první dílčí výsledek, tj. pořadí závažnosti těchto skupin řazených podle naměřené relevance empirického výzkumu v prostředí analytické skupiny BIS.

1. **hrozby v kyberprostoru** (*hybridní hrozby, kybernetická špionáž, kyberterorismus, narušení bezpečnosti eGovernmentu, narušení odolnosti IT infrastruktury a nepřátelské kampaně)*
2. **ohrožení působnosti státu a jeho ekonomické stability** (*kriminalita spojená s insolvenčním řízením, legalizace výnosů z trestné činnosti, organizovaná daňová kriminalita, ovlivňování veřejné správy cizí mocí, prorůstání organizovaného zločinu do veřejné správy, získávání zákonem chráněných informací cizí mocí, zneužití legitimních služeb pro účely organizovaného zločinu a zneužívání veřejných zakázek a rozpočtů)*
3. **hrozby energetické, surovinové, průmyslové a enviromentální** *(dlouhodobé sucho, povodně, narušení dodávek pitné vody velkého rozsahu, narušení dodávek elektrické energie velkého rozsahu, narušení dodávek plynu velkého rozsahu, narušení dodávek ropy velkého rozsahu, surovinová bezpečnost, průmyslová bezpečnost, narušení dodávek potravin velkého rozsahu, radiační havárie, únik nebezpečné látky)*
4. **hrozby geopolitické** (*nebezpečí ruského vlivu, nebezpečí čínského vlivu a nebezpečí severokorejského vlivu)*
5. **hrozby spojené s migrací a terorismem** (*neřízená migrace, terorismus osamělých vlků, hrozba neúspěšné integrace, islámský radikalismus a zahraniční bojovníci)*
6. **hrozby extremismu** (*politický extremismus, levicový extremismus a pravicový extremismus).*

V rámci vyhodnocení kybernetických hrozeb je patrný určitý rozdíl mezi spojenými tématy kybernetické špionáže, narušení odolnosti IT infrastruktury (zde jsou evidentní spíše nízké odchylky okolo 0,7) a hrozbami získávání zákonem chráněných informací cizí mocí a kybernetického terorismu (zde jsou odchylku vyšší okolo 1,0). Z tohoto hlediska je zajímavý naměřený vyšší průměr i odchylka u klasické špionáže, než je tomu v případě kybernetické špionáže. Kybernetická špionáž vykazuje vyšší průměr a menší odchylku, ale zároveň lze konstatovat, že je jakousi podmnožinou klasické špionáže. Z toho plyne, že **respondenti empirického průzkumu označili kybernetickou špionáž za hrozbu vyšší relevance, než je tomu v případě klasické formy špionáže**. Toto zjištění koresponduje s již konstatovaným, že jsou kybernetické hrozby s ohledem na budoucnost velmi závažnou bezpečnostní hrozbou. Rovněž v případě kybernetického terorismu byl u respondentů zjištěn vyšší průměr, ale zároveň i vyšší odchylka, což napovídá, že ho zřejmě někteří respondenti zařadili na úroveň kybernetické špionáže, což opět naznačuje zásadní akcent udělený kybernetickým hrozbám.

V případě hrozby extremismu lze prohlásit, že byla ve všech případech naměřena vysoká směrodatná odchylka i vysoký průměr a je v podstatě nedůležité, zda se jedná o pravicový nebo levicový extremismus. Tyto hodnoty naznačují, že většina respondentů považuje extremismus za hrozbu spíše nízké relevance, ale byly zaznamenány i zcela protichůdná hodnocení. V tomto případě tedy nelze stanovit jednoznačný průměr směřující k určení skutečně přesné relevance hrozby.

Velmi zajímavá zjištění byla nalezena v případě narušení dodávek energií, surovin, pitné vody atd. Ve všech případech byla zjištěna vysoká směrodatná odchylka (více než 1,0) s průměrem okolo 3. Je zajímavé, že všechny typy dodávek mají velice podobné výsledky – plyn, ropa, elektřina, pitná voda jsou postaveny na velmi podobnou úroveň, přičemž se dalo očekávat podstatně větší odlišení.

Souhrnně lze konstatovat, že jsou **u hrozeb vysoké relevance obecně panuje názorový konsensus respondentů, zatímco u hrozeb nízké relevance je vidět větší názorový rozpor**.

První dílčí závěr empirického výzkumu seřadil skupiny bezpečnostních hrozeb setříděných podle společné faktorové skladby a podle největší naléhavosti v oblasti a) **kybernetické bezpečnosti,** b) **nepřátelských aktivních kampaní cizí moc proti ČR,** c) **ohrožení ekonomické stability státu,** d) **energetické bezpečnosti,** e) **nepřátelských akcí cizích státních aktérů proti ČR,** f) **terorismu a migraci a** g) **extremismu.**

Tento seznam v podstatě koresponduje s aktuálním bezpečnostním a zahraničněpolitickým vývojem ve světě:

- Veškeré lidské aktivity se přesouvají do **kybernetického prostoru** a dnes již neexistuje prakticky žádný druh lidské činnosti, který by nebyl jeho součástí. Rychlý vývoj nových technologií, s akcentem na zjednodušení a zrychlení lidských aktivit, předznamenává jeho další masivní rozvoj. Konkrétními ukazateli tohoto stavu je například rychlý nástup 5G sítí, rozvíjející se programy tzv. umělé inteligence (Artificial Intelligence) nebo kvantové počítače. Kybernetický prostor je však zákonitě i místem stále intenzivnějších pokusů jeho zneužití pro partikulární zájmy jednotlivců, skupin osob, ale i celých států, kteří nalézají jeho slabiny a využívají ho k páchání nejrůznějších druhů nelegálních aktivit. ČR do procesu ochrany kybernetického prostoru investuje nemalé prostředky. Je však zřejmé, že jejich aktuální výše není a nebude dostatečná. Kybernetický prostor se z hlediska útočníků jeví jako hlavní platforma příštího ohrožení lidstva. Výhodou toho jsou malé náklady a vysoký benefit. ČR na tyto trendy reaguje zákonodárnými a institucionálními aktivitami. Z hlediska působnosti zpravodajských služeb poskytuje kybernetický prostor dvě dimenze. První je vnímána z pozice ochrany a obrany českých zájmů a národní bezpečnosti. Druhý rozměr však představuje prostor pro získávání zpravodajsky důležitých informací a jeho význam bude stoupat na úkor

tradičních, dnes běžných zpravodajských metod. Z těchto důvodů jsou nezbytné další investice do náboru, vyškolení a zapracování nových kvalifikovaných kapacit, technického vybavení a dalšího rozvoje. V českých podmínkách jde dnes tímto směrem především VZ s celostátní gescí obrany českého kybernetického prostoru. Obsahem těchto aktivit není jen národní kybernetický prostor bránit, ale v případě nezbytnosti i proti protivníkům účinně útočit. Navzdory řečenému však všechny české zpravodajské služby čeká transformace jejich aktivit z tradičních metod na nové kybernetické metody. To je zřejmě největší výzvou pro budoucí zaměření všech tří českých zpravodajských služeb, neboť právě kybernetická oblast je nejrizikovějším prostředím nejen budoucího, ale již současného soupeření.

- Demokratické země jsou stále více ohrožovány **hybridními způsoby** vedení konfliktu kombinací konvenčních a nekonvenčních prostředků a s využitím stále zákeřnějšího využívání tzv. informační války s pomocí desinformací a falešných zpráv, ale i kybernetických útoků a dalších druhů nátlaku. Hrozba hybridní války je fakticky propojena s ochranou kybernetického prostoru, proto i v této oblasti platí nezbytnost systematické přípravy a nových investic do kapacit českých bezpečnostních civilních a vojenských složek, včetně zpravodajských služeb. Z logiky věci zde má hlavní působnost VZ, avšak i obě civilní služby musí na tyto bezpečnostní hrozby reagovat.

- Boj s **ekonomickými zločiny** je stálicí aktivit nejenom zpravodajských služeb, ale především orgánů činných v trestním řízení. I když ČR udělala za poslední dekády velký krok vpřed, jsou zde ekonomické zločiny stále nejenom přítomné, ale mají podobu více promyšlených aktivit často spojených s organizovaným zločinem. V boji s těmito jevy a s ohledem na působnost zpravodajských služeb je v českých podmínkách nejvíce aktivní BIS, jako významný partner specializovaných policejních složek. Zpravodajské služby však mají pouze informační, a nikoliv vyšetřovací

působnost. Ta podle zákona náleží pouze orgánům činným trestním řízení, což zpravodajské služby nejsou.

- **Energetika** a **energetická bezpečnost** jsou oblastmi, které bývají našimi protivníky stále intenzivněji zneužívány jako nástroj nátlaku, ale i přímé konfrontace. Negativní dopady závislosti některých evropských států (v čele s ČR) na dodávkách strategických surovin z autoritativních, nedemokratických a nespolehlivých zemí se plně projevila jako průvodní jev ruské války na Ukrajině. Moskva použila v průběhu války tento prostředek nejenom jako formu nátlaku na svobodné země s cílem dosáhnout ukončení západní podpory bránící se Ukrajině. Významnějším ruským cílem zde byly záměry poškodit evropské hospodářství, vyvolat nesoulad v sociálním smíru a narušit soudržnost a integritu nejenom EU, ale i konkrétních národních států. České zpravodajské služby v boji s těmito jevy plní úlohu včasného varování formou kvalifikované analytické predikce, ale i prostřednictvím sběru zpravodajských informací důležitých pro vedoucí představitele státu. Výraznější působnost zde mají dvě civilní zpravodajské služby – BIS a ÚZSI.

- Ohrožení ČR z několika **geopolitických** směrů, především z Ruska a Číny, ale i z jiných totalitních států (Írán, Severní Korea atd.) je aktivitami těchto státních aktérů plně propojeno fakticky se všemi zkoumanými bezpečnostními hrozbami. I když tato komparativní část přiřadila geopolitickým hrozbám středně vysokou míru relevance, v projevech konkrétních států (v čele s Ruskem a Čínou) jsou tyto hrozby vnímány jako největší ohrožení bezpečnosti ČR. Působnost zde vyvíjejí všechny tři české zpravodajské služby, které se plně orientují na eliminaci hrozeb mající původ v Rusku, Číně, Íránu atd.

- Svobodný svět je stále výrazněji ohrožen mezinárodním **terorismem** a novými masivními **migračními vlnami** potencionálně směřujícími z postižených oblastí do států relativního dostatku. I když doposud nebyly obě hrozby (terorismus a migrace) v českých národních podmínkách

hodnoceny jako významné, může se situace rychle změnit. Proto jsou obě hrozby vnímány zpravodajskými službami a dalšími bezpečnostními orgány velmi senzitivně, jako potencionální riziko závažného ohrožení české národní bezpečnosti. Mezinárodní výměna informací, jako nezbytný předpoklad úspěšného čelení těmto hrozbám, zde hraje klíčovou roli. Působnost zde mají všechny tři české zpravodajské služby.

- Krize způsobené mixem různých výše jmenovaných okolností bývají intenzivně zneužívány nejrůznějšími populistickými a **extremistickými** proudy, ale i našimi zahraničními protivníky. V případě domácího extremismu hraje nejvýznamnější roli BIS a vnitřní část VZ, v případě zahraničního přesahu např. ve formě zahraniční podpory těmto aktivitám v ČR pak ÚZSI a vnější část VZ.

Z pohledu působnosti českých zpravodajských služeb lze skupiny hrozeb seřazených podle konkrétních faktorových skladeb setřídit takto:

Tabulka č. 50 Působnost českých zpravodajských služeb podle faktorových skladeb

Skupina hrozeb podle jejich faktorové skladby	Působnost BIS	Působnost ÚZSI	Působnost VZ
1.HROZBY V KYBERPROSTORU	**vnitřní bezpečnost státu; prostor pro získávání zpravodajských informací**	**zahraniční přesah hrozby; prostor pro získávání zpravodajských informací**	**vojenské otázky s vedoucí gescí v kybernetické obraně státu; prostor pro získávání zpravodajských informací**
2.OHROŽENÍ PŮSOBNOSTI STÁTU A JEHO EKONOMICKÉ STABILITY	**kontrarozvědná činnost a ekonomická bezpečnost**	**zahraniční aspekty nepřátelských aktivit**	**vojenské aspekty nepřátelských aktivit**
3.HROZBY ENERGETICKÉ, SUROVINOVÉ, PRŮMYSLOVÉ A ENVIREMENTÁLNÍ	**energetická bezpečnost s ohledem na vnitřní ochranu státu**	**energetická bezpečnost, analytické hodnocení zahraničních nepřátelských aktivit**	**dílčí gesce s důrazy na vojenské aspekty**
4.HROZBY GEOPOLITICKÉ	**vnitřní kontrarozvědka**	**zahraniční aktivity státních aktérů ohrožující bezpečnost a zájmy státu**	**všechny aspekty spojené s vojenskou sférou, tj. oblast rozvědná i kontrarozvědná**
5.HROZBY MIGRACE A TERORISMU	**zásadní podíl v oblasti vnitřní bezpečnosti**	**zahraniční přesah obou bezpečnostních hrozeb**	**dílčí gesce ve vojenské oblasti**
6.HROZBY EXTREMISMU	**zásadní podíl gesce v domácích podmínkách**	**dílčí podíl gesce se zahraničním přesahem**	**dílčí podíl gesce v případné vojenské oblasti**

BIS je prakticky jedinou domácí zpravodajskou službou, která má z hlediska národní bezpečnosti klíčovou působnost téměř ve všech skupinách zkoumaných hrozeb. Výjimku tvoří oblast kybernetické bezpečnosti, kde v otázkách kybernetické obrany státu aktuálně hraje vedoucí úlohu VZ. Působnost

VZ se je často shodná se zaměřením BIS, avšak s důrazem na vojenskou oblast, resp. na působnost v gesci ministerstva obrany. BIS i VZ každoročně zveřejňují části svých výročních zpráv, z kterých lze většinu jejich zákonné působnosti vysledovat. ÚZSI jako jediná česká zpravodajská služba nezveřejňuje žádnou část výroční zprávy, čímž veřejně sděluje nejméně podrobností o své zákonných aktivitách. Tato praxe je však v případech zahraničních zpravodajských služeb běžná.

