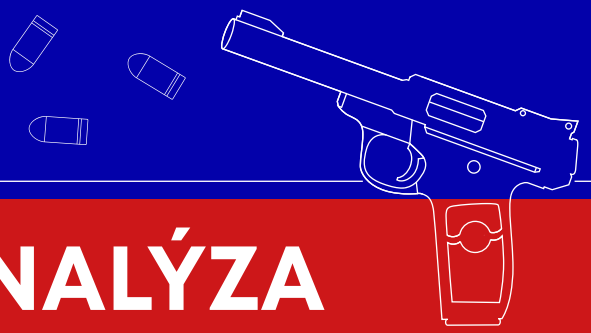
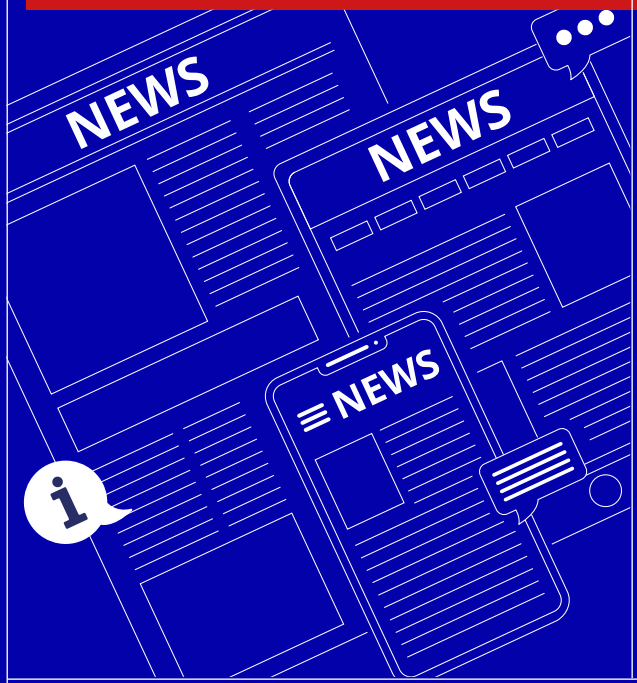
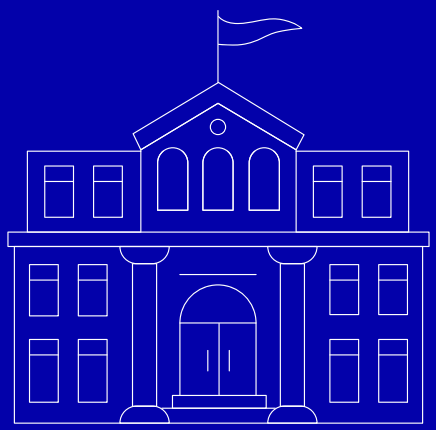
CENTRUM BOJA PROTI HYBRIDNÝM HROZBÁM



HĹBKOVÁ ANALÝZA ZRANITEĽNOSTÍ VYBRANÝCH ORGÁNOV ŠTÁTNEJ SPRÁVY VOČI HYBRIDNÝM HROZBÁM

2023





MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

Operačný program Efektívna verejná správa

Európska únia
Európsky sociálny fond

Autor: autorský tím Centra boja proti hybridným hrozbám ISBA MV SR

Dátum vydania verejnej verzie: august 2023

Centrum boja proti hybridným hrozbám
Inštitút správnych a bezpečnostných analýz
Ministerstvo vnútra SR
Pribinova 2
812 72 Bratislava
Slovenská republika

Táto publikácia bola vytvorená s finančnou podporou Európskej únie. Jej cieľom je sprístupniť verejnosti informácie vychádzajúce z neverejného analytického materiálu, ktorý Bezpečnostná rada SR schválila uznesením č. 818 na svojom zasadnutí 12. apríla 2023. Publikácia obsahuje časti predmetnej analýzy, v rámci ktorej boli identifikované zraniteľnosti vybraných orgánov štátnej správy voči hybridnému pôsobeniu a navrhnuté opatrenia na ich odstránenie. Táto publikácia reprezentuje výlučne názory autorov. Európska únia nezodpovedá za obsah a názory prezentované v tejto publikácii.

Národný projekt „Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy". Kód projektu v ITMS2014+: 314011CDW7

Tento projekt je podporený z Európskeho sociálneho fondu.

Táto analýza je výsledkom širokej spolupráce Centra boja proti hybridným hrozbám MV SR s mnohými zložkami rezortu vnútra, ako aj s nasledovnými inštucionálnymi partnermi, bez ktorých by jej spracovanie nebolo možné. **Ďakujeme!**

- Úrad vlády Slovenskej republiky,
- Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky,
- Ministerstvo hospodárstva Slovenskej republiky,
- Ministerstvo kultúry Slovenskej republiky,
- Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky,
- Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky,
- Ministerstvo spravodlivosti Slovenskej republiky,
- Národný bezpečnostný úrad,
- Slovenská informačná služba,
- Národné bezpečnostné analytické centrum,
- Vojenské spravodajstvo.

Obsah

Úvod

„Najväčšie umenie spočíva v zlomení odporu nepriateľa mimo bojového poľa. V protivníkovej krajine musíte zničiť všetko, čo je dobré.“

Sun-Tzu, Umenie vojny

Dezinformácie, propaganda, kybernetické útoky, vplyvové a informačné operácie, zasahovanie do volieb, strategická korupcia, polovojenské skupiny – všetky tieto pojmy majú niečo spoločné. Sú to najčastejšie využívané nástroje hybridných hrozieb. Pojem hybridné hrozby je síce nový, ale tento koncept je využívaný už stáročia. Spočíva v snahe oslabiť a ochromiť protivníka bez nasadenia vojenských síl.

Presadzovanie vlastných ekonomických či geopolitických záujmov v medzinárodných vzťahoch pomocou diplomacie a ostatných „mäkkých“ foriem pôsobenia je bežnou súčasťou vzťahov medzi štátmi. **To, čím sa hybridné hrozby líšia od týchto foriem medzinárodnej politiky, je úroveň koordinácie medzi rôznymi nástrojmi a najmä cieľ takéhoto pôsobenia.** Ním je ochromenie a rozvrat spoločnosti, či jej bezpečnostných a vládnych štruktúr.

Hybridné hrozby sa v posledných rokoch stali jednou z najdôležitejších tém v oblasti bezpečnosti. Rovnako na Slovensku ako i na úrovni EÚ či NATO. Dôvodom, prečo je tejto oblasti prikladaný čoraz väčší význam, je zmena spôsobu presadzovania strategických záujmov zo strany nepriateľských aktérov a zvyšujúci sa dopad technológií na všetky oblasti spoločnosti.

Vojny v 21. storočí nahrádza koordinované využívanie celej palety nástrojov v oblasti informačného pôsobenia, ekonomického vplyvu, energetického nátlaku či pôsobenia tajných služieb. Zároveň sa technológie stali neoddeliteľnou súčasťou života celej spoločnosti a vďaka nim dnes dokážu nepriateľskí aktéri pôsobiť kdekoľvek na svete – šíria strategickú propagandu, ovplyvňujú volebné procesy, útočia na kritickú infraštruktúru, prenikajú do počítačových sietí atď.

Aktérmi hybridných hrozieb bývajú väčšinou cudzie nepriateľské štáty, ktorých politické či strategické ciele sú v rozpore so životnými a strategickými záujmami Slovenskej republiky a organizácií, ktorých je členom, ako napr. EÚ či NATO. **Najčastejšie sa preto v našich podmienkach pri hybridných hrozbách vyskytujú aktivity Ruskej federácie. Tá dokonca zaradila Slovensko spolu s ďalšími krajinami EÚ na zoznam nepriateľských krajín.**[1] Ďalej je to Čína, ktorá využíva primárne ekono-

[1] Nariadenie vlády č. 1998-r z 22.7.2022 http://government.ru/en/docs/46080/ a Russian government approves list of unfriendly countries and territories - Russian Politics & Diplomacy - TASS.

mické formy a nástroje. Takéto hodnotenie vyplýva jednak z výročných správ Slovenskej informačnej služby[2] či Vojenského spravodajstva[3], ako aj z dokumentov prijímaných na úrovni EÚ a NATO[4]. Hybridnými aktérmi môžu byť aj neštátne subjekty. Typickým príkladom je ISIS, ktorý využíval na vrchole svojich aktivít viaceré vzájomne prepojené a koordinované nástroje v oblasti informačných operácií, kybernetických útokov či terorizmu.

Slovensko začalo pracovať na zvyšovaní svojej odolnosti voči hybridným hrozbám už v roku 2018, kedy bola prijatá prvá *Koncepcia pre boj SR proti hybridným hrozbám*[5]. Význam tejto oblasti bol podčiarknutý aj v aktuálnej *Bezpečnostnej stratégii SR* z roku 2021 a zatiaľ najnovším materiálom v danej oblasti je *Akčný plán koordinácie boja proti hybridným hrozbám* (ďalej len „APHH") z roku 2022[6].

Základom pre úspešné čelenie nebezpečenstvu, ktoré takéto skryté, podvratné pôsobenie voči strategickým a životným záujmom SR predstavujú hybridné hrozby, je poznať vlastné slabé miesta. Z tohto dôvodu vznikla v rámci národného projektu *„Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy"* potreba analyzovať procesy, štruktúry a legislatívu vybraných subjektov štátnej správy vo vzťahu k možnému hybridnému pôsobeniu. Jej výsledkom je *Hĺbková analýza zraniteľností vybraných orgánov štátnej správy voči hybridným hrozbám* (ďalej len „hĺbková analýza"), ktorá je premietnutím úlohy A.1 vyplývajúcej z APHH.

Tento materiál je výsledkom širokej spolupráce Ministerstva vnútra Slovenskej republiky s viacerými ústrednými orgánmi štátnej správy a bezpečnostnými zložkami. Cieľom hĺbkovej analýzy bolo nielen identifikovať zraniteľnosti, ale taktiež navrhnúť opatrenia na ich odstránenie. Analýza obsahuje úvodnú kapitolu, skúmajúcu celkovú architektúru systému na riešenie hybridných hrozieb v rámci štátnej správy, a 22 tematických kapitol, v ktorých sú analyzované zraniteľnosti voči špecifickým nástrojom hybridných hrozieb.

Vzhľadom na citlivosť informácií obsiahnutých v hĺbkovej analýze bol materiál schválený na zasadnutí Bezpečnostnej rady SR uznesením č. 818 dňa 12. apríla 2023 ako materiál podliehajúci ochrane utajovaných skutočností. Verzia, ktorú držíte v rukách, je upravenou verziou tejto analýzy pre potreby verejného šírenia a diskusie v radoch odbornej verejnosti. Boli z nej odstránené citlivé informácie, stále však **predstavuje najkomplexnejšie zmapovanie zraniteľností voči hybridným hrozbám a zároveň ponúka konkrétne opatrenia na ich odstránenie**.

[2] Správa o činnosti SIS za rok 2021 Slovenská informačná služba | Pre Vás | Správa o činnosti SIS (gov.sk).
[3] Správa o činnosti VS za rok 2021 Sprava_o_cinnosti_vs_2021_svk.pdf (mosr.sk).
[4] Ruská federácia bola označená za najvýznamnejšiu a najpriamejšiu hrozbu pre bezpečnosť spojencov, ako aj pre mier a stabilitu v euroatlantickom priestore v rámci NATO Strategickej koncepcie 2022, ktorá bola prijatá na samite v Madride dňa 29. júna 2022. Na úrovni EÚ bol Radou EÚ prijatý dňa 21. marca 2022 Strategický kompas, v ktorom sú identifikované ruské hrozby a Európsky parlament v novembri 2022 deklaroval, že Ruská federácia je štát podporujúci terorizmus a využívajúci teroristické praktiky.
[5] Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám, schválená uznesením vlády č. 345/2018 dňa 11.7.2018 https://rokovania.gov.sk/RVL/Material/23100/1.
[6] Akčný plán koordinácie boja proti hybridným hrozbám na roky 2022 až 2024, schválený uznesením vlády SR č. 235/2022 zo dňa 30.3.2022.

Nástroje hybridných hrozieb

Hybridní aktéri môžu využívať rôzne nástroje za účelom dosiahnutia sledovaných cieľov. Pri určení nástrojov hybridných hrozieb táto analýza vychádza z konceptuálneho modelu, ktorý bol vytvorený v rámci Spoločného výskumného centra EÚ (Joint Research Center, ďalej len „JRC"). Model vytvorený JRC definuje 40 nástrojov hybridných hrozieb v 13 doménach.

V rámci tejto analýzy bol tento model upravený na podmienky SR a počet nástrojov bol upravený na 25. Nástroje sú zoradené podľa identifikovaného rizika od najzávažnejšieho po najmenej závažné:

1. Dezinformačné kampane a propaganda	**14.** Nátlak na politikov alebo členov vlády
2. Ovplyvňovanie volieb	**15.** Veľvyslanectvá
3. Rozširovanie zbraní (aj hromadného ničenia)	**16.** Využívanie diaspór k ovplyvňovaniu
4. Narušenie kybernetickej bezpečnosti - narušenie dôvernosti, integrity a dostupnosti v kybernetickom priestore	**17.** Diplomatické a ekonomické sankcie
5. Fyzické operácie proti infraštruktúre	**18.** Ovládanie a zasahovanie do médií
6. Podpora sociálnych nepokojov a zneužívanie sociokultúrneho štiepenia	**19.** Priame zahraničné investície
7. Využívanie slabých miest v štátnej správe	**20.** Vytvorenie a zneužívanie závislosti infraštruktúry (energetika, energetická infraštruktúra a civilno-vojenské závislosti)
8. Zneužívanie migrácie ako nástroja hybridnej hrozby	**21.** Vytváranie a zneužívanie ekonomických ťažkostí a závislostí
9. Zneužívanie slabých miest, nejednoznačností a medzier v legislatíve	**22.** Vojenské cvičenia *
10. Polovojenské skupiny	**23.** Narušenie vzdušného priestoru *
11. Financovanie náboženských a kultúrnych skupín	**24.** Konvenčné / nekonvenčné operácie ozbrojených síl *
12. Ovplyvňovanie učebných osnov a akademickej obce	**25.** Spravodajské / utajené operácie a infiltrácia *
13. Podpora a využívanie korupcie	

*vzhľadom na citlivú povahu týchto nástrojov, tieto nástroje neboli rozpracované do samostatných kapitol verejnej verzie

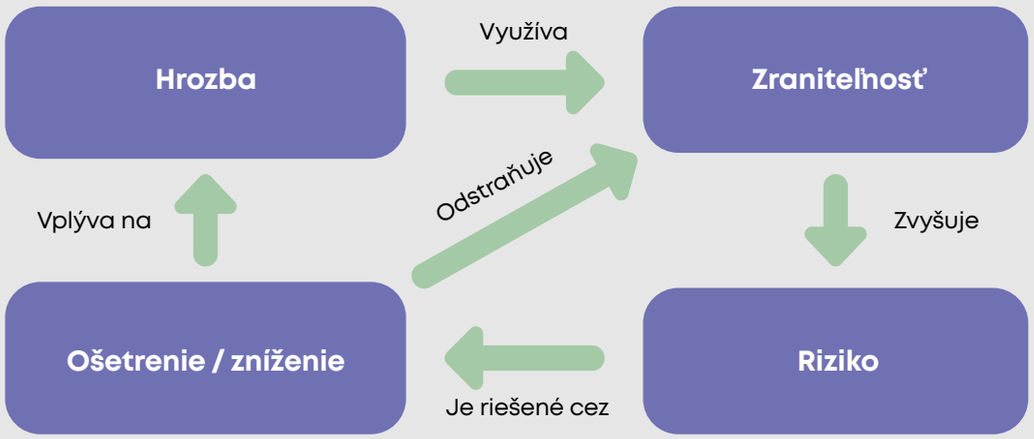
Metodológia

Metodológia, ktorá bola pripravená pracovníkmi CBHH špeciálne pre túto analýzu, sa opiera o už spomínaný konceptuálny rámec a model Spoločného výskumného centra EÚ (Joint Research Center, JRC), ako aj o ďalšie postupy zamerané na analýzu rizík a zraniteľností. Jej skrátená verzia je predstavená v tejto kapitole.

