HYBRIDNÁ HROZBA – IDENTIFIKÁCIA PRÍZNAKOV VEDENIA HYBRIDNEJ VOJNY

kpt. JUDr. Milan **KUSÁK**, LL.M.

ÚVOD

V súčasnosti čelíme výzvam, ktoré zásadným spôsobom menia naše chápanie konfliktov a vojnových stratégií. Jedným z takýchto nových fenoménov je hybridná vojna, ktorá sa stala kľúčovým konceptom v oblasti bezpečnosti a obrany. Termín „hybridná vojna" sa často používa na označenie konfliktu, ktorý kombinuje tradičné vojenské operácie s rôznymi nevojenskými metódami, vrátane kybernetických útokov, dezinformačných kampaní a politického či ekonomického nátlaku.

Článok, ktorý máte pred sebou, sa zaoberá detailnou analýzou pojmu hybridná vojna, jej definíciami a praktickými prejavmi v rôznych konfliktoch. Zameriava sa na rôzne definície a prístupy k hybridnej vojne, ktoré sa líšia medzi rôznymi školami a analytikmi. Kľúčovou otázkou však stále zostáva, ako efektívne rozpoznať a reagovať na hybridné hrozby. Článok ponúka prehľad najpravdepodobnejších príznakov a identifikátorov hybridného konfliktu, vrátane kombinácie vojenských a nevojenských prostriedkov, kybernetických útokov, informačných operácií a politickej destabilizácie. Podrobne tiež rozoberá prípadové štúdie, ktoré ilustrujú konkrétne prejavy hybridnej vojny v modernom svete, ako napríklad konflikt na Ukrajine a udalosti v Hongkongu.

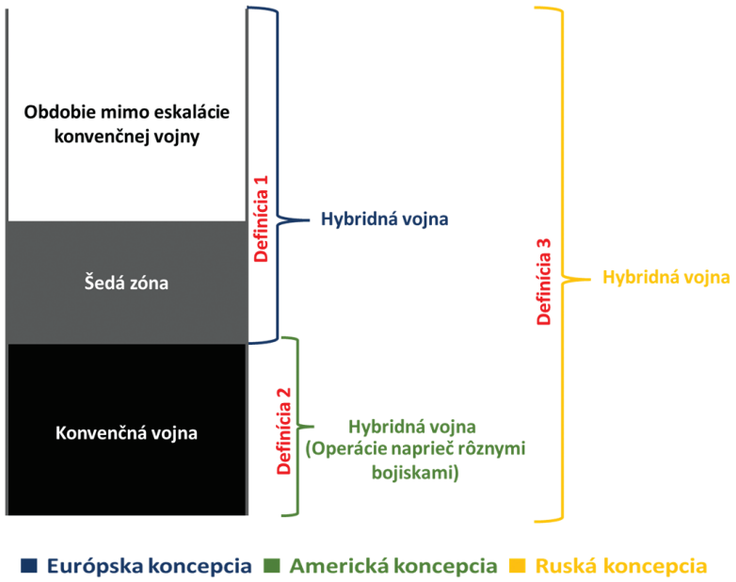
V závere sa článok venuje obranným stratégiám a reakciám na hybridné hrozby, zdôrazňuje význam koordinácie medzi rôznymi bezpečnostnými zložkami a využívania pokročilých technológií na zaistenie národnej bezpečnosti. Hybridná vojna predstavuje dynamický a komplexný fenomén, ktorý si vyžaduje neustálu adaptáciu a inovácie v oblasti bezpečnostných opatrení.

1 CHARAKTERISTIKA A DEFINÍCIA HYBRIDNEJ VOJNY

Slovo „hybrid" sa pôvodne používalo v biológii, predovšetkým však vo vede o šľachtení domestikovaných zvierat a rastlín. Označovalo sa ním kríženie dvoch rôznych línií. [1]) S postupom času sa tento termín vyvíjal a v súčasnosti slúži na opis používania viacerých prostriedkov v ich kombinácii, ako sú napríklad hybridné vozidlá poháňané benzínom a elektrinou. S ohľadom na túto etymológiu, termín „hybridná vojna" slúži na označenie typu vojny, ktorá kombinuje tradičné vojenské prostriedky s rôznymi nevojenskými prostriedkami. Medzi analytikmi vo všeobecnosti panuje v tomto bode konsenzus. V čom sa však analytici výrazne rozchádzajú, je spôsob akým odlišujú hybridnú vojnu v súvislosti s konvenčne ponímanou vojnou. Vojnu ako takú charakterizuje vysoko intenzívny konflikt medzi pravidelnými silami dvoch alebo viacerých štátov, pričom každá využíva svoje vlastné schopnosti palebnej sily. Ako je znázornené na obrázku 1, definícia hybridnej vojny v súvislosti s konvenčnou vojnou môže byť ponímaná z pohľadu troch vzájomne sa prekrývajúcich koncepcií.

1) HOENBY, A. S.: *Oxford Advanced Learner's Dictionary of Current English*, 1974, s. 425.

Variácie zahŕňajúce vojenský a nevojenský charakter hybridnej vojny



Obrázok 1: Definície hybridnej vojny
(Zdroj: vlastné spracovanie)

Najširšia definícia je definícia 3, ktorá zahŕňa všetko od bojov v období mimo eskalácie konvenčnej vojny a situácií šedej zóny, ako aj použitie rôznych hybridných metód v konvenčnej vojne. Táto definícia je presadzovaná predovšetkým v rámci ruskej koncepcie hybridnej vojny. Za zakladateľa konceptu hybridnej vojny v Rusku sa považuje náčelník Generálneho štábu Ozbrojených síl Ruskej federácie a prvý námestník ministra obrany armádny generál Valerij Vasilievič Gerasimov. Vo svojom článku Ценность науки в предвидении : Новые вызовы требуют переосмыслить формы и способы ведения боевых действий [Hodnota vedy je predvídavosť : Nové výzvy si vyžadujú prehodnotenie foriem a metód vedenia vojny] používa termín „hybridná vojna" v širokom zmysle, a to bez toho, aby ju presne definoval. Podľa generála Gerasimova *„hybridná vojna je vojnou novej generácie, v ktorej tradičné vojenské metódy a postupy sú nahradené hybridnými, to znamená širokou škálou politických, ekonomických, informačných, medzinárodných, humanitárnych a ďalších nástrojov".* Ďalej uvádza *„v 21. storočí začína prevládať tendencia, kedy hranice medzi vojnou a mierom sú rozmazané. Vojny sa nevyhlasujú a ak sa začnú, neprebiehajú podľa obvyklej šablóny. Skúsenosti z konfliktov spojených s tzv. farebnými revolúciami v severnej Afrike a na Blízkom Východe poukazujú na to, že prosperujúci štát sa môže stať za niekoľko mesiacov, ba dokonca aj dní arénou vojenského zápasu, obeťou zahraničnej intervencie, a dostať sa do stavu humanitárnej katastrofy, chaosu a občianskej vojny".* [2])

Generál pokračuje *„v žiadnej z krajín, kde vypukla tzv. arabská jar nie je oficiálne vyhlásená vojna, avšak sociálne, ekonomické a politické dôsledky pre jednotlivé štáty a spoločnosti sú zrovnateľné s následkami skutočnej vojny. K dosiahnutiu politických a strategických cieľov už nie sú potrebné zbrane, resp. existujú účinnejšie nástroje. Pre dosiahnutie stanovených cieľov je mnohokrát vhodnejšie použitie politických, ekonomických, informačných, humanitárnych a ďalších nevojenských opatrení, vrátane protestného potenciálu obyvateľstva cieľovej krajiny."* [2]) Z toho vyplýva, že politické a strategické ciele sa dosahujú hlavne prostredníctvom nevojenských opatrení, vrátane skrytých vojenských

2) GERASIMOV, V. V.: *Cennosť nauky v predvidenii...*, 2013.

akcií, a otvorené použitie sily prichádza až na konci konfliktu na dosiahnutie konečných cieľov. *„To všetko je doplnené o skryté vojenské akcie informačného charakteru alebo špeciálnych jednotiek. Otvorené použitie sily so zámienkou „udržania mieru a regulácie krízy" sa deje až na konci konfliktu za účelom „dosiahnutia konečných cieľov"*. [3])

Generál Gerasimov poukazuje na to, že *„samotné pravidlá vojny sa zmenili. Narástla úloha nevojenských spôsobov dosiahnutia politických a strategických cieľov, ktoré v mnohých prípadoch svojou efektívnosťou prevyšujú silu zbraní. Vojenské sily sa často používajú pod pláštikom mierových operácií, ktoré majú dosiahnuť uzmierenie znepriatelených strán"*. [2]) A ďalej uvádza *„nepriateľa je možné poraziť kombináciou politických, ekonomických, technologických, informačných a ekologických operácií"* [2])

Definíciu 3 možno zhrnúť, že moderná vojna zahŕňa široké spektrum nevojenských prostriedkov, ako sú politické, ekonomické, informačné a humanitárne opatrenia, ktoré sú často účinnejšie ako tradičné zbrane. Konflikty dnes často prebiehajú bez formálneho vyhlásenia vojny, pričom skryté vojenské akcie a informačné operácie zohrávajú kľúčovú úlohu, pričom otvorená sila sa používa až na dosiahnutie konečných cieľov. Tým sa rozmazávajú hranice medzi vojnou a mierom, pričom štáty môžu rýchlo upadnúť do chaosu a občianskej vojny bez tradičného vojenského konfliktu.

