David Stonič
DOI:10.33179/BSV.99.SVI.11.CMC.20.4.5

PREDSTAVITEV MODELA ZA PREPOZNAVANJE HIBRIDNIH GROŽENJ

INTRODUCING A HYBRID-THREAT IDENTIFICATION MODEL

Povzetek V spremenjenem varnostnem okolju moramo razviti ustrezne koncepte in orodja za pravočasno prepoznavanje in opredelitev hibridnih groženj, da bi se lahko uspešno odzvali.

Oblikovali smo model, ki grožnje poveže z akterjem. Ovrednoteni obveščevalni podatki so vstopne informacije v izdelan model za ocenjevanje hibridne ogroženosti nacionalne varnosti. Izhodna informacija je identificirana hibridna grožnja.

Ob izpolnitvi pogoja hibridne ogroženosti lahko nacionalnovarnostni sistem začne izvajati ukrepe, ki bi zmanjšali zmožnosti delovanja hibridnega akterja. Zavedanje o obstoju hibridnih groženj in njihovo identificiranje bo spodbudilo odločevalce v nacionalnovarnostnem sistemu, da bodo zagotovili ustrezno hibridno odpornost države, saj je primarna odgovornost za spoprijemanje s hibridnimi grožnjami predvsem odgovornost države. Nujen je celostni vladni pristop v povezavi z Evropsko unijo in Severnoatlantskim zavezništvom.

Ključne besede ***Hibridne grožnje, indikatorji konvencionalnega ogrožanja, indikatorji nekonvencionalnega ogrožanja.***

Abstract In order to ensure a successful response in a changed security environment, we have to be able to develop appropriate concepts and tools for timely identification and definition of hybrid threats.

We have developed a model, which relates threats with actors. The evaluated intelligence then serves as input information for the national security hybrid threat evaluation model. The output information is an identified hybrid threat.

When a hybrid threat is identified, the national security system can take adequate measures to hinder the operational ability of hybrid actors. The awareness of hybrid threats and their identification will encourage decision makers in the national security system to ensure adequate hybrid resilience of the country, since countering hybrid threats is a state's primary responsibility, which requires a comprehensive governmental approach in cooperation with the European Union and the North Atlantic Alliance.

Key words ***Hybrid threats, conventional threat indicators, unconventional threat indicators.***

Uvod

Rdeča nit članka so hibridne grožnje. Namen članka je predstaviti model za prepoznavanje hibridnih grožen, ki ga je avtor uspešno testiral na primeru Slovenije. Osnova modela so identificirani indikatorji konvencionalnega in nekonvencionalnega ogrožanja.

Visoka predstavnica Evropske unije (EU) za zunanje zadeve in varnostno politiko je 6. aprila 2016 izdala skupno sporočilo Evropskemu parlamentu in Svetu (Skupni okvir o preprečevanju hibridnih groženj – odziv Evropske unije, 2016, str. 3), v katerem je med drugim navedeno, da je cilj hibridnih groženj izkoristiti ranljivosti države in pogosto tudi spodkopati temeljne demokratične vrednote in svoboščine.

Bistvo članka je, da sledimo skupnemu sporočilu. Predvsem v ukrepu št. 1, ki ga je izdala visoka predstavnica, da države članice, po potrebi ob podpori Komisije in visoke predstavnice, začnejo pripravljati raziskavo o hibridnih grožnjah za opredelitev pomembnih ranljivosti, vključno s posebnimi kazalniki, povezanimi s hibridnimi grožnjami, ki lahko potencialno vplivajo na nacionalne in vseevropske strukture in mreže (Skupni okvir o preprečevanju hibridnih groženj – odziv Evropske unije, 2016, str. 3─4).

V obdobju po drugi svetovni vojni, imenovanem hladna vojna, se je svet srečeval s stalno napetostjo zaradi možnosti izbruha nove konvencionalne vojne, ki bi po vseh projekcijah vodila v za človeštvo uničujoč jedrski spopad dveh vojaško političnih polov. V obdobju hladne vojne, ki se je končala s padcem berlinskega zidu, je kljub stalni prisotnosti možnega izbruha konvencionalne jedrske vojne potekalo več konfliktov. Svete navaja, da tretjino teh konfliktov lahko označimo kot tradicionalne, simetrične meddržavne vojne. Preostalo so bile notranje vojne, ki so bile po svoji naravi večinoma asimetrične, čeprav lahko mnoge spopade umestimo med posredniške oziroma tako imenovane proxy vojne. Za druge konflikte je značilna asimetričnost z gverilskim uporništvom, to so kartelni spopadi in vojne ter tudi mednarodni terorizem (Svete 2016, str. 99). Način končanja obdobja stalnih konvencionalnih groženj in s tem hladne vojne se kaže v tako imenovani veliki strategiji ZDA ali Reaganovi veliki strategiji, ki vsebuje konvencionalno grožnjo odvračanja, ki je bila le nastavek za poznejše asimetrične prijeme in propad Sovjetske zveze ter Varšavskega pakta.

