

# ZVÝŠENIE ODOLNOSTI SLOVENSKA VOČI HYBRIDNÝM HROZBÁM POMOCOU POSILNENIA KAPACÍT POLICAJNÉHO ZBORU A VEREJNEJ SPRÁVY

Kód projektu: 314011CDW7

Realizácia projektu v rámci operačného programu  
„Efektívna verejná správa“ financovaného  
z Európskeho sociálneho fondu

## ÚVOD, ZÁKLADNÁ CHARAKTERISTIKA HYBRIDNÝCH HROZIEB, POJMY A VÝCHODISKÁ SÚVISIACE S PROBLEMATIKOU HYBRIDNÝCH HROZIEB

kpt. JUDr. Patrícia Krásná, PhD., LL.M.  
Katedra vyšetrovania  
Akadémie Policajného zboru v Bratislave



**Európska únia**  
Európsky sociálny fond



**AKADÉMIA  
POLICAJNÉHO ZBORU  
V BRATISLAVE**



- Obsah danej prednášky reaguje na bezpodmienečnú potrebu charakteristiky a špecifikácie nebezpečenstva hybridných hrozieb.
  - Štruktúru prednášky tvorí základný, úvodný, popis hybridných hrozieb, pojmov a východísk súvisiacich s touto problematikou.
    - Cieľom je špecifikovať koncept, teóriu, aktérov, domény, nástroje a fázy hybridných hrozieb vo všeobecnosti, ale aj v konkrétnych súvislostiach, ako primárnych prvkov podmieňujúcich hybridné hrozby a ich riziká.
- Cieľom prednášky je taktiež poukázať na vybrané spôsoby zvyšovania odolnosti proti hybridným hrozbám - StratCom, zvyšovanie a budovanie povedomia o hybridných hrozbách.
- Zámerom prednášky je aj interpretovať zhrnutie a odporúčania do budúcnosti v kontexte efektívneho boja proti hybridným hrozbám.

# Východiskové pojmy - bezpečnosť, nebezpečenstvo



Zdroj obrázka:

[https://www.google.com/search?sxsrf=AB5stBh2rOCvYLRsxwauV0QAvSeI5\\_XJlg:1690805122693&q=protection&tbm=isch&source=lnms&sa=X&ved=2ahUKEwiRreP187iAAxUVgv0HHTx1CPMQ0pQJegQIDBAB&biw=1536&bih=682&dpr=1.25#imgc=Fi9SHnTVZZxUeM](https://www.google.com/search?sxsrf=AB5stBh2rOCvYLRsxwauV0QAvSeI5_XJlg:1690805122693&q=protection&tbm=isch&source=lnms&sa=X&ved=2ahUKEwiRreP187iAAxUVgv0HHTx1CPMQ0pQJegQIDBAB&biw=1536&bih=682&dpr=1.25#imgc=Fi9SHnTVZZxUeM)

Zdroj obrázka: <https://www.istockphoto.com/photos/danger-sign>.

Vnútrošnú bezpečnosť môžeme definovať ako „súhrn vnútrošných bezpečnostných podmienok, legislatívnych noriem a opatrení, ktorými štát zabezpečuje demokraciu, ekonomickú prosperitu, bezpečnosť občanov, ako aj presadzovanie právnych a morálnych noriem.“<sup>1</sup> Bezpečnosť = „snaha o odstránenie hrozby“.<sup>2</sup>

Nebezpečenstvo je „potenciálne škodlivá fyzická udalosť, jav alebo ľudská činnosť, ktorá môže spôsobiť straty na životoch, škodu na majetku, sociálny a hospodársky rozvrat alebo poškodenie životného prostredia“.<sup>3</sup>



Riziko je situačná charakteristika činnosti, ktorá spočíva v tom, že výsledok činnosti je neistý.<sup>1</sup>

Zdroj obrázka:  
<https://www.irmi.com/articles/expert-commentary/the-role-of-the-cio-in-the-risk-intelligent-enterprise>.



Hrozba je pojem používaný v riadení rizík pre označenie zdroja negatívnej udalosti, sily, osoby alebo aktivity, ktorá chce alebo môže poškodiť nejakú hodnotu. Niekedy sa tiež používa pojem nebezpečenstvo. Hrozba má nežiaduci vplyv na bezpečnosť alebo môže spôsobiť škodu, stratu, nežiaduce zmenu, či iný nežiaduci jav.<sup>2</sup>

Hrozba v praxi...?



Zdroj obrázka:  
<https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/octave-threat-model-benefits/>.

- „súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny a pod prahom zvyčajnej reakcie.
- Tieto činnosti sú realizované aktivitami charakterizovanými centrálne riadeným spravodajským a informačným pôsobením, pôsobením neštátnych aktérov, vrátane polovojenských skupín, či nasadením ozbrojených síl štátneho aktéra bez označenia.
- Takéto aktivity sa môžu začať skôr, než dôjde k otvorene deklarovanej vojenskej operácii. Polarizujú spoločnosť, vnášajú neistotu, a tým podkopávajú legitimitu, dôveryhodnosť, akcioskopnosť štátnych inštitúcií a demokratický ústavný poriadok a majú tak negatívny vplyv na realizáciu bezpečnostných záujmov štátov, ktoré sú im vystavené“.<sup>1</sup>

Nátlak je/zahrňa prinútenie strany, aby konala nedobrovoľne, použitím hrozieb, vrátane hrozieb použitím sily proti tejto strane. Zahrňa súbor násilných akcií, ktoré porušujú slobodnú vôľu jednotlivca s cieľom vyvolať požadovanú reakciu.

Podvracanie - ide o akt, ktorým sa má v celej oblasti, na ktorú má vplyv, zmeniť štruktúra a tým sa zmení, resp. ohrozí jej bezpečnosť. Či už je to umelecká, morálna, sociálna, ale najmä politická oblasť.<sup>1</sup> V prípade podvracania nestačí, že sa zmení jeden prvok alebo faktor, má za cieľ zmeniť čo najviac elementov.

Subverzia - je radikálna zmena od miestnej úrovne. To znamená, že sa snaží úplne zmeniť prvky, ktoré definujú zloženie spoločnosti.