5.1.7. DÍLČÍ ZÁVĚRY I.

Zjištěné pořadí skupin hrozeb setříděných ve faktorových skladbách a seřazených podle naměřené relevance metodou srovnání jednoznačných odpovědí, tj. odpovědí, kde relevance hrozby byla označena pouze v pásmech „velmi vysoké“ a „vysoké“ relevance, umožňuje učinit první dílčí závěr:

a) ***Z hlediska české národní bezpečnosti jsou hrozby s nejvyšší mírou rizika přítomny především A) v kybernetickém prostoru s významným přispěním tzv. B) hybridních hrozeb (např. nepřátelských kampaní, kybernetické špionáže, kyberterorismu, pokusů narušit odolnost IT infrastruktury atd.). Tyto nepřátelské aktivity jsou nejčastěji realizovány ze strany některých C) státních aktérů (především Ruska a Číny), které se snaží destruktivně působit nejenom v politické oblasti (snahy ovlivňovat vnitřní záležitosti ČR a její vnitropolitickou a zahraničněpolitickou orientaci), ale i v otázkách D) narušení energetické a surovinové bezpečnosti ČR s dopady na ekonomickou a sociální stabilitu státu . E) Ekonomická kriminalita má kromě zahraničních vlivů i významnou domácí dimenzi v podobě organizované daňové kriminality, korupce nebo prorůstání organizovaného zločinu do státní správy. F) Hrozby terorismu a G) neřízené migrace nejsou aktuálně vnímány jako naléhavé, ale mají vysoce negativní potenciál, stejně jako nebezpečí eskalace populismu a politického extremismu.***

b) ***V kontextu uvedeného musí české zpravodajské služby (BIS, ÚZSI a VZ) zaměřit svou pozornost především na budování a posilování kapacit a nových metod práce v kybernetické oblasti, ať již formou zvýšených investic s cílem rozšířit stávající počty nových kvalifikovaných expertů, tak i v oblasti jejich vybavení nejmodernější technikou a špičkovými technologiemi.***

5.2. KONKRÉTNÍ HROZBY A JEJICH ŘAZENÍ DO SETŘÍDĚNÝCH FAKTOROVÝCH SKLADEB PODLE RELEVANCE V KONTEXTU PŮSOBNOSTI ČESKÝCH ZPRAVODAJSKÝCH SLUŽEB

5.2.1. HROZBY PÁSMA VYSOKÉ RELEVANCE

První skupina hrozeb zařazených do pásma **vysoké relevance** obsahuje čtrnáct bezpečnostních hrozeb (*působení a vliv Ruska, kybernetická špionáž, ovlivňován veřejného mínění cizí mocí, působení a vliv Číny, ovlivňování veřejné správy cizí mocí, narušení odolnosti IT infrastruktury, zneužívání veřejných zakázek a rozpočtů, hybridní hrozby, nepřátelské kampaně, narušení bezpečnosti eGovernmentu, dlouhodobé sucho, prorůstání organizovaného zločinu do veřejné správy, získávání zákonem chráněných informací cizí mocí a kyberterorismus*) ve čtyřech faktorových skupinách (*hrozby v kyberprostoru, ohrožení působnosti státu a jeho ekonomické stability, geopolitické hrozby a hrozby energetické, surovinové, průmyslové a enviromentální).* Tyto čtyři oblasti představují podle výsledků empirického výzkumu největší bezpečnostní hrozby pro národní bezpečnost ČR. Z logiky věci by měly být zároveň nejdůležitější částí působnosti českých zpravodajských služeb.

Jako samostatná, konkrétní entita empirického průzkumu byla bezprecedentně označena největší bezpečnostní hrozbou hrozba **působení a vlivu Ruska**. Byla zde naměřena nejnižší hodnota průměru (1,6), nízká směrodatná odchylka (0,776), což mj. prokazuje malý názorový rozptyl respondentů a jejich kladné hodnocení relevance hrozby v pásmu „velmi vysoké“ a „vysoké“ závažnosti dosáhlo téměř 90%.

Tabulka č. 51 Působení a vliv Ruska

Průměr	Směrodatná odchylka	Faktorová skupina	Relevance v %	Působnost zpravodajských služeb
1,6	0,776	Geopolitické hrozby	**vv** 54% **v** 35% **s** 7% **n** 4%	BIS ano ÚZSI ano VZ ano

Z geopolitického hlediska se na významné pozici (4. místo) umístila i hrozba spojená s nepřátelskými aktivitami další cizí moci vůči ČR – **působení a vliv Číny.** I v tomto případě byla naměřena nízká hodnota průměru (1,79) a malá směrodatná odchylka (0,895) dokazující relativně malý názorový rozptyl respondentů. Součet jednoznačně kladných reakcí respondentů v pásmu „velmi vysoké“ a „vysoké“ relevance dosáhl více jak 80%.

Tabulka č. 52 Působení a vliv Číny

Průměr	Směrodatná odchylka	Faktorová skupina	Relevance v %	Působnost zpravodajských služeb
1,79	0,895	Geopolitické hrozby	**vv** 44% **v** 37% **s** 16% **n** 3%	BIS ano ÚZSI ano VZ ano

Při podrobném zkoumání zbylých hrozeb zařazených v pásmu vysoké relevance docházíme k závěru, že většina z nich je buď přímo spojena s nepřátelskými aktivitami Ruska a Číny proti ČR nebo jsou tyto země jejich hlavními a někdy i jedinými aktéry. Konkrétně se jedná o tyto hrozby:

- **Kybernetická špionáž** (průměr 1,68; směrodatná odchylka 0,659; součet jednoznačně kladných reakcí respondentů 93%). Nepřátelské aktivity jsou prostřednictvím kybernetické špionáže realizovány především ze strany autoritativních a nedemokratických režimů. Na základě studia veřejných částí výročních zpráv zde hlavní aktivitu vyvíjejí **Rusko s Čínou**, ale i jiné nepřátelské režimy (např. Irán, Severní Korea atd.). Hrozba je tedy spojena především s nepřátelskými aktivitami Moskvy a Pekingu.

- **Ovlivňování veřejného mínění cizí mocí** (průměr 1,74; směrodatná odchylka 0,917 a součet jednoznačně kladných reakcí respondentů 80%). Na základě studia výše uvedených zdrojů zde zásadní roli hraje **Rusko**, které se těmito cestami snaží změnit prozápadní narativ v ČR ve prospěch prosazování svého vlivu. Důležitou část těchto aktivit však hraje i **Čína.**
- **Ovlivňování veřejné správy cizí mocí** (průměr 1,86; směrodatná odchylka 0,895; součet jednoznačně kladných reakcí respondentů 77%). Podle dostupných zdrojů zde hraje klíčovou roli **Rusko**, které se nejrůznějšími formami špionáže, korupce a vydírání snaží získat vliv na místní samosprávy a státní správu jako takovou. Významnou aktivitu zde představují i aktivity organizovaného zločinu získat touto cestou benefit pro jejich nezákonnou činnost.
- **Narušení odolnosti IT infrastruktury** (průměr 1,91; směrodatná odchylka 0,739; součet jednoznačně kladných odpovědí respondentů 77%). Tato hrozba je spojena se všemi dalšími hrozbami v oblasti kybernetické bezpečnosti a představuje základní předpoklad pro páchání dalších nepřátelských aktivit protivníka v oblasti kyberprostoru. Zveřejněné informace zpravodajských služeb v tomto segmentu usvědčují především **Rusko, Čínu** a některé další autoritativní mocnosti z této nepřátelské aktivity.
- **Hybridní hrozby** (průměr 2,11; směrodatná odchylka 0,908; součet jednoznačně kladných odpovědí respondentů 64%). Tento druh hrozeb v podstatě představuje souhrnnou množinu dalších konkrétních hrozeb, které lze považovat za hybridní. Tento způsob nepřátelských aktivit realizovaných především **Ruskem** je v konkrétních aktivitách tvořený celou řadou dalších konkrétních hrozeb, jako jsou např. nepřátelské kampaně, diplomatický, vojenský a politický nátlak, často spojených s problematickou identifikací protivníka.
- **Nepřátelské kampaně** (průměr 2,11; směrodatná odchylka 0,985; součet jednoznačně kladných odpovědí respondentů 61%). Hrozba je realizována nejrůznějšími prostředky především s využitím kybernetických, internetových nástrojů (internetová diskusní fóra, hromadné emaily,

diskusní příspěvky pod novinovými články zveřejněnými v internetových vydáních atd.) s cílem umístit do prostoru narativ, který mění dosavadní kurz. V této oblasti vyvíjí největší aktivitu **Rusko** a opět se jedná o útoky, které jsou realizovány státními i nestátními aktéry, kteří často pracují ve shodě, avšak jejich identita je namnoze těžko odhalitelná.

- **Narušení bezpečnosti eGovernmentu** (průměr 2,25; směrodatná odchylka 0,879; součet jednoznačně kladných odpovědí respondentů 63%). Další konkrétní příklad hybridního kybernetického ohrožení ČR s cílem narušit nebo vyřadit z provozu moderní elektronický nástroj výkonu státní správy směrem k občanovi. V rámci kybernetických nepřátelských aktivit vůči ČR byly tyto aktivity zaznamenány ze strany **Ruska** nebo konkrétních ruských aktérů.
- **Získávání zákonem chráněných informací cizí mocí** (průměr 2,46; směrodatná odchylka 0,965; součet jednoznačně kladných odpovědí respondentů 52%). Bezpečnostní hrozba mající charakter špionážních aktivit vůči ČR jak v kybernetickém prostoru, tak v klasickém slova smyslu. Hrozba tvoří hlavní náplň působnosti zpravodajských služeb kontrarozvědného charakteru, tj. civilních (BIS) nebo vojenských (VZ). Na základě mnohých důkazů předloženými českými bezpečnostními složkami veřejnosti zde klíčovou roli hrají **Rusko a Čína**, jako nejaktivnější zpravodajští hráči.
- **Kyberterorismus** (průměr 2,50; směrodatná odchylka 1,079; součet jednoznačně kladných odpovědí respondentů 54%). Hrozba, která může být využita jak ze strany teroristických organizací nebo jednotlivců, tak ze strany nepřátelských státních aktérů. Jedná se o vysoce nebezpečnou aktivitu, která bude mít stále masivnější využití v budoucnosti s ohledem na přechod všech lidských aktivit do kybernetického prostoru. Hrozba je všemi bezpečnostními složkami vnímána jako vysoce senzitivní. Vzhledem ke skutečnosti, že se **Rusko** jako stát již vůči ČR dopustilo teroristických aktivit (případ Vrbětice), ale i k realitě ruské války na Ukrajině a nepřátelskému postoji Ruska vůči ČR nelze státní aktivity Ruska ani v této oblasti podceňovat.

Zbývající tři bezpečnostní hrozby nelze průkazně spojovat s nepřátelskými aktivitami Ruska a Číny proti ČR:[356]

- **Zneužívání veřejných zakázek a rozpočtů** (průměr 2,11; směrodatná odchylka 0,724; součet jednoznačně kladných odpovědí respondentů 72%). Hrozba spíše spojená s domácími kriminálními aktivitami a organizovaného zločinu. Z hlediska působnosti zpravodajských služeb plně v kompetenci BIS a ve vojenské oblasti VZ.
- **Dlouhodobé sucho** (průměr 2,28; směrodatná odchylka 0,978; součet jednoznačně kladných odpovědí respondentů 61%). Neintencionální hrozba bez aktivit zpravodajských služeb.
- **Prorůstání organizovaného zločinu do veřejné správy** (průměr 2,41; směrodatná odchylka 0,848; součet jednoznačně kladných odpovědí respondentů 50%). Hrozba především v kompetenci BIS.