Razpad Varšavskega pakta in s tem bipolarnosti je pripeljal do sprostitve nakopičenega konvencionalnega orožja, kar je v novonastalih državah povečalo možnost groženj. Namesto do takrat značilnega asimetričnega jedrsko konvencionalnega (ne) ravnotežja, v katerem je Nato številčno podrejenost v konvencionalnem orožju nadomeščal z jedrsko premočjo in konceptom zračno-kopenske bitke, taktičnim jedrskim orožjem in samovodljivimi izstrelki, sta se strani sporazumno odločili za simetrično konvencionalno ravnotežje v okviru podpisa prvega sporazuma CFE TLE (Conventional Forces in Europe Treaty Limited Equipment).

Vendar je tako dosežena stabilnost, ki je temeljila na simetričnem ravnotežju konvencionalnih sil, postala nezanesljiva že leta 1998, ko so Poljska, Češka in Madžarska, ki so bile prej kot članice budimpeške skupine sporazuma CFE TLE vključene v seštevek z Rusko federacijo, postale članice Nata (Žabkar, 2003, str. 323).

1 UMESTITEV HIBRIDNEGA VOJSKOVANJA

Izraz hibrid se že dolgo uporablja na različnih področjih življenja, tako v kmetijstvu, avtomobilizmu idr. Vsekakor je hibrid nekaj, kar ni nastalo samo od sebe s pomočjo narave, ampak je spremenjeno s pomočjo človeka in moderne tehnologije. Svete hibridno vojskovanje predstavi kot kombinacijo različnih konvencionalnih in nekonvencionalnih oblik/orodij vojskovanja (Svete, 2016, str. 103). Škerbinc hibridno vojskovanje povezuje s sinergijskimi učinki materialnih in kognitivnih zmogljivosti ter prikrito ali odkrito agresijo z neupoštevanjem legalnih omejitev ob simultani izrabi prvin mednarodne moči za vsiljevanje lastnih strateških mednarodno nelegitimnih ciljev (Škerbinc, 2015, str. 26).

Članek Spreminjajoča se podoba vojne, ki ga je objavil William S. Lind (Lind in drugi, 1989), izpostavi štiri generacije vojne moderne zgodovine. Za četrto pravi, da je vojna, ki vključuje celotno družbo. Hibridna vojna je tako lahko peta generacija vojskovanja. Čeprav se je koncept hibridne vojne uporabljal že davno, ga je prvič zapisal leta 2006 polkovnik ameriške vojske Frank Hoffman.

Eno od pomembnih dejstev v članku bo opredelitev novih groženj, ki so predvsem povezane z razvojem novih tehnologij in vse večjo družbeno celovitostjo. Ne smemo tudi mimo dejstva, da nekatere grožnje, ki jih lahko uvrstimo med nekonvencionalne, obstajajo že dolgo časa, vendar jih nismo zaznavali.

Malešič in Žabkar navajata Rentza in Smitha, ko ugotavljata, da se hkrati s hibridnimi zasnovami uporabljajo tudi druge zasnove, »nove vojne, vojskovanje četrte generacije in asimetrično bojevanje«. Četrta generacija vojskovanja v povezavi z visoko tehnologijo naj bi bilo vojskovanje šeste generacije (Malešič in Žabkar, 2016, str. 28). V citiranem besedilu avtorja ne omenita pete generacije vojskovanja. Omenili smo že, da bi hibridno vojskovanje lahko bilo peta generacija vojskovanja, kar omenjeno besedilo posredno nakazuje. Ko raziskujemo definicije šeste generacije vojskovanja, naletimo na blog Raya Aldermana (2015), ki zapiše,

da je šesta generacija vojskovanja tista, ki lahko vpliva na sofisticirano tehnologijo, da deluje neodvisno od prostora in časa. Cigler navaja, da je šesta generacija vojskovanja stanje, ko vojna ni več nadaljevanje politike z nasilnimi sredstvi za zagotavljanje končne zmage, temveč je začetek politike za zagotovitev končnih ciljev z nevojaškimi sredstvi (Cigler, 2016, str. 85).

Ugotavljamo, da je na konceptualnem področju, ki se ukvarja s hibridnim vidikom varnosti, še precej nedorečenosti. Pogled na to s stališča javnosti (laične) pa je lahko še bolj nejasen.