Zdroj obrázka: <https://sk.economy-pedia.com/11040363-subversion>





Zdroj obrázka:  
<https://mwi.westpoint.edu/failing-to-train-conventional-forces-in-irregular-warfare/>.

Konvenčný ozbrojený konflikt predstavuje typ ozbrojeného konfliktu, kedy jednotlivé strany používajú konvenčné zbrane - všetky zbrane okrem zbraní hromadného ničenia, jadrových, biologických a chemických zbraní, pričom bojujú otvorene na zemi, vo vzduchu či na mori.<sup>1</sup> Sily obidvoch bojujúcich strán sú jasne definované a organizované.

Základným cieľom konvenčnej vojny je oslabiť alebo zničiť nepriateľské ozbrojené sily, obsadiť územie a narušiť jeho schopnosť ďalej viesť konvenčnú vojnu.<sup>2</sup>



Zdroj obrázka: <https://www.scientificamerican.com/article/theres-a-psychological-vaccine-against-misinformation/>.

Nekonvenčný konflikt predstavuje viacero foriem a nástrojov, ktoré majú za cieľ oslabiť konkrétny štát, spoločnosť, napr. - nepriateľská propaganda, podpora extrémizmu, využívanie národnostných alebo náboženských komunít nespokojných s ich postavením v spoločnosti, podpora kriminálnych aktivít, útoky na kritickú infraštruktúru, či kyberútoky.<sup>1</sup>



# Vojenský vs. nevojenský konflikt

Vojenský konflikt - vojna, medzinárodný ozbrojený konflikt alebo zdĺhavý ozbrojený konflikt na území štátu medzi vládnyimi orgánmi a organizovanými ozbrojenými skupinami alebo medzi takýmito skupinami navzájom s výnimkou vnútorných nepokojov a napätí, ako sú vzbury, izolované a ojedinelé akty násilia alebo iné akty podobnej povahy.<sup>1</sup>

Nevojenský konflikt - neozbrojený konflikt.



Zdroj obrázka: <https://www.ccpl.org/news/conflict-resolution-skills-needed-soft-skill-employees-workplace>.

- Tradičnými metódami ale aj s použitím moderných technológií sa dnes rad štátnych, štátni sponzorovaných ale aj neštátnych aktérov otvoreným alebo skrytým spôsobom koordinovane naprieč celou škálou nástrojov moci snaží dosiahnuť svoje politické, ale aj ekonomické ciele.
- Zvyšuje sa relevancia hrozieb schopných vyvolať významné ekonomické straty z dôvodu prerušenia, poškodenia fungovania základných funkcií štátu alebo služieb, ktoré sú potrebné na bežné fungovanie štátu a spoločnosti.
- Zvyšuje sa pripravenosť a schopnosti rôznych aktérov presadzovať svoje záujmy na úkor iných.
- Tento vývoj je daný meniacim sa charakterom moci a vplyvu, keď vzájomné závislosti, technológie a ich prepojenia dávajú štátom nové možnosti ovplyvňovať svojich konkurentov.
- Všetko bez ohľadu na medzinárodné pravidlá alebo národné zákony.

- a/ale chápanie/vnímanie témy zo strany rôznych štátnych subjektov, médií a podobne sa významne líši,



pričom je potrebné si uvedomiť, že hybridné hrozby majú prierezový, multiinštitucionálny, charakter a spadajú do kompetencie viacerých štátnych orgánov a je ich potrebné riešiť aj na základe poznania ďalej uvádzaných 4 pilierov.



Zdroj obrázka:

[https://www.google.com/search?q=mutual&tbm=isch&ved=2ahUKEwizr-e427uAAxWOu6QKHdabDagQ2-cCegQIABAA&oq=mутal&gs\\_lcp=CgNpbWcQAZIFCAAQgAQyBAGAEb4yBAgAEb4yBAgAEb4yBAgAEb4yBAgAEb4yBAgAEb4yBAgAEb4yBAgAEb46BAgjECdQlQQZYlQQZggApoAHAAeACAAVWIAZ8BKgEBMpgBAKABAoBCd23cy13aXotaWI1nwAEB&scient=img&ei=fxzJZZPz4L73kgXWt7bACg&bih=739&biw=1536#imgr=c=SJMouligMeD-gM](https://www.google.com/search?q=mutual&tbm=isch&ved=2ahUKEwizr-e427uAAxWOu6QKHdabDagQ2-cCegQIABAA&oq=mутal&gs_lcp=CgNpbWcQAZIFCAAQgAQyBAGAEb4yBAgAEb4yBAgAEb4yBAgAEb4yBAgAEb4yBAgAEb4yBAgAEb4yBAgAEb4yBAgAEb46BAgjECdQlQQZYlQQZggApoAHAAeACAAVWIAZ8BKgEBMpgBAKABAoBCd23cy13aXotaWI1nwAEB&scient=img&ei=fxzJZZPz4L73kgXWt7bACg&bih=739&biw=1536#imgr=c=SJMouligMeD-gM).



Operačný program  
**Efektívna  
verejná správa**



**Európska únia**  
**Európsky sociálny fond**





# Štyri hlavné piliere, ktoré je potrebné poznať pre pochopenie konceptu hybridných hrozieb

- Aktéri (kto) a ich strategické ciele (prečo).
- Nástroje (ako) používané aktérmi.
- Domény (kde), ktoré sú cieľom hybridných hrozieb.
- Fázy (vrátane typov činností pozorovaných v každej fáze).  
(Ako môže vyzerat' priebeh hybridnej operácie?)

## • Aktéri a ich strategické ciele.

Aktéri hybridných hrozieb sú pôvodcovia, resp. šíritelia hybridnej hrozby.

Je zrejmé, že aktéri hybridných hrozieb využívajú kombináciu rôznych nástrojov tak, aby dosiahli strategické ciele. Podľa toho, aké nástroje využívajú, vieme následne aj diferencovať samotných aktérov (štátni aktéri, neštátni aktéri) a ich ciele.