Analýza sa zamerala na **4 hlavné oblasti:**

- **legislatíva** a interné normatívne právne akty,
- **inštitucionálna štruktúra** a vnútorné vzťahy,
- **proces prenosu a zdieľania informácií** v jednotlivých subjektoch a medzi subjektami a
- **rozhodovacie procesy** a vstupy, ktoré sa na nich podieľajú.

Je dôležité zdôrazniť, že ide o analýzu systémového nastavenia štátnej správy, a nie o analýzu operatívneho a informačného obsahu spomínaných procesov. **V rámci tohto prístupu boli východiskom analýzy jednotlivé hybridné hrozby, ktoré sú relevantné pre národnú bezpečnosť a záujmy SR**. Tieto hybridné hrozby môžu zneužívať špecifické zraniteľnosti existujúce v štátnej správe, ktoré v kombinácii s možným dopadom týchto hrozieb vedú k riziku. Riziko môže byť ošetrené alebo znížené aj odstránením špecifických zraniteľností, v kontexte schémy:



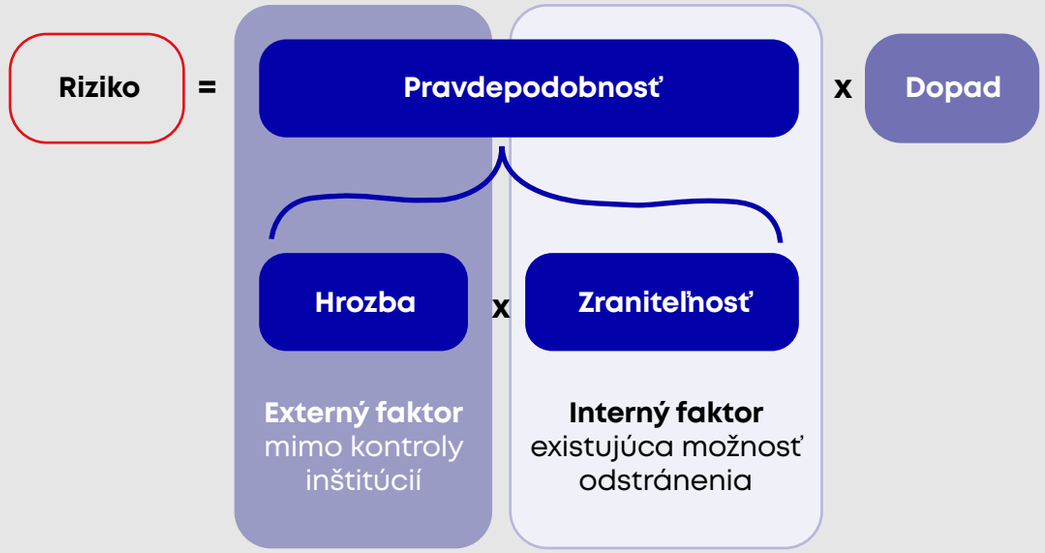
Obrázok 1: Zobrazenie vzťahov medzi hrozbou, zraniteľnosťou a rizikom[1]

[1] Inšpirované na základe Figure 1. z *Toosarvandani, Marzieh & Modiri, Nasser & Afzali, Mehdi. (2012). The risk assessment and treatment approach in order to provide lan security based on isms standard. 10.5121/ijfcst.2012.2602*

Ku jednotlivým hrozbám boli priradení **gestori** – t.j. inštitúcie, ktoré majú najväčšiu mieru zodpovednosti v predmetnej oblasti – **ktorí zodpovedali za spracovanie kapitoly o danej hrozbe** v spolupráci s ďalšími zúčastnenými inštitúciami. Úlohou gestorov bolo v spolupráci s CBHH identifikovať zoznam pod nich spadajúcich procesov, ktoré môžu byť ovplyvnené nástrojmi hybridných hrozieb a definovať hypotetický scenár toho, ako by tieto procesy mohli byť zneužité. Následne gestori postupovali na základe reflektívneho modelu *"What? So what? Now what?"* (slovenský preklad „Čo? Čo to znamená? Čo teraz?") v troch fázach:

1. **popis aktuálneho stavu** z hľadiska 4 hlavných oblastí,
2. **hodnotenie aktuálneho stavu a analýza zraniteľností** pri identifikovaných procesoch a
3. **návrh opatrení** na odstránenie identifikovaných zraniteľností + ich priorizácia na základe kvalitatívnej analýzy rizík.

Kvalitatívna analýza rizika spojeného s hybridnou hrozbou bola vykonaná na základe hodnotiaceho rámca v rámci ktorého bolo riziko vyjadrené ako prienik príslušnej hodnoty pravdepodobnosti naplnenia scenára rizika a hodnoty úrovne možných dopadov:



Obrázok[2]: Vyjadrenie rizika ako prieniku pravdepodobnosti a dopadu

[2] Inšpirované na základe Koen van Impe (2017) Simplifying Risk Management.
Dostupné: https://securityintelligence.com/simplifying-risk-management/

Gestori **určovali výsledné riziko** - mimoriadne závažné (A), vysoké (B), nízke (C) alebo zanedbateľné (D) - **ako kombináciu pravdepodobnosti naplnenia scenára rizika a „najhoršieho“ možného dopadu**, s pomocou definícií jednotlivých úrovní pravdepodobnosti a dopadu od CBHH.

Pravdepodob-nosť hrozby	Dopad hrozby				
	Zanedbateľný	Minimálny	Stredný	Závažný	Katastrofický
Vysoká	D	C	B	B	A
Stredná	D	C	C	B	A
Nízka	D	D	D	C	B
Veľmi nízka	D	D	D	D	C

Tabuľka 1: Určenie úrovne výsledného rizika

Kapitoly, ako aj návrhy jednotlivých opatrení, boli finálne priorizované podľa výslednej úrovne rizika a sú označené zodpovedajúcou farbou.

Systém boja proti hybridným hrozbám

Široké možnosti použitia hybridných nástrojov proti SR vedú k potrebe zvýšenej koordinácie aktivít v rámci štátnej správy, ako aj zvýšenia personálnych kapacít a udržateľnosti jednotlivých útvarov určených na boj proti hybridným hrozbám.

Systém boja proti hybridným hrozbám musí obsahovať:

- **Efektívne nastavenú architektúru zapojených inštitúcií**, vrátane deľby ich kompetencií
- **Funkčné procesy koordinácie a výmeny informácií** medzi zapojenými inštitúciami, na zabezpečenie praktických opatrení na zmiernenie dopadov hybridného pôsobenia
- **Dlhodobú stratégiu SR** ktorá zabezpečí udržateľnosť horeuvedenej inštitucionálnej architektúry a procesov koordinácie.

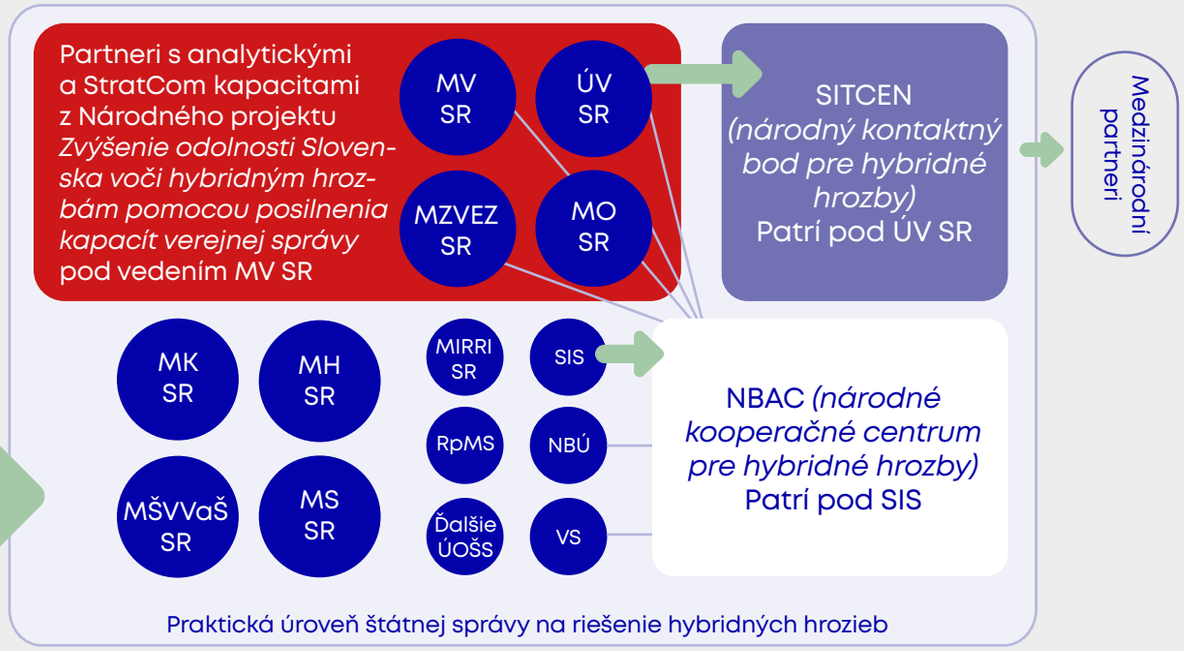
Nerealizovanie opatrení k zabezpečeniu koordinácie a udržateľnosti odborných zložiek štátnej správy zaoberajúcimi sa hybridnými hrozbami **predstavuje vysoké riziko stagnovania, alebo dokonca zníženia odolnosti SR voči hybridným hrozbám.**

Výbor Bezpečnostnej rady SR pre hybridné hrozby

(strategická úroveň medzirezortnej spolupráce)

Identifikované zraniteľnosti	Čo je potrebné urobiť?
Absencia legislatívneho ukotvenia kompetencií a určenie primárnej zodpovednosti za boj s hybridnými hrozbami	*Ukotviť kompetencie a určiť primárnu zodpovednosť za koordináciu boja s hybridnými hrozbami v jednotlivých doménach v rámci štátnych inštitúcií*
Nezabezpečená udržateľnosť existujúcich odborných útvarov a nedostatočné zapojenie štátnych inštitúcií, ktoré nemajú špecializované kapacity na riešenie hybridných hrozieb	*Zabezpečiť trvalú udržateľnosť odborných útvarov zriadených na strategickú komunikáciu a boj proti hybridným hrozbám a vybudovať kapacity v rámci štátnych inštitúcií, kde sú potrebné*
Nedostatočná koordinácia medzi inštitúciami, ktoré riešia hybridné hrozby	*Vytvoriť centrálny koordinačný mechanizmus alebo platformu na praktickú a operatívnu koordináciu útvarov na boj proti hybridným hrozbám*

Inštitúcie ktoré sa venujú riešeniu hybridných hrozieb



Dezinformačné kampane a propaganda

Dezinformácie sú najčastejšie využívaným nástrojom hybridných hrozieb. Hybridní aktéri ich môžu využiť na ovplyvnenie verejnej mienky, oslabenie dôvery v inštitúcie, destabilizovanie politického systému alebo vyvolanie nepokojov. Ich cieľom je manipulovať s vnímaním skutočnosti a ovplyvniť rozhodovanie ľudí.

Formy možného hybridného pôsobenia

- **šírenie nepravdivých alebo manipulatívnych informácií** s cieľom uškodiť, získať určité výhody alebo ovplyvniť cieľové publikum,
- **šírenie protichodných naratívov alebo konšpiračných teórií** na vytvorenie informačného chaosu či zníženie dôvery,
- **zámerné informovanie v prospech hybridného aktéra,**
- **šírenie dezinformácií** prostredníctvom falošných účtov či botov,
- **cielená diskreditácia osôb** či skupín obyvateľstva v záujme hybridného aktéra.

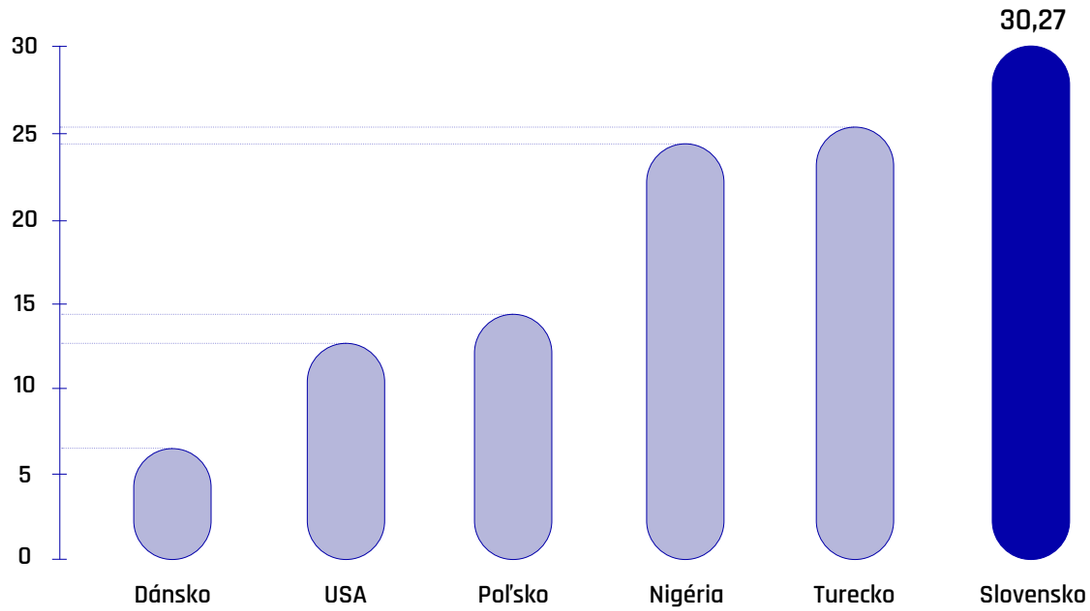
Intenzívne a dlhodobé dezinformačné kampane a propaganda spôsobujú **polarizáciu spoločnosti,** narušenie konsenzu o zahraničnopolitickej orientácii SR, zníženie dôvery v demokratické inštitúcie, ako aj **podkopanie či ochromenie rozhodovacích procesov.**

Zodpovedné inštitúcie

- Úrad vlády SR
- Ministerstvo vnútra SR
- Ministerstvo zahraničných vecí a európskych záležitostí SR

Konšpiračný index

Tzv. konšpiračný index sa počíta ako priemer kladných odpovedí na štandardné konšpiračné otázky. Na Slovensku je v porovnaní so svetom extrémne vysoký.



Zdroj: https://fmk.sk/konspiracny-index-na-slovensku/
Najviac veria konšpiráciám Slováci, ukázal prieskum UCM. In fmk.sk [online].

Identifikované zraniteľnosti

Nemožnosť blokovania webov s prepojením na hybridného aktéra.

Neformálnosť prenosu a zdieľania informácií medzi subjektami, pod ktorých agendu spadá boj proti dezinformáciám.

Čo je potrebné urobiť?

Prijať novelu zákona o kybernetickej bezpečnosti, ktorá by tento krok v oprávnených prípadoch umožnila.

Zvážiť zmenu kompetenčného zákona s cieľom určiť subjekt primárne zodpovedný za koordináciu boja proti dezinformáciám.

Ovplyvňovanie volieb

Ide o zásadnú hrozbu pre SR v dlhodobom horizonte. Ovplyvňovaním volieb sa oslabuje nielen samotná integrita tohto procesu, ale aj demokratické zriadenie štátu.

Formy možného hybridného pôsobenia

- **skrytá podpora** pre konkrétnych politických kandidátov alebo strany,
- **obchádzanie obmedzení a pravidiel** na financovanie kampaní a strán,
- **znižovanie dôvery** verejnosti vo výsledky volieb a v štátne inštitúcie,
- **zneužívanie internetu** a sociálnych sietí na polarizáciu spoločnosti.

Úspešné ovplyvnenie volieb môže spôsobiť **zníženie dôvery** občanov **v demokratické inštitúcie a voľby.** Ďalej tiež spochybnenie euroatlantického smerovania SR, čo prináša závažné bezpečnostné dôsledky.

