

JEDAN PRISTUP U SUPROTSTAVLJANJU HIBRIDNIM PRETNJAMA

Miroslav Terzić¹ Miloš Živković² Ivan Orbović³

Резиме: Rad predstavlja jedan pristup suprotstavljanju hibridnim pretnjama izradom dva modela. U uvodnom delu rada opisano je shvatanje hibridnih pretnji od strane pojedinih autora i Evropske unije. Jedan model suprotstavljanja hibridnim pretnjama odnosi se na varijantu vertikalne de(escalacije) u kome se kombinuju različite strategije delovanja prema određenom subjektu. Drugi model suprotstavljanja hibridnim pretnjama odnosi se na varijantu horizontalne de(escalacije) gde se deluje unutar svake oblasti.

Ključne reči: hibridne pretnje, suprotstavljanje, modeli, varijante.

ONE APPROACH TO COUNTERING HYBRID THREATS

Abstract: The paper presents one approach to countering hybrid threats by creating two models. In the introductory part of the paper, the understanding of hybrid threats by individual authors and the European Union is described. One model of countering hybrid threats refers to a variant of vertical de(escalation) in which different strategies of action against a specific subject are combined. The second model of countering hybrid threats refers to a variant of horizontal de(escalation) where one acts within each area..

Key words: hybrid threats, countermeasures, models, variants.

1. UVOD

U prvoj deceniji XXI veka Džordž Fridman [1] je govorio o razvoju pete generacije ratovanja u kontekstu suprotstavljanja novim oblicima pretnji koje će doći iz Rusije i Kine. Prema dostupnoj literaturi prelazak sa četvrte na petu generaciju izgleda nejasno, s obzirom da se dogodio u kratkom vremenskom periodu. Peta generacija rata se bazira uglavnom na korišćenju tehnologije za širenje i odbranu vlastitih ideologija u informacionoj dimenziji operativnog okruženja.

Pri opisivanju hibridnih pretnji najčešće se citira general Valerij Vasiljevič Gerasimov, koji je 2013. godine u ruskom vojnom časopisu objavio članak pod naslovom „Vrednost nauke je u iščekivanju: novi izazovi zahtevaju preispitivanje oblika i metoda vođenja borbenih dejstava“ [2]. Hibridne pretnje se mogu identifikovati kod: primene nevojnih mera za oblikovanje javnog mnjenja, kreiranja krize, upravljanja krizom i rešavanja krize, a ako sukob eskalira i primenu vojne sile za rešavanje krize. Pored Gerasimova često se citira i Janis Berzins koji je hibridne pretnje opisao kao „kombinaciju asimetričnih i modernih oblika pretnji bezbednosti koja je usmerena ka manama neprijatelja, imajući u vidu da svaka država poseduje neke slabosti“ [3] i smatra ih nosiocem šeste generacije ratovanja.

Pojedini autori [4], [5] ističu da su nove tehnologije promenile način ratovanja, meka sila je zamenila tvrdu silu pa krajnje željeno stanje (npr. promena neodgovarajućih režima u pojedinim državama) je moguće dostići korišćenjem socijalnih mreža za tzv. „tviter revolucije“. Taktika je jednostavna: podsticanje političkih diskusija na socijalnim mrežama poput Tvitera, Fejsbuka, političke aktivnosti blogera, stavljanje video sadržaja sa sugestivnim porukama i sl. Ali i u ovom slučaju, rasuđivanja i procene moraju se razraditi ne u kategoričkim i apodikličnim dimenzijama, već posebno u relativnim, složenim i dinamičnim procenama.

Evropska unija ističe da hibridne pretnje utiču i iskorišćavaju ranjivosti da bi nanele štetu ispod praga otvorene agresije. Oni su mešavina prinudnih i subverzivnih aktivnosti, konvencionalnih i nekonvencionalnih metoda, korišćenih na koordinisan način u više domena. Takođe, navodi da

¹ Doktor vojnih nauka, Univerzitet odbrane, Škola nacionalne odbrane „Vojvoda Radomir Putnik“, terzicmiroslav@yahoo.com.

² Ministarstvo odbrane, Vojnoobaveštajna agencija, mornarzile@gmail.com.