Na druhej strane, definícia 2 je založená na predpoklade, že samotný pojem „vojna" sa používa pre ozbrojené konflikty vysokej intenzity. Preto použitie hybridných metód v situáciách, ktorých intenzita sa nezvýšila, nie je zahrnuté do tejto kategórie hybridnej vojny. Túto koncepciu zastáva najmä americká škola. Z rovnakej perspektívy sú aj takí, ktorí tvrdia, že samotná analýza kategórie, ktorá pozostáva z rámca hybridnej vojny, je zavádzajúca. Namiesto toho by sa malo uvažovať o použití operácií naprieč rôznymi bojiskami (označované aj ako operácie na všetkých bojiskách alebo operácie na viacerých bojiskách) v rámci rozsiahlej konvenčnej vojny. Zástancovia tohto prístupu zastávajú názor, že podstatou vedenia vojny bude aj naďalej použitie sily, predovšetkým palebnej, a že v oblasti konvenčnej vojny sa budú najúčinnejšie využívať nové a rôznorodé metódy.

V súvislosti s definíciou 2 je vhodné upozorniť, že hlavným predstaviteľom tohto smeru je podplukovník Frank Hoffman z Inštitútu národných strategických štúdii Národnej univerzity obrany vo Washingtone. Podplukovník Hoffman je považovaný za „znovuobjaviteľa" termínu hybridná vojna. V jeho ponímaní a s ohľadom na vyššie spomenuté hybridná vojna *„predstavuje viac ako len konflikt medzi štátmi a inými ozbrojenými skupinami. Je aplikáciou rôznych foriem konfliktu, ktoré najlepšie odlišujú hybridné hrozby alebo hybridné konflikty. To platí najmä odvtedy, odkedy môžu byť hybridné vojny vedené ako štátmi, tak i rôznymi neštátnymi aktérmi"*. [4]) Podľa Hoffmana hybridná vojna zahŕňa konflikt, v ktorom sa zapájajú štátni aj neštátni aktéri, pričom využívajú metódy, ktoré predstavujú kombinované hrozby. Tieto hybridné (kombinované) hrozby *„zahŕňajú celú škálu spôsobov boja, vrátane konvenčných spôsobov a schopností, neregulárnej taktiky a nepravidelných formácií, ako aj kriminálne a teroristické činy, ktoré zahŕňajú neobmedzené násilie, nátlak, spoločenské nepokoje a rozvrat"*. [5]) S ohľadom na uvedené poukazuje podplukovník Hoffman na to, že *„tieto rôznorodé aktivity môžu byť vykonávané viacerými samostatnými jednotkami (alebo dokonca tou istou jednotkou), pričom sú operačne a takticky riadené a koordinované v priestore operácie za účelom dosiahnutia synergického efektu vo fyzickom i psychologickom rozmere konfliktu. Želané účinky pritom možno dosiahnuť na všetkých úrovniach konfliktu"*. [4])

3) GROHMANN, J.: *Hybridní války podle Valerije Gerasimova*, 2015.
4) HOFFMAN, F. G.: Hybrid Warfare and Challenges, 2009, s. 36.
5) HOFFMAN, F. G.: *Conflict in the 21st Century : The Rise of Hybrid Wars*, 2007.

Podplukovník David J. Kilcullen (Austrálčan pracujúci pre americkú vládu vo Washingtone D.C.) potvrdzuje tento pohľad, keď popisuje hybridnú vojnu ako moderný konflikt zahŕňajúci kombináciu konvenčnej vojny, neregulárnej vojny, občianskej vojny, povstania a terorizmu. [6]) Major William J. Nemeth vo svojej práci o čečenskej vojne charakterizuje hybridnú vojnu ako moderný spôsob gerilovej vojny, kde sú využité moderné technológie a metódy mobilizácie. [7])

K definícii 2 z vyššie uvedeného možno vyvodiť záver, že hybridná vojna predstavuje komplexný konflikt, kde sa kombinujú rôzne formy bojovej činnosti zahrňujúce konvenčnú aj neregulárnu vojnu, povstanie, terorizmus a kriminálne činy, využívané tak štátnymi ako aj neštátnymi aktérmi. Tento prístup umožňuje dosahovať synergický efekt vo fyzickom i psychologickom rozmere konfliktu. Moderné technológie a metódy mobilizácie sú kľúčové pre realizáciu hybridných hrozieb a dosahovanie stanovených cieľov na všetkých úrovniach konfliktu. Americká škola považuje hybridné metódy za súčasť konvenčnej vojny a zdôrazňuje význam palebnej sily v moderných konfliktoch.

Definícia 1, naopak, definuje hybridnú vojnu ako použitie rôznych vojenských a nevojenských prostriedkov v situáciách, ktoré neeskalujú do konvenčnej vojny alebo v situáciách, ktorých zámerom je vyhnúť sa tomu, aby sa pretransformovali do konvenčnej vojny v plnom rozsahu. Táto definícia je často používaná mnohými analytikmi.

V rámci európskej koncepcie ponímania hybridnej vojny je potrebné spomenúť holandského generálmajora a poslanca parlamentu Franka van Kappena. Bol jedným z prvých Európanov, ktorý sa o danú problematiku zaujímal a dokázal zadefinovať pojmy s ňou súvisiace. Z jeho pohľadu možno hybridnú vojnu chápať ako *„široké spektrum nepriateľských aktivít, v ktorých úloha vojenského komponentu je skôr malá, pretože politický, informačný, ekonomický a psychologický vplyv sa stáva hlavným prostriedkom vedenia boja. Takéto metódy pomáhajú dosiahnuť významné výsledky: teritoriálne, politické a ekonomické straty nepriateľa, chaos a rozvrat systému výkonu štátnej moci, a oslabenie morálky spoločnosti“*. [8]) V tejto súvislosti je potrebné poukázať na to, že štáty sú povinné dodržiavať medzinárodné právo, ako sú Ženevské konvencie na ochranu obetí vojny a Haagský dohovor o používaní zbraní vo vojne. Ženevské konvencie a ich dodatkové protokoly tvoria základ medzinárodného humanitárneho a vojnového práva, ktoré chráni dôstojnosť ľudskej bytosti počas ozbrojených konfliktov. Tieto zásady zaručujú ochranu tých, ktorí sa priamo nezúčastňujú konfliktu alebo boli vyradení z boja. Všetky štáty sú zmluvnými stranami týchto konvencií, a preto sú povinné ich dodržiavať, pričom porušenie týchto pravidiel je považované za vojnový zločin s následnou trestnou zodpovednosťou podľa medzinárodného práva. Kappenov prínos však spočíva práve v tom, že významne poukázal na skutočnosť, podľa ktorej *„štáty, ktoré vedú hybridnú vojnu, uzatvárajú dohody s neštátnymi aktérmi, bojovníkmi (žoldniermi), súkromnými organizáciami a skupinami miestnych obyvateľov, avšak akúkoľvek komunikáciu s nimi dôrazne popierajú. Títo aktéri totiž môžu vykonávať (realizovať) také veci (kroky), ktoré si štát nemôže dovoliť podniknúť. Všetka špinavá robota tak môže byť potom hodená na plecia nevládnych organizácií“.* [9])

V tomto prípade je pojem „vojna“ rozšírený na širší význam, ktorý nie je nevyhnutne potrebný vnímať ako použitie plnej vojenskej sily. Táto definícia sa však často používa zámerne, možno preto, aby upriamila pozornosť na túto novú formu „vojny“ ako donucovací prostriedok na dosiah-

6) KILCULLEN, D.: *The Accidental Guerrilla : Fighting Small Wars in the Midst of a Big One*, 2009.
7) HOFFMAN, F. G.: Hybrid vs. Compound War, 2009.
8) *Kremlin hybrid war against Ukraine and EU : Energy Component*, 2014.
9) *Hybrid Warfare as a Key Instrument of Russian Revenge Geostrategy*, 2015.

nutie cieľov používaných štátmi (alebo mocnými neštátnymi aktérmi) namiesto konvenčnej vojny v plnom rozsahu. Aj keď rozsiahle konvenčné vojny v budúcnosti úplne nezmiznú, dôležité sa stanú nové metódy vedenia vojny, ktoré nevedú k rozsiahlemu vojenskému konfliktu za plného využitia zbraní. V tejto súvislosti by jasné rozlíšenie medzi koncepciou hybridnej vojny, ako by mala byť zavedená v rámci definície 1 a konvenčnou vojnou prispelo k jasnejšej a presnejšej diskusii.