Prezelj je raziskal vojaške razsežnosti ogrožanja nacionalne varnosti. Identificiral je štirinajst temeljnih indikatorjev konvencionalnega ogrožanja, ki nam bodo smernica tudi pri določevanju indikatorjev nekonvencionalnega ogrožanja (Prezelj in drugi, 2007, str. 182).

1.1 Konvencionalne grožnje

Konvencionalne grožnje izhajajo predvsem iz oboroženih formacij neke države ali organizacije, orožja, ki ga uporabljajo, in stopnje tehnološke razvitosti tega orožja. Prezelj navaja Clausewitza, ki ugotavlja, da je vojna učinkovito politično orodje in povsem logično nadaljevanje političnih odnosov z drugimi sredstvi. Vendar pa danes Ustanovna listina Organizacije Združenih Narodov (OZN) ne prepoveduje samo vojne, temveč tudi vsako grožnjo ali uporabo sile proti ozemeljski nedotakljivosti in politični neodvisnosti katerekoli države (Prezelj in drugi, 2007, str. 167). Na podlagi tega je vsaka vojna modernega časa za napadalca nelegalna.

Prezelj zapiše definicijo, da vojaško ogrožanje nacionalne varnosti temelji na grožnjah z uporabo vojaških ali paravojaških oboroženih sil ali z njihovo dejansko uporabo (Prezelj in drugi, 2007, str. 170). Bistveno pri tem je, da gre za grožnjo z uporabo ali dejansko uporabo orožja vojaških ali paravojaških institucij ali oseb. Grozi lahko država (oziroma pripadajoča vojaška ali paravojaška oborožena sila) ali militantna nedržavna organizacija.

1.1.1 Indikatorji konvencionalnih groženj

Zelo pomemben dejavnik pri razumevanju ogrožanj in njihove povezanosti pri ugotavljanju hibridnosti so indikatorji konvencionalnih groženj, ki nam osvetlijo snov, ki jo preučujemo. Predstavljeni indikatorji (povzeto po Prezelj in drugi, 2007, str. 182) nam nakazujejo močno povezanost z nekonvencionalnimi grožnjami, ki jih bomo obdelali pozneje. Temeljni indikatorji so:

- demonstracija vojaške sile oziroma moči, kar vključuje parade, premike enot, koncentracijo ali grupiranje sil,
- sklepanje ofenzivnih vojaških zavezništev,
- nespoštovanje mednarodnih varnostnih pogodb,
- povečana sovražna vojaška dejavnost, ki vključuje vojaške vaje, vojaške aktivnosti v obmejnem pasu oziroma koncentracijo vojaških enot, vojaške kršitve meje na

kopnem, zraku in morju ─ obmejni incidenti, povečana vojaška obveščevalna dejavnost,
- sovražne izjave visokih predstavnikov držav z implicitno vojaško grožnjo (vključno s komentarji novinarjev in akademikov),
- informacijska oziroma psihološka vojna,
- povečano oboroževanje (nakupi orožja, proizvodnja, kar se še posebej nanaša na število kosov orožja in vrsto, pri čemer je poudarek na ofenzivnem orožju),
- povečanje obrambnih izdatkov oziroma proračuna,
- povečanje strateških rezerv (za potrebe varnostnih sil),
- mobilizacija vojske (delna, popolna),
- prekinitev meddržavnega sodelovanja,
- širjenje vojaškoindustrijskega kompleksa (vključuje tudi vlaganje sredstev v proizvodne zmogljivosti za orožje za množično uničevanje),
- operativna podpora sovražnih skupin znotraj države,
- vojaška agresija z omejenim ali radikalnim ciljem (tudi na sporna področja).

Pri omenjenih indikatorjih izstopa informacijska (psihološka) vojna, ki po našem mnenju ne spada v indikatorje konvencionalnih groženj. Prezelj (in drugi 2007) navede, da je bilo tovrstno ogrožanje zaznano pred izvedbo ogrožajočih vojaških operativnih ukrepov, med njimi in po njih pri pregledu preteklih mednarodnih konfliktov. S tem se lahko strinjamo, vendar bomo ta indikator v njegovi izvirni obliki uvrstili med indikatorje nekonvencionalnega ogrožanja.

1.2 Nekonvencionalne grožnje

Nekonvencionalen navadno pomeni biti zunaj običajnega oziroma zunaj zavez in konvencij. Da grožnji pripišemo nekonvencionalnost, mora izpolniti pogoje redkosti, nerazširjenosti in biti v nasprotju s prevladujočimi družbenimi pravili in normami. Nekonvencionalno lahko postane konvencionalno, ko se spremenijo okvirni pogoji (Eikenberry, 2014, str. 1).