³ Univerzitet odbrane, Škola nacionalne odbrane „Vojvoda Radomir Putnik“.

autoritarni režimi sve više pokušavaju da potkopaju zajedničke demokratske vrednosti EU i polariziraju naša društva za svoje potrebe koristeći različite vrste hibridnih aktivnosti, kao što su manipulacija informacijama, sajber napadi, zakon, ekonomska prinuda ili instrumentalizacija migranata [6].

Različite pretnje ugrožavaju bezbednost Republike Srbije tokom čitave njene istorije i predstavljaju prepreku za ostvarivanje nacionalnih interesa. Te pretnje razlikovale su se po svom obliku, prirodi i karakteristikama, u zavisnosti od projektovanih ciljeva neprijatelja. Na osnovu karaktera pretnji koje su ugrožavale bezbednost Republike Srbije može se zaključiti da su mnoge od njih bile i hibridnog karaktera.

Republika Srbija svoju odbranu zasniva na totalnoj odbrani, vojnoj neutralnosti i odvracanju. Savremene koncepcije i ideje o borbi protiv hibridnih pretnji uglavnom, pored razvoja sposobnosti, nalaze uporište u teoriji odvracanja i na kraju, delovanjem (pružanjem odgovora) na hibridno delovanje.

2. MODELI SUPROTSTAVLJANJA HIBRIDNIM PRETNJAMA

Hibridne pretnje je teško sprečiti samo odvracanjem iz više razloga. U globalno povezanom, multipolarnom bezbednosnom okruženju, tehnološki razvoj je doprineo da instrumenti nasilja dobiju različite oblike, kojima odvracanje nije dovoljno da bi se suzbio njihov ofanzivni karakter. Neki autori ukazuju da manipulacija strahom u različitim domenima može samo delimično da se suzbije delovanjem na polju bezbednosti. Razumevanje uloge psihologije i percepcije je napredovalo do tog stepena da je neophodno proširiti okvir koji definiše strategije odvracanja, u koje je pre svega potrebno uključiti ubeđivanje neprijatelja. Ovakav zaključak nas vraća ka tradicionalnoj vojnoj misli koja odvracanje definiše kao „proces uticanja na neprijateljske namere, bez obzira na okolnosti, nasilne ili nenasilne“ [7].

Na osnovu gore navedenog, jedan od modela za suprotstavljanje hibridnim pretnjama, koji je moguće primeniti u praksi, kombinuje pun konceptualni opseg strategija u dve varijante, po vertikalnoj i horizontalnoj osi, koje se primenjuju u odgovoru na hibridne pretnje [8].

2.1. Varijanta vertikalne (de)eskalacije za suprotstavljanje hibridnim pretnjama

Vertikalna osa se u navedenoj varijanti sastoji od pet opštih strategija: saradnja, ubeđivanje, zaštita, prinuda i kontrola koje su prikazane u tabeli 1. Navedenih pet strategija se oslanjaju na primenu „štapa ili šargarepe“ kako bi uticale na ponašanje druge strane, kao što je objašnjeno u nastavku.

Tabela 1 – Strategijski okvir za suzbijanje hibridnih pretnji

Strategija	Opis
Saradnja	Težnja ka uzajamno korisnim politikama radi ostvarenja obostrane dobiti i za izvor i za cilj.
Ubeđivanje	Korišćenje nagrada radi postizanja saradljivosti cilja.
Zaštita	Povećanje sposobnosti izvora da izdrži ili apsorbuje neprijateljske mere.
Prinuda	Upotreba pretnji da bi se sprečilo ili promenilo ponašanje cilja.
Kontrola	Upotreba sile za ograničavanje slobode delovanja cilja.

Saradnja, kao što je prikazano u tabeli 1, je težnja ka uzajamno korisnim politikama kako bi se povećali obostrani dobici i za izvor i za cilj kroz preplitanje, pomirenje i sporazumevanje. Preplitanje podrazumeva stvaranje uzajamnih zavisnosti, obično ekonomske ili logističke, čiji bi prekid recipročno naneo štetu za oba aktera i na taj način obeshrabrio akcije koje bi vodile ka destabilizaciji. Pomirenje se odnosi na uklanjanje ključnih prepreka za postizanje sporazuma, bez pristajanja na veći deo zahteva druge strane. Ovaj način pregovaranja zahteva win-win rešenje, a ne pregovaranje po principu „dobitnik-gubitnik“ ili „pobednik ne gubi ništa“. Sporazumevanje podrazumeva manje ustupke sa jedne strane (iako mogu biti predloženi kao suštinski ustupci cilju) da bi se postigao dogovor. Ključ saradnjeje obostrano poverenje. U odsustvu istog, druga strana može iskoristiti strategiju saradnje za postizanje sopstvenih ciljeva ili se vratiti konfrontacionom pregovaranju. Saradnja može