Z pohľadu definície 1 je teda hybridná vojna využiteľná ako donucovací prostriedok spočívajúci v tom, že štáty a neštátni aktéri využívajú kombináciu vojenských a nevojenských metód, ako sú politické, ekonomické, informačné a psychologické vplyvy na dosiahnutie svojich cieľov bez toho, aby sa zapojili do plnohodnotnej konvenčnej vojny. Týmto spôsobom môžu spôsobiť značné škody nepriateľovi, ako sú teritoriálne, politické a ekonomické straty, chaos a oslabenie jeho morálky. Táto koncepcia si je však plne vedomá aj nekalých praktík zo strany nepriateľa pri vedení hybridnej vojny, ktoré podčiarkujú diverzný charakter jeho konania.

Záverom k tejto časti je treba konštatovať, že v každom prípade by nejednoznačná definícia „hybridnej vojny" v tomto článku mohla viesť k zmätku. Preto je potrebné stanoviť definíciu v počiatočnej fáze diskusie, ale ako už bolo spomenuté vyššie, ktorú definíciu je vhodné prijať, bude závisieť od zamerania diskusie. V tomto článku sa zameriame na vznik štátov a neštátnych aktérov, ktorých cieľom je dosiahnuť ciele, ktoré sa predtým dosiahli prostredníctvom rozsiahlej konvenčnej vojny rôznymi metódami, vrátane vojenských a nevojenských prostriedkov, bez toho, aby sa uchýlili ku konvenčnej vojne. Preto v tomto článku budeme používať termín „hybridná vojna" v zmysle definície 1, aby bol zameraný na hybridné metódy.

2 PRÍZNAKY A IDENTIFIKÁTORY HYBRIDNÉHO KONFLIKTU

2.1 Príznaky

Samotný proces identifikácie hybridného konfliktu je náročný. Dôvodom je, že tieto stratégie často zahŕňajú maskovanú a skrytú činnosť.

Najpravdepodobnejšie príznaky, ktoré môžu naznačovať, že ide o hybridnú vojnu: sú:

1. Kombinácia vojenských a nevojenských prostriedkov

Zahŕňa použitie tradičných vojenských síl spolu s nekonvenčnými metódami, ako sú kybernetické útoky, informačné operácie a podpora miestnych militantných skupín.

Kybernetické útoky sú považované za dôležitú súčasť hybridnej vojny. Využívajú digitálne prostriedky, aby narušili, poškodili alebo ovládli kritickú infraštruktúru protivníka. Kompozične môžu pozostávať z:

- **malwaru a vírusov –** ich úlohou je infikovať počítačové systémy, ktoré môžu napríklad vymazať dáta alebo prevziať kontrolu nad systémom;
- **DDoS útokov –** tieto majú za cieľ preťažiť servery, a tým ich učiniť nedostupnými pre ich používateľov;
- **phishingu a sociálneho inžinierstva –** inými slovami ide o získavanie citlivých informácií s použitím klamstva a manipulácie;
- **hackovania kritických systémov** – predstavuje narúšanie napríklad systémov riadenia energetických sietí, finančných systémov, ale aj dopravnej infraštruktúry.

Informačné operácie zase opisujú širokú škálu aktivít, ktoré sú zamerané na ovplyvňovanie verejnej mienky a rozhodovacích procesov. Sem sú zaradené:

- **psychologické operácie (PSYOPS) –** využívanie psychologických techník na ovplyvnenie morálky a správania buď jednotlivcov, alebo skupín;
- **manipulácia médií –**používanie médií na šírenie želanej propagandy, ale aj na potláčanie nepriaznivých informácií;
- **propaganda** – šírenie informácií za účelom ovplyvniť postoje a vnímanie cieľovej populácie. Tieto informácie môžu byť pravdivé, skreslené alebo úplne falošné;
- **dezinformácie** – úmyselne rozširovanie nepravdivých informácií s cieľom zmiasť protivníka, prípadne ovplyvniť verejnú mienku.

Podstatná je predovšetkým intenzívna kampaň dezinformácií a propagandy s cieľom zmiasť, destabilizovať a ovplyvniť verejnú mienku a rozhodovacie procesy protivníka. Dezinformácie a propaganda môžu byť šírené rôznymi kanálmi, vrátane sociálnych médií, tradičných médií, falošných webových stránok a cez rôzne formy digitálnych platforiem. [10]) Rozhodujúcim účelom tejto taktiky sú:

a) **zmätenie a polarizácia spoločnosti –** vytvárajú a šíria sa protichodné informácie, ktoré spôsobujú zmätok a rozdeľujú spoločnosť na rôzne skupiny s rozdielnymi názormi;
b) **oslabenie dôvery –** dôvera verejnosti v úradné inštitúcie, médiá a vládu je podkopávaná, čo môže viesť k politickej nestabilite;
c) **ovplyvnenie politických rozhodnutí** – použitím manipulácie verejnej mienky a volieb je možné dosiahnuť politické zmeny výhodné pre útočníka;
d) **demoralizácia protivníka** – predstavuje šírenie pesimistických alebo demoralizujúcich myšlienok.

Osobitné miesto v tejto súvislosti zastáva kultúrna a náboženská manipulácia. Jej podstatou je využívanie kultúrnych a náboženských rozdielov na vytváranie napätia a rozdeľovanie spoločnosti. Táto forma manipulácie je obzvlášť účinná, pretože zasahuje do základných identít a hodnôt jednotlivcov a skupín, čo môže viesť k hlbokým a dlhotrvajúcim konfliktom.

Kultúrne rozdiely medzi rôznymi etnickými a národnostnými skupinami sú v kontexte hybridnej vojny zraniteľným miestom. Zúčastnené strany hybridnej vojny môžu využívať takéto rozdiely s úmyslom šíriť medzi obyvateľstvom dezinformácie a propagandu s podporou nedôvery a nepriateľstva. Príkladom môžu byť falošné správy a manipulatívny obsah na sociálnych sieťach, ktorý prezentuje určité kultúrne praktiky negatívnym spôsobom, čo vyvoláva negatívne dojmy a emócie, a taktiež polarizuje spoločnosť. [11]) Náboženské rozdiely predstavujú hlbokú a citlivú tému, ktorá je ľahko zneužiteľná na vyvolanie konfliktov. Prostredníctvom dezinformácií a propagandy, tak môže útočník šíriť nenávisť a strach medzi rôznymi náboženskými skupinami. Typicky môže ísť o vytváranie falošnej správy o útokoch alebo urážkach jednej náboženskej skupiny smerom k druhej, čo vyvolá násilnú reakciu a eskaláciu napätia. [12])

10) HUGHES, H.C. - WAISMEL-MANOR, I.: The Macedonian fake news industry..., 2021.
11) *Cultural Property : A Hybrid Threat Issue*, 2021.
12) BILAL. A.: Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote, 2021.

Existuje mnoho príkladov zneužívania kultúrnych a náboženských rozdielov v hybridnej vojne. Počas konfliktu na Ukrajine sa vo veľkej miere využíva napätie medzi pro-ruskými a pro-ukrajinskými skupinami, pričom propaganda a dezinformácie hrajú kľúčovú úlohu v polarizácii spoločnosti. [13]) Inak to nie je ani na Blízkom východe, kde sú náboženské rozdiely medzi sunnitmi a šiitmi vo veľkej miere zneužívané na šírenie násilia a destabilizáciu regiónu. [11])

Podpora miestnych skupín môže v praxi spôsobiť, že nepravidelné vojenské jednotky napadnutého štátu budú vykonávať podpornú činnosť v záujme agresora. Nasadenie takýchto nepravidelných vojenských jednotiek môže prebiehať skryto a mimo formálnych vojenských štruktúr. Príkladom takýchto aktivít agresora sú:

- **finančná a materiálna podpora –** poskytovanie zbraní, financií a iných zdrojov na podporu miestnych skupín;
- **výcvik a poradenstvo –** poskytovanie vojenského výcviku a strategických rád militantným skupinám;
- **spravodajská podpora –** poskytovanie spravodajských informácií na zlepšenie efektívnosti operácií týchto skupín;
- **skrytá intervencia –** nepriamy zásah a manipulácia prostredníctvom miestnych aktérov, aby agresor mohol dosiahnuť svoje ciele bez priameho angažovania sa a zvýšenia medzinárodnej pozornosti.

2. Ekonomický tlak

Príkladom sú sankcie, obchodné obmedzenia alebo manipulácia s cenami surovín, a to s cieľom oslabenie ekonomiky protivníka.