Ameriško ministrstvo za obrambo je leta 2014 naredilo pregled obrambnih zmogljivosti (Defense Review-QDR). V poročilu je razširilo kategorije nekonvencionalnih groženj v prihodnjem varnostnem okolju. Med nekonvencionalne grožnje je uvrstilo teroristične organizacije, kriminalna omrežja (predvsem trgovanje z narkotiki), piratstvo, orožje za množično uničevanje in uporabo smrtonosnih bioloških sredstev. Poleg tega je QDR opredelil različne multiplicirane grožnje, kot so negativni vpliv podnebnih sprememb, nadzor nad izkoriščanjem naravnih virov, vladni nadzor nad urbanizacijo, širjenje naprednih tehnologij in ranljivost vojske ter gospodarstva ZDA na področjih, kot sta vesolje in kibernetski prostor.

Nekonvencionalne grožnje bomo obravnavali skozi prizmo asimetričnosti. Za asimetrične grožnje bomo ugotovili, da je novost večinoma v poimenovanju »asimetrije«, narava groženj pa seže daleč nazaj v zgodovino.

Liang in Xiangusi sta že leta 1999 zapisala v poglavju Vojaško, transvojaško in nevojaško, da lahko različne tipe in metode operacij kombiniramo, da dobimo povsem novo metodo operacije (Liang in Xiangusi, 1999, str. 123).

Pri obravnavanju asimetričnih groženj se pri teoretskem preučevanju pri mnogih avtorjih pojem začne pojavljati hkrati s hibridnimi grožnjami in asimetrično vojskovanje s hibridnim. Tu bo treba narediti ločnico in predvsem pojem hibridna grožnja ločiti od pojma hibridno vojskovanje.

Osredotočili se bomo tudi na novejše grožnje. Kibernetske grožnje lahko uvrstimo med nekonvencionalne asimetrične grožnje. Glede na Eikenberryjevo definicijo nekonvencionalnosti se prav kibernetske grožnje spogledujejo s konvencionalnostjo. Ko bomo preučevali hibridne grožnje in hibridno vojskovanje, bomo ugotovili, da je informacijsko-komunikacijska tehnologija (IKT) pomembnejši subjekt pri obravnavi hibridnega ogrožanja, saj je lahko osnovno orodje za prenašanje hibridnih groženj, orožje za kibernetsko napadanje in na drugi strani tudi pomembni obrambni steber za odvračanje ne le kibernetskih, temveč tudi drugih ogrožanj, ki jih združujemo v hibridne. Vsekakor je IKT predvsem pomembna za prepoznavanje indikatorjev celotnega spektra hibridnega ogrožanja, ki ga raziskujemo.

1.2.1 Indikatorji nekonvencionalnih groženj

Asimetričnost navadno obsega taktike in strategije nekonvencionalnega vojskovanja, šibkejši nasprotnik pa poskuša z uporabo določene strategije zmanjšati pomanjkljivosti v svojih vrstah (Ancker in drugi, 2003, str. 18–25). Vendar se asimetrija ne nanaša samo na kvantitativne indikatorje, temveč tudi na neprimerljivost, neenakost in različnost sodelujočih v spopadu (Svete, 2002, str. 12).

Škerbinc piše o značilnostih hibridnega vojskovanja. To, pravi, da je kombinirana uporaba konvencionalnih, specialnih, neregularnih sil in plačancev (Škerbinc, 2015, str. 26). Konvencionalne indikatorje smo že izpostavili. Asimetričnost poleg specialnih, neregularnih sil in plačancev najdemo v nadaljevanju Škerbinčeve razlage, ko izpostavi intenzivno uporabo propagande, izvajanje psiholoških operacij in zavajanj, agresivne ekonomske pritiske, ustvarjanje in uporabo »petokolonašev«, ofenzivno kibernetsko delovanje, prevrate, ustvarjanje in izkoriščanje družbenih kriz, državne udare, teroristične akcije, gverilo, akcije prikrivanja in prebega (Škerbinc, 2015, str. 26).

Gologranc (2015) pri preučevanju razmerja šibki/močnejši med akterji asimetričnosti izpostavi pet dejavnikov, in sicer so to vojaški, politični, mednarodni, ekonomski in informacijsko-komunikacijski. Vojaški nas pri določanju indikatorjev asimetričnih groženj ne zanimajo. Izpostavimo pa lahko indikatorje preostalih štirih dejavnikov, ki jih obravnava Gologranc. Ti indikatorji so politični cilji in interesi, podpora ljudstva, vrsta političnega režima, zavezniki, mednarodno pravo, ekonomske sankcije, ekonomska moč, psihološko vojskovanje in IKT.