6. ZÁVĚRY

Dizertační práce se zaměřila na hledání odpovědí na dvě výzkumné otázky:

1. Jaká je relevance bezpečnostních hrozeb obsažených v českých národních bezpečnostních dokumentech pohledem analytické skupiny BIS jako významné autority v oblasti analýzy národní bezpečnosti?
2. Je aktuální zákonná působnost, organizace a koordinace činnosti českých zpravodajských služeb v souladu se stanovenou relevancí národních bezpečnostních hrozeb?

Dříve než přistoupíme k závěrečnému vyhodnocení musíme zopakovat, že tato dizertační práce a její výsledky nemají ambici navrhnout finální model popisu relevance zkoumaných bezpečnostních hrozeb, ani v kontextu toho projektovat nový zpravodajský systém ČR. Práce nabízí jednu z metod, která byla v případě zjišťování relevance bezpečnostních hrozeb použita v rámci realizovaného

[356] V některých případech ekonomické kriminality a organizovaného zločinu je sice přítomna ruská část, ale tyto aktivity nelze a priori spojovat s nepřátelskou činností ruského státu.

empirického výzkumu. Z tohoto hlediska není důležité, že dizertační práce vyhodnocuje data z počátku roku 2019 a není ani podstatné, že vláda ČR již veřejnosti předložila v létě 2023 novou aktualizovanou Bezpečnostní strategii ČR (2023). Zvolená metoda byla založena na pokusu oslovit bezpečnostní experty klíčové zpravodajské služby (BIS) a empirickými prostředky zjistit jejich názory na relevanci celé škály bezpečnostních hrozeb obsažených ve strategických dokumentech ČR platných v roce 2019. Jednalo o experiment, při kterém byly v průzkumu osloveni čeští bezpečnostní experti, kteří mají exkluzivní přístup ke kompletní škále informací důležitých pro bezpečnost ČR. Práce nabízí cestu, jakým způsobem by mohly být měřeny a zobecňovány hodnoty, pokud možno nejpřesnější relevance bezpečnostních hrozeb v daném časovém období. S určením validity jednotlivých bezpečnotsních hrozeb jde ruku v ruce i otázka působnosti zpravodajských služeb, jako významného nástroje boje s těmito hrozbami. Práce se pokusila popsat a zanalyzovat stávající stav a zamyslet se nad jeho možným efektivnějším využitím.

Dynamicky se měnící mezinárodní bezpečnostní situace přímo volá po častějších cyklech odborného posuzování aktuálních bezpečnostních hrozeb, rozhodně častěji než jen v průběhu 5–10 let.

Hodnocený vzorek názorů analytické skupiny BIS by mohl být v případě dalších šetření rozšířen i na další relevantní zástupce bezpečnostních sborů, bezpečnostních expertů na univerzitách a vysokých školách, ale i jiných zainteresovaných odborníků, jejichž názory jsou pro potřeby bezpečnosti státu důležité. Celkově lze tuto skupinu shrnout do pojmu „bezpečnostní komunita ČR“.

Analytici BIS, kteří pracují v každodenní interakci s informacemi domácího i zahraničního původu, se zpravodajskými a jinými bezpečnostními informacemi vlastní i cizí produkce mají z tohoto hlediska určité výjimečné postavení. Ne všechny jejich poznatky se však zákonitě promítají do všech zpravodajských výstupů, které zpravodajskou službu opouštějí. Proto stanovení relevance bezpečnostních hrozeb touto cestou má důležitou vypovídající hodnotu, která je

určována nejen přístupem daných expertů ke konkrétním informacím, ale i jejich pracovními a životními zkušenostmi a jejich odborným portfoliem.

Empirický výzkum byl proveden na vzorku pracovníků analytické skupiny jen jedné, avšak pro vnitřní bezpečnost státu klíčové zpravodajské služby (BIS). Byl sice učiněn pokus, aby se do výzkumu zapojily i dvě zbývající české zpravodajské služby (ÚZSI a VZ), avšak vedení obou služeb účast na tomto výzkumu odmítlo. I když by rozšířené kvantum respondentů o analytiky civilní zahraniční rozvědky a vojenských zpravodajců mohlo poskytnout další zajímavé údaje a naměřené výsledky by mohly ještě více zpřesnit naměřená data (mohla by být provedena i komparativní analýza výsledků zjištěných ve všech třech českých zpravodajských službách), nemyslím si, že není tento „omezený" vzorek dostatečně reprezentativní. Vývoj posledních událostí na mezinárodní scéně a rychlá proměna bezpečnostního prostředí ve světě v porovnání s názory bezpečnostních expertů v roce 2019 a situací dnes jasně dokazuje, že na základě tohoto výzkumu mohou být vyřčeny důležité závěry, minimálně ze dvou důvodů:

Prvním důvodem je již konstatovaná vysoká odbornost dotazovaných expertů, avšak druhým důvodem je i charakter této práce, která primárně nepracuje s aktuálně naměřenými daty a zvolenými algoritmy v daném čase, ale nabízí metodu, jak co možná nejpřesněji určit a akcentovat takové bezpečnostní hrozby, které mají pro národní bezpečnost ČR nejvyšší relevanci. Analyzovaná data mají svůj původ primárně ve dvou hlavních zdrojích. Jednak ve výsledcích empirického výzkumu, který byl ukončen již v roce 2019 a podruhé v národních strategických dokumentech, které primárně posloužily k sestavení kompletní škály bezpečnostních hrozeb, které jsou v těchto materiálech obsaženy, a které byly v empirickém výzkumu zkoumány.

Výsledky empirického výzkumu z roku 2019 přinesly ještě jedno důležité zjištění. Analytici BIS již na počátku roku 2019 označili za nejzávažnější hrozby přesně ty, které jsou i roce 2023 zcela zásadní. Lze tedy právem konstatovat, že se jejich predikce v průběhu několika let plně potvrdila. Dotazovaná expertní skupina analytiků BIS již před několika lety (tj. dlouhou dobu před eskalací

mezinárodní bezpečnostní krize způsobené ruskou agresivní válkou proti Ukrajině), akcentovala ty bezpečnostní hrozby, které přicházejí z Ruska (a z Číny) a označila je za nejvíce nebezpečné i navzdory tomu, že tyto poznatky nekorespondovaly s tehdejšími oficiálními stanovisky určité části domácí politické reprezentace. BIS již v roce 2019 kladla důraz na roli Ruska (a Číny) jako klíčového zdroje bezpečnostního ohrožení českých národních zájmů: politických, vojenských, a v neposlední řadě i ekonomických. Aktivity takto definovaných nepřátelských státních aktérů jsou dále zcela provázány i ve většině kompletní škály zkoumaných bezpečnostních hrozeb.

Vedle již zmíněného geopolitického rozměru je nutné také zdůraznit i další problematiky, např. kybernetickou bezpečnost a s ní spojenou ruskou a čínskou účast ve využívání (resp. zneužívání) všech prostředků, které mají za cíl poškodit naše národní zájmy a zajistit nebo znovuobnovit ruský (a čínský) vliv ve středoevropském a celoevropském prostoru. Jako jasná ukázka může posloužit příklad ruských (a čínských) nepřátelských zpravodajských aktivit, které v domácích podmínkách vyvrcholily Vrbětickou kauzou a v celoevropském a světovém kontextu agresivní ruskou válkou nejen proti Ukrajině, ale i proti celému civilizovanému světu. Konkrétně lze dále vzpomenout např. nepřátelské kampaně realizované s pomocí nejrůznějších hybridních metod nebo sofistikovanou dezinformační válkou či aktivitami ruskojazyčného organizovaného zločinu v ČR atd. Všechny tyto oblasti vyžadují významné posílení kapacit českých zpravodajských služeb.

Již v roce 2019 (a namnoze i dávno předtím) BIS na tyto tendence hlasitě upozorňovala, avšak tehdejší politická reprezentace v čele s bývalým prezidentem M. Zemanem, podobná varování nejen bagatelizovala, ale často je i iracionálně a veřejně odmítala[357]. V našich domácích podmínkách byl tak vytvořen celoevropský unikát, kdy se vládnoucí politická reprezentace nejen nepostavila za práci svých zpravodajských služeb, ale spolupráci s nimi odmítala, mediálně na

[357] Podrobně viz PAĎOUREK, Jan, Rozdílné pohledy českých expertů a politiků na klíčové bezpečnostní hrozby. Jedna středoevropské lekce, New Direction, Brusel, 2021

ně útočila, dehonestovala a v občanském povědomí vytvářela velmi negativní narativy. České zpravodajské služby (a především BIS) se tím dostaly do složité situace, neboť se někteří z jejich zřizovatelů nebo konzumentů jejich zpravodajských informací stali pro jejich práci zásadní překážkou. Někteří zástupci nejvyšších pater české politické scény tak byli pro některé české bezpečnostní organizace v podstatě další, iracionální bezpečnostní hrozbou.

V kontextu zmíněného lze i tímto empirickým výzkumem a s pomocí jeho výsledků doložit, že profesionální (a někdy až vizionářský) charakter práce analytiků a zpravodajců BIS podtrhuje a dokládá celkové schopnosti českých zpravodajců velmi relevantně pracovat s dostupnými informacemi, správně je vyhodnocovat, analyzovat, zařazovat do příslušného kontextu, bez ohledu na politické tlaky, které se snažily nebo mohou snažit tuto tendenci přímo ovlivňovat. I toto je jedním z hlavních důvodů proč předkládaná dizertační práce nabízí cesty měření relevance bezpečnostních hrozeb právě tímto způsobem, a právě za využití expertízy těchto, ale i dalších národních bezpečnostních expertů.

6.1. RELEVANCE BEZPEČNOSTNÍCH HOZEB VS. PŮSOBNOST ZPRAVODAJSKÝCH SLUŽEB

Empirický výzkum pracoval s rozsáhlým počtem konkrétních bezpečnostních hrozeb (celkem 37), které byly obsaženy v národních strategických dokumentech ČR platných v roce 2019, a které byly téměř kompletně analyzovány především v Auditu národní bezpečnosti z roku 2016.[358] Z tohoto počtu má celkem 35 položek intencionální charakter a pouze 2 hrozby jsou neintencionálními bezpečnostními hrozbami[359]. Z hlediska působnosti zpravodajských služeb byla pozornost výzkumu zaměřena především na intencionální bezpečnostní hrozby. Všechny zkoumané položky byly s pomocí explorační faktorové analýzy shromážděných dat seřazeny do 6 faktorových skladeb:

[358] Bezpečnostní strategie ČR 2015, Audit národní bezpečnosti 2026 a Obranná strategie 2017.
[359] Výčet opomíjí velké virové epidemie, které v době realizace výzkum v roce 2019 nebyly ještě zřetelné, avšak v následujícím období se plně promítly v oblasti narušení světového pořádku.

1) ohrožení působnosti státu a jeho ekonomické stability,

2) hrozby v kyberprostoru,

3) hrozby spojené s hrozbami migrace a terorismu,

4) hrozby extremismu,

5) hrozby energetické, surovinové, průmyslové a environmentální,

6) hrozby geopolitické.

Naměřené výsledky ukázaly, že nejvíce relevantní hrozby jsou obsaženy ve dvou faktorových skladbách, konkrétně ve faktorové skladbě **hrozby v kyberprostoru** a **ohrožení působnosti státu a jeho ekonomické stability**. Stejně vysokou relevanci lze však přiřadit i dvěma ze tří zkoumaných bezpečnostních hrozeb setříděných ve faktorové skladbě **geopolitických hrozeb** (tj. vliv Ruska a vliv Číny[360]), neboť zásadní vliv Ruska nebo Číny je patrný ve všech významných bezpečnostních hrozbách obsažených ve faktorových skladbách hrozby v kyberprostoru a ohrožení působnosti státu a jeho ekonomické stability. Pokud tři nejvýznamnější okruhy bezpečnostních hrozeb obsažené v příslušných faktorových skladbách analyzujeme podrobněji (položky 1,2 a 6 výše uvedeného seznamu), lze konstatovat, že jsou i s ohledem na novou verzi Bezpečnostní strategie ČR (2023) i dnes naprosto zásadní. Řeč je o bezpečnostních hrozbách, na kterých byla zjištěna většinová shoda z hlediska použitých identifikátorů, jako je naměřený průměr a určená hodnota směrodatné odchylky. Konkrétně se jedná o tyto hrozby:

[360] Empirický výzkum nepotvrdil, že další zkoumaná bezpečnostní hrozba Působení a vliv Severní Koreje má zásadní dopad na přímé ohrožení bezpečnostních zájmů ČR. Severní Korea je však nástrojem právě Ruska a Číny v mnohých nepřátelských aktivitách a může sehrát (a již hraje) zprostředkovanou roli.