Ekonomický tlak s použitím ekonomických nástrojov možno využiť na oslabenie ekonomiky protivníka a destabilizáciu jeho politického systému. Do tejto stratégie môžu byť začlenené sankcie za účelom obmedzenia prístupu k medzinárodným trhom, obchodné obmedzenia na narušenie dodávateľských reťazcov, ale aj manipulácie s cenami surovín, čoho výsledky môžu mať výrazný dopad na hospodárstvo cieľovej krajiny. Ekonomický tlak možno považovať za efektívny nástroj hybridnej vojny, a to z dôvodu, že môže spôsobiť hospodársku nestabilitu, zvýšiť nezamestnanosť, znížiť životnú úroveň a vyvolať sociálne nepokoje, čo môže potenciálne viesť k oslabeniu vládnej moci a zvýšeniu vnútropolitických konfliktov. [14])

3. Politická destabilizácia

Podpora vnútorných politických konfliktov, etnických napätí alebo separatistických hnutí s cieľom oslabiť alebo rozložiť politickú stabilitu cieľovej krajiny.

Politickou destabilizáciou rozumieme jednu z možnosti využitia taktiky hybridnej vojny. Cieli na podporu zintenzívnenia vnútorných politických konfliktov, etnických napätí alebo separatistických hnutí v cieľovej krajine s úmyslom oslabiť jej politickú stabilitu. [15]) Účelom je rozložiť vnútornú jednotu štátu, oslabiť dôveru občanov vo vládu a vytvoriť prostredie chaosu a neistoty. Na tento účel sú využívané nástroje vrátane vyššie spomenutých ako sú dezinformácie, propagan-

13) ROSÉN, F.: *Putin's Upper Hand : Cultural Domain Warfare*, 2024.
14) BALDWIN, D. A: *Economic statecraft : Uses of economic power in international relations*, 1985.
15) THIELE, R. (ed.): *Hybrid Warfare: Future and Technologies*, 2021.

da, kyberútoky a financovanie opozičných skupín, čo môže viesť k vnútorným nepokojom, politickej polarizácii a oslabeniu schopnosti vlády účinne reagovať na vonkajšie hrozby. [16])

4. Právne a diplomatické manévre

Je to používanie právnych nástrojov a diplomatických tlakov na ospravedlnenie agresie alebo na získanie medzinárodnej podpory pre svoje akcie.

V hybridnej vojne štáty využívajú právne argumenty na ospravedlnenie svojich agresívnych činov. Používajú medzinárodné právo selektívne vyberajúc si tie aspekty, ktoré podporujú ich akcie, zatiaľ čo ignorujú ostatné. Týmto spôsobom chcú legitimizovať svoje kroky na medzinárodnej scéne. [17]) Hybridná vojna zahŕňa aj intenzívne diplomatické úsilie na získanie podpory alebo neutralizáciu opozície voči ich akciám. Štáty používajú diplomatické kanály na ovplyvňovanie medzinárodného spoločenstva, vyvíjajú tlak na spojencov a neutrálne krajiny, aby získali politickú a ekonomickú podporu. Právne a diplomatické manévre sú často sprevádzané šírením dezinformácií a propagandy. Dochádza aj k zneužívaniu médií a sociálnych sieti na manipuláciu verejnej mienky doma i v zahraničí, čo má za cieľ vytvoriť priaznivý obraz o ich akciách a diskreditovať oponentov. [18]) V hybridnej vojne nie je neobvyklé, že štáty sa pokúšajú ovplyvniť medzinárodné organizácie ako je OSN, EÚ alebo NATO prostredníctvom právnych a diplomatických nástrojov. Snažia sa presadiť svoje záujmy a získať medzinárodné uznanie pre svoje kroky, čo môže zahŕňať aj manipuláciu s rezolúciami a hlasovaniami v týchto organizáciách.

5. Psychologické operácie (PSYOPS)

Tieto operácie znamenajú použitie psychologických techník na ovplyvnenie morálky a správania obyvateľstva a vojenských jednotiek protivníka.

PSYOPS používajú psychologické techniky na ovplyvnenie myslenia, morálky a správania obyvateľstva, politických lídrov a vojenských jednotiek protivníka. Ich hlavný cieľ smeruje k destabilizácii spoločnosti, čo znamená vytvoriť zmätok a šíriť dezinformácie. To má za následok oslabenie protivníkových schopností efektívne reagovať na hroziace hrozby.

PSYOPS sa používajú k rozširovaniu propagandy, falošných správ a na manipuláciu verejnej mienky prostredníctvom médií, sociálnych sietí a ďalších komunikačných kanálov. Tieto operácie môžu podkopať dôveru verejnosti v jej vlastnú vládu, oslabiť morálku vojenských síl a podporiť politickú nestabilitu. Okrem toho môžu byť PSYOPS zamerané na konkrétne skupiny alebo jednotlivcov s cieľom vyvolať strach, nedôveru a rozdelenie v rámci spoločnosti. Efektívne vykonávanie PSYOPS v hybridnej vojne vyžaduje dôkladné plánovanie, porozumenie kultúrnym a sociálnym špecifikám cieľového publika a využívanie moderných technológií na šírenie informácií. Výsledkom je schopnosť ovplyvniť protivníka bez priameho použitia vojenskej sily, čo robí z PSYOPS mocný nástroj v arzenáli hybridných vojen.

6. Skryté a asymetrické taktiky

Sú to taktiky, ktoré sú zamerané na využívanie slabých miest protivníka a asymetrické útoky, ktoré sú ťažko predvídateľné a odhaliteľné.

16) SCHMID, J.: Introduction to Hybrid Warfare..., 2021.
17) *Hybrid warfare : Legal arguments and justifications*, 2020.
18) Misinformation and propaganda in hybrid conflicts, 2019.

Tieto taktiky sa zameriavajú na využívanie slabých miest protivníka, často na nečakaných frontoch, čím je protivník zraniteľnejší a menej schopný efektívne reagovať. Asymetrické útoky sú často ťažko predvídateľné a odhaliteľné, čo z nich robí efektívne nástroje na destabilizáciu a demoralizáciu cieľových krajín a organizácií. [19])

Hybridná vojna mnohokrát zahŕňa synchronizáciu rôznych metód a nástrojov na dosiahnutie strategických cieľov bez vyhlásenia otvoreného konfliktu. Identifikácia hybridnej vojny vyžaduje komplexnú analýzu a monitorovanie rôznych aspektov, od vojenských aktivít až po ekonomické a informačné operácie.

2.2 Identifikátory

V kontexte európskej koncepcie moderných konfliktov sa hybridná vojna chápe ako komplexný a multidimenzionálny spôsob vedenia boja. Na rozdiel od tradičných vojenských konfliktov, hybridná vojna zahŕňa využitie rôznorodých prostriedkov a taktík, ktoré často prekračujú rámec klasických vojenských operácií. Tento typ boja sa vyznačuje nielen kombináciou vojenských a nevojenských prostriedkov, ale aj sofistikovanou spoluprácou medzi štátnymi a neštátnymi aktérmi, čo vedie k vytvoreniu situácií s vysokou mierou neprehľadnosti a neistoty.

Aktéri – sú prvý charakteristický znak hybridnej vojny. Hoci pôvodcom týchto hrozieb môžu byť štátni aj neštátni aktéri, dominantnú úlohu v nich zohráva predovšetkým štát. Ako už bolo spomenuté, neštátni aktéri často pôsobia ako podporujúci prvok štátu. Štáty ich zapájajú najmä do aktivít, na ktoré nemajú dostatočné kapacity a táto spolupráca nie je na verejnosti otvorene prezentovaná. Z uvedeného teda možno vyvodiť, že prvým identifikujúcim znakom hybridného spôsobu boja je teda fakt, že:

- pôvodcom týchto činností je štát alebo neštátny aktér v spolupráci so štátnou mocou.

Ciele – podstatnou charakteristikou hybridného konfliktu je jeho cieľ. Odborníci na predmetnú problematiku sa viac-menej zhodujú na fakte, že hybridná vojna sa pri dosiahnutí cieľa spolieha predovšetkým na zraniteľné miesta oponenta, prostredníctvom ktorých sa ho snažia donútiť k aktivitám, ktoré sa nezhodujú s jeho obvyklým smerovaním alebo oficiálnou politikou. Európska komisia zhrnula spoločný rámec boja proti hybridným hrozbám ako „Snahu zneužívať zraniteľnosť cieľa a vytvárať neprehľadné situácie s cieľom narušiť rozhodovacie procesy". [20])

V podmienkach Slovenskej republiky je hrozbou narúšanie hodnoty a jej pevného ukotvenia v štruktúrach EÚ a NATO. V tomto kontexte je za slabé stránky, využiteľné pri spochybňovaní týchto hodnôt, možné označiť predovšetkým polarizovanú spoločnosť alebo nedostatočnú legislatívu, prípadne nepripravenosť k boju s hybridnými hrozbami. Preto je možné za ďalší identifikátor hybridného spôsobu boja uviesť, že:

- zo strany činnosti vonkajšieho aktéra dochádza k polarizácii spoločnosti a následnej destabilizácii usporiadania štátu v otázkach napadania jeho hodnôt.