Každý nástroj, ktorý využívajú aktéri sa zameriava na jednu alebo viacero dôležitých domén, ale tiež i na citlivé „rozhranie“, resp. „hranicu“ týchto domén. Sledovaný cieľ sa snažia dosiahnuť buď priamym alebo postupným účinkom.<sup>1</sup>

Aktéri hybridných hrozieb sa často prikláňajú k ovplyvňovaniu samotného rozhodovacieho procesu v rámci ich cieľa. Môže ísť, napr. o vplyv na rozhodovanie v malom rozsahu, ale aj na rozhodovanie veľkého rozsahu - ovplyvňovanie obchodných operácií, rozhodnutí jednotlivcov počas volieb, rozhodnutí tých, ktorí praktizujú, ktorí formujú politiky a legislatívu, ktorí vykonávajú činnosť vo verejnom záujme, v štátnom záujme a pod.

Konanie aktéra môže byť úspešné aj v prípade, ak využije iba niektoré prvky hybridných hrozieb a preto je potrebné bezpochyby skúmať a sledovať aj počiatočné štádiá vplyvu hybridných hrozieb prostredníctvom ich aktérov.

Ich cieľom je ovplyvniť systémové zraniteľné miesta demokracie za využitia všetkých nástrojov.



## ☐ Štátni aktéri

Autoritárske štáty čoraz častejšie využívajú hybridné hrozby ako nástroj v boji proti demokratickým štátnym systémom, pretože ich vnímajú ako existenčnú hrozbu pre svoje mocenské postavenie. Toto vnímanie je jedným z dôvodov, prečo cítia potrebu pokúsiť sa podkopať a oslabiť schopnosti demokratických štátov.

Manipulatívne zasahovanie do informačnej domény je jedným z ich hlavných aktív. Jedným z najpoužívanějších nástrojov je manipulácia prostredníctvom dezinformácií na sociálnych sieťach, ktorá zvyšuje šance ovplyvniť a zacieliť na určité publikum (prostredníctvom mikrotargetingu).



Zdroj obrázka:

[https://www.google.com/search?q=akt%C3%A9r&tbm=isch&ved=2ahUKEwimx9qu6LuAAxU4rycCHcTOBQM2-cCegQIABAA&oeq=akt%C3%A9r&gs\\_lcp=CgNpbWcQAziHCAAQGBCABDIHCAAQGBCABDIHCAAQGBCABDIHCAAQGBABDoECCMQJzoHCAAQigUQQzoECAAQAzOICAAQgAQQsQM6BQgAEIAEUABYmgdgoQloAHAAeACAAYwBiAGyA5IBAzQuMZgBAKABAaoBC2d3cy13aXotaW1nwAEB&scient=img&ei=DCrJZKaRBLjensEPxJ2XGA&bih=739&biw=1536#imgre=cNKL1ljWXIcuVM](https://www.google.com/search?q=akt%C3%A9r&tbm=isch&ved=2ahUKEwimx9qu6LuAAxU4rycCHcTOBQM2-cCegQIABAA&oeq=akt%C3%A9r&gs_lcp=CgNpbWcQAziHCAAQGBCABDIHCAAQGBCABDIHCAAQGBCABDIHCAAQGBABDoECCMQJzoHCAAQigUQQzoECAAQAzOICAAQgAQQsQM6BQgAEIAEUABYmgdgoQloAHAAeACAAYwBiAGyA5IBAzQuMZgBAKABAaoBC2d3cy13aXotaW1nwAEB&scient=img&ei=DCrJZKaRBLjensEPxJ2XGA&bih=739&biw=1536#imgre=cNKL1ljWXIcuVM)

## ❖ Revizionisti.<sup>1</sup>

Aktér súpera ovplyvní tak, že súper je presvedčený o svojom konaní a má za to, že to bolo z jeho vôle.<sup>1</sup>

## ❖ Darebáci.<sup>2</sup>

Paranoidné odchyľovanie sa od pravidiel reálnych politík, čo podľa bezpečnostných stratégov nemôže vyústiť v nič iné ako vo vojnový konflikt. Vyznačujú sa aj tým, že národné bohatstvo zneužívajú pre osobný prospech vodcov alebo pre megalomanské plány na získanie zbraní hromadného ničenia.

Darebácke štáty využívajú hybridné hrozby na to, aby prispeli k rozpadu súčasného systému a pretvorili ho na podobu fungovania svojho režimu. Tiež významnú úlohu v týchto prípadoch zohrávajú finančný zisk a vôľa uškodiť.

## ❑ Neštátni aktéri.

Neštátni aktéri môžu byť pôvodcami hybridných hrozieb vo svojom vlastnom záujme s vlastnými strategickými cieľmi.

Títo neštátni aktéri môžu byť zároveň „proxy“ aktérmi (zástupnými), ktorých využívajú štátni aktéri na naplnenie svojich strategických cieľov a sťažujú tým svoju skutočnú atribúciu.

„Proxy“ aktéri môžu byť motivovaní finančne, ideologicky a môže ísť o záujmovú skupinu, hackerov, ale ja o jednotlivcov.



## • Nástroje používané aktérmi

- ✓ Fyzické operácie proti infraštruktúre.
- ✓ Vytváranie a využívanie závislosti na infraštruktúre (vrátane civilno-vojenskej závislosti).
- ✓ Vytváranie alebo využívanie ekonomických závislostí.
- ✓ Priame zahraničné investície.
- ✓ Priemyselná špionáž.
- ✓ Narúšanie národného hospodárstva protivníka.
- ✓ Ovplyvňovanie volieb. ( V súčasnosti je identifikovaných 40 nástrojov.)