Tabulka č. 53 Top 10 nejvýznamnějších bezpečnostních hrozeb

1. Působení a vliv Ruska
2. Kybernetická špionáž
3. Ovlivňování veřejného mínění cizí mocí
4. Působení a vliv Číny
5. Ovlivňování veřejné správy cizí mocí
6. Narušení odolnosti IT infrastruktury
7. Zneužívání veřejných zakázek a rozpočtů
8. Hybridní hrozby
9. Nepřátelské kampaně
10. Narušení bezpečnosti eGovermentu

Pokud využijeme již výše zpracovaný dílčí závěr této dizertační práce, potom lze konstatovat, že jsou tyto hrozby (snad kromě položky zneužívání veřejných zakázek a rozpočtů) úzce a většinou plně spojené s aktivitami cizích státních aktérů (explicitně Ruska nebo Číny) a s jejich pokusy efektivně zneužívat nejmodernější technologie v různých oblastech života státu, především v kybernetické oblasti. Zaměříme-li se na konkrétní výsledky empirického výzkumu v otázce těchto tří zásadních bezpečnostních hrozeb (vliv Ruska, vliv Číny a kybernetické hrozby) lze souhrnně konstatovat, že ve všech těchto oblastech byla naměřena nízká směrodatná odchylka[361], tzn. že v názorech respondentů panovala nebývalá názorová shoda. Lze proto tvrdit, že na základě naměřených výsledků byla Česká republika v období kolem roku 2019 ohrožována především nepřátelskými aktivitami Ruska a Čína, přičemž zásadní akcent je zde kladen na kybernetickou oblast. Zjištěná data jsou platná v téměř nezměněné podobě i v současnosti. To potvrzují nejen aktuální procesy na

[361] Působení a vliv Ruska – směrodatná odchylka 0,776, Působení a vliv Číny – směrodatná odchylka 0,840 a Kybernetická špionáž – směrodatná odchylka 0,659.

mezinárodní scéně, ale i kriticky zhoršené mezinárodní bezpečnostní prostředí a časté projevy těchto nepřátelských entit přímo vůči ČR.

Z hlediska vyhodnocení závěrů práce s důrazem na působnost zpravodajských služeb lze použít dílčí závěr učiněný na základě analýzy výsledků empirického výzkumu realizovaného v prostředí české domácí zpravodajské služby (BIS). Jedná se v podstatě o shrnutí odpovědi na otázku, jaké jsou nejvíce relevantní hrozby pro českou národní bezpečnost? I když využijeme analýzu dat z roku 2019 je nepochybné, že je aktuální podoba tohoto stavu téměř totožná:

A) Ruská federace, B) Čínská lidová republika a C) některé další nepřátelské režimy (např. Severní Korea nebo Írán) představují hlavní hrozbu pro národní bezpečnost ČR. Rusko společně s Čínou vyvíjejí proti ČR širokou škálu nepřátelských aktivit s masivním využitím všech prostředků v D) kybernetické oblasti (kybernetická špionáž, ovlivňování veřejného mínění, nepřátelské kampaně, ovlivňování veřejné správy, pokusy narušit odolnost národní IT infrastruktury atd.) Děje se tak často za využití E) hybridních forem soupeření (válčení) s účastí jak státních, tak nestátních aktérů. Vedle kybernetické oblasti Rusko i Čína podnikají proti ČR F) nepřátelské špionážní aktivity s cílem získat senzitivní utajované informace, ale i změnit vnitropolitickou, zahraničněpolitickou a bezpečnostní politiku státu a získat tím výhody pro vlastní politiku, ekonomiku a vliv. Rusko zneužívá českou (evropskou) závislost na ruských G) dodávkách strategických surovin jako nástroj vydírání a útoku na ekonomickou, politickou a sociální stabilitu státu s cílem rozvrátit stávající stav a znovuobnovit svůj vliv. Vedle toho představují nelegální H) aktivity domácího i zahraničního organizovaného zločinu, ale i jednotlivců, realizované především v oblasti zneužívání veřejných zakázek a rozpočtů nebo snah o ovlivnění veřejné správy, závažnou bezpečnostní hrozbu s riziky narušení právního a demokratického pořádku země. Bezpečnostní hrozby vysokého rizika reprezentují i některé neintencionální hrozby, které jsou CH) spojené se změnou klimatu (např. hrozba dlouhodobého sucha). Tyto hrozby mohou v případě pokračování negativního vývoje způsobit vážné ekonomické, sociální i politické potíže.

České zpravodajské služby sice proaktivně a dlouhodobě posilují své aktivity a kapacity všemi výše uvedenými směry. Je však nezbytné, aby nadále pokračovaly v úsilí rozvíjet své nové schopnosti především pro eliminaci hrozeb pocházejících od dvou hlavních soupeřů, tj. Ruska a Číny, potencionálně ale i z jiných nepřátelských entit (např. Irán, Severní Korea atd.). Autoritářské státy se totiž snaží systematicky a cíleně narušovat nejenom samu podstatu bezpečnosti státu, ale i jeho zahraničněpolitickou a ekonomickou orientaci a jeho právní a demokratickou podstatu.

Kapacity českých zpravodajských služeb zřejmě nikdy nebudou takové, aby dokázaly účinně čelit všem bezpečnostním hrozbám ve stejné intenzitě a shodné kvalitě. Proto je žádoucí, aby na základě kvalifikovaných analýz hrozeb a rizik došlo k předefinování, resp. trvalé aktualizaci priorit jejich práce. Zpravodajské služby, jako elitní bezpečnostní sbory, by měly být koncentrovány především na takové hrozby, které jsou z hlediska českých národních a euroatlantických zájmů nejvýznamnější a zbylá bezpečnostní ohrožení by měla být spíše v gesci ostatních bezpečnostních sborů (především Policie ČR). Inspirativním příkladem tohoto stavu může být již dříve zmíněná situace britských zpravodajských služeb, které se ve svém zaměření postupně vyprofilovaly do elitních bezpečnotsních institucí, které primárně (a často výhradně) věnují pozornost jen těm nejožehavějším bezpečnostním hrozbám jako je terorismus, špionáž, kybernetická bezpečnost nebo proliferace zbraní hromadného ničení. Například problematikou organizovaného zločinu se britské služby zabývaly pouze v určitém období a pouze v rámci vnitřní zpravodajské služby MI5. Od roku 2006 předala i MI5 gesci boje s organizovaným zločinem britským policejním složkám.[362] Proto i v českých podmínkách stojí za zvážení vytvoření užší profilace zpravodajských služeb na skutečně nejvážnější bezpečnostní hrozby, které jsou dlouhodobě i aktuálně spojeny především s nepřátelskými aktivitami totalitních velmocí (Rusko, Čína), a které jsou řazeny ve faktorových skladbách kybernetická bezpečnost, terorismus

[362] Center for the Protection of National Infrastructure (https://www.cpni.gov.uk/national-security-threats)

(migrace) nebo ohrožení působnosti státu a jeho ekonomické stability. Zaměření na tyto hrozby by měla být rovněž zohledněno specifikami zpravodajské práce, které v určitých případech nejenom nahrazují, ale i významně informačně doplňují práci policie. Jinými slovy by měl být boj s těmi hrozbami, kde mají oproti policii větší možnosti zpravodajské služby, v kompetenci těchto složek a naopak, kde se jedná spíše o policejní charakter práce, tak by zde zpravodajské služby neměly hrát významnou roli. Při sběru informací i v rámci své omezené působnosti zákonitě narážejí zpravodajské služby na informace, které jsou využitelné policií. V těchto případech musí být zajištěno, aby byly relevantní informace policii včas předány, avšak bez reálné zpravodajské gesce.

Systémové změny v zákonné působnosti bezpečnostních složek pochopitelně nejsou realizovatelné ze dne na den a vyžadují důkladnou přípravu. Potencionálním změnám by měla předcházet podrobná analýza zaměřená na stálé posilování bezpečnostních kapacit i mimo zpravodajské struktury, ale také posílení výkonnosti zpravodajských služeb, v již zajišťovaných oblastech, které lze označit za klíčové. Řeč je především o investicích (lidských, ale i materiálních) do schopností čelit všem přicházejícím hrozbám v kybernetické oblasti s ohledem na ty hrozby, které přinášejí nepřátelské aktivity Ruska a Číny. Zúžené portfolio aktivit zpravodajských služeb (resp. přesněji definované portfolio jejich působnosti) se musí zákonitě odrazit ve vyšší efektivitě zpravodajské práce.

Dosažení tohoto stavu při jasně formulovaných gescích v boji s konkrétními bezpečnostními hrozbami má ještě jednu podmínku. Takto pojatá zodpovědnost stanovených gescí (působnosti) se neobejde bez kvalifikované koordinace. Systémová koordinace aktivit jednotlivých bezpečnostních složek, především zajištění jejich optimální spolupráce, vytváření společných týmů pro boj s konkrétními aktuálními hrozbami atd. Zlepšení tohoto stavu může napomoci vládou nově zřízená pozice poradce pro národní bezpečnost.[363] Čas ukáže, zda budou pravomoci a kapacity úřadu národního bezpečnostního poradce české vlády dostatečné i v oblasti koordinace práce zpravodajských služeb nebo zda

[363] Podrobněji dostupné v https://www.vlada.cz/cz/ppov/zmocnenci_vlady/poradce-pro-narodni-bezpecnost-201905/ [online, cit. 2023-01-016]

bude nutný vznik nové pozice vládního koordinátora pro práci zpravodajských služeb (a pravděpodobně i ostatních bezpečnostních složek)[364]. Funkci vládního koordinátora zpravodajských služeb, která je výhradně zodpovědná za jejich optimální spolupráci, ale i za koordinaci jejich zákonné působnosti, má některé vzory v zahraničí. Jako příklad lze opět uvést britský model, který mj. disponuje tzv. Společným (smíšeným) zpravodajským výborem – Joint Intelligence Committee (JIC). Tento výbor s profesionální analytickou kapacitou působící nad analytickými týmy zpravodajských služeb, byl vytvořený na vládní platformě a spadá přímo pod úřad britského premiéra. JIC mj. monitoruje aktuální hrozby a varuje vládu před těmito riziky. Vzhledem k vývoji událostí může vytvářet dočasné koordinační podvýbory a pracovní skupiny, které se zaměřují na boj s konkrétní aktuální hrozbou. V neposlední řadě JIC udržuje spojení i se zahraničními zpravodajskými organizacemi a podle potřeby jim zpřístupňuje své poznatky. Primárně však slouží jako kvalifikovaný orgán syntetizující výstupy britských zpravodajských služeb vládě a jejímu ministerskému předsedovi.[365]

V domácích podmínkách Výbor pro zpravodajskou činnost (VZČ) sice v určitých parametrech připomíná JIC, avšak zcela jistě nemá skutečně koordinační kapacitu nad českými zpravodajskými službami. Pokud by byla v ČR vytvořena efektivní a systémová koordinace zpravodajských služeb (třeba i revoluční transformací VZČ) a zároveň by došlo k aktualizaci priorit (resp. přesnějšímu vymezení) práce zpravodajských služeb, mohlo by to mít pozitivní dopady nejen na vyšší efektivitu zpravodajské práce (a jejich vzájemné spolupráce) v jasně vymezených kompetencích, ale i na přesnější tvorbu rozpočtů, zamezení nežádoucích překryvů zpravodajských aktivit a s tím i spojené nežádoucí konkurence. Nová systémová struktura koordinace zpravodajských služeb se však neobejde bez jasně určených kompetencí tohoto orgánu především vůči zpravodajským službám. Nová pozice koordinátora

[364] Osobní názor autora je, že pozice národně bezpečnostního poradce sice musí se zpravodajskými službami spolupracovat v každodenní nejtěsnější interakci, avšak funkci koordinátora jejich práce musí vykonávat zcela jiná autorita, tj. k tomu speciálně určená.
[365] https://www.gov.uk/government/groups/joint-intelligence-committee [online, cit. 2023-08-05]

zpravodajských služeb, posílená o analytické kapacit by neměla představovat byrokraticky nabubřelý orgán, ale jen malou a efektivní skupinu odborníků.

Stranou lze nyní ponechat současnou skladbu českého zpravodajského aparátu. Po obnovení demokracie v naší zemi po roce 1989 byla v podstatě zkopírována tradiční sktruktura využívaná v předlistopadovém období. Pravdou je, že je tento model běžný i v současných podmínkách většiny evropských zemí. Řeč je o zastaralém členění zpravodajských služeb na vnitřní a vnější civilní službu a na vojenskou zpravodajskou službu. Autor si nemyslí, že nyní nazrál čas na hlubší systémové změny. Porevoluční doba však nabízela i několik jiných a možná i více efektivních variant, které nebyly využity. Autor má na mysli např. vznik jednotné národní zpravodajské služby s civilním a vojenským zaměřením, vnější i vnitřní působností, nebo vytvoření jen dvou zpravodajských organizací – civilní a vojenské atd. Nové bezpečnostní podmínky ve světě a rychlý nástup nových technologií však dříve nebo později povedou i k revoluční proměně struktury a faktického zaměření zpravodajských služeb.