Prostriedky – spoločným znakom všetkých troch definícii pojmu „hybridná vojna" je využitie kombinácie vojenských a nevojenských prostriedkov. Vzhľadom k všeobecnej znalosti vojenských

19) RENZ, B. - SMITH, H.: Russia and Hybrid Warfare – Going Beyond the Label, 2016.
20) *Spoločné oznámenie Európskemu parlamentu a rade...*, 2016.

prostriedkov sa budeme zaoberať nevojenskými prostriedkami. Ide o súbor politických, ekonomických, sociálnych a informačných prostriedkov [21]), prípadne aj o činnosť spravodajských služieb spolu s kybernetickými a informačnými operáciami alebo využitím protestného potenciálu obyvateľstva. [2]) NATO sa pri definovaní pojmu opiera aj o politické, informačné či ekonomické zastrašovanie a manipuláciu". [22])

Slovenská Koncepcia boja proti hybridným hrozbám uvádza nasledujúce identifikátory:

- externý alebo interný politický nátlak na najvyšších štátnych predstaviteľov a štátne inštitúcie;
- ekonomický alebo energetický nátlak ako rozšírenie politického nátlaku;
- rozsiahle sabotáže proti kľúčovej infraštruktúre;
- kybernetické útoky s potenciálom spôsobiť škody veľkého rozsahu;
- informačné a propagandistické operácie s cieľom podkopať dôveru v štátne inštitúcie, vyvolať spoločenské nepokoje a vážne destabilizovať politickú a bezpečnostnú situáciu;
- ovplyvňovanie etnických, náboženských a kultúrnych menšín a ich manipulácia na politické účely; hrozba použitia vojenskej sily. [23])

Posledným identifikátorom je:

- Neprehľadnosť situácie, čím sa znižuje schopnosť obete adekvátne zareagovať

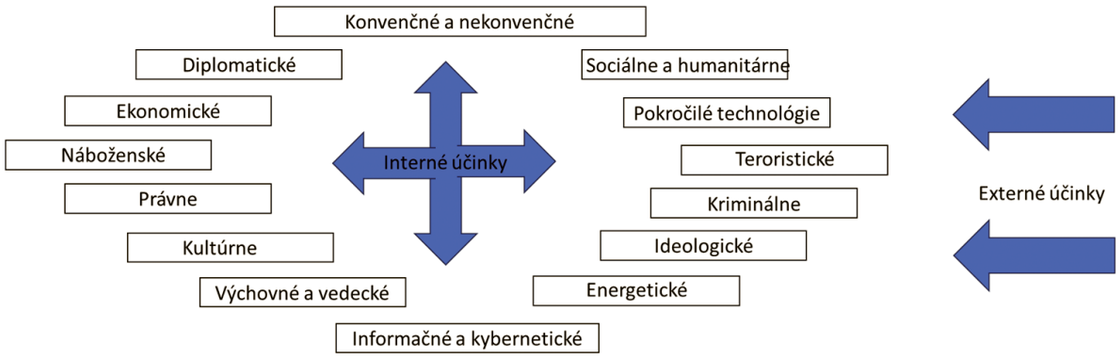
Ako bolo vyššie napísané už Gerasimov poukázal na to, že „*hranice medzi mierom a vojnou sa stierajú a to, či vojna prebieha, nie je na prvý pohľad jasné*". [2]) Podobný názor prebral aj Spoločný rámec pre boj proti hybridným hrozbám Európskej komisie. Poukazuje na hybridné hrozby, ktoré môžu rôzne štátne aj neštátne subjekty koordinovaným spôsobom využívať na to, aby dosiahli konkrétne ciele bez toho, aby formálne vyhlásili vojnu. [20])

3 REAKCIA A OBRANNÉ STRATÉGIE

Z hľadiska obranných stratégii je dôležité vyvodiť aké sú sféry hybridnej vojny. Podstatným faktorom sú kroky agresora, ktorého cieľom je zvýšiť vnútornú nestabilitu v rôznych sférach hybridnej vojny. Očakávané dopady zahŕňajú nárast nedôvery voči inštitúciám, spoločným hodnotám, zníženie ekonomickej činnosti, ale aj obmedzenie dôvery, zmätok v objektivite, odbornosti, ideológii a ďalších zdrojoch sociálnej súdržnosti.

Za súčasných podmienok je pre štátnu obranu vysokou prioritou návrh a implementácia efektívnych systémov protiopatrení. Takéto systémy musia zahŕňať technologicky pokročilé formy spravodajstva, elektronického spravodajstva, informačných a psychologických operácií a kybernetických operácií, ktoré môžu byť koordinované na dosiahnutie spoločnej stratégie a zároveň schopné operovať samostatne aj ako súčasť integrovaných operácií. Kľúčovým komponentom tejto nezávislej operabilnosti v rámci spravodajstva, sledovania a prieskumu, ako aj bojových operácií je vývoj a využívanie bezpilotných vzdušných prostriedkov (UAV).

21) GLENN, R.: Thoughts on Hybrid Conflict, 2009.
22) *Hybrid warfare - Calha report NATO*, 2015.
23) *Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám*, 2018.



Obrázok 2: Sféry hybridnej vojny

Rastúce využívanie dronov pre rôzne funkčné oblasti (spravodajstvo, elektronické protiopatrenia, priame útoky atď.) a rôzne operačné prostredia (zem, more, vzduch, obojživelné operácie) predstavuje zásadný faktor pre zaistenie flexibility v dynamických konfliktných situáciách. [24])

Nasadenie pokročilých spravodajských a reakčných schopností musí byť vyvíjané paralelne s adekvátnym výcvikom vojenského a civilného personálu, ktoré bude potrebné integrovať do týchto systémov. Efektívna implementácia technológií je podmienená prítomnosťou vysoko kvalifikovaného personálu, ktorý je schopný tieto komplexné systémy používať, udržiavať a ďalej rozvíjať, aby sa adaptovali na meniace sa podmienky bojového prostredia. Plná a efektívna kapacita môže byť dosiahnutá len vtedy, keď sú stratégie a technológie vyvíjané v súlade s profesionálnym výcvikom. Nedostatočná odbornosť pri používaní týchto technológií často vedie k ich neefektívnemu využitiu, ako je to v prípade, keď štandardné operačné postupy vo výcviku zohľadňujú zastarané koncepcie problémov (napríklad kybernetické prenikanie do informačných sietí je považované len za technický problém, namiesto jeho vnímania ako rizika pre národnú bezpečnosť). [25])

Štát nesie primárnu zodpovednosť za riadenie kariérneho rozvoja a výcviku obranného personálu. Preto by sa jednotlivé krajiny mali sústrediť na tvorbu a rozvoj technologických obranných systémov, ktoré integrujú výskum a experimentovanie s cieľom poskytovať primerané úrovne obrannej podpory. Tieto snahy by mali prekračovať rámec včasného varovania dostupného z centier pre hybridné hrozby, ktoré sú zriadené v niektorých krajinách NATO. Cieľom týchto centier je vyvíjať vhodné technológie a stratégie na riešenie budúcich hrozieb, ktoré budú schopné identifikovať.

Takéto centrum v kontexte hybridnej vojny by malo zahŕňať:

- **Systém vojenského výskumu –** tento systém by mal byť podporovaný správnou vedeckou organizačnou štruktúrou, ktorá umožní efektívne riadenie a koordináciu výskumných projektov zameraných na obranu. Dôraz by mal byť kladený na interdisciplinárny prístup, ktorý zahrnie rôzne oblasti technológie, vedy a inžinierstva na podporu vojenských potrieb.
- **Akademické zameranie na odborné znalosti v oblasti pokročilých technológií –** univerzity a akademické inštitúcie by mali byť orientované na rozvoj expertízy v pokročilých technológiách, ktoré sú relevantné pre obranu. Toto zahŕňa oblasti ako kybernetická bezpečnosť, umelá inteligencia, robotika a ďalšie moderné technológie, ktoré môžu byť integrované do vojenských systémov.

24) GRUMMAN, N.: *Survivability soars when the countermeasures are infrared and multispectral*, 2023.
25) DANYK, Y. - MALIARCHUK, T. - BRIGGS, Ch.: Hybrid War : High-tech, Information and Cyber Conflicts, 2023.