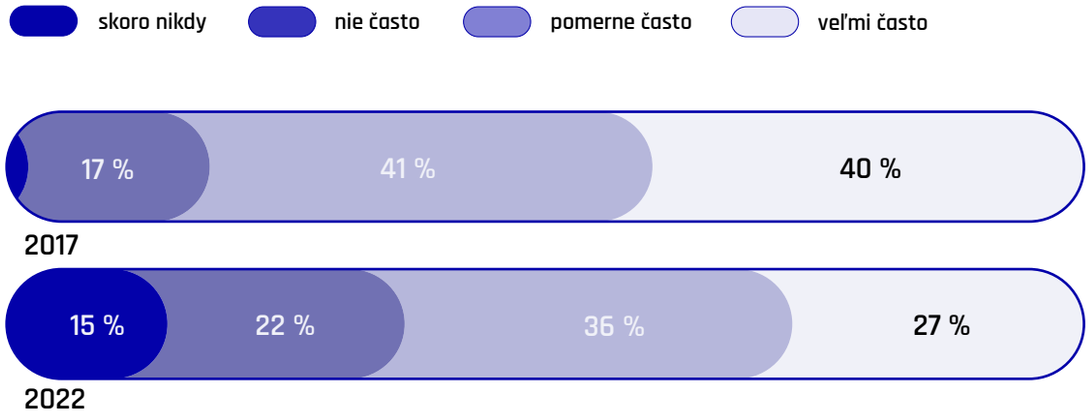
Zodpovedné inštitúcie

- Ministerstvo vnútra SR,
- Štátna komisia pre voľby a kontrolu financovania politických strán

Dôvera vo voľby na Slovensku

Porovnanie roku 2017 s 2022

Ako často sa podľa vás vo voľbách v našej krajine počítajú hlasy spravodlivo?



Zdroj: prieskum agentúry Focus pre Denník N

Zdroj: https://dennikn.sk/minuta/2958750/

Identifikované zraniteľnosti

Legislatíva nepriamo **umožňuje financovanie politických strán** a volebných kampaní **zahraničnými aktérmi.**

Absencia explicitnej **zákonnej úpravy** volebnej kampane pred referendom.

Legislatíva špecificky **nereflektuje priebeh volebných kampaní v online priestore.**

Čo je potrebné urobiť?

Prijať detailnejšiu právnu úpravu financovania politických strán, hnutí a volebnej kampane s cieľom zvýšiť transparentnosť financovania volieb.

Doplniť právnu úpravu referendovej volebnej kampane.

Zaviesť právnu úpravu online volebnej kampane. Plus presnejšie vymedziť, čo sa považuje za volebnú kampaň vedenú na internete (napr. nielen sponzorované príspevky).

Rozširovanie zbraní

Na území SR existuje niekoľko významných zbrojárskych firiem s produkciou prevažne do zahraničia. Tieto zbrane putujú do vojnou zmietaných krajín či do takých, ktoré porušujú medzinárodné embargá. Zároveň sa v SR vyskytujú tzv. 80 % zbrane a narastá problém s 3D zbraňami.

Výsledky zbraňovej amnestie v SR

(november 2020 - apríl 2021)

Odovzdaných

1 615 kusov

nelegálne držaných zbraní

53 025 kusov

nelegálne držaného streliva

Skončila 4. zbraňová amnestia, Slováci dali preskúmať vyše 1600 strelných zbraní.

Tlačová správa MV SR z 06. 05. 2021

Zdroj: https://www.minv.sk/?tlacove-spravy&sprava=statistika-4-zbrojova-amnestia

Formy možného hybridného pôsobenia

- **nelegálne a legálne obchodovanie** so zbraňami, strelivom, výbušninami, zbraňovými komponentmi, prekurzormi výbušnín a chemických bojových látok a s položkami s dvojakým použitím,
- **rozširovanie zbraní prostredníctvom nových technológií** (tzv. 3D zbraní, ktoré sú ťažko detekovateľné bez evidencie a tzv. 80% zbraní explicitne neregulovaných),
- výskyt množstva **zbraní a streliva v nelegálnej držbe** v SR.

Kontinuálne rozširovanie zbraní môže spôsobiť **závažné ohrozenie bezpečnosti občanov SR,** ako aj EÚ.

Zodpovedné inštitúcie

- Policajný zbor,
- Finančná správa SR,
- Ministerstvo hospodárstva SR.

Identifikované zraniteľnosti

Absencia právnej úpravy v oblasti tzv. 80% zbraní a nedostatočné uplatňovanie platnej legislatívy v súvislosti s tzv. 3D zbraňami.

Absencia analýz a proaktívneho **monitorovania** vývozu položiek s dvojakým použitím.

Nízke analytické a technické kapacity PZ na boj s nelegálnym obchodovaním so zbraňami.

Čo je potrebné urobiť?

Aktívne sa podieľať na príprave legislatívy EÚ v oblasti tzv. 80% zbraní. Dôsledne uplatňovať legislatívu SR pri nedovolenom ozbrojovaní s tzv. 3D zbraňami.

Zaviesť systém proaktívnych analýz v oblasti exportu položiek dvojakého použitia.

Navýšiť personálne a technické kapacity na boj s nelegálnym obchodovaním so zbraňami.

Narušenie kybernetickej bezpečnosti

Vzhľadom na rozsiahle využívanie informačných systémov predstavujú kybernetické útoky jeden z najčastejšie využívaných nástrojov hybridných hrozieb. Hybridní aktéri môžu narušiť kybernetickú bezpečnosť preniknutím do sietí a informačných systémov.

Formy možného hybridného pôsobenia

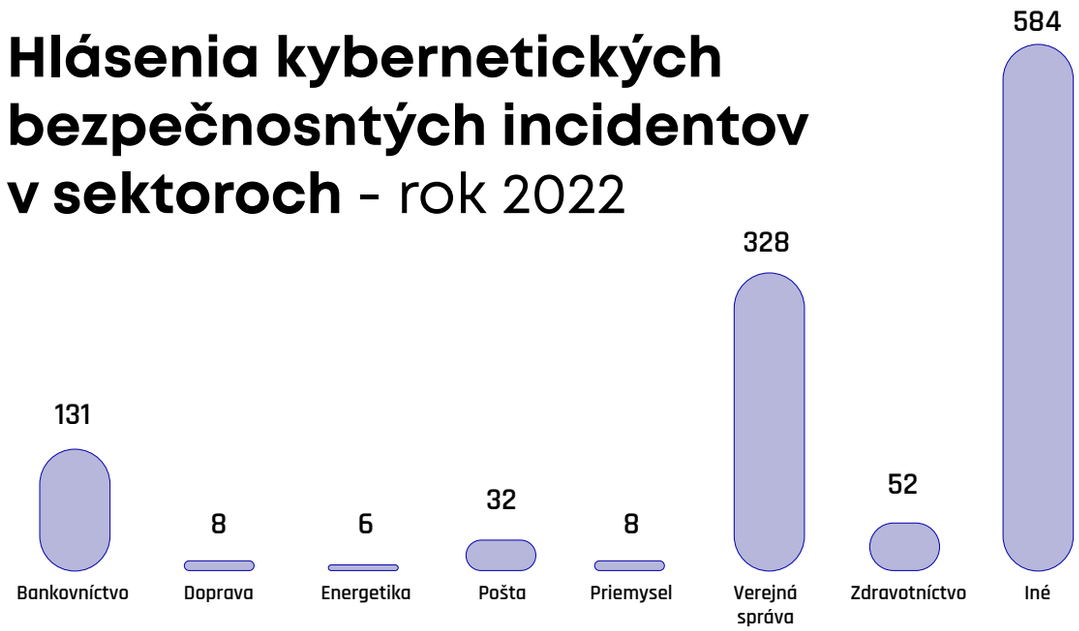
- **komplexné kybernetické útoky,** ak sú organizované s cieľom ovládnuť kľúčové systémy alebo znefunkčniť digitálne služby,
- **kybernetická špionáž,** ktorou sa nepriateľský aktér snaží získať prístup k utajovaným skutočnostiam, citlivým údajom alebo duševnému vlastníctvu, pre získanie výhod nad konkurenčnou spoločnosťou alebo vládnym subjektom.

Narušenie kybernetickej bezpečnosti môže mať katastrofický **dopad na poskytovanie základných služieb štátu, ochranu osobných údajov** všetkých občanov **a verejný poriadok.**

Zodpovedné inštitúcie

- Národný bezpečnostný úrad,
- ústredné orgány štátnej správy,
- prevádzkovatelia základných služieb,
- poskytovatelia digitálnych služieb.

Hlásenia kybernetických bezpečnosntých incidentov v sektoroch - rok 2022



Zdroj: https://www.nbu.gov.sk/wp-content/uploads/urad/Vyrocne_spravy/sprava_kyber_2022.pdf

Identifikované zraniteľnosti

Nedodržiavanie zákonnej **povinnosti hlásiť každý závažný kybernetický bezpečnostný incident** Národnému centru kybernetickej bezpečnosti SK-CERT Národného bezpečnostného úradu.

Analýza rizík kybernetickej bezpečnosti niektorých subjektov býva často spracovaná **bez riadneho posúdenia hrozieb a zraniteľností** prevádzkovateľa. Nie sú prijaté dostatočné bezpečnostné opatrenia.

Neefektívne spôsoby budovania kapacít / **poddimenzovanie odborných kapacít** v oblasti kybernetickej bezpečnosti

Čo je potrebné urobiť?

Subjekty, ktorým zo zákona o kybernetickej bezpečnosti vzniká povinnosť poskytovať informácie, ich musia ihneď bezodplatne a bezodkladne poskytnúť.

Subjekty pri analýze rizík môžu postupovať podľa metodiky posúdenia rizík, dostupnej na webe Národného bezpečnostného úradu.

Zabezpečiť adekvátne odborné kapacity verejnej správy.

Fyzické operácie proti infraštruktúre

Hybridné operácie sú často cielené proti významnej infraštruktúre na území SR a EÚ. Hybridní aktéri môžu využívať na destabilizáciu kritickej infraštruktúry (KI) rôzne druhy útokov, ktorých účinky sa môžu prejaviť v rôznych sektoroch.

Formy možného hybridného pôsobenia

- **korupcia,**
- **špionáž,**
- **sabotáž,** kybernetické a fyzické útoky na kritické systémy a zariadenia,
- **šírenie dezinformácií** a falošných informácií s cieľom destabilizovať KI, spôsobiť chaos a neistotu,
- **ovplyvňovanie kľúčových pracovníkov** kritických zariadení alebo politických lídrov.

K najzávažnejšiemu ohrozeniu by došlo pri narušení KI. To by malo nepriaznivé dôsledky na schopnosť štátu zaistiť ochranu života, zdravia, bezpečnosti, majetku či životného prostredia.

Zodpovedné inštitúcie

- Vláda SR,
- Ministerstvo vnútra SR.

Sektory KI v pôsobnosti ústredných orgánov

Zdroj: https://www.zakonypreludi.sk/zz/2011-45
Zákon č. 45/2011 Z. z., Zákon o kritickej infraštruktúre. In zakonypreludi.sk [online].

Identifikované zraniteľnosti

Čo je potrebné urobiť?

Neaktuálnosť súčasnej právnej úpravy a stratégií ku KI**.** → *Novelizovať Zákon o KI tak, aby odrážal aktuálne bezpečnostné výzvy a trendy v tejto oblasti.*

Neaktuálnosť hodnotenia rizík na úseku KI. → *Prevziať odporúčania z APHH v oblasti KI, zapracovať problematiku hybridných hrozieb do hodnotení rizík, integrovaných postupov a procesov krízového riadenia a civilnej ochrany.*

Nedostatok odborníkov na pokrytie agendy ochrany KI. → *Navýšiť kapacity odborníkov a analytikov v oblasti KI a krízového riadenia naprieč ÚOŠS, zabezpečiť dlhodobú udržateľnosť týchto pozícií.*

Podpora sociálnych nepokojov a zneužívanie sociokultúrneho štiepenia

Hybridní aktéri sa v sociokultúrnej oblasti zameriavajú na širokú škálu tém, ako národná identita, história krajiny či náboženstvo, s cieľom vytvárať a prehlbovať rozpory v spoločnosti. Zneužité môžu byť aj nezamestnanosť, chudoba, migrácia a ďalšie témy, ktoré dokážu spôsobiť spoločenské napätie.

Formy možného hybridného pôsobenia

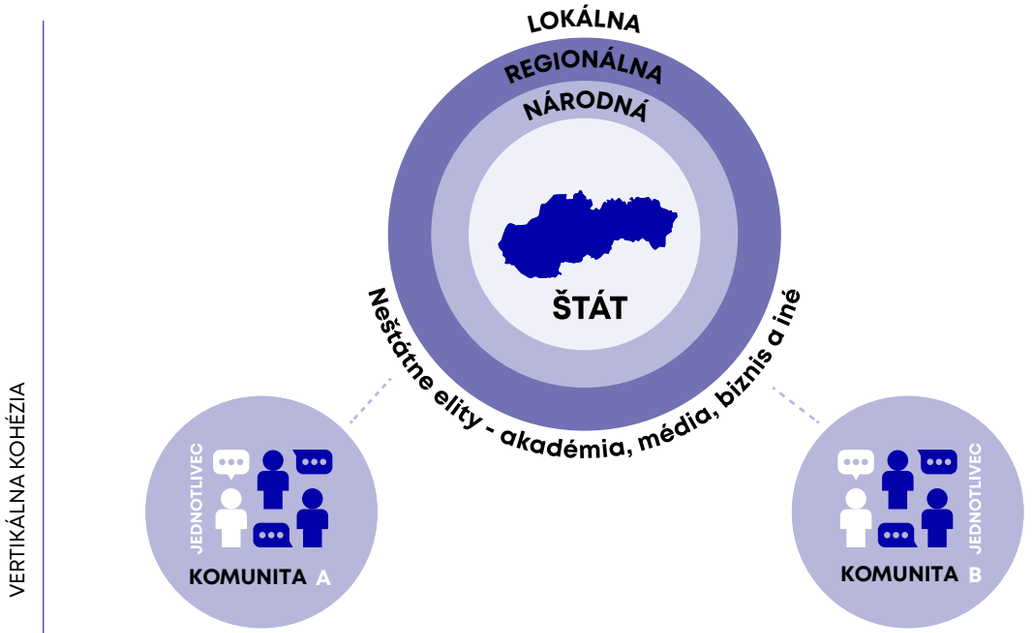
- **Zneužívanie citlivých tém** a ich zosilňovanie prostredníctvom dezinformačných naratívov s cieľom vytvárať pnutie v spoločnosti
- **Zneužívanie existujúcich spoločenských rozdielov** s cieľom posilniť sociálne napätie, polarizáciu či strach
- **Podpora spoločenských nepokojov** so zámerom ovplyvniť či narušiť rozhodovacie procesy štátu

Snahou hybridného aktéra je **zmena zahraničnopolitického smerovania štátu alebo znefunkčnenie jeho rozhodovacích procesov.** Tým môže dôjsť k oslabeniu plnenia základných funkcií štátu a zníženiu schopnosti adekvátne reagovať v krízových situáciách.

Zodpovedné inštitúcie

Splnomocnenci vlády SR – pre ochranu slobody vierovyznania alebo presvedčenia, pre rozvoj občianskej spoločnosti, pre rómske komunity a pre národnostné menšiny.

Podoba spoločenskej súdržnosti v štáte



Identifikované zraniteľnosti

Absencia princípov a štruktúr na zabezpečenie **strategického vládnutia** v SR

Neexistencia koncepcie budovania spoločenskej kohézie

Čo je potrebné urobiť?

Inštitucionálne ukotviť princípy strategického vládnutia na riešenie komplexných spoločenských problémov presahujúcich dĺžku volebných cyklov.

Vypracovať koncepciu budovania spoločenskej kohézie a odolnosti voči zneužívaniu sociokultúrneho štiepenia a zámernej podpory sociálnych nepokojov

Využívanie slabých miest v štátnej správe

Slabé miesta v štátnej správe sú pre hybridných aktérov vhodným cieľom na oslabenie alebo ovplyvnenie výkonu štátnej správy. Zneužitá môže byť slabá ochrana a výmena citlivých informácií, či nedostatočné vzdelávanie a povedomie o hybridných hrozbách.