poboljšati strategije ubeđivanje i zaštite. Može se kombinovati sa prinudom, a malo je verovatno da će funkcionisati uporedo sa kontrolom.

Ubeđivanje koristi nagrade za postizanje saradnje sa ciljem, kao alternativu za nastavak sukoba. Ono zahteva dobru volju od strane cilja i na taj način obezbeđuje primirje ili prekid eskalacije nasilja, kao i efikasnu komunikaciju u svrhu pravdanja kapitulacije ili gubitaka legitimiteta cilja. Uspešno ubeđivanje dovodi do scenarija ostvarenja pobeđe. Materijalni oblici ubeđivanja uključuju ekonomske podsticaje ili druge opipljive nagrade. Nematerijalne forme uključuju status, prestiž, dobre odnose ili kredibilne garancije o bezbednosti druge strane u sukobu. Ubeđivanje se može kombinovati sa nekim od oblika prinude ili prinude na saradnju. Ubeđivanje ne funkcioniše dobro uz strategiju kontrole, jer gubi značajan deo kredibiliteta zato što se u akciju uvodi jednostrano nasilje.

Zaštita ima za cilj povećanje sposobnosti izvora da izdrži ili apsorbira neprijateljske mere i obično rezultira scenarijom „pobeda-gubitak“. Dva osnovna oblika zaštite su elastičnost i odbrana. Funkcija odbrane je da osujeti napade, dok je funkcija elastičnosti je da ublaži njegove posledice. I elastičnost i odbrana se mogu sprovoditi u svim oblastima. Njihova osnovna svrha je odgovor na aktivnosti neprijatelja. Ukoliko su jaki, odbrana i elastičnost mogu pomoći u odvrćanju cilja da izvodi neprijateljske akcije jer iste ne mogu doneti očekivanu korist. Ova osobina daje zaštitnim strategijama potencijal da unaprede metode odvrćanja. Iz navedenih razloga, oba oblika zaštite moraju se stalno unapređivati kako bi se održao korak sa modernim pretnjama.

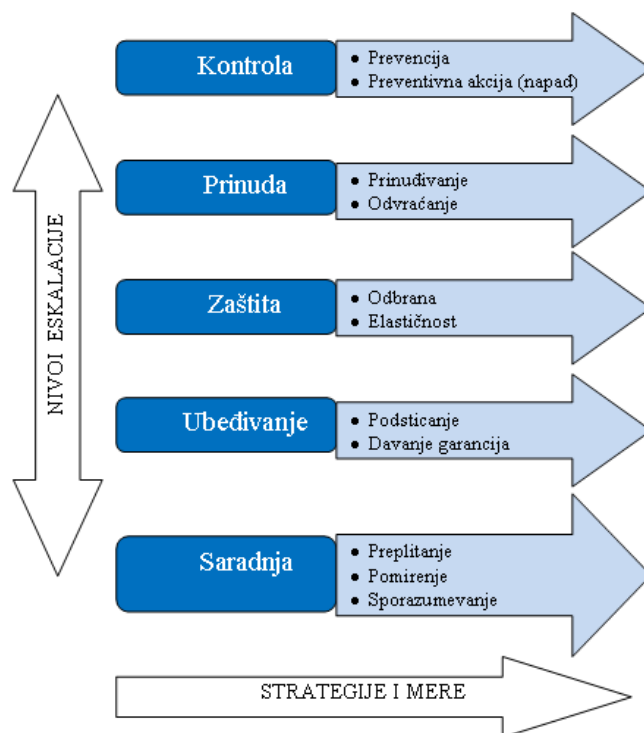
Prinuda, za razliku od strategija saradnje i ubeđivanja, koje su usmerene na nagradu, ubeđuje protivnika, ali negativnim sredstvima. Ona primorava drugog aktera u sukobu da preduzme akciju koju ne želi da učini putem odvrćanja. Podrazumeva upotrebu pretnji da se odvrati cilj od preduzimanja određene akcije, kao i ubeđivanje cilja da preduzme određenu akciju. Uspešna prinuda obično rezultira scenarijom „pobeda-poraz“. Primeri prinude obuhvataju: režim sankcija, bilateralnu diplomatiju i korišćenje sajber i hibridnih alata, pri čemu je upotreba vojne prinude poslednjih decenija značajno smanjena. Strategije prinude se mogu sprovoditi putem izlaganja negativnoj medijskoj kampanji ili stigmatizaciji. Za razliku od zaštitnih strategija, strategije prinude ciljaju direktno određenog protivnika sa tačno određenim ciljem. Isto uzrokuje da pretnje treba da budu prilagođene karakteru cilja i nameravanoj promeni njegovog ponašanja. Stoga, sprovođenje prinude treba da bude ukorenjeno u jasnom razumevanju nečije ranjivosti, kao i detaljanom razumevanju željene promene ponašanja koju neko želi da izazove. Ukoliko isto izostane prinuda može dovesti do nepotrebne provokacije i eskalacije sukoba.