Med asimetrične indikatorje bomo uvrstili tudi ekonomsko bojevanje. Kopač navede več avtorjev, ki ga utemeljujejo kot sredstvo za doseganje nacionalnih interesov. Kopač izpostavi, da ekonomsko bojevanje zajema postopke za slabljenje in motenje nasprotnikovega gospodarstva (Kopač in drugi 2007, str. 60). Indikatorje lahko po Kopaču opredelimo kot ekonomsko varnost prebivalstva, notranjo stabilnost države, razvojno uspešnost države, izpostavljenost ekonomskemu bojevanju, stopnjo vključenosti v mednarodne ekonomske odnose in zunanjo stabilnost, prosperiteto in stabilnost mednarodnega okolja (Kopač in drugih, 2007, str. 62). Omeniti je treba tudi povezanost notranjega slabenja gospodarstva zaradi domačih menedžerjev, ki se jih preganja kot gospodarski kriminal.

Prezelj izpostavi indikatorje terorističnega ogrožanja kot odraz števila terorističnih napadov, števila žrtev terorističnih napadov, števila groženj terorističnih napadov ter delujoče teroristične in ekstremistične skupine na območju neke države (Prezelj in drugi, 2007, str. 88).

Že omenjeni organizirani kriminal obdelata Meško in Dobovšek in predlagata naslednje indikatorje organizirane kriminalitete, ki izhajajo iz kaznivih dejanj: umor, huda telesna poškodba, protipravni odvzem prostosti, ugrabitev, zvodništvo, neupravičena proizvodnja in promet z mamili, odvzem motornega vozila, izsiljevanje, ponarejanje denarja, pranje denarja, tihotapstvo, dajanje podkupnin in hudodelsko združevanje (Meško in Dobovšek in drugi, 2007, str. 119).

Izpostavimo še indikatorje migracijskega ogrožanja, kot jih vidi Kopač. Regularne migracije izpostavi z indikatorjem migracijskega gibanja oziroma selitvenega prirasta prebivalstva. Najprimernejši indikator za ilegalne migracije je količinski glede na število ljudi, ki so nezakonito prestopili mejo neke države. Kopač izpostavi še prisilne migracije, za katere je najprimernejši indikator prav tako izražen v številu beguncev v državi (Kopač in drugi, 2007, str. 64).

1.3 Hibridne grožnje

Na podlagi preučevane teorije ugotavljamo, da je hibridnost novi pojem za lažje razumevanje starih pojavov.

Malešič in Žabkar povzameta Lanoszka in zapišeta, da uradna ameriška opredelitev hibridno grožnjo prepoznava kot vsakega nasprotnika, ki sočasno in prilagojeno uporablja mešanico konvencionalnih, neregularnih, terorističnih in kriminalnih sredstev ali dejavnosti na območju operacije, pri čemer hibridna grožnja ni ena entiteta, ampak je kombinacija državnih in nedržavnih akterjev (Lanoszka v Malešič in Žabkar, 2016, str. 26). Definicija omejuje hibridne grožnje na območje operacije, kar morda ni prav posrečeno, saj s tem ne priznava hibridnega ogrožanja v mirnodobnem času. Priznava pa tako državne kot nedržavne akterje.

Podobno razmišljajo tudi Britanci, vojskovanje je po njihovo trajnostni element mednarodnega sistema, čeprav se njegov značaj skozi čas spreminja. Značilnost tega razvoja je pojav — nekateri trdijo, ponovni pojav — spojine ali hibridnih groženj.

To stanje nastane, ko se države ali nedržavni akterji odločijo, da bodo izkoristili vse načine vojskovanja s hkratno uporabo naprednega konvencionalnega orožja, neregularne taktike, terorizma in kriminala, z namenom destabilizirati veljavni red. S tem grozijo državni in nedržavni akterji, ki imajo dostop do nekaterih sofisticiranih orožij in sistemov, po navadi nastopajo skupaj z rednimi silami. Konflikti so vedno bolj značilna mešanica tradicionalne in netradicionalne taktike, decentraliziranega načrtovanja in izvedbe državnih ali nedržavnih akterjev, ki lahko uporabljajo preprosto in zapleteno tehnologijo na popolnoma nov način (Fleming, 2011, str. 35).

Thiele pravi, da je vojskovanje kameleon in da je enaindvajseto stoletje čas dinamičnega strateškega okolja, v katerem lahko nasprotnik deluje s hibridnimi sredstvi tako na ohranjanje političnega ravnotežja kot na vojsko in na celotno družbo. Agresijo s hibridnimi grožnjami lahko državni in nedržavni akterji izvajajo po celotnem spektru konvencionalne in nekonvencionalne linije delovanja in vključijo diplomacijo ter vojaško in gospodarsko razsežnost konflikta. Vsaka grožnja ima pred sabo cilj in Thiele jih povezuje s kibernetskimi, kritičnimi informacijskimi sistemi ter motnjami kritičnih storitev, kot so oskrba z energijo in finančnimi storitvami, s čimer se zmanjša zaupanje v državne institucije in socialno kohezijo. Zaradi omenjenega je prav javnost postala privlačna tarča (Thiele, 2016, str. 3).