Slúžia aktérom na dosiahnutie požadovaného cieľa, čo najefektívnejším spôsobom. Jednotlivé nástroje môžu pôsobiť na jednu alebo na viacero domén súčasne.<sup>1</sup>

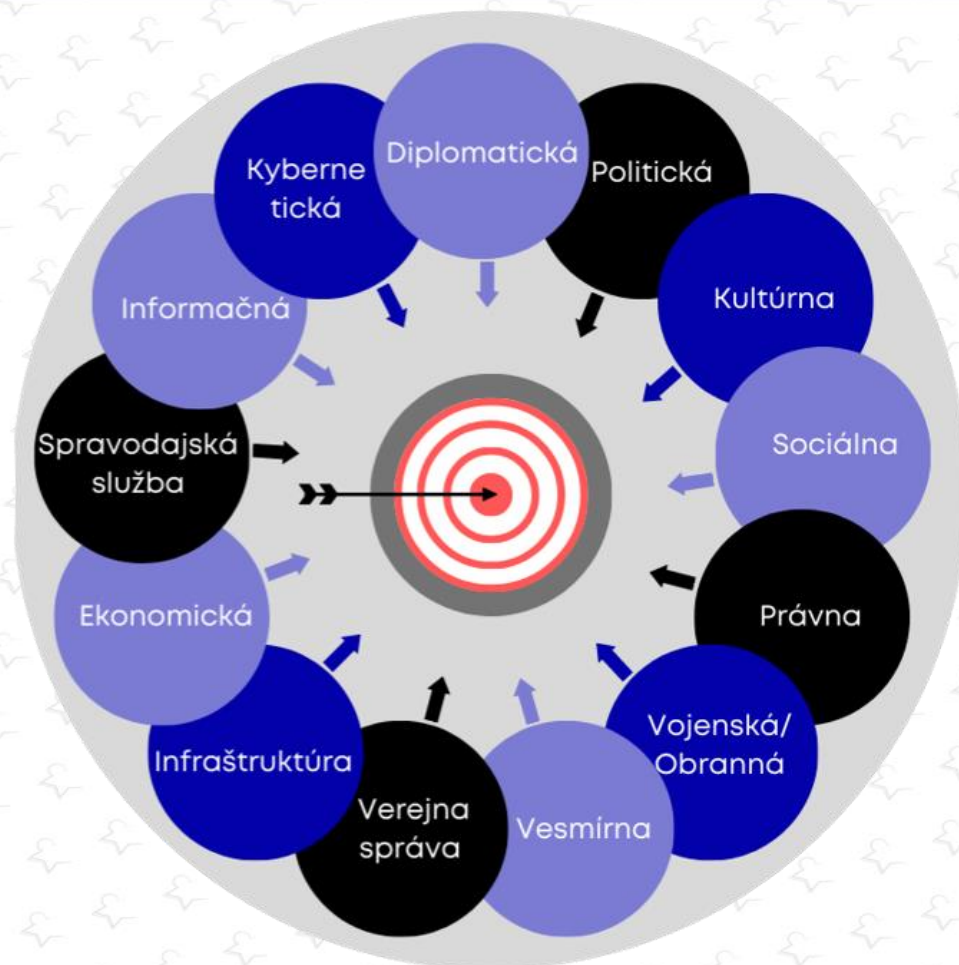
## Domény, ktoré sú cieľom hybridných hrozieb.

Na domény, ktoré sú cieľom hybridných hrozieb pôsobí najčastejšie kombinácia nástrojov používaných aktérmi.

Charakteristické je, že každý nástroj sa zameriava na jednu, resp. viaceré domény alebo rozhranie medzi nimi - vytvorením alebo zneužitím zraniteľnosti.<sup>1</sup>

Domény sú kľúčovými oblasťami štátu, na ktoré sa zameriavajú nástroje hybridných hrozieb.

# Domény hybridných hrozieb



Zdroj obrázka: ISBA MV SR.



Operačný program  
**Efektívna  
verejná správa**



**Európska únia**  
Európsky sociálny fond



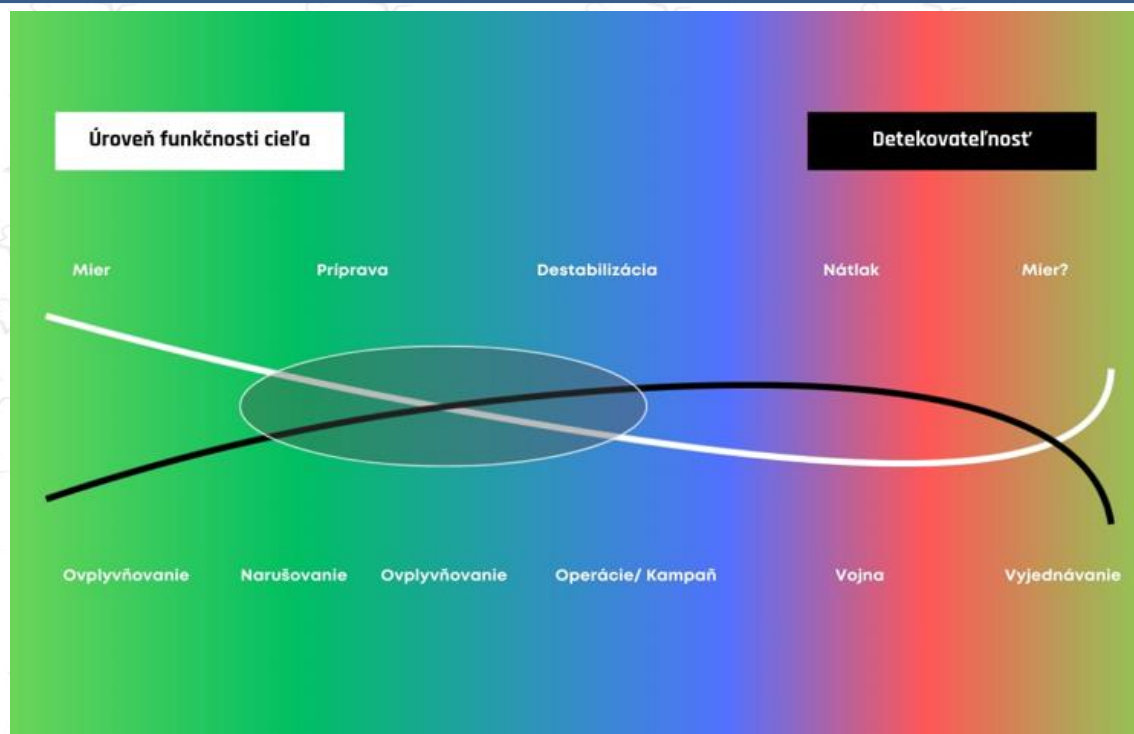


# Vplyv nástrojov na domény hybridných hrozieb

Nástroje	Ovplyvnené domény
Fyzické operácie proti infraštruktúre	Infraštruktúra, ekonomická, kybernetická, vojenská/obranná, verejná správa
Vytváranie a využívanie závislosti na infraštruktúre (vrátane civilno-vojenskej závislosti)	Infraštruktúra, ekonomická, kybernetická, vojenská/obranná, verejná správa
Vytváranie alebo využívanie ekonomických závislostí	Ekonomická, diplomatická, politická, verejná správa
Priame zahraničné investície	Ekonomická, infraštruktúra, kybernetická, vojenská/obranná, verejná správa, politická
Priemyselná špionáž	Ekonomická, infraštruktúra, kybernetická, informačná
Kybernetická špionáž	Infraštruktúra, kybernetická, vojenská/obranná, verejná správa

Zdroj obrázka: The landscape of Hybrid Threats: A conceptual model, s. 38.