6.2. Bezpečnostní strategie ČR 2023 vs. výsledky empirického výzkumu

Předkládaná dizertační práce je analýzou výsledků empirického výzkumu z roku 2019 a jejich komparace v této době platné Bezpečnostní strategie ČR 2015. Nelze však opominout, že na podzim 2023 přijala Vláda ČR novou bezpečnostní strategii[366], která po osmi letech odráží zásadní změny bezpečnostního prostředí v Evropě a ve světě. Nová bezpečnostní strategie 2023 je konkrétní reakcí na zvyšující se hrozby především ze strany některých státních aktérů (Ruska, Číny, ale i Severní Koreje a Íránu), ale i dalších jevů, které jsou ve své pestré paletě a zvyšující se intenzitě v současnosti i budoucnosti patrně nejvýznamnější (např. nelegální migrace, změna klimatu, epidemie, kybernetická bezpečnost a šíření dezinformací, ekonomická bezpečnost atd.). Nově akcentované bezpečnostní hrozby, resp. zdůraznění jejich relevance umožnuje komparativní analýzu mezi výsledku výzkumu, starou bezpečnostní stratégují

[366] Bezpečnostní strategie České republiky 2023, Praha 2023, ISBN 978-80-7441-099-4, 35 s.

2015 a novou bezpečnostní strategií 2023. V neposlední řadě rovněž poslouží jako závěrečná verifikace výsledků empirického výzkumu, neboť závěry výzkumu zjištěné relevance konkrétních bezpečnostních hrozeb nová redakce Bezpečnostní strategie ČR 2023 většinově potvrzuje. A to především v oblasti nepřátelských aktivit Ruska, Číny nebo jiných totalitních států jako zdroje bezpečnostního ohrožení ČR a euroatlantických spojenců.

Nová bezpečnostní strategie 2023 se od předchozí verze z r. 2015 liší především tím, že zcela mění svůj základní akcent. Strategie 2015 totiž konstatuje, že „*pravděpodobnost přímého ohrožení území ČR masivním vojenským útokem je nízká*“[367]. Bezpečnostní strategie 2023 naopak uvádí, že „*Česko není v bezpečí. Zdrojem ohrožení je zejména výrazně zhoršené mezinárodní prostředí…Válka Ruska proti Ukrajině definitivně ukončila období míru, stability a spolupráce, jemuž se Evropa těšila po konci studené války…*“[368] Strategie 2023 dále konstatuje, že ČR se musí připravit na to, že se stane „*součástí ozbrojeného konfliktu*“[369].

BS ČR 2015 sice celkem podrobně a výstižně popsala hrozby přicházející ze strany některých autoritářských států, avšak tento popis je zcela neadresný a jen dává tušit, o které konkrétní státy se jedná: *„Některé státy usilují o revizi stávajícího mezinárodního uspořádání a jsou připraveny k dosažení svých mocenských cílů použít metod hybridního válčení, kombinujících konvenční i nekonvenční vojenské prostředky s nevojenskými nástroji (propaganda využívající tradiční i nová média, zpravodajské dezinformační akce, kybernetické útoky, politický a ekonomický nátlak, vysílání neoznačených příslušníků ozbrojených sil). Tyto země posilují svůj vojenský potenciál a snaží se budovat si exkluzivní sféry vlivu prostřednictvím destabilizace sousedních zemí a využívání místních konfliktů a sporů.“*[370] Aktuální BS 2023 je ve svých vyjádřeních již zcela transparentní a konkrétní: „*Rusko záměrně působí proti politické, ekonomické a společenské stabilitě v Česku. Je zásadní hrozbou pro naši bezpečnost…Čína zpochybňuje mezinárodní řád. To přináší negativní důsledky i pro euroatlantickou*

[367] BS ČR 2015, IV. Bezpečnostní prostředí, čl. 17, s. 8.
[368] BS ČR 2023, Hlavní sdělení Bezpečnostní strategie České republiky, s. 6.
[369] BS ČR 2023, Hlavní sdělení Bezpečnostní strategie České republiky, s. 6.
[370] BS ČR 2015, Bezpečnostní hrozby, s. 11.

bezpečnost…Rusko a Čínu spojuje zájem oslabit vliv a jednotu demokratických zemí…“[371]

BS ČR 2015 konkrétně jmenuje především tyto klíčové bezpečnostní hrozby:

1. Oslabování mechanismu kooperativní bezpečnosti i politických a mezinárodněprávních závazků v oblasti bezpečnosti (tj. nepřátelské aktivity „některých států“)
2. Nestabilita a regionální konflikty v euroatlantickém prostoru a jeho okolí.
3. Terorismus.
4. Šíření zbraní hromadného ničení a jejich nosičů.
5. Kybernetické útoky.
6. Negativní aspekty mezinárodní migrace.
7. Extremismus a nárůst interetnického a sociálního napětí.
8. Organizovaný zločin.
9. Ohrožení funkčnosti kritické infrastruktury.
10. Přerušení dodávek strategických surovin nebo energie.
11. Pohromy přírodního a antropogenního původu a jiné mimořádné události.[372]

BS ČR 2023 akcentuje především tyto bezpečnostní hrozby:

1. Rusko jako největší a dlouhodobá přímá hrozba.
2. Rusko jako hybridní ohrožení.
3. Čína jako zásadní systémová výzva.
4. Čína jako hrozba ve svém regionu.
5. Další země jako hrozba (Severní Korea, Írán).
6. Západní Balkán jako zdroj nestability.
7. Aktivní konflikty a nestabilita Blízkého východu a severní Afriky.
8. Nelegální migrace.
9. Změna klimatu a životního prostředí.

[371] BS ČR 2023, Hlavní sdělení Bezpečnostní strategie České republiky, s. 6.
[372] BS ČR 2015, Bezpečnostní hrozby, s. 11-12.

10. Pandemie.
11. Kybernetická bezpečnost a dezinformace.
12. Ekonomická bezpečnost.
13. Použití konvenční vojenské síly proti ČR.
14. Použití jaderných zbraní proti ČR.
15. Použití chemických zbraní proti ČR.
16. Terorismus.
17. Katastrofy přírodního a antropogenního původu.[373]

Tabulka č. 54 Srovnání relevance klíčových bezpečnostních hrozeb v BS 2015, BS 2023 a empirickém výzkumu 2019

BS ČR 2015	**BS ČR 2023**	**Empirický výzkum 2019**
Nepřátelské aktivity „některých států“	Rusko jako největší a dlouhodobá přímá hrozba	Působnost a vliv Ruska
Nestabilita a regionální konflikty v euroatlantickém prostoru a jeho okolí	Rusko jako hybridní ohrožení	Kybernetická špionáž
Terorismus	Čína jako zásadní systémová výzva	Ovlivňování veřejného mínění cizí mocí
Šíření zbraní hromadného ničení a jejich nosičů	Čína jako hrozba ve svém regionu	Působnost a vliv Číny
Kybernetické útoky	Další země jako hrozba (Severní Korea, Írán)	Ovlivňování veřejné správy cizí mocí
Negativní aspekty mezinárodní migrace	Západní Balkán jako zdroj nestability	Narušení odolnosti IT infrastruktury
Extremismus a nárůst interetnického a sociálního napětí	Aktivní konflikty a nestabilita Blízkého východu a severní Afriky	Zneužití veřejných zakázek a rozpočtů
Organizovaný zločin	Nelegální migrace	Hybridní hrozby
Ohrožení funkčnosti kritické infrastruktury	Změna klimatu a životního prostředí	Nepřátelské kampaně
Přerušení dodávek strategických surovin nebo energie	Pandemie	Narušení bezpečnosti eGovernmentu
Pohromy přírodního a antropogenního původu a jiné mimořádné události	Kybernetická bezpečnost a dezinformace	Dlouhodobé sucho

[373] BS ČR 2023, Bezpečnostní hrozby a zdroje nestability, s. 15-18.

	Ekonomická bezpečnost	Prorůstání organizovaného zločinu do veřejné správy
	Použití konvenční vojenské síly proti ČR	Získávání zákonem chráněných informací cizí mocí
	Použití jaderných zbraní proti ČR	Kyberterorismus
	Použití chemických zbraní proti ČR	Organizovaná daňová kriminalita
	Terorismus	Politický extremismus
	Katastrofy přírodního a antropogenního původu	Zneužití legitimních služeb pro účely organizovaného zločinu

Na základě srovnání relevance klíčových bezpečnostních hrozeb obsažených v BS ČR 2015, BS ČR 2023 a v empirickém výzkumu 2019 lez konstatovat, že došlo u nejzásadnějších bezpečnostních hrozeb k vyrovnání akcentů zjištěných v empirickém výzkumu z roku 2019 a BS ČR 2023. Oba materiály hodnotí jako nejzávažnější bezpečnostní hrozby nepřátelské aktivity Ruska, resp. Číny. Empirický výzkum zařadil do první desítky nejvýznamnějších hrozeb další konkrétní hrozby, které jsou často nebo výhradně spojovány s nepřátelskými aktivitami Ruska a Číny proti ČR, resp. proti celému euroatlantickému společenství. Konkrétně se jedná o hrozby kybernetické nebo klasické špionáže, ovlivňování veřejného mínění nebo veřejné správy cizí mocí, narušování odolnosti IT infrastruktury, hybridní působení, nepřátelské kampaně nebo získávání zákonem chráněných informací cizí mocí. Tato shoda v důrazu na ruský a čínský element vede k závěru, že výsledky empirického výzkumu z prostředí analytické skupiny BIS byly již v roce 2019 plně shodné s realitou, která se v plné síle projevila o několik let později vypuknutím ruské agrese proti Ukrajině a v posílení nepřátelských ruských a čínských aktivit proti svobodnému světu. Na rozdíl od BS ČR 2015, která sice některé podobné tendence naznačovala, ale nebyla ještě schopna tyto hrozby konkrétně a jasně pojmenovat.

BS ČR 2023, na rozdíl od empirického výzkumu 2019, klade dále v klíčových bezpečnostních hrozbách větší důraz na některé další geopolitické problémy (např. Severní Korea, Írán, Západní Balkán nebo Blízký východ a Severní Afrika). Rovněž akcentuje konkrétní hrozby spojené s možným vojenským

ohrožením našeho prostoru, jako např. je použití konvenční vojenské síly, chemických nebo dokonce jaderných zbraní proti ČR. Tento prvek nebyl v době konání empirického výzkumu tak zřetelný a soudobá realita tento vývoj spíše negovala. Přesto lze tvrdit, že se empirický výzkum a jeho výsledky v nejzásadnějších akcentech shodují s popisem situace v BS ČR 2023, což lze vnímat jako další důležitý výsledek této dizertační práce, a především zvolené metody při určování přesné relevance významných bezpečnotsních hrozeb. Lze také říci, že analytici BIS bez ohledu na tehdejší politickou situaci, resp. fakt odmítání těchto výsledků některými nejvyššími představiteli státu, navzdory domácím překážkám fungovali zcela profesionálně a svými názory, zkušenostmi a profesionalitou již v roce 2019 rozpoznaly hlavní kontury příštího vývoje bezpečnostní situace nejen v ČR, ale i v Evropě a ve světě.

6.3. FINÁLNÍ ZÁVĚRY JAKO ODPOVĚDI NA VÝZKUMNÉ OTÁZKY DIZERTAČNÍ PRÁCE

S ohledem na výše uvedené jako odpovědi na stanovené výzkumné otázky autor předkládá následující závěry:

1. Empirický výzkum realizovaný v roce 2019 explorativní metodou dotazníkové akce v prostředí centrální analytiky Bezpečnostní informační služby ČR (BIS) stanovil s využitím faktorové analýzy dat descendentní relevanci souboru 37 bezpečnostních hrozeb, které byly obsaženy (popsány) v klíčových strategických dokumentech ČR (v Bezpečnostní strategii ČR 2015, v Auditu národní bezpečnosti 2016 a v Obranné strategie ČR 2017). K analýze byl použit volně dostupný freewarový produkt ve verzi FACTOR 10.10.03[374]. V souladu se standardním nastavením programu FACTOR 10.10.01 byla pro extrakci faktorů použita metoda nevážených nejmenších čtverců (ULS – Unweighted Least Squares) a k dosažení jednoduché faktorové struktury metoda faktorové rotace PROMIN.[375] Výzkum se zaměřil na stanovení relevance rozborem každé konkrétní

[374] Jeho autoři jsou URBANO LORENZO-SEVA a PERE JOAN FERRANDO (2012). Manuál i samotný program je dostupný z: http://psico.fcep.urv.es/utilitats/factor/Download.html [online, cit. 2021 08 16].
[375] LORENZO-SEVA, URBANO. (1999). Promin: A method for oblique factor rotation. Multivariate Behavioral Research, 34, s. 347-356.

bezpečnostní hrozby s ohledem na posouzení daného průměru a směrodatné odchylky. Ve spektru oslovených respondentů byl obsažený téměř shodný poměr dotázaných seniorních a juniorních analytiků BIS. Stanovení výsledků s pomocí explorační faktorové analýzy u zkoumaných 37 bezpečnostních hrozeb předpokládalo, že kvantitativní přístup k nalezení širší skladby pro zarámování jednotlivých bezpečnostních hrozeb na základě jejich relevance pro Českou republiku je schopen přinést věcně srozumitelné výsledky. Hlavní výsledky tohoto výzkumu seřadily relevanci bezpečnostních hrozeb v následujícím pořadí:

Tabulka č. 55 Setříděná relevance bezpečnostních hrozeb

	N	Průměr	Směrodatná odchylka
Působení a vliv Ruska	57	1,60	,776
Kybernetická špionáž	57	1,68	,659
Ovlivňování veřejného mínění cizí mocí	57	1,74	,917
Působení a vliv Číny	57	1,79	,840
Ovlivňování veřejné správy cizí mocí	57	1,86	,895
Narušení odolnosti IT infrastruktury	57	1,91	,739
Zneužívání veřejných zakázek a rozpočtů	57	2,11	,724
Hybridní hrozby	56	2,11	,908
Nepřátelské kampaně	56	2,11	,985
Narušení bezpečnosti eGovernmentu	56	2,25	,879
Dlouhodobé sucho	57	2,28	,978
Prorůstání organizovaného zločinu do veřejné správy	56	2,41	,848
Získávání zákonem chráněných informací cizí mocí	57	2,46	,965
Kyberterorismus	56	2,50	1,079
Organizovaná daňová kriminalita	57	2,63	,816
Politický extremismus	57	2,63	1,029
Zneužití legitimních služeb pro účely organizovaného zločinu	57	2,68	,848
Legalizace výnosů z trestné činnosti	57	2,82	,735
Povodně	57	2,91	,950
Kriminalita spojená s insolvenčním řízením	57	3,11	,880
Terorismus osamělých vlků	57	3,19	1,043
Narušení dodávek plynu velkého rozsahu	57	3,25	1,106
Narušení dodávek pitné vody velkého rozsahu	56	3,25	1,254
Narušení dodávek elektrické energie velkého rozsahu	55	3,29	1,212
Narušení dodávek ropy velikého rozsahu	57	3,33	1,091
Surovinová bezpečnost	57	3,35	1,110
Průmyslová bezpečnost	56	3,38	,964
Islámský radikalismus	55	3,55	1,051
Hrozba neúspěšné integrace	57	3,58	1,017
Levicový extremismus	53	3,60	1,098
Pravicový extremismus	54	3,61	1,156
Únik nebezpečné látky	56	3,66	,769
Působení a vliv Severní Koreje	53	3,68	1,015
Zahraniční bojovníci	56	3,77	,894
Narušení dodávek potravin velkého rozsahu	53	3,89	1,171
Neřízená migrace	54	3,91	,917
Radiační havárie	54	4,15	,998

2. Zjištěná relevance 37 bezpečnostních hrozeb demonstruje, že hrozby nejvyššího významu jsou obsaženy především ve třech faktorových skladbách – **hrozby v kyberprostoru** (*kybernetické špionáže, narušení odolnosti IT infrastruktury, hybridní hrozby, nepřátelské kampaně, narušení bezpečnosti eGovernmentu a kyberterorismus*) s nejvyšším výskytem podílu hrozeb řazených v pásmu vysoké relevance (43%); **ohrožení působnosti státu a jeho ekonomické stability** (*ovlivňování veřejného mínění cizí mocí, ovlivňování veřejné správy cizí mocí, zneužívání veřejných zakázek a rozpočtů, prorůstání organizovaného zločinu do veřejné správy a získávání zákonem chráněných informací cizí mocí*) s druhým nejvýše naměřeným podílem hrozeb v pásmu vysoké relevance (36%) a **hrozby geopolitické** (*působení a vliv Ruska a působení a vliv Číny*). Nepřátelské působení Ruska a stále častěji i Číny, které lze označit za hrozby kritické relevance koresponduje i s celkovým pořadím setříděné relevance bezpečnostních hrozeb. Rusko zde jako nejvýznamnější bezpečnostní hrozba zaujímá bezprecedentně první pozici s téměř 90% shodou v pásmech velmi vysoké a vysoké relevance. Čína ze čtvrté pozice výsledné tabulky vykazuje více jak 80% shodu oslovených analytiků v zařazení této hrozby v pásmech velmi vysoké a vysoké relevance. Závažným zjištěním je i skutečnost, že bezpečnostní hrozby obsažené ve jmenovaných třech faktorových skladbách (částečně ale i ve všech ostatních), tj. faktorové skladby kybernetické hrozby, ohrožení působnosti státu a jeho ekonomické stability a hrozby geopolitické, jsou naplněny především nepřátelskými aktivitami Ruska a Číny. Z uvedeného vyplývá, že **hlavní výzvou českých bezpečnostních složek v čele se zpravodajskými službami musí být aktivity vedoucí k eliminaci nepřátelského působení Ruska a Číny proti českým národním zájmům**. Konkrétní hrozby naměřené v pásmu velmi vysoké a vysoké relevance jsou postihnuty v těchto položkách:

- ***Kybernetická špionáž*** *(velmi vysoká relevance 40%, vysoká relevance 53%)* ***93%***
- ***Narušení odolnosti IT infrastruktury*** *(vv 31%, v 46%)* ***77%***
- ***Hybridní hrozby*** *(vv 30%, v 34%)* ***64%***
- ***Narušení bezpečnosti eGovernmentu*** *(vv 20%, v 43%)* ***63%***
- ***Nepřátelské kampaně*** *(vv 34%, v 27%)* ***61%***
- ***Kyberterorismus*** *(vv 17%, v 34%)* ***51%.***

Z těchto závěrů plyne, že **největší výzvou pro českou vládu a pro českou bezpečnostní komunitu musí být boj s hrozbami spojenými s nepřátelskými aktivitami Ruska a Číny především v kybernetické oblasti**. Toto konstatování znamená, že i ve světle aktuálních událostí v oblasti bezpečnostního ohrožení ČR a kriticky zhoršené mezinárodní bezpečnostní situace hrají významnou roli nejmodernější technologie, které s rychlým nástupem umělé inteligence a dalších technologických novinek, svoji intenzitu ještě více urychlí a znásobí tato rizika, budou-li zneužívaná nepřátelskými režimy. Naměřená data relevance bezpečnostních hrozeb z roku 2019 plně korespondují i s aktuální současností, a tuto tendenci významně posilují.

3. Použitý algoritmus empirického výzkumu explorativní metodou dotazníkové akce s využitím faktorové analýzy dat v prostředí centrální analytiky BIS nabízí model, jak i v budoucnosti určovat přesnou relevanci bezpečnostních hrozeb. Pokud budou do těchto výzkumů přizváni i experti dalších bezpečnostních a akademických institucí, kvalitu výzkumu to jenom posílí. Při využití expertízy dalších klíčových expertů může tento model nabídnout nové závěry, využitelné v plánování aktivit českých národních bezpečnostních složek, jejich působnosti nebo efektivnějšímu plánování jejich rozpočtů atd.

4. Z výše konstatovaného vyplývá, že **důležitým akcentem pro práci českých bezpečnostních složek, v čele se zpravodajskými službami,**

musí být kybernetický charakter jejich práce. Toto konstatování je však komplikováno mnohými negativními faktory. Tento směr s sebou nese nezbytnost zásadního navýšení rozpočtů bezpečnostních složek, které se neobejdou bez trvalé modernizace technických zařízení, ale ani bez možnosti náboru, motivace a dlouhodobého uplatnění velkého počtu kvalifikovaných pracovníků s vysokou kybernetickou specializací. Aktuální problém tkví v tom, že skutečně špičkoví IT experti pracují ve státních strukturách v nedostatečném množství, neboť evropské vlády nedokáží konkurovat soukromému sektoru v motivaci zaměstnávat experty na srovnatelné úrovni se soukromou sférou. Určitou cestou by mohla být, vedle změny v nasazení nových vládních investic do kybernetických projektů, ale i zúžená (nově vyprofilovaná) působnost zpravodajských služeb, které musí většinu svých prostředků investovat do rozvoje kybernetických schopností. Schůdnou cestou by mohla být i užší spolupráce státu a soukromého sektoru, který musí být v otázkách zajišťování národní bezpečnosti podstatně více zainteresován. Jak již však bylo konstatováno, stanovení nových působností, resp. přerozdělení stávajících gescí českých bezpečnostních složek není možné realizovat bez kompetentní analýzy dopadů při zohlednění všech relevantních skutečností. Aktuální situace však připouští uplatnění aktualizované prioritizace práce zpravodajských služeb, které již dnes pokrývají velkou většinu aktivit spojených s bezpečnostními hrozbami i s ohledem na aktuální vývoj bezpečnostní situace ve světě. Aktualizovaná prioritizace práce zpravodajských služeb může být předstupněm rozsáhlejších systémových změn, které si vynutí stále se zhoršující kvalita mezinárodní bezpečnostní situace i masivní využívání (resp. zneužívání) moderních technologických kapacit našimi protivníky proti českým národním a bezpečnostním zájmům. Tyto trendy v podstatě předznamenávají velké systémové změny ve všech oblastech lidských aktivit, zpravodajské služby nevyjímaje. Akcent kladený analytiky BIS na hrozby spojené se zneužíváním moderních technologií pouze potvrzuje, že si české zpravodajské služby tento trend uvědomují. Proto je důležité, aby tyto potřeby byly shodně vnímány i vládou, která má ve všech otázkách

působení zpravodajských služeb klíčové pravomoci, včetně jejich zaměření, úkolování a kontroly.

5. Významné bezpečnostní hrozby obsažené ve stále se stupňujících nepřátelských aktivitách nedemokratických režimů (především Ruska a Číny) proti ČR jsou náplní práce zpravodajských služeb již dlouhou dobu. Podle veřejně dostupných zpráv si české zpravodajské služby i v této oblasti vedou kvalitně a jejich práce je oceňována i v zahraničí. Právě mezinárodní přesah těchto aktivit spojený s aktivní spoluprací českých zpravodajských služeb se svými euroatlantickými protějšky (často prostřednictvím vzájemné výměny zpravodajských informací nebo společných operací) je klíčem k pevnějšímu zajišťování bezpečnosti státu. I zde musí být hlavní důraz kladen na rozvoj kybernetických kapacit spojený s rychlým nástupem umělé inteligence a dalších moderních technologií ve vztahu k nepřátelským aktivitám (aktuálním i potenciálním) Ruska a Číny. Dnes již nikdo v Evropě nemůže pochybovat o tom, že je tento směr pro přežití euroatlantické civilizace, jejích hodnot a ideálů, naprosto klíčový.

Závěrečné shrnutí

Empirický výzkum realizovaný v prostředí analytické skupiny BIS, jehož validitu potvrdila aktuální BS ČR 2023 a i aktuální stav bezpečnostního prostředí ve světě s viditelnými tendencemi, prokázal použitelnost zvolené metody při stanovování relevance klíčových bezpečnostních hrozeb s využitím odborného názoru bezpečnostních expertů z české zpravodajské komunity. Použité metody výzkumu napomohly zařadit jednotlivé hrozby nejenom do souhrnných faktorových skladeb, ale především sestavily pořadí relevance jednotlivých bezpečnostních hrozeb ve škále od nejvíce po nejméně závažné. Tento seznam v podstatě určuje i priority práce českých bezpečnostních složek, v čele se zpravodajskými službami.

Zpravodajské služby ČR se dlouhodobě a úspěšně snaží těmto bezpečnostním hrozbám čelit. Rozsah pojmenovaných a analyzovaných hrozeb je však tak rozsáhlý, že není v silách žádné bezpečnostní složky čelit všem hrozbám ve stejné intenzitě a kvalitě. Proto by mohlo být smysluplné předefinovat zaměření českých zpravodajských služeb tak, aby se zpravodajské služby mohly plně soustředit jen na nejzásadnější bezpečnostní výzvy aktuálně a potencionálně ohrožující zájmy ČR (dnes spojené především s ruskými a také čínskými nepřátelskými aktivitami, se zásadním akcentem na budování nových, moderních kapacit v kybernetické oblasti). Tento proces by bylo možné realizovat za podmínky gesčního zapojení ostatních bezpečnostních sborů při vzdorování některým dílčím bezpečnostním výzvám. Za zvážení rovněž stojí transformace českých zpravodajských služeb, stejně jako vytvoření vládní koordinační skupiny s jednoznačně definovanými kompetencemi a pravomocemi. Obojí by by zajistilo efektivnější spolupráci všech tří zpravodajských složek. Rovněž by měla být řešena podřízenost jednotlivých zpravodajských složek konkrétním autoritám. Jako jedna z reálných možností se nabízí podřízenost všech služeb, nebo alespoň těch civilních (ÚZSI stejně jako BIS), přímo vládě. Tento systém by umožnil efektivnější koordinaci, a ještě vyšší efektivitu samotné práce českých zpravodajských služeb.

PUBLIKAČNÍ A EDITORSKÁ ČINNOST AUTORA K OBSAHU DIZERTAČNÍ PRÁCE

- **Impaktovaná studie v databázi SCOPUS**

PAĎOUREK, Jan, MAREŠ Miroslav (2020), The Threats of Russian Influence and Terrorism within National Security Strategies of the Visegrad Four, The Journal of Slavic Military Studies, 33/2, Taylor and Francis Londýn, s. 173-197

- **Kapitoly v monografiích a editorská práce**

KURFÜRST, Jaroslav, PAĎOUREK , Jan (eds.), (2021), Za zrcadlem: Hybridní válka jako staronový fenomén mezinárodních vztahů, nakladatelství Academia, 387 s.