- **Vedecky založený výrobný komplex –** tento komplex by mal zahŕňať stacionárne a mobilné vzorky zbraní a vojenskej techniky, veliteľské stanice a laboratóriá. Výrobný komplex by mal byť navrhnutý tak, aby umožnil rýchlu adaptáciu a nasadenie nových technológií podľa potrieb ozbrojených síl. Taktiež by mal slúžiť ako centrum pre testovanie a hodnotenie nových zbraní a technológií.
- **Technologicky pokročilé experimentálne bojové jednotky –** tieto jednotky by mali byť vyvinuté s prihliadnutím na akademický a vedecký výskum realizovaný v rámci centra. ybavené by mali byť najnovšími technológiami a mali by byť schopné vykonávať komplexné bojové operácie v rôznych prostrediach. Tieto jednotky by mali slúžiť ako model pre budúci vývoj a integráciu nových bojových systémov a techník.

Rozvoj týchto komponentov by mal byť kľúčový pre zabezpečenie národnej bezpečnosti a obranyschopnosti. Integrácia vedeckého výskumu, technologických inovácií a vojenského výcviku by tak vytvorila systém schopný reagovať na moderné ale aj budúce hrozby.

Praktický výcvik vojenského personálu, testovanie a implementácia nových technologických systémov zbraní a vojenskej techniky, ako aj tvorba nových jednotiek, musia byť založené na vývoji a inováciách realizovaných obranným technologickým centrom a aktívnymi vojenskými jednotkami.

V kontexte boja proti hybridným hrozbám je na Slovensku zriadené Centrum pre boj proti hybridným hrozbám, ktoré je v pôsobnosti Ministerstva vnútra Slovenskej republiky a má za úlohu identifikovať a reagovať na rôzne typy hybridných útokov, vrátane kybernetických útokov, dezinformácií a ďalších foriem nevojenských hrozieb. [26]) Preto z vojenského hľadiska a z pohľadu hybridnej vojny, hybridné hrozby často zahŕňajú komplexné vojenské prvky, ako sú kybernetické útoky na vojenskú infraštruktúru, elektronické rušenie, psychologické operácie a nepriame vojenské akcie. Rovnako vyžadujú efektívnu koordináciu medzi rôznymi zložkami ozbrojených síl, spravodajskými agentúrami a ďalšími bezpečnostnými zložkami. Ich efektívne riešenie často vyžaduje prístup k špecifickým vojenským zdrojom a informáciám, ako sú vojenské satelity, šifrované komunikačné systémy a špeciálne jednotky. Mnoho hybridných hrozieb má medzinárodný charakter a vyžaduje spoluprácu s medzinárodnými vojenskými alianciami, ako je NATO.

V súvislosti s obranou proti hybridným vojnám je potrebné zvážiť vytvorenie Vojenského vedecko-technického expertízneho centra v tejto oblasti, ktorého cieľom by bolo:

- **vyhnúť sa duplicitnej činnosti rôznych celkov –** takáto centralizácia výskumu a vývoja by umožnila efektívnejšie využívanie zdrojov a elimináciu prekrývajúcich sa funkcií, čo by malo za následok efektivitu a znížilo by to náklady;
- **koncentrácia výskumného a vývojového úsilia –** sústreďovanie aktivít na jednom mieste by umožnilo lepšiu koordináciu a synergický efekt pri výskume, návrhu, tvorbe, testovaní a používaní pokročilých technologických systémov;
- **výcvik personálu v oblasti pokročilých technológií –** zabezpečenie odborného výcviku pre všetky zložky ozbrojených síl a ďalšie inštitúcie národného bezpečnostného a obranného sektora by prispelo k zvýšeniu kompetencií a pripravenosti personálu na nasadenie moderných technológií;

26) *Základné informácie.*

- **využitie vojenskej a priemyselnej základne –** integrácia vojenskej zložky s priemyselnou a výrobnou základňou by podporila rozvoj slovenskej ekonomiky a zabezpečila udržateľný rozvoj vojenskej technológie.

Praktickosť a opodstatnenosť takéhoto centra by mala byť podložená využitím skúseností vedúcich krajín sveta, ako napríklad Spojených štátov, kde Agentúra pre pokročilé výskumné projekty obrany (DARPA) zohráva kľúčovú úlohu pri hľadaní a implementácii inovatívnych technológií vo vojenskej oblasti. DARPA je známa svojím prístupom k rýchlej inovácii a spolupráci s akademickými, priemyselnými a vojenskými partnermi na vývoji prelomových technológií. [27])

Racionálna realizácia všetkých praktických aspektov takéhoto centra by musela byť vykonaná v úzkej koordinácii s centrálnym vojenským velením a riadiacimi organizáciami. Toto centrum by malo pracovať priamo so silami kooperujúcimi s centrálnymi riadiacimi orgánmi, ktoré by zabezpečili komunikáciu s vojenskými jednotkami a im podriadenými celkami, vrátane ich výcvikových základní a spolupracujúcich organizácií a štruktúr. To by zabezpečilo, že nové technologické systémy by boli efektívne integrované do existujúcich vojenských štruktúr a personál by bol adekvátne vyškolený na ich použitie, čím by sa zvýšila celková obranyschopnosť Slovenskej republiky.

Efektívna obrana proti hybridným hrozbám spočíva nielen v technologických inováciách, ale aj v komplexnom prístupe, ktorý zahŕňa výskum, vývoj, výcvik a medzinárodnú spoluprácu. Iba takto môže byť Slovensko pripravené čeliť súčasným aj budúcim výzvam a zabezpečiť stabilitu a bezpečnosť svojej krajiny a jej obyvateľov.

4 PRÍPADOVÉ ŠTÚDIE

4.1 Hybridná vojna na Ukrajine počas Ruského útoku (2022 – 2024)

Hybridná vojna na Ukrajine predstavuje kombináciu konvenčných vojenských operácií, nekonvenčných taktík, kybernetických útokov, dezinformačných kampaní a ekonomického nátlaku. Tento konflikt, ktorý vyeskaloval do otvorenej vojny v roku 2022, demonštruje komplexnosť a multifunkčnosť hybridnej vojny, ktorú Rusko využilo na dosiahnutie svojich cieľov.

Historické pozadie tejto vojny sa začalo po anexii Krymu v roku 2014 a vypuknutí konfliktu v Donbase, na základe ktorého sa napätie medzi Ukrajinou a Ruskom neustále zvyšovalo. V roku 2022 Rusko spustilo rozsiahlu vojenskú inváziu na Ukrajinu, ktorá kombinovala tradičné vojenské operácie s rôznymi hybridnými taktikami s cieľom destabilizovať Ukrajinu a oslabiť jej schopnosť odporovať. [28]) Príkladom takejto taktiky je dezinformačná kampaň, ktorú Ruská vláda rozširovala na sociálnych médiách, aby diskreditovala ukrajinskú vládu a prezentovala konflikt ako nevyhnutný krok na ochranu rusky hovoriaceho obyvateľstva na Ukrajine. Propagandistické články a príspevky na sociálnych sieťach boli šírené prostredníctvom trollov a botov, čo zvýšilo dosah a účinnosť týchto kampaní. Dezinformačné kampane sa zameriavali na podkopávanie morálky ukrajinských občanov a na získanie medzinárodnej podpory pre ruské akcie.

Reakciou Ukrajinskej vlády bolo rozvinutie stratégií na boj proti ruským dezinformačným kampaniam. Jednou z hlavných odpovedí bolo vytvorenie špecializovaných jednotiek na monitorovanie a odhaľovanie dezinformácií. Tieto jednotky analyzujú obsah na sociálnych médiách a verejne

27) *Defense Advanced Research Projects Agency*, 2024.
28) PLOKHY, S.: *The Russo-Ukrainian War : The Return of History,* 2023.

vyvracajú nepravdivé informácie prostredníctvom oficiálnych komunikačných kanálov. [29]) Okrem toho bola zvýšená spolupráca s medzinárodnými organizáciami a technologickými spoločnosťami, ako sú Facebook a Twitter, na odstraňovanie škodlivého obsahu a zatváranie účtov, ktoré šírili propagandu. Ukrajinské média a neziskové organizácie, ako je napríklad StopFake, hrali kľúčovú úlohu v identifikovaní a odhaľovaní falošných správ a manipulácií.