Formy možného hybridného pôsobenia

- **ovplyvňovanie mienky zamestnancov** ŠS v dôsledku nízkeho povedomia o hybridných hrozbách a nedostatočného vzdelávania,
- **zneužitie pomalej reakcie štátu,** spôsobenej komplikáciami spojenými s prenosom utajovaných skutočností (personálne a technické),
- **zneužitie absencie bezpečnostných technológií** na strane štátu, spôsobenej dlhým procesom verejného obstarávania.

V prípade zlyhania ŠS hrozí **zníženie reakcieschopnosti štátu** a **narušenie dôvery spoločnosti voči štátnym inštitúciám.**

Zodpovedné inštitúcie

- Ministerstvo vnútra SR,
- všetky ústredné orgány štátnej správy.

Prieskum o problematike hybridných hrozieb v radoch verejnej správy (2018)

Je podľa Vás Vaša inštitúcia pripravená čeliť hybridným hrozbám?

Myslíte si, že máte dostatočné znalosti o problematike hybridných hrozieb?

Nie áno

(Zdroj: Anonymný dotazníkový prieskum zamestnancov verejnej správy v rámci projektu „Zvyšovanie pripravenosti a kapacit verejnej správy na hybridné hrozby", GLOBSEC, november 2018)

Identifikované zraniteľnosti

Čo je potrebné urobiť?

Absencia posúdenia spoľahlivosti uchádzačov o zamestnanie v štátnej správe v online prostredí (napr. sociálne siete).

→ *Doplniť legislatívu v oblasti posudzovania spoľahlivosti o aktivity v online prostredí.*

Nedostatočné vzdelávanie zamestnancov v oblasti hybridných hrozieb.

→ *Zaviesť pravidelné vzdelávanie zamestnancov ŠS v témach súvisiacich s hybridnými hrozbami.*

Zdĺhavý a komplikovaný proces verejného obstarávania moderných bezpečnostných technológií.

→ *Urýchliť proces verejného obstarávania v oblasti bezpečnosti.*

Zneužívanie migrácie ako nástroja hybridnej hrozby

Hybridní aktéri môžu zneužiť alebo aj úmyselne vyvolať masívny prílev cudzincov do SR a EÚ na polarizáciu spoločnosti. Dôsledkom môže byť nárast extrémizmu a rozvrat spoločnosti, ktorému štát nemusí byť schopný čeliť.

Formy možného hybridného pôsobenia

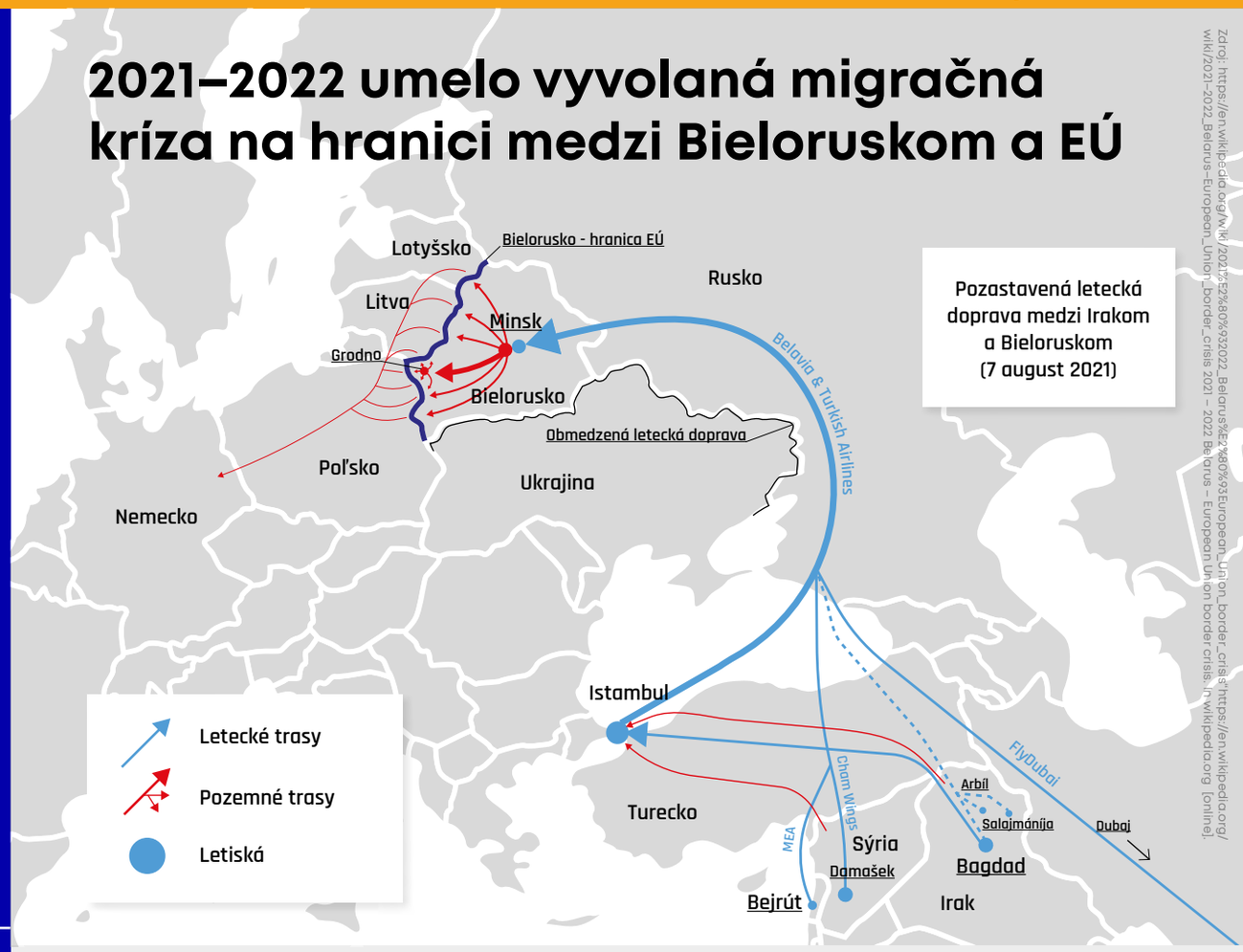
- **organizovanie a podnecovanie neregulárnych migračných tokov** s cieľom vyvolávať strach,
- snahy o zníženie dôveryhodnosti v štátne inštitúcie a **ovplyvnenie verejnej mienky,**
- **polarizácia spoločnosti**, vyvolávanie nepokojov a šírenie dezinformácií o migrantoch.

Za účelom destabilizácie spoločnosti hybridní aktéri **vyvolávajú konflikty** a **zvyšujú napätie** medzi miestnymi obyvateľmi a cudzincami. Dochádza k preťaženiu hraničnej infraštruktúry a **oslabeniu vnútornej stability** SR aj EÚ.

Zodpovedné inštitúcie

- Ministerstvo vnútra SR,
- Ministerstvo zahraničných vecí a európskych záležitostí SR.

2021–2022 umelo vyvolaná migračná kríza na hranici medzi Bieloruskom a EÚ



Zdroj: https://en.wikipedia.org/wiki/2021%E2%80%932022_Belarus%E2%80%93European_Union_border_crisis https://en.wikipedia.org/wiki/2021–2022_Belarus–European_Union_border_crisis [online]

Identifikované zraniteľnosti

Neaktuálnosť integračnej politiky SR.

Rozdelenie kompetencií agendy migrácie medzi viaceré inštitúcie.

Nejednotnosť systému štruktúry zberu dát a ich medzirezortného zdieľania.

Čo je potrebné urobiť?

Aktualizovať národnú stratégiu riadenej integrácie odídencov a migrantov.

Centralizovať agendu migrácie do jednej štátnej inštitúcie.

Vytvoriť jednotný systém štruktúry zberu dát umožňujúci ich efektívne medzirezortné zdieľanie a analýzu.

Zneužívanie slabých miest, nejednoznačností a medzier v legislatíve

Hybridný aktér môže zneužívať proti štátom ich vlastné právo a demokratické princípy, ako aj proces tvorby právnych predpisov a ich aplikáciu proti štátnym záujmom.

Formy možného hybridného pôsobenia

- **vykonávanie legislatívne neupraveného lobingu** na podporu strategických cieľov hybridného aktéra,
- **zneužitie zákona o slobodnom prístupe k informáciám,** vedúce k sprístupneniu informácií pre hybridných aktérov,
- **ovplyvnenie poslanca** alebo skupiny poslancov k účelnému predloženiu legislatívy a jej schvaľovaniu.

Pokusy ovplyvňovať legislatívny proces a prácu zákonodarných zborov sú častým javom. V prípade nevhodnej alebo nedostatočnej úpravy legislatívy môže pri presadení záujmov hybridného aktéra dôjsť až k **znefunkčneniu bezpečnostného systému SR.**

Zodpovedné inštitúcie

- Orgány štátnej správy,
- Legislatívna rada vlády SR,
- poslanci alebo poslanecké kluby.

Zákon o lobingu neprijatý už skoro 2 dekády

31. máj 2005

Klub 500: Zákon o lobingu by mal podrobne vymedziť formy práce lobistu

Bratislava 31. mája (TASR) - Slovenskí podnikatelia združení v Klube 500 privítali návrh zákona o lobingu, ktorý iniciovalo ministerstvo spravodlivosti, ...

TASR
Tlačová agentúra

Zdroj: https://domov.sme.sk/c/2241437/klub-500-zakon-o-lobingu-by-mal-podrobne-vymedzit-formy-prace-lobistu.html
Klub 500: Zákon o lobingu by mal podrobne vymedziť formy práce lobistu. In sme.sk [online].

Identifikované zraniteľnosti

Čo je potrebné urobiť?

Chýbajúci zákon o lobingu.	*Schváliť zákon o lobingu, zaviesť pravidlá transparentnosti vzťahov medzi ústavnými činiteľmi a lobistami.*
Nejasné aplikačné pravidlá zákona o slobodnom prístupe k informáciám.	*Zaviesť jednotnú metodiku pre aplikáciu zákona o slobodnom prístupe k informáciám.*
Chýbajúca diskusia pri skrátenom legislatívnom konaní, kedy nie je možné zhodnotiť potenciálne bezpečnostné riziká.	*Upraviť zákonné podmienky pre skrátené legislatívne konanie, kontrola využívania tohto inštitútu iba vo výnimočných situáciách.*

Polovojenské organizácie

Polovojenské skupiny, ktoré nie sú začlenené do bezpečnostných zborov štátu, predstavujú značné bezpečnostné riziko z dôvodu ich ovplyvňovania a manipulácie hybridnými aktérmi. Indoktrinácia ich členov postojmi, ktoré sú v rozpore s národno-štátnymi záujmami SR môže viesť najmä počas období destabilizácie bezpečnostnej situácie k ich zneužitiu na fyzické operácie, či ohrozovaniu bezpečnosti.

Formy možného hybridného pôsobenia

- **ozbrojená a agresívna účasť na nepokojoch,**
- fyzické **operácie proti bezpečnostným zložkám** SR,
- **zastrašovanie** obyvateľstva,
- vykonávanie **sabotáží a fyzických útokov** na kritické systémy a zariadenia,
- **snaha nahradiť štátne silové zložky,**
- aktivity smerujúce k **podpore domácich radikálnych organizácií.**

K najzávažnejšiemu ohrozeniu by došlo pri úplnom prebratí kontroly nad takýmito organizáciami hybridným aktérom. Ich zneužitie by malo závažné dôsledky na schopnosť štátu zabezpečiť ochranu života, zdravia, bezpečnosti, ako aj majetku vlastných občanov.

Zodpovedné inštitúcie

- Ministerstvo obrany SR,
- Ministerstvo vnútra SR,
- spravodajské služby.

Aktivity polovojenských organizácií v SR

4. októbra 2015 18:55

Slovenských brancov cvičí profesionálny vojak, armáda mlčí

MIRO KERN + Zapnúť články e-mailom

Inštruktorom polovojenskej organizácie je vojak z protivzdušnej brigády, ktorý absolvoval výcvik ruskej „vojensko – vlasteneckej" asociácie. Branci sa opäť chystajú chodiť do škôl.

Zdroj: https://dennikn.sk/256730/slovenskych-brancov-cvici-profesionalny-vojak-armada-mlci/ Slovenských brancov cvičí profesionálny vojak, armáda mlčí. In dennikn.sk [online].

Identifikované zraniteľnosti	Čo je potrebné urobiť?
Nízka kontrola štátu nad už existujúcimi polovojenskými organizáciami.	*Zaviesť mechanizmy k zabezpečeniu lepšej kontroly štátnych inštitúcií nad polovojenskými organizáciami.*
Chýbajúca legislatíva zaoberajúca sa **mládežou a mladými dospelými prejavujúcimi záujem o branné aktivity.**	*Zaviesť legislatívu, ktorá by umožňovala rozvoj branného povedomia a zdravého vlastenectva postaveného na demokratických hodnotách a zameraných na vojenstvo.*
Chýbajúca atraktívna a dostupná alternatíva k polovojenským organizáciám.	*Vytvoriť štátom akreditovanú a regulovanú alternatívu k polovojenským organizáciám pod vedením inštruktorov z radov súčasných či bývalých príslušníkov ozbrojených síl alebo bezpečnostných zborov.*

Financovanie kultúrnych skupín alebo think-tankov

Viaceré štáty využívajú kultúru a tzv. think-tanky ako spôsob šírenia svojej moci (napr. Čína prostredníctvom Konfuciových inštitútov). Nástrojom hybridného pôsobenia sa môžu stať aj náboženské spoločnosti a sekulárne organizácie.

Formy možného hybridného pôsobenia

- **poskytovanie financií** zo zahraničia,
- **zapájanie členov cirkví a náboženských spoločností do protizákonnej činnosti** či ozbrojených konfliktov mimo územia SR,
- **šírenie dezinformácií** alebo škodlivých informácií,
- vyvíjanie úsilia o zmenu demokratického zriadenia SR.

Hybridný aktér môže tieto skupiny využiť pre realizáciu svojich strategických cieľov. **Výsledkom môže byť dlhodobý vplyv na verejnú mienku,** šírenie extrémizmu a vplyv na politický vývoj v krajine.

Zodpovedné inštitúcie

- Ministerstvo kultúry SR

Komunikácia riaditeľa Konfuciovho inštitútu

22. apríla 2021 13:00

Spíte dobre? Mali by ste byť vo veľkom strese. Šéf čínskeho inštitútu píše slovenskému expertovi

MIREK TÓDA + Zapnúť články e-mailom

Čína si buduje vplyv v akademickom svete a snaží sa potlačiť slobodnú a kritickú debatu o svojom režime, hovorí slovenský výskumník Matej Šimalčík, ktorému šéf Konfuciovho inštitútu napísal výhražný email.

Zdroj: https://dennikn.sk/2361789/sef-cinskeho-institutu-pise-slovenskemu-expertovi/?ref=in Spíte dobre? Mali by ste byť vo veľkom strese. Šéf čínskeho inštitútu píše slovenskému expertovi. In sme.sk [online].

Identifikované zraniteľnosti

Nedostatočný prehľad o činnosti neregistrovaných cirkví a nedostatočná komunikácia s nimi.

Nedostatočné personálne kapacity pre výkon analýz a nízky počet súdnych znalcov v oblasti náboženského a politického extrémizmu.

Nedostatočná spolupráca so spravodajskými zložkami a chýbajúci monitoring.

Čo je potrebné urobiť?

Rozšíriť kompetencie MK SR a prehodnotiť proces registrácie cirkví a náboženských spoločností.