- Fázy (vrátane typov činností pozorovaných v každej fáze).



Zdroj obrázka: ISBA MV SR.

Vo fáze prípravy je konečným cieľom aktéra hybridnej hrozby, že cieľ dobrovoľne urobí škodlivé rozhodnutia a nesprávne konanie.

Podstatou tejto fázy je „pripraviť si pôdu“ pre ďalšie úspešne pôsobenie - aktivity sú veľmi ťažko detegovateľné, nie je jasný ich zámer. Cieľom týchto aktivít je prinútiť štát (terč hybridného pôsobenia), aby začal robiť škodlivé rozhodnutia v súlade so záujmami aktéra.



Zdroj obrázka: <https://www.insidehighered.com/opinion/career-advice/career-careers/2023/05/08/how-optimize-your-career-preparation>.



Fáza destabilizácie je štádiom, v ktorom aktér zintenzívňuje svoju činnosť, napr. spôsobom kampane (realizácia viacerých operácií). Cieľom aktéra v rámci tejto fázy je získať čo najviac informácií, aby mohol svoj cieľ čo najefektívnejšie ohroziť.<sup>1</sup>

V tejto fáze sú aktivity aktéra čoraz viditeľnejšie, avšak aktér sa k ich vykonávaniu nepriznáva a cieľový štát nemá dostatok dôkazov na to, aby to dôveryhodne preukázal.

Môže sa v malej miere vyskytovať aj prvok násilia.



Zdroj obrázka: <https://restofworld.org/series/the-destabilization-experiment/>.

V tejto fáze prekročili aktivity rámec nenápadnosti a možno ju označiť za hybridnú vojnu.

Hybridná vojna predstavuje „tvrdý koniec“ eskalačného spektra činností hybridných hrozieb. Hybridná vojna je v zásade kombináciou skrytých a otvorených vojenských operácií v kombinácii s politickými a ekonomickými opatreniami, rozvratom, informačnými/dezinformačnými operáciami, propagandou/falošnými správami, skrytým alebo zjavným nasadením špeciálnych síl, ako aj armády, ale aj kybernetických útokov.<sup>1</sup>

Kľúčovým prvkom je použitie sily na dosiahnutie aktérovho zámeru – použitie sily (teror, sabotáž, konvenčná vojna) nie je iba ďalším prvkom hybridných hrozieb, ale zároveň mení charakter celého konfliktu na vojnu.



Zdroj obrázka: <https://behorizon.org/hybrid-warfare-through-the-lens-of-strategic-theory/>.

# Budovanie odolnosti voči hybridným hrozbám v Slovenskej republike



Zdroj obrázka: <https://www.dreamstime.com/illustration/resisting.html>.



Strategická komunikácia je jedným z kľúčových nástrojov pri budovaní bezpečnejšej krajiny a odolnejšej spoločnosti, ktorá je pripravená čeliť novodobým výzvam a krízam, prostredníctvom systematickej a koordinovanej kooperácie ministerstiev, Úradu vlády Slovenskej republiky a ostatných ústredných orgánov štátnej správy.<sup>1</sup>



Zdroj obrázka: <https://clairebahn.com/strategic-communication/>.

Strategická komunikácia je systematická koordinovaná aktivita štátu, ktorá je zameraná na informovanie verejnosti a ostatných relevantných subjektov prostredníctvom využívania objektívnych informácií a dostupných zdrojov na dosiahnutie vopred stanovených cieľov.

Strategická komunikácia pozostáva z komunikačných kampaní založených na vopred stanovených míľnikoch podložených kvantitatívnym alebo kvalitatívnym výskumom a reflektuje dlhodobé strategické záujmy štátu.<sup>1</sup>

Strategická komunikácia prináša ucelenosť komunikovaného obsahu, pozerá sa za hranice každodenného života, snaží sa nasmerovať cieľové publikum k dlhodobej zmene v zmýšľaní a prezentovať dlhodobé vízie a základné hodnoty spoločnosti. Strategická komunikácia štátnej inštitúcie zároveň znamená, že daná inštitúcia a jej zamestnanci vedia, aké sú priority, politiky a hodnoty danej inštitúcie.<sup>2</sup>

Výhody strategickej komunikácie spočívajú v zlepšenej schopnosti štátu brániť sa voči dezinformačným kampaniam, intenzívnejšej spolupráci a komunikácii s občanmi ako s dôležitými partnermi, čo prispieva k posilneniu dôvery verejnosti v demokratický a právny štát. Implementácia princípov strategickej komunikácie štátnymi inštitúciami je rovnako jedným z kľúčových predpokladov efektívnej reakcie štátu na hybridné pôsobenie.<sup>1</sup>



Zdroj obrázka: <https://discoveria.org/komunikacia/>.



Nedostatočná a nesystematická komunikácia štátu bez strategického rámca prispieva v informačnom priestore k etablovaniu subjektov, ktoré, ako poukazuje Slovenská informačná služba, systematicky šíria škodlivý obsah vrátane dezinformácií a zavádzajúcich, tendenčných a polarizujúcich naratívov. Tie sú často súčasťou informačných operácií, ktoré svojím pôsobením podkopávajú relevanciu štátnych inštitúcií, demokratické a geopolitické ukotvenie Slovenskej republiky v EÚ a NATO, čo predstavuje pre Slovenskú republiku významnú bezpečnostnú hrozbu.<sup>1</sup>

# Kľúčové témy strategického významu na úrovni Slovenskej republiky

Strategická komunikácia reflektuje dlhodobé strategické záujmy Slovenskej republiky, ktorými sú:

- Demokratické zriadenie Slovenskej republiky.
- Geopolitické ukotvenie Slovenskej republiky.
- Bezpečnostné témy vrátane hybridných hrozieb a informačných operácií.
- Potreba chrániť princípy právneho štátu v krízových situáciách.<sup>1</sup>

Efektívna strategická komunikácia nepozostáva len z verbálnych prejavov. Opiera sa aj o činy, gestá a symboly, reflektuje aktuálne potreby občanov a využíva široké zapojenie všetkých relevantných subjektov do celospoločenského prístupu k informačnej bezpečnosti.