Kontrola se odnosi na upotrebu sile za ograničavanje slobode delovanja cilja. Uspešna kontrola obično dovodi do scenarija „pobeda-poraz“. Strategije kontrole podrazumevaju prevenciju. Kontrola koristi aktivne mere koje umanjuju sposobnost cilja da predstavlja neposrednu pretnju, kao i nasilnu eliminaciju neposredne pretnje. Najveći rizik kontrole je potencijal da poveća, a ne da smanji spremnost cilja da primeni neprijateljske mere u odgovoru na napad. Drugim rečima, kontrola može da izazove napade uprkos nameri da se isti spreče.

Navedenih pet strategija se mogu primenjivati istovremeno ili uzastopno. U oba načina, strategije treba pažljivo odabrati, kako bi se međusobno ispravili nedostaci svake i poboljšala njihova upotrebljivost. Neke strategije, kao što su saradnja i zaštita, uvek pojačavaju potencijal jedna drugoj. Druge strategije, kao što su kontrola i ubeđivanje, potkopavaju jedna drugu, ako se koriste istovremeno. Sve strategije sadrže ograničenja i rizik od neuspeha i nijedna pojedinačna ne može predstavljati univerzalan model za borbu protiv hibridnih pretnji.

Na slici 1. prikazano je pet strategija na skali eskalacije, od najnižeg do najvišeg nivoa. Eskalacija se odnosi na povećanje intenziteta ili obima sukoba, koji se smatraju značajnim za jednog ili više učesnika. Skala eskalacije predstavlja upravljanje krizom tokom kog akteri preduzimaju korake radi regulisanja intenziteta sukoba, kroz eskalaciju, deeskalaciju, ili kroz kombinaciju ova dva putem različitih kanala komunikacije sa neprijateljem (protivnikom).

18. KONFERENCIJA SA MEĐUNARODNIM UČEŠĆEM RIZIK I BEZBEDNOSNI INŽENJERING

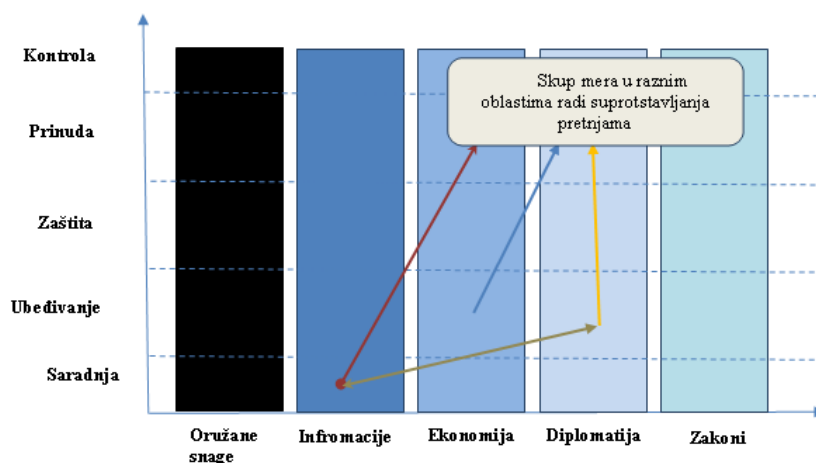


Slika 1 – Lestvica strategija i nivoa eskalacije [9]