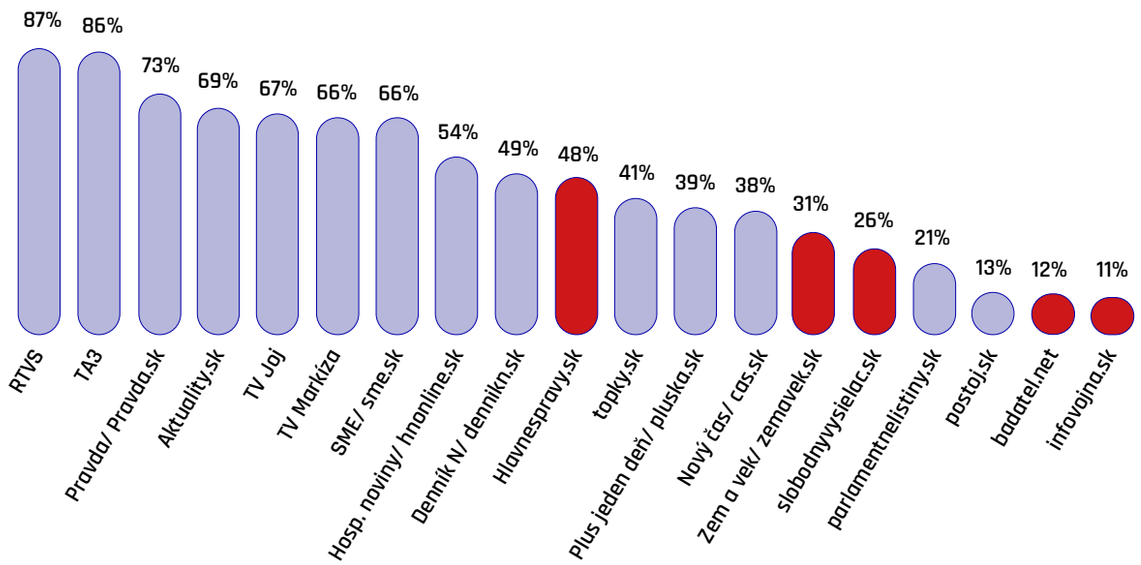
Rozšíriť kapacity MK SR o expertov na problematiku extrémizmu.

Vytvoriť medzirezortnú pracovnú skupinu a posilniť inštitucionálnu komunikáciu.

Ovplyvňovanie učebných osnov a akademickej obce

Hybridní aktéri môžu dlhodobo pôsobiť na mladú generáciu prostredníctvom výchovno-vzdelávacieho procesu, formovať jej postoje a presadzovať svoje vlastné politické, ideologické alebo nábožen-ské naratívy v rozpore so systémom základných práv a slobôd a demokratickými hodnotami.

Prieskum medzi učiteľmi o dôveryhodnosti médií



Zdroj: https://eduworld.sk/cd/tos/776/prieskum-medzi-ucitelmi-ockovanie-je-pripravou-na-cipovanie-ludi

Formy možného hybridného pôsobenia

- **ovplyvňovanie učebných osnov -** snaha o manipuláciu ich obsahu hybridným aktérom,
- **nadväzovanie partnerstiev** a budovanie kontaktov **za účelom šírenia propagandy,** vplývania na kritické myslenie alebo presadzovania personálnych zmien,
- **získavanie informácií o** výskume a vývoji kritických inovácií a technológií,
- **vytváranie nátlaku** na zamestnancov rezortu školstva.

Takéto ovplyvňovanie ohrozuje vzdelávací systém a slobodu akademického prostredia. To sa môže prejaviť **znížením spoločenskej súdržnosti a zvýšením sympatií voči hybridnému aktérovi.**

Zodpovedné inštitúcie

- Ministerstvo školstva, vedy, výskumu a športu SR,
- spravodajské služby.

Poznámka: vyznačené stránky sú identifikované ako stránky so sporným obsahom podľa projektu konspiratori.sk https://konspiratori.sk/zoznam-stranok

Identifikované zraniteľnosti

Absencia odborných kapacít v rezorte školstva, ktoré by špecificky pokrývali problematiku hybridných hrozieb.

Nízka úroveň povedomia o hybridných hrozbách v rezorte školstva.

Čo je potrebné urobiť?

Finančne, personálne a materiálno-technicky zabezpečiť vytvorenie odborných kapacít v rezorte školstva a zvýšiť tak spôsobilosť pružne reagovať na prijaté podnety.

Pripraviť osvetové aktivity pre relevantný okruh osôb, v záujme rozvíjania povedomia o hybridných hrozbách v rezorte školstva.

Využívanie strategickej korupcie

Podporou a využívaním korupcie sa hybridní aktéri snažia získať politický vplyv, manipulovať verejnou mienkou či vyzvedať utajované skutočnosti. Korupcia narúša dôveru v právny štát a jeho inštitúcie, a takto oslabený štát je ľahším cieľom pre hybridné pôsobenie.

Formy možného hybridného pôsobenia

- **poskytovanie úplatkov** politicky exponovaným osobám aby presadzovali určité politiky,
- **snaha o získavanie náklonnosti politikov,** médií, či verejne činných osôb prostredníctvom darov, pozvaní na spoločenské akcie alebo iných benefitov,
- **budovanie siete spriaznených osôb** na ovplyvňovanie verejnej mienky a spochybňovanie základných inštitúcii štátu,
- **využívanie osôb, ktoré sú prijímateľmi utajovaných skutočností** na spoluprácu a vyzradenie takýchto skutočností.

Ak štát nekoná proti podpore a využívaniu korupcie, **ohrozuje chod základných inštitúcií a podkopáva ich rozhodovacie mechanizmy.** Výsledkom môže byť narušená spoločenská a politická stabilita.

Zodpovedné inštitúcie

- Úrad vlády SR,
- Ministerstvo vnútra SR,
- spravodajské služby.

Príklad získavania vplyvu prostredníctvom korupcie

Katarský škandál: Europarlament zbavil funkcie podpredsedníčku obvinenú z korupcie

Autor: Barbara Zmušková a EURACTIV.com | EURACTIV.sk | Preklad: Tatiana Turisová

13 Dec 2022 (aktualizované: 14 Dec 2022)

Grécka podpredsedníčka Európskeho parlamentu Eva Kaili bola zadržaná pre podozrenia z korupcie po tom, ako u nej doma belgickí vyšetrovatelia našli „tašky plné peňazí". Konferencia predsedov navrhla, aby bola zbavená funkcie a europarlament návrh schválil s iba jedným hlasom proti.

Okrem nej boli obvinení a zadržaní ďalší štyria podozriví vrátane jej partnera Francesca Giorgioho, ktorý pôsobil ako asistent inej europoslankyne. Obvinení boli aj bývalý europoslanec Pier Antonio Panzeri, v ktorého dome sa našlo veľké množstvo peňazí, a Panzeriho bývalý asistent.

Zdroj: https://euractiv.sk/section/buducnost-eu/news/katarsky-skandal-europarlament-zbavil-funkcie-podpredsednicku-obvinenu-z-korupcie/

Identifikované zraniteľnosti

Nesystematické zaradenie niektorých korupčných trestných činov v rámci členenia Trestného zákona.

Chýbajúca komplexná výmena informácií medzi Ministerstvom vnútra SR a spravodajskými službami.

Čo je potrebné urobiť?

Preskúmať ustanovenia Trestného zákona s cieľom vypustiť, doplniť, či presunúť niektoré skutkové podstaty trestných činov pod trestné činy korupcie.

Prispôsobiť aktivity výboru Bezpečnostnej rady SR pre koordináciu spravodajských služieb tak, aby predstavoval platformu pre efektívnu a pravidelnú výmenu informácii medzi Ministerstvom vnútra SR a spravodajskými službami.

Nátlak na politikov alebo členov vlády

Hybridní aktéri môžu využívať širokú škálu nátlakových prostriedkov na politikov alebo predstaviteľov štátu spôsobom, ktorý je za hranicou legitímnych spôsobov na presadzovanie záujmov (napr. lobing). Takýto nátlak zahŕňa protiprávne konanie alebo hrozbu použitia násilia.

Formy možného hybridného pôsobenia

- **vyhrážanie, vydieranie** a vyvíjanie nátlaku,
- **poskytnutie citlivých informácií** hybridným aktérom,
- **tzv. doxxing –** uverejňovanie osobných informácií, ako adresa, telefónne číslo a pod.,
- **organizované zhromaždenia** alebo protesty s prvkom násilia,
- **očierňovanie a diskreditácia** vo verejnom priestore s využitím falošných informácií / vizuálov.

Cieľom hybridných aktérov je predovšetkým **ovplyvniť, ochromiť alebo podkopať rozhodovacie procesy štátu,** a tak dosiahnuť svoje záujmy. Nátlak môže byť vyvíjaný cudzími nepriateľskými aktérmi prostredníctvom organizovaných zločineckých skupín, alebo aj rôznych právnických osôb.

Zodpovedné inštitúcie

- Ministerstvo vnútra SR,
- spravodajské služby.

Príklad nátlaku na politických predstaviteľov (2021)


KRVAVÝ ODKAZ CELEJ VLÁDE SLOVENSKEJ REPUBLIKY,PREZIDENTKE ČAPUTOVEJ,POSLUHOVAČOM A VLASTIZRADCOM

ULTIMÁTUM NA PODANIE DEMISIE CELEJ VLÁDY

Vy čo si hovorite vláda Slovenskej republiky vás vyzývame na odchod s termínom do 31.3.2021.Nebudeme s vami vyjednávať! V prípade že tak neurobíte čakajú vás kruté a krvavé časy. Nepomôže vám nikto, máte málo ľudí na to aby vás pred nami ochránili.

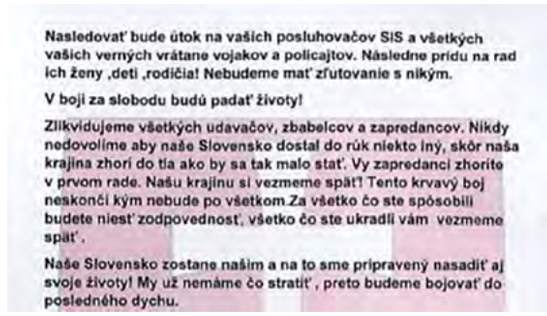
Máme kontakty s adresami aj s tými prechodnými na vás všetkých vrátane vašich rodín, armádnych predstaviteľov a celej zostavy polície. Pre prípad že tak neučiníte sme pripravení ísť do krvavého boja za slobodu!

Postupne vám začneme likvidovať vládne budovy a pridružené úrady, neskôr objekty ochranných a obranných zložiek štátu, nasledovať bude kompletný vozový park celého štátneho aparátu. Toľko hasičských jednotiek nemáte aby ste všetko uhasili.

Úrad vlády zhorí v plameňoch!

Vy ste nám tu nastolili režim chaosu teraz vám ukážeme chaos my v pravom slova zmysle.

Slovensko bude v plameňoch ktoré sa vám vryjú do vašich žíl a bolesť ktorú pocítite nikdy neskončí!


Nasledovať bude útok na vašich posluhovačov SIS a všetkých vašich verných vrátane vojakov a policajtov. Následne prídu na rad ich ženy ,deti ,rodičia! Nebudeme mať zľutovanie s nikým.

V boji za slobodu budú padať životy!

Zlikvidujeme všetkých udavačov, zbabelcov a zapredancov. Nikdy nedovolíme aby naše Slovensko dostal do rúk niekto iný, skôr naša krajina zhorí do tla ako by sa tak malo stať. Vy zapredanci zhoríte v prvom rade. Našu krajinu si vezmeme späť! Tento krvavý boj neskončí kým nebude po všetkom.Za všetko čo ste spôsobili budete niesť zodpovednosť, všetko čo ste ukradli vám vezmeme späť.

Naše Slovensko zostane našim a na to sme pripravený nasadiť aj svoje životy! My už nemáme čo stratiť , preto budeme bojovať do posledného dychu.

Vizuál vyhrážok zaslaných viacerým štátnym inštitúciám v roku 2021

Identifikované zraniteľnosti

Nízke povedomie poslancov NR SR a ich asistentov o problematike nátlaku na politikov a možnostiach riešenia.

Trestná legislatíva neumožňuje efektívne objasňovať a postihovať takýto nátlak, ak sa dotknutá osoba necíti byť ohrozená.

Čo je potrebné urobiť?

Vytvoriť špecializované školenia pre poslancov NR SR a ich asistentov.

Vytvoriť pracovnú skupinu na prehodnotenie postihovania nátlaku na politikov a členov vlády v Trestnom zákone.

Veľvyslanectvá

Veľvyslanectvá môžu byť zneužité na vyvíjanie diplomatického nátlaku, tiež ako miestne veliteľské, riadiace a koordinačné centrá pre informačné a spravodajské operácie. Môžu byť zneužité aj na šírenie propagandy a vytváranie siete domácich aktérov podporujúcich ciele hybridného aktéra.

Formy možného hybridného pôsobenia

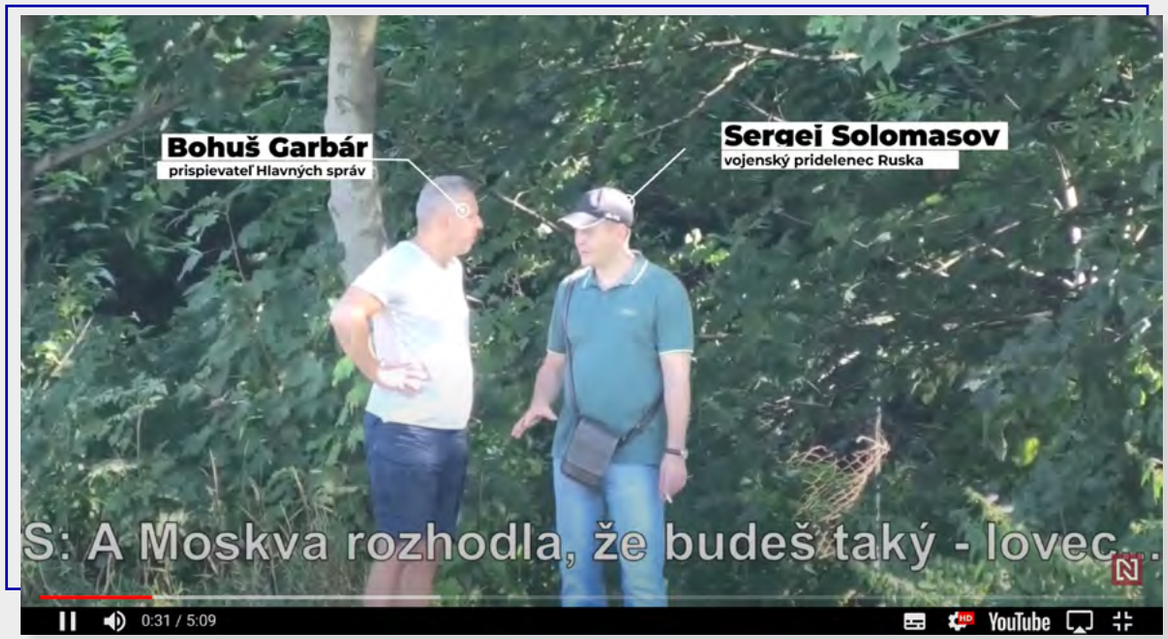
- **vysielanie pracovníkov** informačných služieb pod diplomatickým krytím,
- **nadväzovanie kontaktov** so zamestnancami štátnej správy, snahy o získanie citlivých informácií,
- **podplácanie dezinformačných a kvázi-médií** výmenou za publikovanie článkov, ktoré vyhovujú cudzím zahraničnopolitickým záujmom,
- **šírenie dezinformácií** cez oficiálne účty veľvyslanectva na sociálnych sieťach.

V SR **boli zaznamenané aktivity** niektorých krajín zneužívajúce ich zastupiteľské úrady. Využívanie veľvyslanectiev na vplyvové aktivity má potenciál **ovplyvňovať nálady v spoločnosti, destabilizovať krajinu a narúšať jej zahraničnopolitické smerovanie.**

Zodpovedné inštitúcie

- Ministerstvo zahraničných vecí a európskych záležitostí SR,
- spravodajské služby.

Zábery ruského „diplomata“ pri uplácaní redaktora Hlavných správ



Uniknutá nahrávka bezpečnostných zložiek zachytáva vojenského pridelenca na ruskej ambasáde v Bratislave, ako poskytuje úplatok prispievateľovi Hlavných správ a verbuje ho na špionáž.