Strategická komunikácia ministerstiev a ostatných subjektov štátnej správy, ktoré pracujú v prospech zvrchovanej, bezpečnej, prosperujúcej a demokratickej Slovenskej republiky je založená na nasledujúcich princípoch:<sup>1</sup>





# Kľúčové princípy strategickej komunikácie

- ☐ Verejný záujem.
- ☐ Strategická komunikácia ako súčasť tvorby politík.
- ☐ Celospoločenský prístup.
- ☐ Kredibilita.
- ☐ Znalosť publika.
- ☐ Informačné prostriedky.
- ☐ Plánovanie.
- ☐ Komunikačná kampaň.
- ☐ Koordinácia.
- ☐ Inklúzia.
- ☐ Merateľné výsledky.<sup>1</sup>

Komunikačné tímy zaoberajúce sa strategickou komunikáciou koordinujú ostatných kolegov tým, že určujú čo, kedy, ako a komu komunikovať. Ich význam spočíva v pochopení komplexných informácií, navrhovaní stratégií a hodnotení výsledkov komunikácie.

Základné kroky, ktoré musia odborníci zaoberajúci sa strategickou komunikáciou vykonať, sú štruktúrované do štyroch fáz procesu plánovania strategickej komunikácie:

- porozumenie kontextu a cieľovej skupiny,
- návrhy riešení,
- ich implementácia
- a následné zhodnotenie.<sup>1</sup>

# Strategická komunikácia na úrovni NATO

## - NATO StratCom COE

*„Keďže vojny začínajú v mysliach ľudí, obrana mieru musí byť postavená v mysliach ľudí.“*

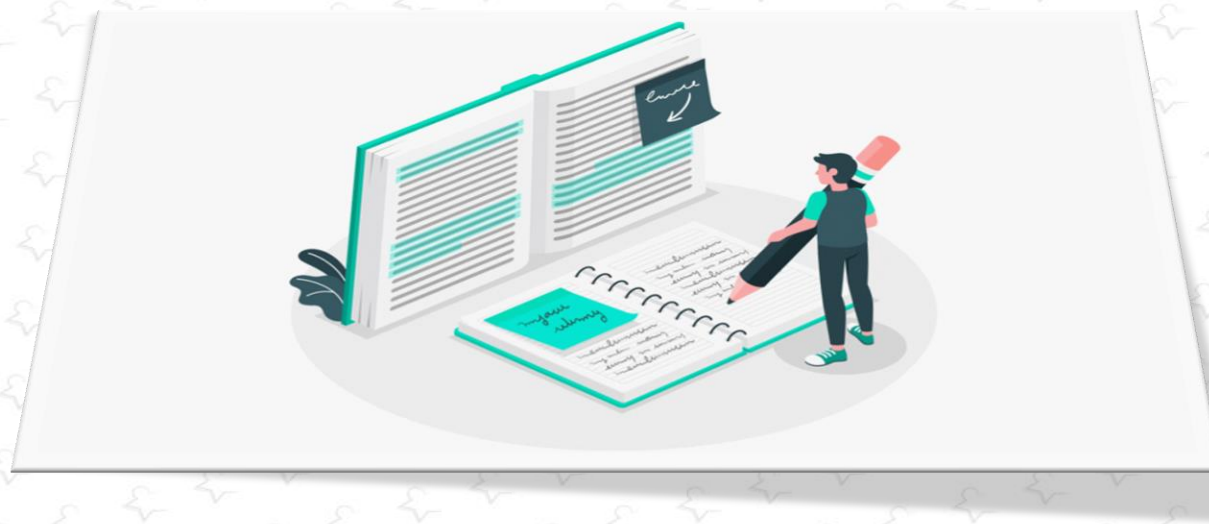
Preambula Ústavy UNESCO (1946)

Centrum excelentnosti NATO pre strategickú komunikáciu (NATO StratCom COE) začalo fungovať v januári 2014. 1. júla toho istého roku podpísalo sedem členských štátov – Estónsko, Nemecko, Taliansko, Lotyšsko, Litva, Poľsko a Spojené kráľovstvo memorandá o porozumení o založení StratCom COE. Stredisko získalo akreditáciu NATO 1. septembra 2014 a ako sa uvádza vo vyhlásení z Waleského summitu z roku 2014, spojenci privítali „... založenie StratCom COE ako zmysluplného príspevku k úsiliu NATO ...“ v oblasti strategickej komunikácie.<sup>1</sup>



Zdroj obrázka: <https://stratcomcoe.org/>.





Zdroj obrázka: <https://basmo.app/how-to-write-a-book-summary/>.



Operačný program  
**Efektívna  
verejná správa**



**Európska únia**  
Európsky sociálny fond



- Nedostatočné kapacity v oblasti strategickej komunikácie na úrovni ústredných orgánov štátnej správy.
- Poddimenzované analytické kapacity v oblasti kybernetickej bezpečnosti a absencia dostatočne konkrétnych a merateľných opatrení na zlepšenie súčasného stavu v tejto oblasti.
- Nedostatočná pozornosť energetickej infraštruktúry v kontexte hybridných hrozieb a dosahu prípadného útoku na túto infraštruktúru nad rámec prerušenia dodávok energií.
- Absencia právnej úpravy polovojenských/paramilitárnych skupín.
- Nedostatočné zohľadnenie prvku cudzej moci pri iných typoch ohrození bezpečnosti a stability Slovenskej republiky.
- Absencia zohľadnenia iných než čisto finančných motívov v anti-korupčnej legislatíve - strategická korupcia s politickými motívami a zapojením cudzej moci.
- Absencia špecifickej právnej úpravy o vedení volebnej kampane v prostredí internetu a sociálnych sietí.<sup>1</sup>