Sve strategije se mogu koristiti i za eskalaciju i za deeskalaciju, osim saradnje koja po definiciji vodi do deeskalacije. Sa tim u vezi, strategije treba pažljivo koristiti za povećanje međusobnog (de)eskalacionog potencijala, a ne njegovog umanjivanja. Ako neko teži eskalaciji, onda nema smisla koristiti saradnju uz prinudu ili obrnuto.

2.2. Varijanta horizontalne de(eskalacije) za suprotstavljanje hibridnim pretnjama

Pored varijante vertikalne (de)eskalacije, postoji i koja je prikazana na slici 2. Za njenu svrhu, koristi se *DIMEL*⁴ kategorizacija instrumenta i mera koje preduzimaju državni organi.



Slika 2 – Eskalacija po unakrsnim poljima

⁴ DIMEL - Diplomatic, Information, Military, Economic and Legal (diplomacija, informacije, oružane snage, ekonomija i zakon)

18. KONFERENCIJA SA MEĐUNARODNIM UČEŠĆEM RIZIK I BEZBEDNOSNI INŽENJERING

Vertikalne mere podrazumevaju eskalacije unutar istog polja delovanja. Na primer, ako je vrsta neprijateljske mere sajber špijunaža, vertikalno eskalirajući odgovor može uključivati akte sajber sabotaže usmerene prema neprijatelju. Za razliku od vertikalne varijante, horizontalna eskalacija se odnosi na ulaganje napora izvan jedne DIMEL oblasti na druge oblasti (polja). Na primer, diplomatske i ekonomske sankcije mogu biti upotrebljene kao odgovor na vojnu agresiju, kao što su „zapadne države“ reagovala posle aneksija Krima od strane Ruske Federacije. Horizontalna eskalacija može se preduzimati u okviru vojnih mera i aktivnosti. Izrael je, na primer, koristio vazdušne napade protiv Hamasa u proleće 2019. godine u znak odmazde za seriju sajber napada, koristeći vojnu protivmeru kao odgovor na sajber pretnju bezbednosti.

U hibridnim sukobima, akteri ne deluju samo između različitih polja, već kombinuju različite instrumente moći prilagođavajući nivo intenziteta po oblastima. Čineći to, hibridni akteri se obično kreću gore-dole po lestvici eskalacije što stvara „sivu zonu“ između rata i mira, pri čemu se izbegava prelazak granice ili praga koji bi mogao dovesti do otvorenog (vojnog) sukoba. Ponekad je cilj brzo postizanje vojnih i političkih uspeha, dovodenjem do svršenog čina –ishod je već ostvaren i verovatno nepovratan – pre nego što bi ga savezničko odvrtaćanje ili dodatne mere mogle sprečiti. Suštinska dvosmislenost „hibridne“ upotrebe mera suprotstavljanja može izazvati (opasnu) divergenciju u percepciji između izvora i cilja, što predstavlja eskalacioni ili deeskalacioni korak.

U principu, nivo eskalacije sa slike 1. je izvoran u smislu da može biti primenjen na sve DIMEL oblasti (polja). Međutim, različiti nivoi se prilično razlikuju za različita polja i mogu biti primenljiviji u nekim kombinacijama nego u drugim. Suštinski, određena akcija niskog nivoa u jednom polju može imati veći uticaj od akcije visokog nivoa na drugom polju. Premeštajući se sa jednog DIMEL polja na drugo, prelazi se na (horizontalni) korak eskalacije od strane cilja, čak i ako inicijator nije nameravao da eskalira. Drugim rečima, nivoi eskalacije nemaju apsolutnu vrednost za različite instrumente moći i uticaja.⁵

3. ZAKLJUČAK

Suprotstavljanje hibridnim pretnjama predstavlja jedan veoma složen proces za čiju uspešnu realizaciju je od velikog značaja jasno (decidno, precizno) određenje (definisanje) hibridne pretnje ili izazova koji se može razviti u pretnju kao i pravovremena identifikacija hibridnih pretnji.