Ukrajinská infraštruktúra čelí početným kybernetickým útokom, vrátane útokov na energetické siete, bankové systémy a vládne webové stránky. Tieto útoky majú za cieľ destabilizovať ukrajinskú ekonomiku a vytvoriť chaos v riadení štátu. Kybernetické útoky boli koordinované s vojenskými operáciami, čím sa zvyšoval ich dopad a účinnosť. Na základe toho Ukrajina výrazne investovala do posilnenia svojej kybernetickej obrany. Založila špecializované jednotky kybernetickej bezpečnosti v rámci ozbrojených síl a civilných inštitúcií. Tieto jednotky sú zodpovedné za monitorovanie, identifikáciu a neutralizáciu kybernetických hrozieb. Spolupracujú tiež s medzinárodnými partnermi a organizáciami, ako je NATO a Európska únia, aby získali potrebné technické znalosti a podporu. [30])

V reakcii na kybernetické útoky Ukrajina zlepšila svoje komunikačné a informačné systémy, aby zvýšila odolnosť voči útokom. Modernizovali infraštruktúru a implementovali pokročilé bezpečnostné protokoly, aby minimalizovali riziko úspešných útokov. Zároveň sa zamerali na decentralizáciu kľúčových systémov, čím znížili ich zraniteľnosť voči koordinovaným kybernetickým útokom. Ukrajinské ozbrojené sily koordinovali svoje vojenské operácie s obrannými opatreniami proti kybernetickým útokom. To zahŕňalo integráciu kybernetickej vojny do širšej vojenskej stratégie, čím bolo zabezpečené, že kybernetické a konvenčné operácie sa navzájom podporujú. Napríklad, keď boli energetické siete napadnuté, vojenské jednotky boli pripravené zabezpečiť fyzickú ochranu a rýchlu obnovu kritickej infraštruktúry.

Ukrajina tiež posilnila medzinárodnú spoluprácu v oblasti kybernetickej bezpečnosti. Vymieňala si informácie o kybernetických hrozbách a útokoch s medzinárodnými partnermi, čím získala cenné poznatky a podporu. Spolupracovala na spoločných cvičeniach a tréningoch zameraných na kybernetickú obranu, čo zlepšilo pripravenosť jej obranných síl. Okrem defenzívnych opatrení Ukrajina tiež vykonáva proaktívne kybernetické operácie proti ruským cieľom. Tieto operácie zahŕňajú narušenie ruských komunikačných sietí, zber spravodajských informácií a protiútoky na ruské kybernetické jednotky. Cieľom týchto operácií je nielen odraziť útoky, ale aj vytvoriť tlak na ruské operácie a znížiť ich schopnosť vykonávať ďalšie kybernetické útoky.

Rusko využilo aj právne a ekonomické nástroje na oslabenie Ukrajiny. Zavedenie sankcií proti ukrajinským firmám a jednotlivcom, ktorí podporovali odpor proti ruským silám, malo za cieľ ekonomicky oslabiť Ukrajinu. Zároveň Rusko prijalo opatrenia na legalizáciu svojich akcií na medzinárodnej scéne a ospravedlnenie invázie prostredníctvom medzinárodného práva.

Na okupovaných územiach sú používané tvrdé zásahy proti civilnému obyvateľstvu, vrátane zatýkania, výsluchov a násilia. Ruské bezpečnostné zložky sa zameriavajú na kľúčových ukrajinských aktivistov a lídrov odporu, čím sa snažia potlačiť akýkoľvek organizovaný odpor. Infiltrácia ukrajinských skupín odporu je tiež bežnou praxou, čo umožňuje získať informácie a efektívnejšie potlačiť povstanie.

29) JANKOWICZ, N.: *How To Lose the Information War : Russia, Fake News, and the Future of Conflict,* 2020.
30) GREENBERG, A.: *Sandworm : A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers,* 2019.

Rusko využívalo médiá a vzdelávacie systémy na propagáciu pro-ruských názorov a potlačenie ukrajinských národných identít na okupovaných územiach. Propaganda bola zameraná na zmenu verejnej mienky a podporu ruskej prítomnosti. Vzdelávacie programy boli upravené tak, aby podporovali ruskú kultúru a jazyk, čím sa snažili dlhodobo integrovať tieto regióny do ruskej sféry vplyvu.

Hybridná vojna na Ukrajine demonštruje, ako efektívne môžu byť kombinované rôzne taktiky na dosiahnutie strategických cieľov. Ruská stratégia zahŕňa širokú škálu nástrojov od vojenských operácií až po kybernetické útoky a dezinformačné kampane. Tento konflikt poukazuje na nebezpečenstvo a komplexnosť hybridnej vojny v modernom svete.

4.2 Hybridná Vojna v Hongkongu (2019 – 2020)

Príkladom z histórie je tiež hybridná vojna v Hongkongu, ktorá predstavuje súbor taktík použitých Čínou na potlačenie protestov a udržanie politickej kontroly nad regiónom. Tento konflikt zahŕňal kombináciu dezinformačných kampaní, kybernetických útokov, právnych a ekonomických nástrojov a obmedzených fyzických zásahov.

Hongkong, ako bývalá britská kolónia, sa vrátil pod čínsku správu v roku 1997 s prísľubom zachovania vysokej miery autonómie a občianskych práv na 50 rokov podľa princípu „jedna krajina, dva systémy". Avšak, od roku 2014 začali narastať obavy z erózie tejto autonómie, čo vyvrcholilo masovými protestmi v roku 2019 proti navrhovanému zákonu o extradícii, ktorý by umožňoval odosielanie obyvateľov Hongkongu na súdne konanie do Číny.

Čínska vláda využívala masívne dezinformačné kampane na sociálnych médiách, aby diskreditovala protestné hnutie v Hongkongu a prezentovala protesty ako násilné a riadené zahraničnými silami. Propagandistické články a príspevky na sociálnych sieťach boli šírené prostredníctvom trollov a botov, čo zvyšovalo dosah a účinnosť týchto dezinformačných kampaní. Hongkongskí aktivisti čelili častým kybernetickým útokom, vrátane hackingu ich osobných účtov a zariadení. Zaznamenané boli aj útoky na webové stránky a komunikačné platformy používané protestujúcimi, čo značne komplikovalo ich organizáciu a komunikáciu. [31])

Čína prijala zákon o národnej bezpečnosti, ktorý dával širšie právomoci na stíhanie disidentov a umožňoval kontrolu nad Hongkongom. Tento zákon bol využitý na potlačenie opozície a vytvorenie právneho rámca pre tvrdé zásahy proti protestujúcim. Okrem toho hongkongské spoločnosti a jednotlivci, ktorí podporovali protesty, čelili ekonomickému tlaku, vrátane odvetných opatrení zo strany čínskych úradov. Proti protestujúcim bola použitá aj sila, vrátane slzotvorného plynu, gumových projektilov a masového zatýkania. Čínske bezpečnostné zložky tiež infiltrujú protestné skupiny a zhromažďujú spravodajské informácie na zameranie kľúčových aktivistov, čo zvyšuje efektivitu represívnych opatrení. [32])

Čína taktiež využívala médiá a vzdelávacie systémy na propagáciu pro-čínskych názorov a potlačenie opozičných hlasov. Pro-čínske organizácie a iniciatívy v Hongkongu boli podporované na zvýšenie ich vplyvu a legitimity, čím sa posilňoval pro-čínsky sentiment medzi obyvateľmi Hongkongu. Tieto taktiky spoločne vytvorili komplexný a efektívny rámec hybridnej vojny, ktorým Čína dosiahla významné úspechy v udržaní kontroly nad Hongkongom.

31) MILANO, V.: *Chinese Disinformation Campaign Against the Hong Kong Protests*, 2019.
32) DAVIS, M. C.: *Making Hong Kong China...,* 2020.

5 ZÁVER

Hybridná vojna predstavuje komplexný a mnohovrstvový spôsob vedenia konfliktov, ktorý využíva kombináciu vojenských a nevojenských prostriedkov. Ako ukazuje tento článok, hybridná vojna môže zahŕňať široké spektrum taktík vrátane kybernetických útokov, dezinformačných kampaní, ekonomického tlaku, politickej destabilizácie a využívania neštátnych aktérov. Tento typ vojny sa vyznačuje vysokou mierou neprehľadnosti a často zahŕňa skryté operácie, ktoré môžu viesť k rýchlemu a neočakávanému zhoršeniu situácie.

Európske a americké ponímanie hybridnej vojny sa líši najmä v rozsahu a intenzite zapojenia vojenských prostriedkov. Zatiaľ čo európske prístupy kladú dôraz na politické, ekonomické a informačné aspekty, americká škola zdôrazňuje význam palebnej sily a vojenských operácií v hybridných konfliktoch.

Úspešná obrana proti hybridným hrozbám si vyžaduje koordinovanú a integrovanú stratégiu, ktorá zahŕňa technologicky pokročilé formy spravodajstva, informačné operácie, kybernetickú obranu a výcvik kvalifikovaného personálu. Významnú úlohu zohráva aj medzinárodná spolupráca a výmena informácií, čo zvyšuje schopnosť efektívne reagovať na hybridné útoky.

Ako ukazujú príklady hybridnej vojny na Ukrajine a v Hongkongu, moderné konflikty často prekračujú rámec tradičných vojenských operácií a zahŕňajú rôzne formy nátlaku a manipulácie. Tieto prípady zdôrazňujú potrebu neustálej inovácie a prispôsobenia obranných stratégií, aby sa efektívne čelilo novým výzvam hybridných hrozieb.