Mažeikis pri definiranju hibridne grožnje izhaja iz že znanega akterja in pravi, da mora imeti država ali nedržavni akter zmogljivosti in očitno željo, da uporabi hibridno strategijo. To storijo z aktivnostmi, ki včasih dosežejo raven prave vojaške akcije in se lahko izvajajo tudi v daljših časovnih obdobjih (Mažeikis, 2017, str. 6).

Na tem mestu se prvič srečamo s terminom hibridna strategija. Če definiramo strategijo kot načrt ciljev, podciljev in nalog za uresničitev dodeljenega poslanstva, lahko hibridno vojskovanje dobi povsem novo razsežnost, ki pa ni realna.

Fleming navede, da so značilnosti hibridnih ogrožanj decentralizirano poveljevanje in kontrola, razpršene vojaške in nevojaške aktivnosti, kombinacija tradicionalnih, neregularnih, terorističnih in razrvanih kriminalnih metod (Fleming, 2011, str. 36). S Flemingom se lahko strinjamo in poskušamo ugotoviti, ali lahko govorimo o hibridnosti, ko je ta zapisana. Ali lahko govorimo o doktrinarnosti? Ko govorimo o hibridnih grožnjah, govorimo o vsem, ki državi s pomočjo regularnih in neregularnih sil, kriminalnih združb (ki so predvsem v državah z visoko stopnjo koruptivnosti), podjetij (ki so zdavnaj prerasla nacionalne okvirje) ali terorističnih organizacij pomagajo, da vpliva na drugo državo s ciljem spremembe družbenega reda, z ozemeljskim ciljem in s ciljem ekonomske osamitve ter drugo. Hibridne grožnje vodijo k totalnim grožnjam. Morda pretiravamo, ko zapišemo, da je stalna napetost blokovskega spopada, ki je zaznamovala 45-letno zgodovino, dobila naslednika, ki je nedoločljiv, njegova smer ogrožanja ni le morska, kopenska ali zračna, ampak tudi virtualna in vesoljska. Če pretiravamo oziroma nas vodi misel zarote, se je grožnja s pomočjo farmacevtske industrije naselila že v fetus. Hibridno ogrožanje je stanje, ko človeka, družbo ali svet določene interesne skupine (nedoločljivih

oblik in organiziranosti) držijo v stalni negotovosti. Negotovost je stanje, ki bo človeka motiviralo kot potrošnika prihodnosti, potrošnika v omreženi družbi. Zato ne moremo govoriti ne o hibridni strategiji, ne o doktrinarnih načelih hibridnega vojskovanja in zato tudi težko govorimo o pojmu hibridna vojna. Lahko pa govorimo o hibridnih grožnjah, ki jih je treba prepoznati in se proti njim uspešno odzvati, še preden preidejo v konvencionalni ali asimetrični konflikt in v vojno.

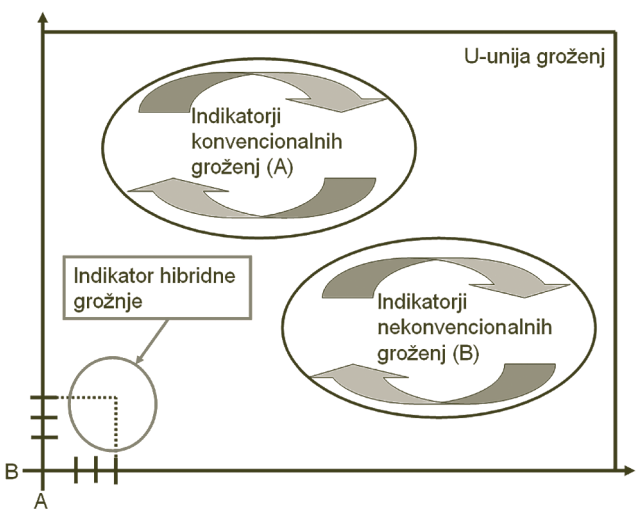
1.3.1 Indikatorji hibridnih groženj

Pri določanju indikatorjev hibridnih groženj na podlagi že predelanih teoretikov in empiričnih opredelitev nekonvencionalnih indikatorjev pridemo do paradoksa. Ali lahko določimo indikatorje hibridnih groženj ali le povežemo že preučene indikatorje konvencionalnih in nekonvencionalnih groženj in jih kot celoto predstavimo kot hibridne indikatorje? Dilemo najlažje prikažemo v obliki slike (glej sliko 1), ki nam prikazuje množico indikatorjev konvencionalnih in množico indikatorjev nekonvencionalnih groženj. Obe množici skupaj nam predstavljata unijo groženj. Puščice nam ponazarjajo dinamičnost in stalnost groženj. Matematika nas uči, da za obstoj unije potrebujemo najmanj dve množici, v našem primeru množico A (konvencionalni indikatorji) in množico B (nekonvencionalni indikatorji), da dobimo unijo U (grožnje). Logični zapis unije množic: $a \in A \cup B \Leftrightarrow ((a \in A) \vee (a \in B))$.