Zdroj: Denník N

Zdroj: https://dennikn.sk/2767779/ako-sa-verbuju-spioni-na-slovensku-povedal-som-v-moskve-ze-si-dobry-chlapec-video/

Identifikované zraniteľnosti

Vydávanie súhlasu v súvislosti s príchodom diplomatických pracovníkov z iných krajín **bez dôsledného preverenia.**

Čo je potrebné urobiť?

Zaviesť účinnejšie kontrolné mechanizmy na zamedzenie zneužívania diplomatického statusu prichádzajúcimi pracovníkmi zahraničných zastupiteľských úradov.

Využívanie diaspór k ovplyvňovaniu

Diaspóry sa môžu stať nástrojom hybridného pôsobenia vtedy, keď ich aktivity skryto manipuluje vláda cudzieho štátu. Cieľom je ovplyvňovanie politických procesov, rozhodovania a verejnej mienky v hostiteľskej krajine v dlhodobom horizonte.

Formy možného hybridného pôsobenia

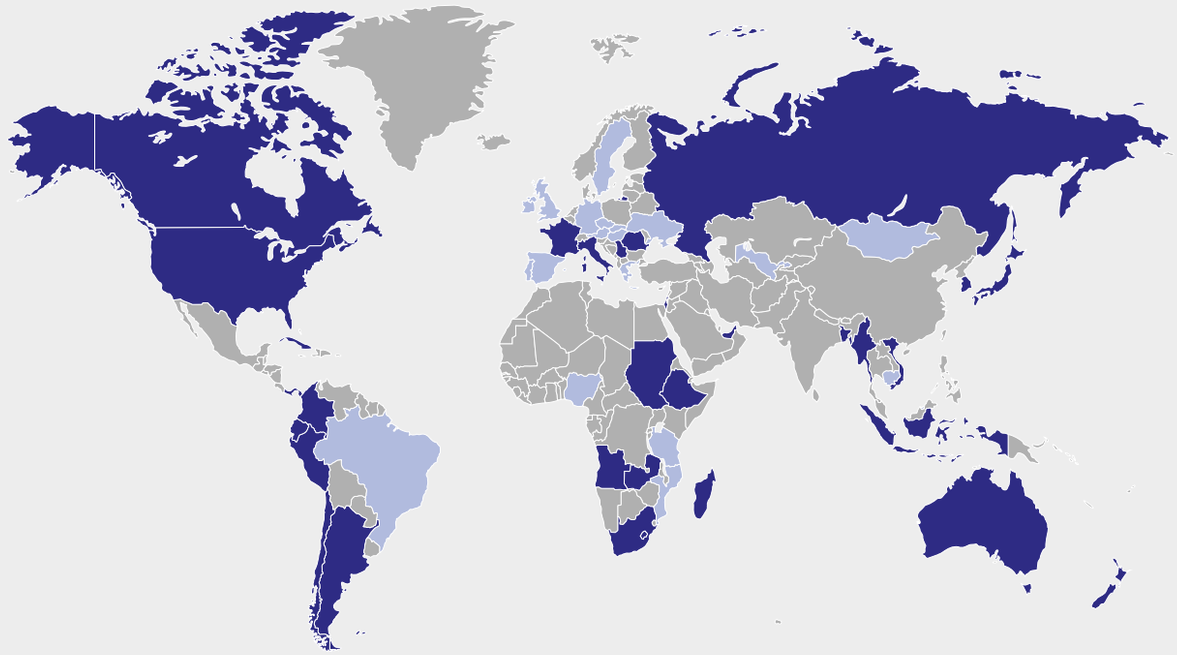
- **financovanie kultúrnych inštitútov,** spolkov či médií a ich zneužívanie na aktivity glorifikujúce vládu cudzieho štátu,
- **šírenie odlišného vnímania histórie** a zahraničnopolitického smerovania medzi členmi diaspóry,
- **znižovanie lojality členov** diaspór k SR,
- **ovplyvňovanie diaspóry** k podpore konkrétnych politických aktérov,
- **pôsobenie agentov** v rámci diaspóry pod podnikateľským krytím a ich participácia na štátnych zákazkách či zabezpečení technologických zariadení v citlivých oblastiach.

V súčasnosti v SR existujú, v porovnaní s ostatnými štátmi EÚ, **relatívne málo početné diaspóry** pochádzajúce z krajín využívajúcich hybridné pôsobenie na dosahovanie svojich cieľov.

Zodpovedné inštitúcie

- Ministerstvo zahraničných vecí a európskych záležitostí SR,
- Ministerstvo kultúry SR,
- Ministerstvo školstva, vedy, výskumu a športu SR.

Takzvané čínske policajné stanice



Zdroj: https://safeguarddefenders.com/en/blog/patrol-and-persuade-follow-110-overseas-investigation

Krajiny so známymi stanicami
Krajiny s novo odhalenými stanicami

Mimovládna ľudskoprávna organizácia Safeguard Defenders publikovala v septembri 2022 správu odhaľujúcu sieť takzvaných čínskych policajných staníc pôsobiacich v 53 krajinách sveta, vrátane SR. Tieto takzvané policajné stanice v niektorých krajinách sa mali podľa správy podieľať na prenasledovaní, zastrašovaní a nátlaku na členov čínskej diaspóry v zahraničí.

Identifikované zraniteľnosti

Nedostatočný prehľad o pohybe a využití finančných prostriedkov vynaložených na aktivity národnostných menšín, etnických skupín a diaspór zo zahraničia.

Čo je potrebné urobiť?

Zaviesť systém monitoringu finančných tokov na podporu diaspór zo zahraničia.

Diplomatické a ekonomické sankcie

Sankcie vo forme embárg, ciel a iných opatrení, môžu byť zneužité na oslabenie ekonomiky, vyvinutie nátlaku a ovplyvňovanie rozhodovacích procesov. Zároveň však ide o legitímny nástroj demokratických krajín na ochranu svojich záujmov voči hybridným aktérom.

Formy možného hybridného pôsobenia

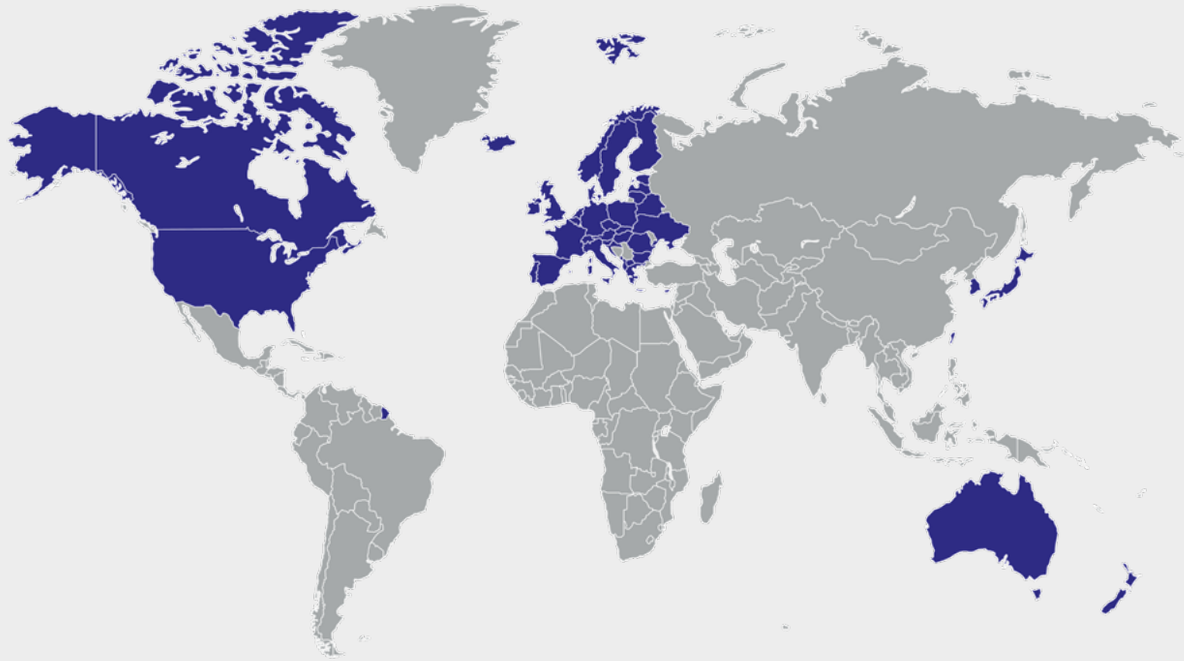
- **zákaz cestovania** ako forma nátlaku,
- **prerušenie diplomatických väzieb** alebo ich obmedzenie,
- **uvalenie exportných obmedzení,**
- **zmrazenie majetku** vybraných spoločností v cudzej krajine.

Uvalenie sankcií má symbolický aj politický charakter a **môže výrazne ovplyvniť nálady v spoločnosti.** Od schopnosti SR a EÚ efektívne a včasne prijímať odvetné opatrenia výrazne závisí rozsah pôsobenia hybridných aktérov.

Zodpovedné inštitúcie

- Vláda SR,
- Ministerstvo zahraničných vecí a európskych záležitostí SR,
- Ministerstvo hospodárstva SR,
- Ministerstvo financií SR,
- Ministerstvo spravodlivosti SR.

Ruský zoznam „nepriateľských krajín“



Zdroj: https://safeguarddefenders.com/en/blog/patrol-and-persuade-follow-110-overseas-investigation

V roku 2021 Rusko zverejnilo zoznam „nepriateľských krajín“, proti ktorým zaviedlo reštriktívne opatrenia v reakcii na ich „nepriateľské“ správanie. Na zoznam odvtedy priebežne pribúdajú ďalšie krajiny (vrátane SR v roku 2022). Reštriktívne opatrenia zahŕňajú vízové obmedzenia, povinnosť platiť za ruský plyn v rubľoch, či obmedzenie počtu miestnych pracovníkov na veľvyslanectvách v Rusku.

Zdroj: oficiálna webstránka vlády Ruskej federácie

Identifikované zraniteľnosti

Nejasné vymedzenie kompetencií národných orgánov v zákone o vykonávaní medzinárodných sankcií.

→ *Špecifikovať zákonnú úpravu v oblasti medzinárodných sankcií, ktorá jednoznačne stanoví a určí právomoci zodpovedných rezortov.*

Chýbajúca prax pri vyhlasovaní národných sankcií.

→ *Zvážiť zavedenie procesu prijímania národných sankcií zo strany SR a následné zriadiť potrebné personálne kapacity.*

Čo je potrebné urobiť?

Ovládanie a zasahovanie do médií

Médiá a mediálne služby sa môžu stať nástrojom hybridného pôsobenia. Hybridní aktéri sa snažia o dosiahnutie vplyvu na tradičné médiá alebo o vybudovanie siete kvázi-médií a informačných kanálov na sociálnych sieťach s cieľom ovplyvniť verejnú mienku a destabilizovať spoločnosť.

Formy možného hybridného pôsobenia

- **ovládanie médií a zasahovanie do ich činnosti,** prostredníctvom politického vplyvu, infiltrácie, sponzorovania médií, alebo získaním vlastníckej kontroly,
- **šírenie dezinformácií,** škodlivých informácií a manipulatívnych naratívov prostredníctvom sociálnych sietí a kvázi-médií,
- **spochybňovanie dôveryhodnosti** tradičných médií.

Ovládanie a zasahovanie do médií predstavuje vážne bezpečnostné riziko, ktoré **môže ohroziť slobodu prejavu, dôveru verejnosti vo verejné informácie a v konečnom dôsledku aj demokraciu samotnú.**

Zodpovedné inštitúcie

- Rada pre mediálne služby,
- Ministerstvo kultúry SR.

Ekosystém médií a kanálov pod kontrolou RF

Zdroj: Russia's Propaganda & Disinformation Ecosystem - 2022 Update & New Disclosures (substack.com)

Identifikované zraniteľnosti

Absencia vykonávacích predpisov k zákonu o mediálnych službách.

Chýbajúca formalizácia spolupráce Rady pre mediálne služby a spravodajských a bezpečnostných zložiek.

Čo je potrebné urobiť?

Prijať chýbajúce vykonávacie predpisy vyplývajúce zo zákona o mediálnych službách.

Formalizovať procesy spolupráce medzi regulátorom a bezpečnostnými zložkami.

Výmena utajovaných skutočností

Pri efektívnej obrane proti spravodajským operáciám a infiltrácii hrajú dôležitú úlohu aj orgány verejnej moci, vrátane ich schopnosti plynule sa oboznamovať s utajovanými skutočnosťami na potrebnej úrovni.

Formy možného hybridného pôsobenia

- **zneužitie neschopnosti dotknutých orgánov** verejnej moci oboznamovať sa s charakterom a rozsahom vznikajúcich hrozieb,
- **využitie pomalého rozhodovacieho procesu** ako prekážky plynulej informačnej výmeny utajovaných skutočností medzi orgánmi verejnej moci.

Niektoré orgány verejnej moci nedisponujú dostatočnými personálnymi kapacitami s danou spôsobilosťou. Dôsledkom toho sa **nedokážu oboznamovať s utajovanými skutočnosťami v maximálnom rozsahu a primeranom čase.**

Zodpovedné inštitúcie

- Národný bezpečnostný úrad,
- spravodajské služby,
- všetky ústredné orgány štátnej správy.

Informovanie občanov o činnosti SIS a VS

Zdroj: https://www.sis.gov.sk/pre-vas/sprava-o-cinnosti.html
https://vs.mosr.sk/aktuality/

Identifikované zraniteľnosti

Nedostatočné personálne **kapacity orgánov verejnej moci oboznamovať sa s utajovanými skutočnosťami** na úrovni vyššej ako je stupeň utajenia Vyhradené.

Čo je potrebné urobiť?

Zabezpečiť dostatočné personálne oprávnenie oboznamovať sa s utajovanými skutočnosťami vyššieho stupňa utajenia v súlade s objektívnymi potrebami orgánov.

Priame zahraničné investície (PZI)

Popri prevažujúcom pozitívnom vplyve prichádzajúcich PZI aktuálne rastie počet nepriateľských investícií vykonaných za účelom ovládnutia infraštruktúry alebo získania know-how. Hybridní aktéri ich môžu využívať na manipuláciu s investičným prostredím a získavanie strategických aktív.

Formy možného hybridného pôsobenia

- **získanie vplyvu v určitom sektore** s cieľom ho narušiť – napr. zdravotníctvo, financie, energetika, obrana, IT, médiá,
- **získanie podielu v médiách** a následné ovplyvňovanie verejnej mienky a šírenie dezinformácií,
- **dosiahnutie prístupu k strategickým surovinám** alebo dodávkam s úmyslom ich narušiť, poškodiť, získať, prípadne umelo ovplyvniť ich dostupnosť.

V prípade nepriateľských PZI môže dôjsť k **prístupu tretích štátov k citlivým technológiám,** know-how, kritickej infraštruktúre, dodávkam alebo službám, ktoré sú **kritické a strategické pre SR.** Takéto investície umožňujú získanie vplyvu v rôznych sektoroch.

Zodpovedné inštitúcie

- Ministerstvo hospodárstva SR,
- Ministerstvo zahraničných vecí a európskych záležitostí SR,
- spravodajské služby.