- Prijat' komplexný prístup v oblasti strategickej komunikácie, zahŕňajúci všetky relevantné zložky verejnej správy.
- Zriadiť špecializované národné kapacity so zameraním na strategickú komunikáciu vo všetkých relevantných rezortoch.
- Vytvoriť analytické kapacity v oblasti kybernetickej bezpečnosti, ktoré by sa zaoberali tvorbou verejných politík.
- Prijat' akčný plán v oblasti kybernetickej bezpečnosti s jasnými, merateľnými kritériami.
- Systematicky riešiť otázku hybridných/kybernetických hrozieb v strategických dokumentoch, ktoré sa venujú energetickej politike, resp. energetickej bezpečnosti.<sup>1</sup>



- Klásť väčší dôraz na špecifiká energetického sektora, ktorý je odlišný od ostatných oblastí kritickej infraštruktúry, pretože hybridné hrozby v tejto oblasti majú dôsledky nielen pre energetickú bezpečnosť, ale aj pre tzv. “hard security”.
- Identifikovať hybridné hrozby a riešenia nielen na úrovni verejnej/štátnej správy, ale aj v rámci(polo)súkromného energetického sektora, ktorý hrá dôležitú úlohu pri zabezpečovaní energetickej bezpečnosti.
- Zahnúť “smart” technológie do diskusie o možných hybridných hrozbách v oblasti energetickej bezpečnosti.
- Novelizovať legislatívu v oblasti zbraní a streliva a prijať legislatívu upravujúcu pôsobenie polovojenských skupín a ich podporu zo strany cudzej moci.<sup>1</sup>

- Dôsledne uplatňovať ustanovenia Zákona č. 300/2005 Z. z. Trestného zákona v znení neskorších predpisov týkajúce sa účasti na bojovej činnosti organizovanej ozbrojenej skupiny na území iného štátu a jej podpory.
- Posilňovať medzinárodné, ale aj domáce nástroje na odhaľovanie podozrivých finančných tokov cez schránkové firmy a daňové raje v kontexte strategickej korupcie s politickými cieľmi.
- Analyzovať nefinančné aspekty korupcie a zakotviť pojem strategická korupcia do verejných politík a legislatívy.
- Prijat' legislatívu, ktorá upraví transparentné financovanie politických strán počas celého volebného obdobia, nielen v čase trvania predvolebnej kampane.

- Upraviť okruh subjektov oprávnených financovať volebné kampane počas volieb do Národnej rady Slovenskej republiky a Európskeho parlamentu podobným spôsobom, ako je to v prípade prezidentských volieb.
- Zaviesť povinnosť informovania o zadávateľovi online politických reklám aj v čase mimo predvolebnej kampane.



## ➤ *Pripraviť, odstrániť, brániť...*

Jednou z podstatných foriem, ktoré podporujú efektívne uplatnenie zodpovednosti a dôslednosti pri aplikácii prvkov zabezpečenia informovanosti, posilnenie situačného povedomia, o existencii a boji proti hybridným hrozbám je aj poskytovanie vzdelávania, resp. školení, kurzov, ako je aj tento. Pretože ak budeme širokú verejnosť informovať a vzdelávať o možnostiach hrozieb a tiež ako predchádzať týmto hrozbám, či eliminovať ich, budeme vedieť zabezpečiť to, že akékoľvek hrozby budú mať na našu spoločnosť minimálny dopad.

- Šírenie osvedčenia a verejné informačné kampane,
- odhaľovanie a reagovanie na dezinformácie,
- rozprávanie o prebiehajúcich trendoch, hrozbách a rizikách,
- špecifické varovania, rady a usmernenia pre verejnosť, využitie prieskumu verejnej mienky,
- zverejňovanie faktov alebo výsledkov výskumu.

Ktoré základné pojmy súvisia s problematikou hybridných hrozieb?

Ako sú definované 4 piliere ktoré je potrebné poznať pre pochopenie konceptu hybridných hrozieb?

Čo je to strategická komunikácia?

Je v rámci Vášho pôsobenia venovaná dostatočná pozornosť problematike hybridných hrozieb?

Ako by ste zefektívnili boj proti hybridným hrozbám?



Zdroj obrázka:

[https://www.google.com/search?q=%C5%BEiarovka+kreslen%C3%A1&tbm=isch&ved=2ahUKEwjM7Lne3ruAAxWPmicCHSG6DxkQ2cCegQIABAA&oeq=%C5%BEiarovka+kreslen%C3%A1&gs\\_lcp=CgNpbWcQAZIFCAAQgAQyBggAEAUQHjoECCMQJzoHCAAQigUQQzoGCAAQCBaEogcIABAYEIAEUPgCWIUSYOMVaABwAHgAgAFaiAGuBZIBAjEwmAEAoAEBqgELZ3dzLXdpei1pbWfAAQE&sclient=img&ei=8x\\_JZltnM4-1nsEPofS-yAE&bih=739&biw=1536](https://www.google.com/search?q=%C5%BEiarovka+kreslen%C3%A1&tbm=isch&ved=2ahUKEwjM7Lne3ruAAxWPmicCHSG6DxkQ2cCegQIABAA&oeq=%C5%BEiarovka+kreslen%C3%A1&gs_lcp=CgNpbWcQAZIFCAAQgAQyBggAEAUQHjoECCMQJzoHCAAQigUQQzoGCAAQCBaEogcIABAYEIAEUPgCWIUSYOMVaABwAHgAgAFaiAGuBZIBAjEwmAEAoAEBqgELZ3dzLXdpei1pbWfAAQE&sclient=img&ei=8x_JZltnM4-1nsEPofS-yAE&bih=739&biw=1536)