Pomen te primarne obrazložitve se kaže v dejstvu, da potrebujemo vsaj en par iz različnih množic v uniji, ki ga bomo uporabili pri modelu prepoznavanja hibridnih groženj. Da lahko izpostavimo indikatorje hibridnih groženj v uniji groženj, potrebujemo vsaj en kartezični produkt množice A in množice B, logični zapis:

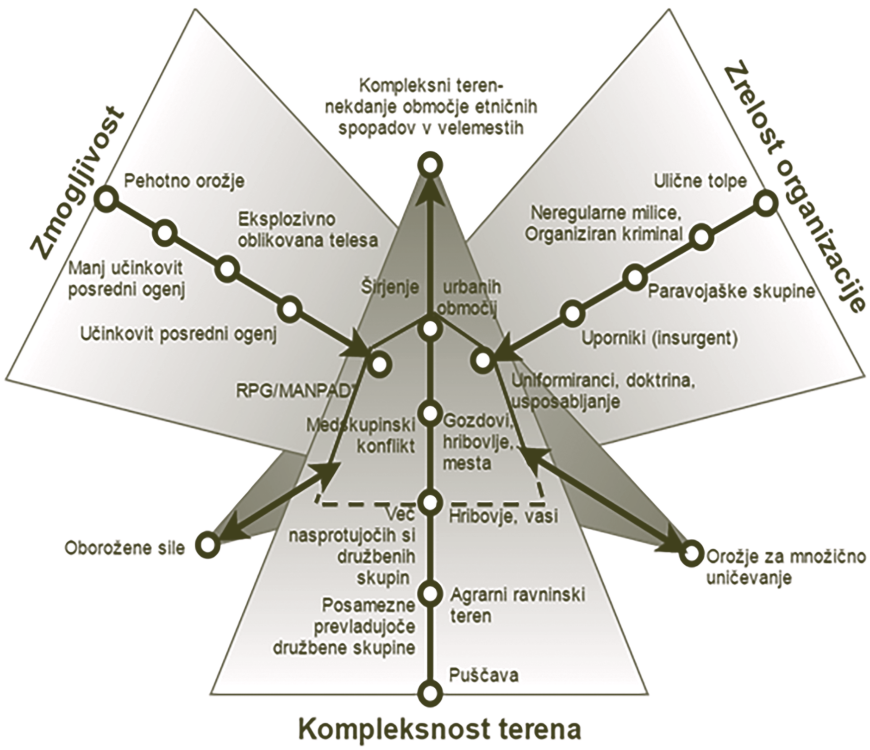
$$A \times B = \{(a,b); a \in A \wedge b \in B\}.$$

Kartezični par indikatorjev je dovolj, da lahko ogrožanje poimenujemo hibridno.



Slika 1: Indikatorji hibridnih groženj, poenostavljeni z unijo množic in kartezičnim produktom
Vir: Stonič (2017, str. 41).

Indikatorje hibridnih groženj lahko poenostavimo tudi kot križišče hibridnih groženj, ki ga je razvil Bowers (2012). Grožnje nam predstavi skozi tri faktorje, in sicer zmogljivost, kompleksnost terena in zrelost določenega akterja. Stičišče vseh treh dejavnikov imenuje »sweet spot«, v prevodu smo to poimenovali območje hibridnega ugodja (glej sliko 2):