PAĎOUREK, Jan (2020), Civilní zpravodajské služby v kontextu spolupráce s pořádkovou policií, kapitola 11, monografie Pořádková činnost policie, nakladatelství Aleš Čeněk, s. 307-316.

PAĎOUREK, Jan (2021), Rozdílné pohledy českých expertů a politiků na klíčové bezpečnostní hrozby, samostatná studie a sešit New Direction, Brusel 2021, 19 s. Dostupné z https://newdirection.online/2018-publications-pdf/NDreportCZ-Rozdi%CC%81lnePohledy.pdf [online, cit. 2021-08-23]

PAĎOUREK, Jan, KOVAŘÍK Zdeněk (2021). Vnímání významu hybridních hrozeb českou (a slovenskou) bezpečnostní komunitou pohledem empirického výzkumu, 18 s., kapitola 9 kolektivní monografie Za zrcadlem: Hybridní válka jako staronový fenomén mezinárodních vztahů, Academia Editoři publikace KURFÜRST, Jaroslav a PAĎOUREK, Jan.

- **Odborné články v recenzovaných časopisech**

PAĎOUREK, Jan (2019), Organizovaný zločin jako bezpečnostní hrozba v kontextu národních bezpečnostních strategií visegrádských států. Problém neexistence jednotné definice, Bezpečnostní teorie a praxe 3, ISSN 1801-8211, s. 13-26.

PAĎOUREK, Jan (2020), Protidrogová problematika ve Velké Británii. Možné náměty na česko – britskou analytickou spolupráci v oblasti drog, Drugs and Forensics Bulletin, s. 40-46, 2020/3.

PAĎOUREK, Jan, DUBSKÝ Josef, KOVAŘÍK Zdeněk, MLÝNEK Jaromír (2022), Výzkum názorů vysokoškolských studentů policejních akademií v Praze a

v Bratislavě na rusko-ukrajinský konflikt a otázky související, Bezpečnostní teorie a praxe 4, ISSN 1801-8211, s. 45-68.

PAĎOUREK, Jan, KOVAŘÍK Zdeněk (2019), Modeling the factor composition of security threats from the perspective of Czech and Slovak respondents and experts in the CR, Bezpečnostní teorie a praxe 4, ISSN 1801-8211, s. 69-90.

PAĎOUREK, Jan, SABOL, Josef (2021), Důsledky pandemie Covid-19 na pašování drog a jejich konzumaci, Drugs and Forensics Bulletin, s. 43-55, 2021/4.

- **Další studie k tématu v internetových zdrojích**

PAĎOUREK, Jan (2021), Má ředitel zpravodajské služby mediálně vystupovat? The Conservative.online, dostupné z https://archive.theconservative.online/article/ma-editel-zpravodajske-sluzhby-medialn-vystupovat [online, cit. 2023-12-09]

PAĎOUREK, Jan (2021), Tajné nebo zpravodajské služby? The Conservative.online, 2021. Dostupné z https://theconservative.online/article/tajne-nebo-zpravodajske-sluzhby, [online, cit. 2020-011-06]

PAĎOUREK, Jan (2021), Sovětský styl Putinovy bezpečnostní strategie, The Conservative.online, 2021. Dostupné z https://archive.theconservative.online/article/sovtsk-styl-putinovy-nove-bezpechnostni-strategie

PAĎOUREK, Jan (2021), Regionální středoevropská zpravodajská spolupráce jako reakce na aktuální hrozby? The Conservative.online, 2021. Dostupné z https://archive.theconservative.online/article/regionalni-stedoevropska-zpravodajska-spoluprace-jako-reakce-na-aktualni-hrozby

PAĎOUREK, Jan (2021), Exkluzivita českých zpravodajských služeb. Srovnání s Velkou Británií, The Conservative.online, 2021. Dostupné z https://archive.theconservative.online/article/exkluzivita-cheskch-zpravodajskch-sluzheb-srovnani-s-velkou-britanii.

7.LITERATURA

Monografie a samostatné studie

- ANDREW Christopher (2018), The Secret World. A History of Intelligence, Allen Lane, London, ISBN 978-0-300-23844-0

- BALABÁN, Miloš, KRULÍK, Oldřich, KRULÍK, Vladimír, Jan, MORAVEC, Luděk, RAŠEK, Antonín, STEJSKAL, Libor (2012). Proces prioritizace hrozeb pro tvorbu Bezpečnostní strategie České republiky, Obrana a strategie, 1, s. 1-14., ISSN 1802-7199

- BALL, Simon (2020). Secret History: Writing the Rise of Britain's Intelligence Services, London – Chicago 2020, 280 s., ISBN 9780228000822

- CARREL-BILLIARD Francois, WING Christine (2010), North Korea and the NPT, Nuclear Energy, Nonproliferation, and Disarmament: Briefing Notes for the 2010 NPT Review Conference, International Peace Institute New York.

- Civilní kontrarozvědka 1990-1993, kolektiv autorů, vydala BIS 2020, 79 s., 0821 - Obrana

- Civilní rozvědka 1990-1993, kolektiv autorů, vydal ÚZSI 2020, 75 s., 0821 - Obrana

- COLLONA Vilasi (2018), A, The Intelligence Cycle. Open Journal of Political Science, 2018/8, 35-46, dostupné z https://www.scirp.org/pdf/OJPS_2017122815101250.pdf [online, cit. 2019-11-20]

- DEATH OF THE SOVIET UNION: Widespread nostalgia but no going back, IntelliNews, 12/2021. Dostupné z https://intellinews.com/death-of-the-soviet-union-widespread-nostalgia-but-no-going-back-228859/

- DICKINSON, Peter (2020), All roads lead to Ukraine in Putin's global hybrid Dostupné z https://tvaremigrace.cz/res/archive/001/000208.pdf?seek=1582901302 [online, cit. 2022-07-26]

- DVOŘÁK Jan, CHROBÁK Jiří (2018): Zákon o ochraně utajovaných informací: Komentář. Wolters Kluwer, 480 s., ISBN 978-80-7598-017-5

- FELČER Petr (2019). Tváře migrace. MÝTY VERSUS REALITA: Imigrace z Blízkého východu a severní Afriky do České republiky.

- GANOR, Boaz (2005) The Counter-Terrorism Puzzle: A Guide for Decision Makers. New Brunswick, Transaction Publishers, ISBN 9781412806022

- GREIF, Václav (2018), Na insolvence navázaná kriminalita pokračuje, specializované orgány jsou zahlceny. Dostupné z https://www.ceska-justice.cz/2018/06/insolvence-navazana-kriminalita-pokracuje-specializovane-organy-jsou-zahlceny/ [online, cit. 2022-06-08]

- HAM, Peter van (1995), ed., The Baltic States: Security and Defence after Independence, Insitute for Security Studies od WEU, 63 s., ISSN 1017-7566

- HAMM, Mark a SPAAJ, Ramon (2015), Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies, s. 4. Dostupné z https://www.ojp.gov/pdffiles1/nij/grants/248691.pdf [online, cit. 2022-06-08]

- HASSAN SAID Gubara (2015), Radical Islam/ Islamic Radicalism: Towards a Theoretical Framing, Canadian Journal of Sociology. Dostupné z https://www.researchgate.net/publication/266030514_Radical_Islam_Islamic_Radicalism_Towards_a_Theoretical_Framing [online, cit. 2022-07-25]

- HAVLÍK Martin (2015). Sdílení zpravodajských informací v rámci principu „potřeba sdílet" , Vojenské rozhledy 2/2015, s. 83-92, ISSN 1210-3292

- HERMAN, Michael (2001). Intelligence Services in the Information Age: Theory and Practice, Frank Cass Publishers, London 2001, 232 s., ISBN 13: 9780714681962

- HOLMES Kim R. (2015), What is National Security? The Heritage Foundation, 2015 Index of US Military Strength, Washington D.C. s. 17-26

- HURLEY Amy E., SCANDURA Terri A., SCHRIESHEIM Chester A, BRANNICK (1997) Michael: Exploratory and Confirmatory Factor Analysis: Guidelines, Issues, and Alternative. Journal of Organizational Behavior , Vol. 18, No. 6, ss. 667-683 Published by: Wiley. Dostupné z: https://www.jstor.org/stable/3100253

- CHRISTOPHER, Andrew (2018). The Secret World. A History of Intelligence, Allen Lane Publishers, London 2018, 875 s. ISBN 978-0-300-23844-0

- JAKUBCOVÁ, L. (2018), Vnímání bezpečnostních hrozeb pro Českou republiku, Bezpečnostní teorie a praxe, 1/2018, s. 65-83, ISSN 1801-8211

- JAKUBCOVÁ, L. (2018). Vnímání bezpečnostních hrozeb pro Českou republiku, Bezpečnostní teorie a praxe, 1, s. 65-83, ISSN 1801-8211

- JAKUBCOVÁ, L., KOVAŘÍK, Z., BLAŽEK, V. (2018). Odhad faktorové skladby bezpečnostních hrozeb pro Slovenskou republiku a její porovnání s Českou republikou, Bezpečnostní teorie a praxe, 3, s. 45-63, ISSN 1801-8211

- JAKUBCOVÁ, L., KOVAŘÍK, Z., BLAŽEK, V. (2018), Odhad faktorové skladby bezpečnostních hrozeb pro Slovenskou republiku a její porovnání s Českou republikou, Bezpečnostní teorie a praxe, 3/2018, s. 45-63, ISSN 1801-8211

- JAKUBCOVÁ, L., ŠESTÁK, B. a KOVAŘÍK, Z., (2017) Exaktní odhad faktorové skladby bezpečnostních hrozeb pro Českou republiku, Bezpečnostní teorie a praxe, 4/2017, s. 5-21, ISSN 1801-8211

- JAKUBCOVÁ, L., ŠESTÁK, B. and KOVAŘÍK, Z., (2017-2) Exact Estimation of factor composition of security threats for the Czech Republic, Bezpečnostní teorie a praxe, Policejní akademie ČR v Praze, 4/2017, s. 5-19, ISSN 1801-8211

- JOHNSON-CARTEE (2003), Karen S – Copeland, Gary A Strategic Political Communication – Rethinking Social Influence, Persuasion, & Propaganda

- KALOUS, Miroslav (2010). Hlavní metody zpravodajské analýzy a způsoby usuzování, Vojenské rozhledy 3/2010, s. 24-33, ISSN 1210-3292

- KAPLAN, Karel (1993). Sovětští poradci v Československu 1949–1956. Praha: Ústav pro soudobé dějiny AV ČR. Sešity Ústavu pro soudobé dějiny, sv. 14. ISBN 80-85270-26-9

- KARAFFA Vladimír, HRINKO, Martin, ZŮNA, Martin a kol. (2022), Vybrané kapitoly o bezpečnosti, CEVRO INSTUTUT, Praha, 621 s., ISBN 978-80-87125-35-9

- KIRK, Roger E. (2008) Statistics: an Introduction. Fift Edition. Belmont, CA: Thomson Wadsworth , 419 s., ISBN 978-0534564780

- KOVAŘÍK Zdeněk (2024), Projekt empirického výzkumu. Výsledky ověřování výzkumných předpokladů, archiv autora dizertační práce, 7 s.

- KRIEGER, Wolfgang (2011). Dějiny tajných služeb: od faraonů k CIA Vyd. 1. Praha: Vyšehrad, 2011, 325 s. Moderní dějiny (Vyšehrad), ISBN 978-80-7429-170-8

- KURFÜRST, Jaroslav, PAĎOUREK , Jan (eds.), (2021), Za zrcadlem: Hybridní válka jako staronový fenomén mezinárodních vztahů, nakladatelství Academia, 387 s., ISBN 978-80-200-3237-9

- KUTĚJ, Libor (2006). Zpravodajské služby a veřejná informovanost Spektrum 1/2006, s. 25-28.

- LOHSE, Mikael (2020). The Intelligence Process in Finland. Scandinavian Journal of Military Studies, 3(1), s. 68–79.

- LORENZO-SEVA, URBANO. (1999). Promin: A method for oblique factor rotation. Multivariate Behavioral Research, 34, s. 347-356

- LOWENTHAL Mark M, Editor (2016). Intelligence; From Secrets to Policy, 7th Edition, CQ Press, Montgomery, Illinois, 624 s.

- MAREŠ Miroslav, NOVÁK Daniel (2019), Ústavní zákon o bezpečnosti ČR. Komentář, Wolters Kluwer, 236 s., ISBN 978-80-7598-202-5

- MAZARR, Michael a kol. (2019): Hostile Social Manipulation, 303 s., Rand Corporation, ISBN 9781977402608

- McDONALD Roderick, Peter (1991). Faktorová analýza a příbuzné metody v psychologii. Praha: Academia, 252 s., ISBN 0-89859-388-3

- MICHÁLEK, Luděk, Ladislav POKORNÝ, Jozef STIERANKA a Michal MARKO (2013). Zpravodajství a zpravodajské služby. Plzeň, Aleš Čeněk, s.r.o., 2013. 303 s., ISBN 978-80-7380-428-2

- MIMRA, Martin (2001). Komparace metod a terminologie vyhodnocování rizik, dílčí studie S–1–002 Ústavu strategických studií Vojenské akademie v Brně, 30 stran.