Nakon jasnog određenja i blagovremene identifikacije hibridnih pretnji primenjuju se određene mere, radnje i postupci za njihovo suzbijanje odnosno za suprotstavljanje hibridnim pretnjama. Primena mera zavisi od karaktera hibridne pretnje prema određenom subjektu, i od sposobnosti subjekta da se suprotstavi identifikovanim hibridnim pretnjama.

Kombinovanjem određenih mera za identifikaciju hibridnih pretnji kao i mera na njihovom suprotstavljanju, moguće je doći do određenih modela za suprotstavljanje hibridnim pretnjama.

Vertikalni model za suzbijanje (deeskalaciju) hibridnih pretnji podrazumeva primenu pet opštih strategija: saradnju, ubeđivanje, zaštitu, prinudu i kontrolu. Kod ovog modela je veoma važno pažljivo korišćenje strategija za povećanje međusobnog deeskalacionog potencijala.

Horizontalni model za suzbijanje (deeskalaciju) hibridnih pretnji podrazumeva primenu mera i aktivnosti unutar istog polja delovanja (vojna komponenta, informaciona komponenta, diplomatska komponenta i sl).

Predloženi model suprotstavljanja hibridnim pretnjama primenom pet opštih strategija: saradnja, ubeđivanje, zaštita, prinuda i kontrola, koje se sprovode kroz diplomatske aktivnosti, kontrolu informacija, oružane snage, ekonomske resurse i vladavinu zakona, moguće je primeniti i na Republiku Srbiju, uz uvažavanje specifičnosti međunarodne pozicije, operativnog okruženja, politike vojne neutralnosti i strategije totalne odbrane. Ovakav pristup je sprovodljiv jedino uz prethodno navedenu potrebu razvoja sposobnosti i jačanja kapaciteta za pravovremenu i stručnu identifikaciju indikatora hibridnih pretnji.

⁵ Bazirano na Multinacionalnoj kampanji za razvoj kapaciteta za suprotstavljanje hibridnom ratu.

4. LITERATURA

- [1] Friedman, G.: *ROA National Security Report*, The Officer, 2007., стр. 56. https://wikileaks.org/gifiles/attach/27/27445_nsr-sept07.pdf, pristupljeno: 01.05.2022.
- [2] Gerasimov, V.: Vrednost nauke je u predviđanju: Novi izazovi zahtevaju preispitivanje oblika i metoda izvođenja borbenih dejstava, 2013. *Voyenno-Promyshlenny y Kurier (VPK) (Military-Industrial Courier)*. http://vpknews.ru/sites/default/files/pdf/VPK_08_476.pdf, pristupljeno: 28.04.2022.
- [3] Berzins, J, Aspen Review: *The New Generation of Russian Warfare*, Aspen Institute Prague, 3/2014. <http://www.aspeninstitute.cz/en/article/3-2014-the-new-generation-of-russian-warfare>, pristupljeno: 11.05.2022.
- [4] Terzić, M.; Miladinović, M.; Coković, S.: Hibridno ratovanje – konceptualna adaptacija, *Vojno delo broj 7*, Medija centar „Obrana“, Beograd, 2017. str. 348. – 357.
- [5] Saković, R.; Terzić, M.: Upotreba društvenih mreža u hibridnom ratovanju, *Vojno delo broj 1*, Medija centar „Obrana“, Beograd, 2018. str. 318. – 334.
- [6] European Commission / High Representative of the Union for Foreign Affairs and Security Policy, “Joint Communication establishing a Joint Framework on Countering Hybrid Threats”, JOIN(2017) 18 final, Brussels, April 6, 2016.
- [7] Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security*., First Edition, University Press, Princeton, 1961.
- [8] King Mallory, *New Challenges in Cross-Domain Deterrence*, (Santa Monica: RAND Corporation, 2018), <https://www.rand.org/pubs/perspectives/PE259.html>, pristupljeno 30.05.2022.
- [9] The visual is an adaptation and extension of the visual developed by King Mallory, King Mallory, „New Challenges in Cross-Domain Deterrence“, Santa Monica: RAND Corporation, 2018, <https://www.rand.org/pubs/perspectives/PE259.html>, pristupljeno: 28.05.2022.