Na záver možno konštatovať, že hybridná vojna je dynamickým a komplexným javom, ktorý vyžaduje multidisciplinárny prístup a flexibilné stratégie na jeho zvládnutie. Efektívna reakcia na hybridné hrozby je kľúčová pre zachovanie národnej bezpečnosti a stability v súčasnom globálnom prostredí.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

BALDWIN, D. A.: *Economic statecraft : Uses of economic power in international relations.* New Jersey : Princeton University Press, 1985. 409 s. ISBN 978-0691078524.

BILAL, A.: Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. In: *NATO Review* [online]. 30. november 2021 [cit. 2024-06-20]. Dostupné na internete: <nato.int/docu/review/articles/2021/06/01/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html>.

Cultural Property : A Hybrid Threat Issue [online].CHAC, 2021 [cit.2024-06-20]. Dostupné na internete: <heritageconflict.org/blog/2021/3/8/cp-hybrid>.

Defense Advanced Research Projects Agency [online]. DARPA, 2024 [cit. 2024-06-20]. Dostupné na internete: <https://www.darpa.mil/>.

DANYK, Y. - MALIARCHUK, T. - BRIGGS, Ch.: Hybrid War : High-tech, Information and Cyber Conflicts. In: *Connections : The Quarterly Journal* [online]. 2023 [cit. 2024-06-20]. Dostupné na internete: <https://connections-qj.org/article/hybrid-war-high-tech-information-and-cyber-conflicts>.

DAVIS, M. C.: *Making Hong Kong China : The Rollback of Human Rights and the Rule of Law*. New York : Columbia University Press, 2020. 166 s. ISBN 9781952636141.

GERASIMOV, V. V.: *Cennosť nauky v predvidenii : Novyje vyzovy trebujut pereosmysliť formy i sposoby vedenija boevych dejstvij* [online]. 2013 [cit. 2024-06-20]. Dostupné na internete: <https://moodle.znu.edu.ua/mod/assign/view.php?id=269845>.

GLENN, R., W.: Thoughts on Hybrid Conflict. In: *Small Wars Journal* [online]. 3. 2. 2009 [cit. 2024-06-20]. Dostupné na internete: <https://www.smallwarsjournal.com/blog/188-glenn.pdf>.

GREENBERG, A.: *Sandworm : A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York : Knopf Doubleday Publishing Group, 2019, s. 150. ISBN 978-0385544405.

GROHMANN, J.: *Hybridní války podle Valerije Gerasimova* [online], AN, 2015 [cit. 2024-06-20]. Dostupné na internete: <http://www.armadninoviny.cz/hybridni-valky-podle-valerije-gerasimova.html>.

GRUMMAN, N.: *Survivability soars when the countermeasures are infrared and multispectral* [online]. Breaking Defense, 2023 [cit. 2024-06-20]. Dostupné na internete: <https://breakingdefense.com/2023/07/survivability-soars-when-the-countermeasures-are-infrared-and-multispectral/>.

HOENBY, A. S.: *Oxford Advanced Learner's Dictionary of Current English*. 3. vyd. Oxford : Oxford University Press, 1974, s. 425. ISBN 0-19-431445-6.

HOFFMAN, F. G: *Conflict in the 21st Century : The Rise of Hybrid Wars* [online]. Potomac Institute, 2007 [cit. 2024-06-20]. Dostupné na internete: <www.potomacinstitute.org/images/stories/publications/potomac_hybrid war_0108.pdf>.

HOFFMAN, F. G.: Hybrid vs. Compound War In: *Armed Forces Journal* [online]. 2009, october [cit. 2024-06-20]. Dostupné na internete: <http://www.armedforcesjournal.com/hybrid-vs-compound-war/>.

HOFFMAN, F. G.: Hybrid Warfare and Challenges. In: *Small Wars Journal* [online]. 2009, č. 52, s. 36. [cit. 2024-06-20]. Dostupné na internete: <smallwarsjournal.com/documents/jfqhoffman.pdf>.

HUGHES, H., C. - WAISMEL-MANOR, I.: The Macedonian fake news industry and the 2016 US election. In: *Political Science & Politics* [online]. 2021, roč. 54, č. 1, s. 19-23 [cit. 2024-06-20]. Dostupné na internete: <https://www.cambridge.org/core/journals/ps-political-science-and-politics/article/macedonian-fake-news-industry-and-the-2016-us-election/79F67A4F23148D230F120A3BD7E3384F>.

Hybrid warfare – Calha report NATO [online]. NATO Parliamentary Assembly, 2015 [cit. 202406-20]. Dostupné na internete: <https://www.nato-pa.int/document/2015-166-dsc-15-e-bishybrid-warfare-calha-report>.

Hybrid warfare : Legal arguments and justifications. In: *NATO StratCom Centre of Excellence Reports* [online]. 2020, roč. 34, č. 2, s. 56-60 [cit. 2024-06-20]. Dostupné na internete: <https://www.osce.org/files/f/documents/2/1/424451.pdf>.

JANKOWICZ, N.: *How To Lose the Information Wa r: Russia, Fake News, and the Future of Conflic*t. London : Bloomsbury/IBTauris, 2020. s. 113. ISBN 978-1838607685.

KILCULLEN, D.: *The Accidental Guerrilla : Fighting Small Wars in the Midst of a Big One.* 1. vyd. Oxford : Oxford University Press, 2009. 384 s. ISBN 9780199754090.

Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám [online]. Vláda SR, 2018 [cit.024-06-20]. Dostupné na internete: <https://rokovania.gov.sk/RVL/Material/23100/1>.

Kremlin hybrid war against Ukraine and EU : Energy Component [online]. SGS, 2014 [cit. 2024-06-20]. Dostupné na internete: <http://geostrategy.org.ua/en/analitika/item/585-/585->.

MILANO, V.: *Chinese Disinformation Campaign Against the Hong Kong Protests.* Homeland Security Digital Library, 2019, s. 135. ISBN 978-0-123456-78-9.

Misinformation and propaganda in hybrid conflicts. In: *OSCE Annual Report*, 2019, s. 22-27.

PLOKHY, S.: *The Russo-Ukrainian War : The Return of History*. Cambridge : Harvard University Press, 2023, s. 425. ISBN 1324051191

RENZ, B.- SMITH, H.: Russia and Hybrid Warfare – Going Beyond the Label. In: *Aleksanteri Papers*, 2016, č. 1. ISSN 1457-9251.

ROSÉN, F.: *Putin's Upper Hand : Cultural Domain Warfare* [online]. JIA, 2024 [cit. 2024-06-20]. Dostupné na internete: <https://jia.sipa.columbia.edu/news/putins-upper-hand-cultural-domain-warfare>.

SCHMID, J.: Introduction to Hybrid Warfare – A Framework for Comprehensive Analysis. In: THIELE, R. (ed.): *Hybrid Warfare : Future and Technologies* [online]. Wiesbaden : Springer VS Wiesbaden, 2021, s. 11-32 [cit. 2024-06-20]. Dostupné na internete: <https://doi.org/10.1007/978-3-658-35109-0>.

Spoločné oznámenie Európskemu parlamentu a rade : Spoločný rámec pre boj proti hybridným hrozbám – reakcia Európskej únie [online]. Európska komisia, 2016 [cit. 2024-06-20]. Dostupné na internete: <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52016JC0018&from=EN>.

THIELE, R. (ed.): *Hybrid Warfare : Future and Technologies*. Wiesbaden : Springer VS Wiesbaden, 2021. 230 s. ISBN 978-3-658-35109-0.

Základné informácie [online]. Centrum boja proti hybridným hrozbám [cit. 2024-06-20]. Dostupné na internete: <https://www.hybridnehrozby.sk/zakladne-informacie/>.

TÉMY NA VEDENIE ZÁVEREČNEJ DISKUSIE

1. Ako efektívne sú jednotlivé zložky hybridnej vojny (kybernetické útoky, dezinformačné kampane, ekonomický nátlak) v dosahovaní strategických cieľov? Ktoré z týchto metód sú najťažšie identifikovateľné a prečo?
2. Ako štáty využívajú spoluprácu s neštátnymi aktérmi (militantné skupiny, súkromné organizácie) na realizáciu hybridných operácií? Aké sú riziká a výhody tejto spolupráce?
3. Aké sú hlavné techniky a kanály používané na šírenie dezinformácií v rámci hybridnej vojny? Ako môžu cieľové krajiny efektívne bojovať proti dezinformačným kampaniam a chrániť svoju verejnosť pred ich vplyvom?
4. Akú úlohu hrajú moderné technológie (napr. umelá inteligencia, internet vecí) v identifikácii a reakcii na hybridné hrozby? Aké sú výzvy spojené s ich implementáciou v obrannej stratégii?
5. Aké právne a diplomatické opatrenia môžu štáty použiť na obranu proti hybridným hrozbám? Ako môžu medzinárodné organizácie ako OSN a NATO podporiť krajiny v ich boji proti hybridnej vojne?