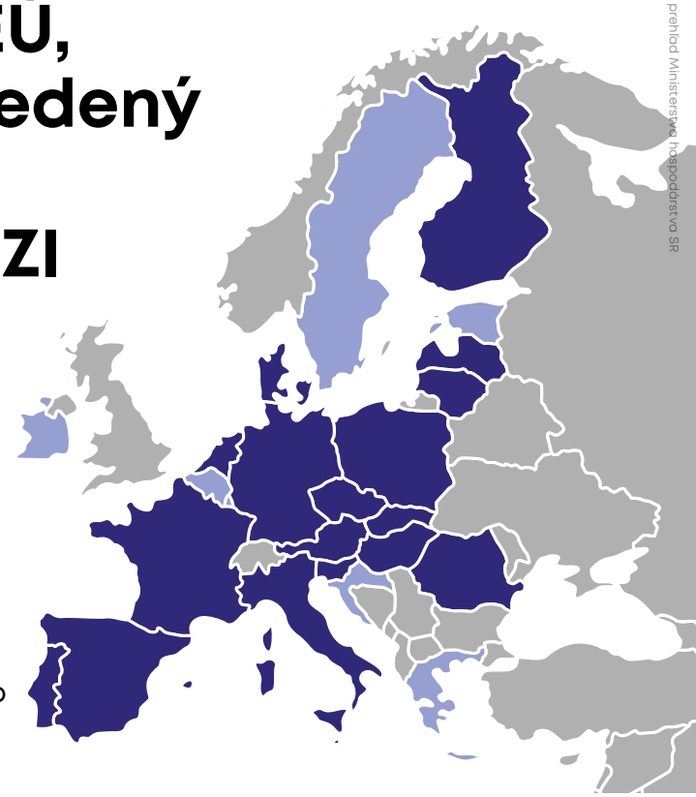
Členské štáty EÚ, ktoré majú zavedený mechanizmus preverovania PZI

Česká republika, Dánsko, Fínsko, Francúzsko, Holandsko, Litva, Lotyšsko, Maďarsko, Malta, Nemecko, Poľsko, Portugalsko, Rakúsko, Rumunsko, Slovensko, Slovinsko, Španielsko, Taliansko

Členské štáty EÚ, ktoré pripravujú mechanizmus preverovania PZI

Belgicko, Chorvátsko, Estónsko, Grécko, Írsko, Luxembursko, Švédsko

stav ku 12.05.2023



Zdroj: prehľad Ministerstva hospodárstva SR

Identifikované zraniteľnosti

Čo je potrebné urobiť?

Absencia prístupov do databáz združujúcich potrebné informácie o podnikateľských subjektoch.

→ *Zakúpiť licencie na prístup do databáz združujúcich potrebné informácie z celého sveta o podnikateľských subjektoch a iných osobách, ktoré sú súčasťou zahraničnej investície.*

Nedostatočné analytické kapacity v rámci MH SR.

→ *Posilniť personálne kapacity MH SR na preverovanie PZI.*

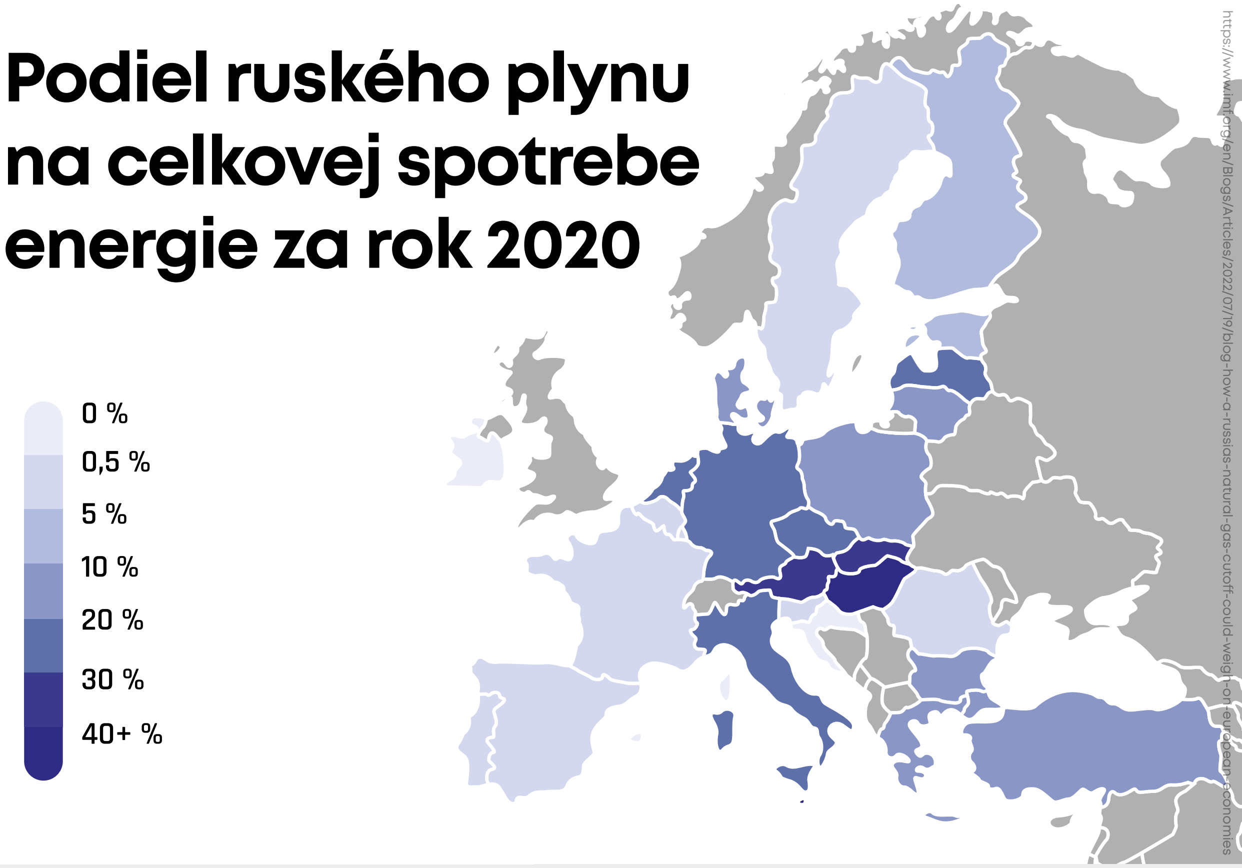
Nedostatočná certifikácia aplikácie pre zdieľanie utajovaných informácií medzi rezortmi a spravodajskými službami.

→ *Certifikovať aplikáciu na zdieľanie utajovaných informácií vo vyšších stupňoch utajenia.*

Vytvorenie a zneužívanie energetickej závislosti

Závislosť od energetických zdrojov iných štátov umožňuje hybridným aktérom manipulovať s ich cenami, kontrolovať infraštruktúru alebo hroziť prerušením dodávok pri nesplnení určitých podmienok.

Podiel ruského plynu na celkovej spotrebe energie za rok 2020



Formy možného hybridného pôsobenia

- **manipulácia s cenami a dostupnosťou** energetických surovín z krajín mimo EÚ,
- **kybernetické útoky** na energetickú infraštruktúru s cieľom prerušenia výroby alebo dodávky elektriny,
- **ovplyvňovanie kľúčových zamestnancov** infraštruktúry.

Energetická závislosť a manipulácia s cenami môže ovplyvniť ekonomiku a spôsobiť znižovanie životnej úrovne obyvateľov. To **môže viesť k polarizácii spoločnosti, ovplyvňovaniu politickej situácie a zníženiu dôvery v štátne inštitúcie.**

Zodpovedné inštitúcie

- Ministerstvo hospodárstva SR,
- Ministerstvo zahraničných vecí a európskych záležitostí SR,
- spravodajské služby.

Identifikované zraniteľnosti	Čo je potrebné urobiť?
Neaktuálny plán pripravenosti SR na riziká v sektore elektrickej energie.	*Aktualizovať plán pripravenosti SR na riziká v sektore elektrickej energie.*
Neaktuálny Integrovaný národný energetický a klimatický plán.	*Aktualizovať integrovaný národný energetický a klimatický plán v súlade s požiadavkami nariadenia Rady a EP č. 2018/1999.*
Chýbajúci spoločný systém zberu dát za oblasť energetiky.	*Podporiť vytvorenie spoločnej databázy v sektore energetiky na úrovni EÚ v rámci reformy REPowerEU.*

Vytváranie a zneužívanie ekonomických ťažkostí a závislostí

Blízke ekonomické väzby môžu zvýšiť strategickú závislosť menších krajín od väčších, môžu ich zaviazať cez štátny dlh, prípadne cez unikátne alebo kritické vzácne komodity. Hybridní aktéri môžu narušiť dodávateľské reťazce, a tým spôsobiť nedostatok dodávok strategických surovín.

Formy možného hybridného pôsobenia

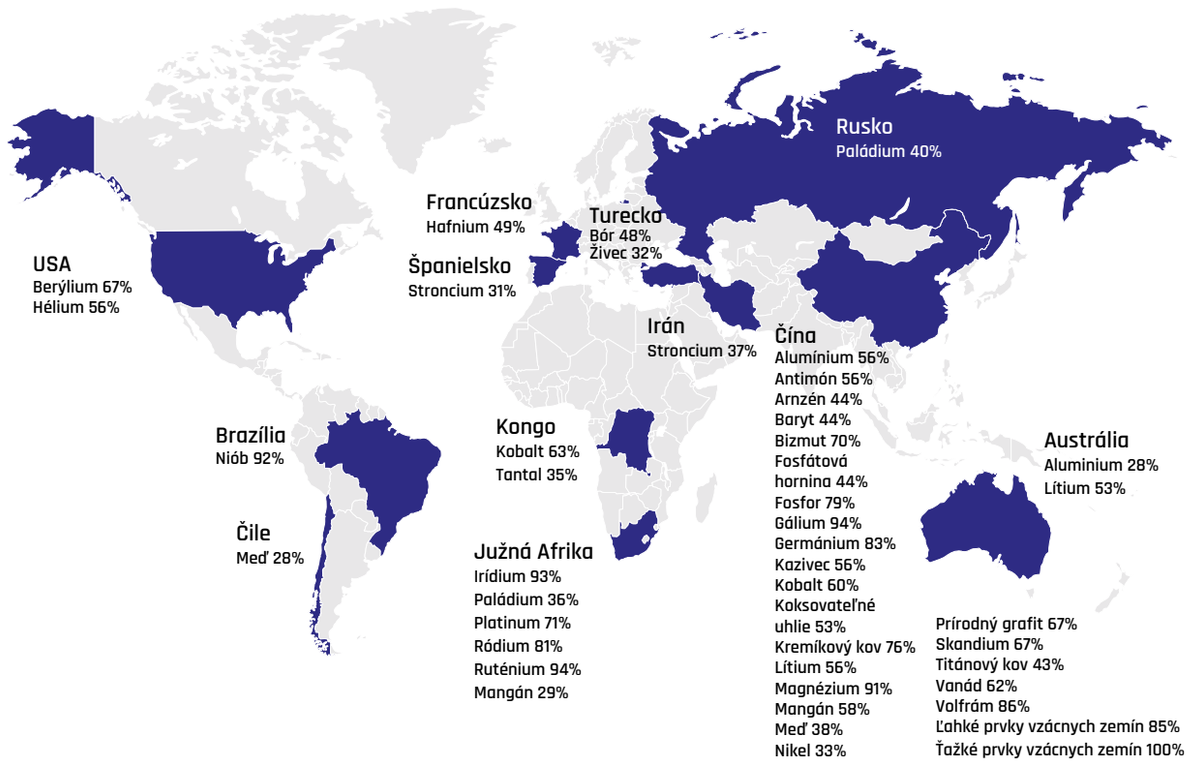
- **budovanie nediverzifikovaných strategických partnerstiev** pre kľúčové komodity,
- **využívanie závislostí krajín** a uprednostňovanie dodávateľských reťazcov so spriaznenými krajinami,
- **ovplyvnenie dodávok a umelé navyšovanie cien kritických surovín** a komodít.

Hybridní aktéri môžu zneužiť spomalenie ekonomického rozvoja a rastu spôsobené nedostatočnou konkurencieschopnosťou a neschopnosťou zabezpečiť financovanie z domácich trhov. Cieľom je **spochybnenie legitímnosti vlády a vykreslenie obrazu zlyhávajúceho štátu.**

Zodpovedné inštitúcie

- Ministerstvo hospodárstva SR,
- Ministerstvo zahraničných vecí a európskych záležitostí SR.

Globálne rozdelenie kritických nerastných surovín



Zdroj: https://www.intereconomics.eu/contents/year/2023/number/2/article/the-eu-s-quest-for-strategic-raw-materials The EU's Quest for Strategic Raw Materials: What Role for Mining and Recycling? In intereconomics.eu [online].

Identifikované zraniteľnosti

Nedostupnosť špecifických dát rezortov v oblasti ekonomických ťažkostí a závislostí.

Zmeny v iniciatívach a politikách EÚ môžu mať priamy dopad na ťažkosti a závislosti slovenského priemyslu.

Čo je potrebné urobiť?

Vytvoriť systém pre zdieľanie dát v oblasti ekonomických ťažkostí a závislostí medzi relevantnými štátnymi orgánmi.

Monitorovať dopady politík a iniciatív EÚ na slovenský priemysel a proaktívne ich komunikovať s podnikateľskými subjektami a združeniami.

Záver

Ďakujeme vám za pozornosť, ktorú ste venovali tejto verejnej analýze zraniteľností voči hybridným hrozbám. **Je výsledkom dlhodobého úsilia a odhodlania skúmať nové bezpečnostné výzvy, ktorým Slovensko čelí v dnešnej dynamicky meniacej sa svetovej scéne**. Sme presvedčení, že spolupráca so všetkými zainteresovanými stranami, vrátane verejného sektora, súkromného sektora a akademických inštitúcií, je nevyhnutná pre efektívne riešenie týchto hrozieb.

Veríme, že táto analýza poskytne základ pre ďalšie budovanie odolnosti Slovenskej republiky voči hybridným hrozbám. **Identifikovali sme kľúčové oblasti, kde je potrebné zvýšiť našu ostražitosť, pripraviť systémové zmeny týkajúce sa legislatívneho alebo inštitucionálneho nastavenia, alebo prijať praktické preventívne opatrenia na úrovni jednotlivých inštitúcií**. Majú za cieľ posilniť obranyschopnosť našej krajiny a zabezpečiť pripravenosť na rôzne možné scenáre.

Sme si vedomí, že taktiky hybridných aktérov, ako aj nimi využívané nástroje, sa neustále menia, a preto **je kritické udržiavať si odborné poznatky a aktualizovať stratégie a analytické výstupy v tejto oblasti pravidelne**. Veríme, že spoločne s našimi partnermi budeme schopní včasného odhaľovania a rýchlej reakcie na potenciálne hrozby.

Táto analýza je však len prvým krokom na dlhej ceste budovania silnej a odolnej spoločnosti. Bude nám slúžiť ako cenný základ a kompas pri tvorbe nových iniciatív a politík, ktoré nás posunú vpred. Počas prípravy tejto verejnej verzie naše Centrum boja proti hybridným hrozbám MV SR začalo pripravovať Koncepciu budovania odolnosti verejnej správy proti hybridným hrozbám v rámci plnenia úlohy C.1 z APHH, za účelom pretavenia zistení analýzy do praxe. Najväčšia pridaná hodnota analýzy má totiž spočívať v implementácií navrhnutých opatrení, ktoré nás môžu posúvať krok za krokom na našej ceste k odolnosti.

Na záver by sme chceli ešte raz vyjadriť našu hlbokú vďaku všetkým, ktorí prispeli k tejto analýze a k posilneniu odolnosti Slovenska voči hybridným hrozbám. Vaša angažovanosť a oddanosť spoločnému cieľu sú kľúčové pre náš spoločný úspech a bezpečnosť!

Slovník pojmov a skratiek

3D zbrane – strelné zbrane, ktoré sa vyrábajú predovšetkým pomocou 3D tlačiarne. Podľa Interpolu ich možno kategorizovať ako plne 3D tlačené strelné zbrane, hybridné 3D tlačené zbrane a strelné zbrane, ktorých rám sa vyrába v 3D tlači.

80% zbrane – tzv. nedokončená zbraň, resp. kus kovu, ktorý sa vo svojej súčasnej podobe nedá použiť ako strelná zbraň, ale ľahko sa dá na ňu upraviť. Komponenty sú neregulované a ľahko dostupné.

APHH – Akčný plán koordinácie boja proti hybridným hrozbám, dokument na posilnenie odolnosti štátu a spoločnosti voči hybridným hrozbám.

Diaspóra – náboženské alebo etnické spoločenstvo žijúce (rozptýlene) v rámci iného (cudzieho) spoločenstva.

Hybridné pôsobenie – aktivity štátnych alebo neštátnych aktérov na oslabenie alebo poškodenie, vybraného cieľa za využitia vojenských i nevojenských metód (dezinformácie, propaganda, kybernetické útoky...).