- AKČNÝ PLÁN KOORDINÁCIE BOJA PROTI HYBRIDNÝM HROZBÁM 2022 – 2024. [online]. [2023-06-30]. Dostupné na internete: <https://rokovania.gov.sk/RVL/Material/27021/1>.
- Bezpečnostná stratégia SR. [online]. [cit. 13- 12-2022]. Dostupné na internete: [https://www.mosr.sk/data/files/4263\\_210128-bezpecnostna-strategia-sr-2021.pdf](https://www.mosr.sk/data/files/4263_210128-bezpecnostna-strategia-sr-2021.pdf).
- BOLT, N., STOLZE, M., HAIDEN, L., ALTHIUS, J. 2023. Understanding Strategic Communications: NATO Strategic Communications Centre of Excellence Terminology Working Group Publication No. 3. Riga: NATO STRATCOM COE, 2023, 44 p. ISBN 978-9934-619-40-3.
- BUZAN, B. 1991. New patterns of global security in the twenty-first century. International Affairs, Volume 67, Issue 3, July 1991, Pages 431-451.
- CULLEN, P. Understanding Hybrid Warfare [online]. [cit. 13- 12-2022]. Dostupné na internete: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/647776/dar\\_mcdc\\_hybrid\\_warfare.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf).
- GLOBSEC. 2022. [online]. [cit.2023.02.14.]. Dostupné na internete: <https://www.globsec.org/what-we-do/publications/prirucka-strategickej-komunikacie-pre-verejnu-spravu>.
- HOFFMAN, F., G. 2007. Conflict in the 21st Century: The Rise of Hybrid Wars (Arlington, VA: Potomac Institute for Policy Studies, 2007), 8.



- HYBRID COE. 2018. [online]. [cit.2023.02.15.]. Dostupné na internete: <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/>.
- HYBRIDNÉ HROZBY NA SLOVENSKU. Strategická korupcia. Analýza legislatívy, štruktúr a procesov. GLOBSEC, 2019, 21 s.
- IW JOC. 2015. [online]. [cit.2023.02.15.]. Dostupné na internete: [http://www.dtic.mil/doctrine/concepts/joint\\_concepts/joc\\_iw\\_v1.pdf](http://www.dtic.mil/doctrine/concepts/joint_concepts/joc_iw_v1.pdf).
- KONCEPCIA BEZPEČNOSTNÉHO SYSTÉMU SLOVENSKEJ REPUBLIKY. 2023. [online]. [cit.2023.08.17.]. Dostupné na internete: <https://rokovania.gov.sk/RVL/Material/28141/1>.
- KONCEPCIA PRE BOJ SLOVENSKEJ REPUBLIKY PROTI HYBRIDNÝM HROZBÁM. 2018. [online]. [cit.2023.01.06.]. Dostupné na internete: <https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf>.
- KONCEPCIA STRATEGICKEJ KOMUNIKÁCIE SLOVENSKEJ REPUBLIKY. 2023. [online]. [cit.2023.08.03.]. Dostupné na internete: [https://www.vlada.gov.sk/share/uvsr/koncepcia\\_strategickej%20komunikacie\\_sr.pdf?csrt=2433846761948488913](https://www.vlada.gov.sk/share/uvsr/koncepcia_strategickej%20komunikacie_sr.pdf?csrt=2433846761948488913).
- MANSOOR, P., R. 2012. Hybrid War in History. In Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present, ed. Williamson Murray and Peter R. Mansoor (Cambridge: Cambridge University Press, 2012), p. 22 -38.
- MILO, D., DAXLER, P., KLINGOVÁ, K., MIŠÍK, M., PIŠKO, M. 2018. MAPOVANIE ZRANITELNOSTI SLOVENSKEJ REPUBLIKY V OBLASTI HYBRIDNÝCH HROZIEB. GLOBSEC, 2018.
- MINISTERSTVO VNITRA ČR. 2023. [online]. [2023-1-30]. Dostupné na internete: <https://www.mvcr.cz/chh/clanek/co-jsou-hybridni-hrozby.aspx>.

- HYBRIDNÉ HROZBY. Krátky terminologický slovník. NBAC. 2023. [online]. [cit.2023.08.16.]. Dostupné na internete: <https://mmqx.sis.gov.sk/storage/files/HH-Slovník-2023.pdf>.
- OSHA. EUROPA. 2018. [online]. [cit.2023.03.15.]. Dostupné na internete: <https://osha.europa.eu/sk/tools-and-resources/eu-osha-thesaurus/term/62115d>.
- Spoločná deklarácia prezidenta Európskej rady, predsedu Európskej komisie a generálneho tajomníka NATO podpísaná 8. 7. 2016 na samite EÚ-NATO vo Varšave.
- Spoločné oznámenie o implementácii Spoločného rámca pre boj proti hybridným hrozbám – reakcia EÚ (J01N(2017) 30 final) z 19. 7. 2017.
- Spoločný rámec pre boj proti hybridným hrozbám - reakcia EÚ (JOIN(2016) 18 final) zo 6. 4. 2016.
- Správa o činnosti Slovenskej informačnej služby za rok 2021. [online]. [cit.2023.08.03.]. Dostupné na internete: [\[https://www.sis.gov.sk/pre-vas/sprava-o-cinnosti.html#hrozby\]](https://www.sis.gov.sk/pre-vas/sprava-o-cinnosti.html#hrozby).
- StratCom CoE. 2014. [online]. [cit.2023.02.14.]. Dostupné na internete: [https://stratcomcoe.org/about\\_us/about-nato-stratcom-coe/5](https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5).

- ŠTEPANOVIČ, D. 2019. Slabiny Slovenskej republiky ako ciele hybridných aktivít. In Zborník príspevkov z 10. medzinárodnej vedeckej konferencie „Národná a medzinárodná bezpečnosť 2019“. Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika. 567 s. ISBN 978-80-8040-582-3.
- The landscape of Hybrid Threats: A conceptual model, 52 p. ISBN 978-92-76-29819-9.
- VEJMEĽKA, O. a kol. 2005. Vojenský výkladový slovník vybraných operačných pojmov. Správa doktrín Ředitelství výcviku a doktrín, Vyškov, 2005, 359 s.
- Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov.
- WITHER, J. K. 2016. Making Sense of Hybrid Warfare. Connections , Vol. 15, No. 2 (Spring 2016), p. 73-87. e-ISSN 1812-2973.



# Ďakujem za pozornosť!



Zdroj obrázka: <https://www.rmit.edu.au/news/ccsri/hybrid-threat-centre-launched>.