- PAĎOUREK, J., KOVAŘÍK, Z. (2019), Modelling the Factor Composition of Security Threats from the Perspective of Czech and Slovak Respondents and Experts in the CR, Bezpečnostní teorie a praxe, Policejní akademie ČR v Praze, 4/2019, s. 69-91, ISSN 1801-8211

- PAĎOUREK, Jan (2020-2), Protidrogová problematika ve Velké Británii. Možné náměty na česko – britskou analytickou spolupráci v oblasti boje s drogami, Drugs and Forensics Bulletin NPC 3/2020, ISSN 1211-8834.

- PAĎOUREK, Jan (2020), Civilní zpravodajské služby v kontextu spolupráce s pořádkovou policií, kapitola 11, In Pořádková činnost policie, nakladatelství Aleš Čeněk, s. 307–320, ISBN 978-80-7380-793-1

- PAĎOUREK, Jan (2021), Rozdílné pohledy českých expertů a politiků na klíčové bezpečnostní hrozby, studie New Direction, Brusel, 19 s. Dostupné z https://newdirection.online/2018-publications-pdf/NDreportCZ-Rozdi%CC%81lnePohledy.pdf [online, cit. 2021-08-23]

- PAĎOUREK, Jan (2021), Tajné nebo zpravodajské služby? The Conservative.online, 2021. Dostupné z https://theconservative.online/article/tajne-nebo-zpravodajske-sluzhby, [online, cit. 2020-011-06]

- PAĎOUREK, Jan, KOVAŘÍK Zdeněk. Vnímání významu hybridních hrozeb českou (a slovenskou) bezpečnostní komunitou pohledem empirického výzkumu, 18 s., kapitola 9 kolektivní monografie o hybridních hrozbách, která vyjde v r. 2021 v nakl. Academia. Editoři publikace KURFÜRST, Jaroslav a PAĎOUREK, Jan, ISBN 978-80-200-3237-9

- PAĎOUREK, Jan, MAREŠ Miroslav (2020), The Threats of Russian Influence and Terrorism within National Security Strategies of the Visegrad Four, The Journal of Slavic Military Studies, 33/2, Taylor and Francis Londýn, ISSN 1351-8046, s. 173-197

- PACHTA Lukáš, Věra ŘIHÁČKOVÁ Věra (2009) (ed.). Příspěvek k debatě o reformě zpravodajských služeb v České republice, Obrana a strategie, s. 107-112, 2/2009, ISSN 1802-7199

- PERNICA, Bohuslav (2008). Riziko ztráty lidského kapitálu při transformaci architektury bezpečnostního systému na příkladu českých zpravodajských služeb, Vojenské rozhledy 2/2008, s. 64-67, ISSN 1210-3292

- PHYTHIAN, Mark (2013). Understanding of Intelligence Cycle (Studies of Intelligence), New York, ISBN-10: 1138856320.

- POKORNÝ, Ladislav (2007). Základy právní úpravy činnosti zpravodajských služeb. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, 73 s., ISBN 978-80-7251-242-3

- POKORNÝ, Ladislav (2012). Zpravodajské služby, jejich působnost a oprávnění, Bezpečnostní teorie a praxe, Praha, 2/2012, ISSN 1801-8211

- POKORNÝ, Ladislav (2012). Zpravodajské služby. 1. vyd. Praha, Nakl. Auditorium, 2012, 150 s., ISBN 978-80-87284-21-6

- POKORNÝ, Ladislav (2013). K otázce právní regulace existence a činnosti zpravodajských služeb, Časopis pro právní vědu a praxi, 21/2013, s. 380-388, ISSN 1210-9126

- POKORNÝ, Ladislav (2014). K otázce vymezení oprávnění zpravodajských služeb, Policejná teória a prax 3/2014, 12 s., ISSN 1335-1370

- POPPER Karl Raimund (1997). Logika vědeckého bádání. Praha: OIKOYMENH, 617 s., ISBN 80-86005-45-3

- Problémy spravodajských služieb v otvorenej spoločnosti: Zborník príspevkov zo sympózia Bratislava 7. decembra 2011. 1. vyd. Bratislava: Eurokódex, 2012, 96 s.

- RICHARDS, Julian (2012). A Guide to National Security: Threats, Responses and Strategies, Oxford University Press, 177 s., ISBN 9780199655069

- ŘEHKA, Karel (2017): Informační válka, Academia, 224 s., ISBN 978-80-200-2770-2

- SMOLÍK, Josef, ŠMÍD Tomáš (2010). Vybrané bezpečnostní hrozby a rizika 21. století. Masarykova univerzita Brno, Ediční řada Monografie, sv. 33, 276 s., ISBN 978-80-210-5288-8

- SUTHERLAND, Edwin H. (1940), White-Coller Criminality, American Sociological Review 5, N. 1, s. 1-12, ISSN 1939-8271

- SYROVÁTKA Jonáš, PINKAS ŠIMON (2021), kapitola CZECHIA, War on People's Hearts and Minds. Societal vulnerabilities to the Kremlin's influence in Central and Eastern Europe & the Western Balkans, s. 11, GLOBSEC Bratislava

- TAYLOR, Philip M. (2003): Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Day. 3rd Edition. Manchester: Manchester University Press, ISBN 978-0719067679

- TOPINKA Daniel (Ed.) (2016). Muslimové v Česku. Etablování muslimů a islámu na veřejnosti. Brno, Barrister a Principal, ISBN 9788074851155

- TVRDÁ, Kateřina (2018). Vnitřní bezpečnostní sbory a zpravodajské služby ve střední Evropě, Centrum pro studium demokracie a kultury, Masarykova univerzita, 1. vyd. Brno, 273 s. Politologická řada, sv. č. 70, 2018, ISBN 978-80-7325-465-0

- URBANO LORENZO-SEVA a PERE JOAN FERRANDO (2012). Manuál i samotný program je dostupný z: http://psico.fcep.urv.es/utilitats/factor/Download.html [online, cit. 2021_08_16]

- WILDE, de J.H. (2001). New Threats on the Security Agenda. M.Drent, D.Greenwood, P.Volten (eds.) „Towards Shared Security, 7 – Nation Perspectives", Harmony Papers No. 14, The Centre of European Security Studies, s. 91—115

- WILLIAMS Kieran, DELETANT, Dennis (2001). Security Intelligence Services in New Democracies: The Czech Republic, Slovakia and Romania, Palgrave, London 2001, 271 s., ISBN 1349403091

- WILSDORF, Jan Ondřej (2020), Praní peněz optikou trestního zákoníku, portál epravo.cz. Dostupné z https://www.epravo.cz/top/clanky/prani-penez-optikou-trestniho-zakoniku-110566.html#_ftn1 [online, cit. 2022-05-31]

- ZEMAN Petr (2008), Co je zpravodajství? Pokusy o definici pojmu a problémy překladu, webový portál Asociácie bývalých spravodajských dôstojníkov Slovenska

- ZEMAN, Jan (2003) Povodeň 2002 v ČR – fakta, úspěchy a prohry. Dostupné z https://www.bezpecnostpotravin.cz/povoden-2002-v-cr-fakta-uspechy-a-prohry.aspx [online, cit. 2022-06-07]

- ZEMAN, Petr (2002-3). Zpravodajské služby po 11. září, Obrana a strategie, 1/2002, s. 63-74, ISSN 1802-7199

- ZEMAN, Petr (2002). Riziko a hrozba – příspěvek do diskuse. Bezpečnostní systém České republiky, sborník z konference, Nakladatelství Linie pro Vysokou školu Karla Engliše, Brno, str. 85—96.

- ZEMAN, Petr (2009). Historie a limity debat o reformě zpravodajských služeb v ČR aneb umíme si už nalít čistého vína?, „Příspěvek k debatě o reformě zpravodajských služeb v České republice: Pracovní panel k reformní agendě“, duben 2009

- ZEMAN, Petr (2010). Zpravodajský cyklus – klišé nebo nosný koncept? Obrana a strategie, 1/2010, s. 45-64, ISSN 1802-7199

- ZEMAN, Petr a kol. (2002-2). Perspektivy vývoje bezpečnostní situace, vojenství a obranných systémů do roku 2015 s výhledem do roku 2025. Část 1: Perspektivy bezpečnostní situace a politického vývoje států střední a východní Evropy do roku 2015, Česká bezpečnostní terminologie, Výklad základních pojmů, heslo 18. Hrozba a riziko, s. 58, ÚSS/202-S-1-031, Ministerstvo obrany Brno.

- ZETOCHA, Karel (2005). Kontrola zpravodajských služeb v nových demokraciích: případová studie České republiky, Politologický časopis, XII/2005, s. 430-454, ISSN 1211-3247

- ZETOCHA, Karel (2006). Úvod do studia zpravodajských služeb, Vojenské rozhledy 1/2006, s. 57-69, ISSN 1210-3292

- ZETOCHA, Karel (2008). Demokratická kontrola zpravodajských služeb, Politologický časopis XV/2008, s. 154-180, ISSN 1211-3247

- ZETOCHA, Karel (2008). Parlamentní kontrola zpravodajských služeb, Institut pro evropskou politiku EUROPEUM, 8 s., „Příspěvek k debatě o

reformě zpravodajských služeb v České republice: Pracovní panel k reformní agendě“.

- ZETOCHA, Karel (2009). Zpravodajské služby v nové demokracii: Česká republika. Brno, Barrister & Principal, 244 s., ISBN 978-80-87029-64-0

- ŽÁČEK, Pavel (2018). První garnitura sovětských poradců v Praze. Ovládnutí a řízení československého bezpečnostního aparátu, 1949–1953, Securitas Imperii, 01, s. 40-69, ISSN 1804-1612

Strategické a koncepční dokumenty

- Audit národní bezpečnosti, Praha 2016
- Bezpečnostní strategie ČR, Praha 2015
- Bezpečnostní strategie ČR, Praha 2023
- Koncepce boje proti organizovanému zločinu do r. 2030, Praha 2022
- Koncepce české zahraniční politiky, Praha 2015
- Koncepce ochrany před následky sucha pro území ČR do r. 2030, Praha 2022
- Koncepce rozvoje boje proti extremismu a předsudečné nenávisti 2021-2022, Praha 2021
- Koncepce rozvoje NÚKIB, Praha 2020
- Národní strategie pro čelení hybridnímu působení, Praha 2021
- Obranná strategie ČR, Praha 2017
- Obranná strategie ČR, Praha 2023
- Státní energetická koncepce, Praha 2015 a 2023

Zákony a právní normy

- Zákon č. 153/1994 Sb. o zpravodajských službách České republiky
- Zákon č. 154/1994 Sb. o Bezpečnotsní informační službě
- Zákon č. 289/2005 Sb. a zákon č. 150/2021 Sb. o Vojenském zpravodajství
- Zákon č. 181/2014 Sb. o kybernetické bezpečnosti
- Zákon č. 250/2017 Sb. o elektronické identifikaci
- Zákon č. 350/2011 Sb. Chemický zákon
- Zákon č. 110/1998 Sb. ústavní zákon o bezpečnosti
- Zákon č. 263/2016 Sb. Atomový zákon

Internetové zdroje použité v práci jsou řádně citovány v příslušných poznámkách pod čarou.

SEZNAM VYBRANÝCH ZKRATEK

AI Artificial Intelligence – umělá inteligence

ANB Audit národní bezpečnosti (ČR)

BIS Bezpečnostní informační služba (ČR)

BS Bezpečnostní strategie (ČR)

CIA Central Intelligence Agency (USA)

DCI Director of Central Intelligence (USA)

FSB Federální bezpečnostní služba (Rusko)

FSO Federální služba ochrany (Rusko)

GRU Hlavní správa rozvědky (Rusko)

JIC Joint Intelligence Committee (Velká Británie)

KYSIO Velitelství kybernetických sil a informačních operací (ČR)

MI5 Military Intelligence Section 5 - kontrarozvědka (Velká Británie)

MI6 Secret Intelligence Service – rozvědka (Velká Británie)

MV Ministerstvo vnitra (ČR)

MZV Ministerstvo zahraničních věcí (ČR)

NCOZ Národní centrála proti organizovanému zločinu (ČR)

NIS2 Network and Information Security (EU)

NÚKIB Národní úřad pro kybernetickou a informační bezpečnost (ČR)

OS Obranná strategie (ČR)

PČR Policie České republiky

StB Státní bezpečnost (ČSSR)

SÚJB Státní úřad pro jadernou bezpečnost (ČR)

SVR Služba zahraniční rozvědky (Rusko)

SZS Společná zpravodajská skupina (ČR)

ÚZSI Úřad pro zahraniční styky a informace (ČR)

VZ Vojenské zpravodajství (ČR)

VZČ Výbor pro zpravodajskou činnost (ČR)

ZS Zpravodajské služby