INEKP – Integrovaný národný energetický a klimatický plán na roky 2021 – 2030, zaoberajúci sa energetickou bezpečnosťou, efektívnosťou, konkurencieschopnosťou a udržateľnosťou, plus dekarbonizáciou.

Lobing – proces ovplyvňovania zákonodarcov, ministrov a iných štátnych úradníkov, prípadne hospodárskych subjektov, záujmovými/nátlakovými skupinami presadzujúcimi spoločný záujem (tzv. loby) s cieľom dosiahnuť určité rozhodnutie/čin.

Migrant – osoba, ktorá sa nachádza mimo územia vlastného štátu, prebývajúca v inej krajine viac ako jeden rok bez ohľadu na dôvody (dobrovoľné, nedobrovoľné, vojnové, ekonomické) a spôsoby jej migrácie do krajiny (regulárne alebo neregulárne).

Odídenec – osoba, ktorá odišla z domova najčastejšie pre obavy z vojnových udalostí; žiadateľ o dočasné útočisko v cudzom štáte.

Polarizácia (spoločnosti) – vyhraňovanie, vyhrocovanie so zreteľom na protiklady, usmerňovanie nejakého zoskupenia na určité javy / skutočnosti.

Položky s dvojakým použitím – produkty alebo technológie vyvinuté na civilné účely, no v nesprávnych rukách zneužité na porušovanie ľudských práv alebo teroristické útoky (drony, chemikálie).

Prekurzory výbušnín – chemické látky zneužiteľné na zostrojenie podomácky vyrobených výbušnín (napr. kyselina dusičná, kyselina sírová, nitrometán...).

PZI – priame zahraničné investície do zahraničného obchodného podniku určené na získanie kontrolného podielu v podniku (vertikálne, horizontálne alebo konglomerátne).

REPowerEU – reforma slúžiaca na úsporu a podporu čistej energie, diverzifikáciu jej dodávok do EÚ, rozumnú kombináciu investícií a reforiem, má za cieľ dosiahnuť do roku 2030 zníženie čistých emisií skleníkových plynov aspoň o 55 % a klimatickú neutralitu do roku 2050.

ŠS – štátna správa, jedna z foriem výkonu verejnej moci.

Think tanky – nezávislé organizácie, ktoré sa zaoberajú výskumom a analýzou tém týkajúcich sa verejných záležitostí. Patria sem napríklad sociálna politika, politická stratégia, ekonomika, vojenské záležitosti, technológia, kultúra.

ÚOŠS – Ústredné orgány štátnej správy - patria sem ministerstvá a dôležité úrady (napr. Úrad vlády SR, Národný bezpečnostný úrad, atď.).

Verejné obstarávanie – pravidlá a postupy pri výbere zmluvného partnera, zastrešujúce zadávanie zákaziek. Ich cieľom je efektívne a hospodárne využitie verejných prostriedkov.

Základná bibliografia ku kapitolám

Systém boja proti hybridným hrozbám

- Koncepcia bezpečnostného systému Slovenskej republiky
- Akčný plán koordinácie boja proti hybridným hrozbám na roky 2022 až 2024
- Bezpečnostná stratégia SR
- Obranná stratégia SR
- Programové vyhlásenie vlády SR 2023
- Programové vyhlásenie vlády Slovenskej republiky na obdobie rokov 2021 – 2024

Dezinformačné kampane a propaganda

- 1st EEAS Report on Foreign Information Manipulation and Interference Threats
- Závery Rady o manipulácii s informáciami a zasahovaní zo zahraničia (FIMI)
- Koncepcia strategickej komunikácie SR
- Zákon č. 264/2022 Z. z. o mediálnych službách a o zmene a doplnení niektorých zákonov (zákon o mediálnych službách)
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

Ovplyvňovanie volieb

- Zákon č. 85/2005 Z. z. o politických stranách a politických hnutiach v znení neskorších predpisov
- Zákon č. 180/2014 Z. z. o podmienkach výkonu volebného práva a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- Zákon č. 181/2014 Z. z. o volebnej kampani a o zmene a doplnení zákona č. 85/2005 Z. z. o politických stranách a politických hnutiach v znení neskorších predpisov
- Zákon č. 395/2022 Z. z. o špeciálnom spôsobe hlasovania v referende vyhlásenom na základe petície občanov prijatej 24. augusta 2022

Rozširovanie zbraní

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/821 z 20. mája 2021, ktorým sa stanovuje režim Únie na kontrolu vývozov, sprostredkovania, technickej pomoci, tranzitu a transferu položiek s dvojakým použitím.
- Zákon č. 190/2003 Z. z. o strelných zbraniach a strelive a o zmene a doplnení niektorých zákonov
- Zákon č. 39/2011 Z. z. o položkách s dvojakým použitím a o zmene zákona Národnej rady Slovenskej republiky č. 145/1995 Z. z. o správnych poplatkoch v znení neskorších predpisov

Narušenie kybernetickej bezpečnosti

- Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025
- Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe

Fyzické operácie proti infraštruktúre

- Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany schválený uznesením vlády SR č. 120 z roku 2007
- Národný program pre ochranu a obranu kritickej infraštruktúry v SR schválený uznesením vlády SR č. 185/2008
- Zákon č. 45/2011 Z. z. o kritickej infraštruktúre

Podpora sociálnych nepokojov a zneužívanie sociokultúrneho štiepenia

- Koncepcia sociálnej inklúzie Bratislavského samosprávneho kraja na roky 2020–2030
- Program Slovensko 2021–27
- Stratégia rovnosti, inklúzie a participácie Rómov do roku 2030
- Vízia a stratégia rozvoja Slovenska do roku 2030

Využívanie slabých miest v štátnej správe

- Zákon č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov
- Zákon č. 73/1998 Z. z. o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície
- Zákon č. 315/2001 Z. z. o Hasičskom a záchrannom zbore
- Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností

Zneužívanie migrácie ako nástroja hybridnej hrozby

- Integračná politika SR 2014
- Kontingenčný plán Slovenskej republiky pre riešenie mimoriadnej situácie v súvislosti s hromadným prílevom obyvateľov Ukrajiny na územie Slovenskej republiky spôsobeným eskaláciou ozbrojeného konfliktu na území Ukrajiny pre obdobie október 2022 – marec 2023
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/1896 z 13. novembra 2019 o európskej pohraničnej a pobrežnej stráži a zrušení nariadení (EÚ) č. 1052/2013 a (EÚ) 2016/1624
- Zákon č. 480/2002 Z. z. o azyle a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Zneužívanie slabých miest, nejednoznačností a medzier v legislatíve

- Zákon Národnej rady Slovenskej republiky č. 350/1996 Z. z. o rokovacom poriadku Národnej rady Slovenskej republiky v znení neskorších predpisov
- Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám
- Zákon č. 400/2015 Z. z. o tvorbe právnych predpisov a o Zbierke zákonov Slovenskej republiky a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Polovojenské organizácie

- Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov
- Zákon č. 83/1990 Zb. o združovaní občanov
- Zákon č. 85/2005 Z. z. o politických stranách a hnutiach
- GLOBSEC – Hybridné hrozby na Slovensku, Polovojenské a extrémistické skupiny, Analýza legislatívy, štruktúr a procesov

Financovanie kultúrnych skupín alebo think-tankov

- Zákon č. 308/1991 Zb. o slobode náboženskej viery a postavení cirkví a náboženských spoločnosti
- Zákon č. 213/1997 Z. z. o neziskových organizáciách poskytujúcich všeobecne prospešné služby
- Zákon č. 370/2019 Z. z. o finančnej podpore činnosti cirkví a náboženských spoločností

Ovplyvňovanie učebných osnov a akademickej obce

- Štátny vzdelávací program
- Zákon č. 131/2002 Z. z. o vysokých školách a o zmene a doplnení niektorých zákonov
- Zákon č. 245/2008 Z. z. o výchove a vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov

Využívanie strategickej korupcie

- Dohovor Organizácie Spojených národov proti korupcii (UNCAC)
- Národný protikorupčný program SR
- Protikorupčná politika SR na roky 2019 – 2023
- Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov

Nátlak na politikov alebo členov vlády

- LP/2020/541 Zásady zaisťovania osobnej bezpečnosti určených osôb a ochrany určených objektov
- Zákona č. 372/1990 Zb. o priestupkoch
- Zákon č. 40/164 Zb. Občiansky zákonník

Veľvyslanectvá

- Viedenský dohovor
- Zákon č. 151/2010 Z. z. o zahraničnej službe

Využívanie diaspór k ovplyvňovaniu

- Európska charta regionálnych a menšinových jazykov
- Rámcový dohovor na ochranu národnostných menšín
- Zákon č. 184/1999 Z. z. o používaní jazykov národnostných menšín

Diplomatické a ekonomické sankcie

- Zákon č. 289/2016 Z. z. o vykonávaní medzinárodných sankcií
- Zákon č. 575/2001 Z. z. o organizácii činnosti vlády

Ovládanie a zasahovanie do médií

- Európsky akt o slobode médií (z angl. European Media Freedom Act)
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách)
- Smernica Európskeho parlamentu a Rady (EÚ) 2018/1808 zo 14. novembra 2018, ktorou sa mení smernica 2010/13/EÚ (Ú. v. EÚ L 303, 28. 11. 2018) (smernica o audiovizuálnych mediálnych službách)
- Zákon č. 264/2022 Z. z. o mediálnych službách a o zmene a doplnení niektorých zákonov (zákon o mediálnych službách)

Priame zahraničné investície (PZI)

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/452, ktorým sa ustanovuje rámec na preverovanie priamych zahraničných investícií do Únie
- Zákon č. 497/2022 Z. z. o preverovaní zahraničných investícií a o zmene a doplnení niektorých zákonov

Vytvorenie a zneužívanie energetickej závislosti

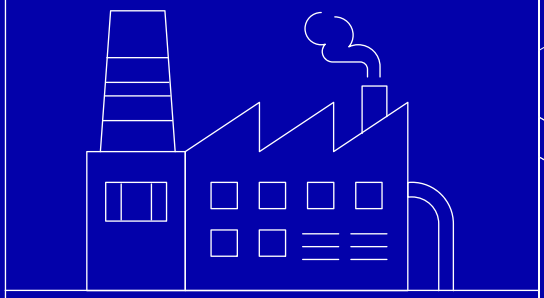
- Energetická politika Slovenskej republiky
- INEKP - Integrovaný národný energetický a klimatický plán na roky 2021 – 2030
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/1938 o opatreniach na zaistenie bezpečnosti dodávok plynu a o zrušení nariadenia (EÚ) č. 994/2010
- Zákon č. 251/2012 Z. z. o energetike a o zmene a doplnení niektorých zákonov spoločností

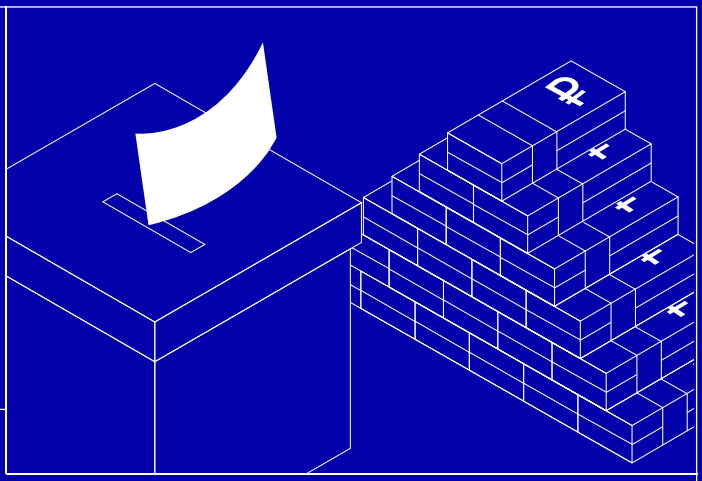
Vytváranie a zneužívanie ekonomických ťažkostí a závislostí

- 1. akčný plán pre realizáciu opatrení vyplývajúcich zo Stratégie hospodárskej politiky Slovenskej republiky do roku 2030
- Európska zelená dohoda
- Nová priemyselná politika EÚ

Poznámky

Poznámky

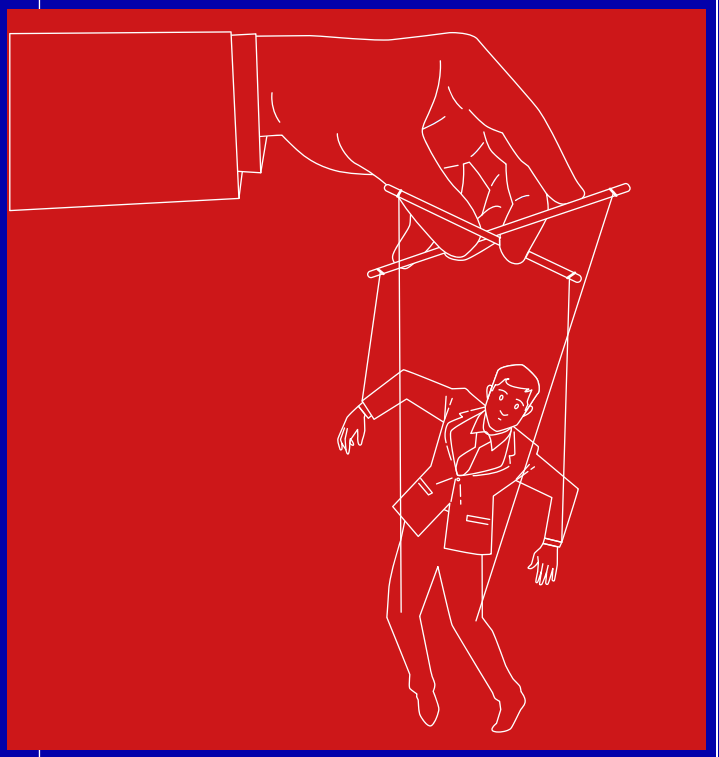


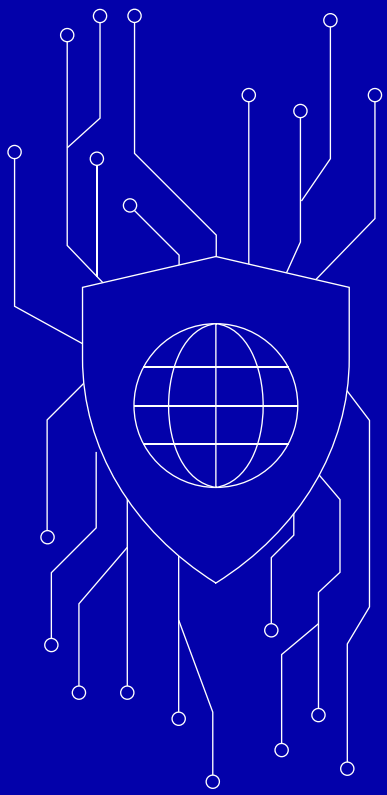


Centrum boja proti hybridným hrozbám
(CBHH)

je analytické, metodické a koordinačné pracovisko rezortu vnútra pre oblasť hybridných hrozieb. Pôsobí v rámci Inštitútu správnych a bezpečnostných analýz MV SR od januára 2022. Hlavným cieľom CBHH je zvýšiť kapacity MV SR v oblasti monitorovania, analýzy a boja proti rôznym formám hybridných hrozieb. CBHH pravidelne zhromažďuje dáta a údaje, analyzuje ich, navrhuje opatrenia a vykonáva činnosti za účelom zvyšovať odolnosť orgánov verejnej správy voči hybridným hrozbám. Práca je zameraná na 6 hlavných oblastí:

- identifikácia kľúčových zraniteľností voči hybridným hrozbám,
- realizácia strategickej komunikácie na základe dát a analýz,
- zefektívnenie procesov, štruktúr a činností verejnej správy,
- zvyšovanie úrovne vedomostí, kompetencií a zručností zamestnancov verejnej správy prostredníctvom vzdelávacích programov,
- aktualizácia regulačného rámca a implementácia tvorby verejných politík na základe dát,
- zvyšovanie personálnych a technických kapacít.





www.hybridnehrozby.sk | @CBHH_SK | hybrid@minv.sk