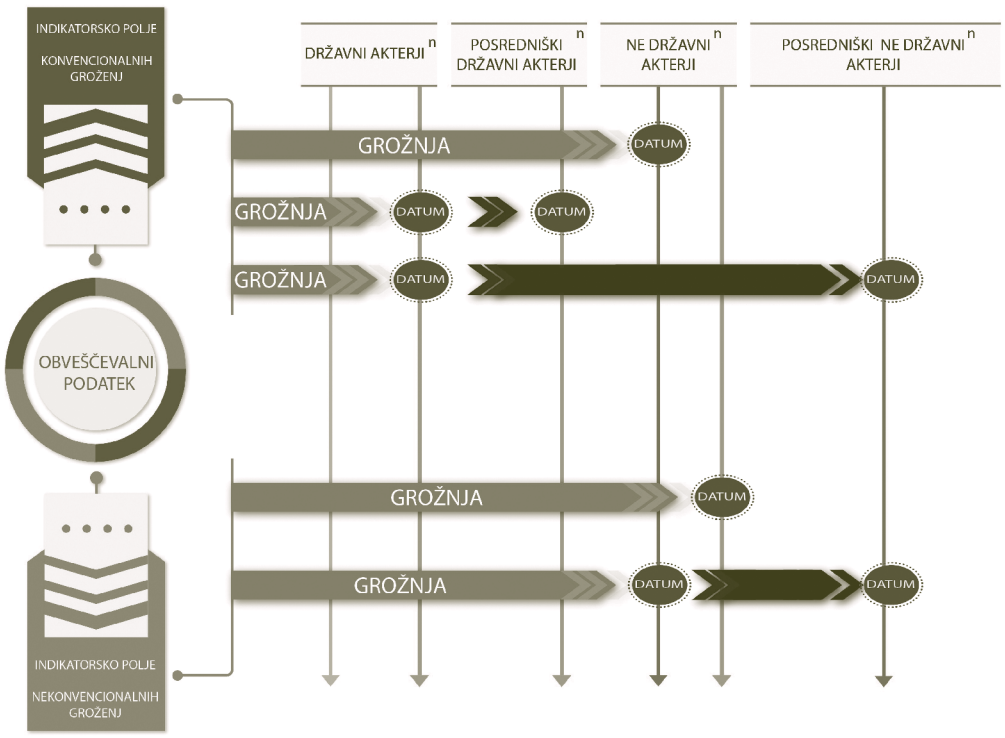


Slika 2: Križišče hibridnih groženj
Vir: Bowers (2012, str. 42).

2 MODEL ZA PREPOZNAVANJE HIBRIDNIH GROŽENJ

Model bomo poenostavili s pomočjo diagrama (glej sliko 3), pri čemer se bomo osredotočili na indikatorje hibridnega ogrožanja na način, kot smo ga poenostavili v podpoglavju 2.3.1 (Indikatorji hibridnega ogrožanja). Ovrednoteni obveščevalni podatek vstavimo v model. Če kateri od indikatorjev zazna grožnjo, jo povežemo z akterjem in časovno premico. Ko se na isti časovni premici pojavita vsaj dve grožnji, ki nista iz istega indikatorskega polja (konvencionalnega ali nekonvencionalnega), lahko začnemo ocenjevati, ali identificirani akter hibridno ogroža. To pomeni, da naredimo novo entiteto, ki jo podrobneje spremljamo. Model je sestavljen iz indikatorskih polj, časovno opredeljenih vektorjev groženj, akterjev in časovne premice, ki posameznega akterja povezuje z vektorjem grožnje.

V indikatorski polji vstavimo vse identificirane indikatorje konvencionalnih in nekonvencionalnih groženj. Akterje sproti dodajamo z identificiranim legalnim ali nelegalnim nazivom. Svetlejši vektor predstavlja posamezno identificirano grožnjo. Svetla časovna premica pomeni, da ni zaznane grožnje, temnejša, da je grožnja zaznana z enega od indikatorskih polj, temna pomeni hibridno ogroženost. Akterje ločimo v dve primarni skupini: državni in nedržavni akterji. Iz primarno nastavljenih entitet se lahko oblikujeta dve novi entiteti in sicer posredniške države in posredniški nedržavni akterji. V diagramu (glej sliko 3) vektor grožnje, ki povezuje isto grožnjo z dvema akterjema, obarvamo v temnejše, tako izločimo iz državnega akterja posredniškega državnega ali posredniškega nedržavnega akterja.



Slika 3: Diagram modela **Vir:** Stonič (2017, str. 56).

Za nadaljnje raziskovanje in razvoj modela bi lahko diagram pretvorili v delujočo aplikacijo. Navedimo najenostavnejši primer povezovanja podatkov s prednastavljenimi identitetami v posameznih tabelah.

Potrebovali bi bazo podatkov (MySQL) in povezane funkcije z algoritmi za uspešno delovanje.

Baza podatkov bi vsebovala tabelo Obveščevalni podatek, v kateri bi definirali dve polji z naslednjimi vnosi:
- (ID, INDIKATORSKO POLJE) vnosi v tabelo: 1 ─ konvencionalne grožnje, 2 ─ nekonvencionalne grožnje.

Druga tabela: Državni akterji bi vsebovala polja:
- (ID, DRŽAVNI AKTER) vnosi v tabelo: 1 ─ državni akterji, 2 ─ posredniški državni akterji, 3 ─ nedržavni akterji, 4 ─ posredniški nedržavni akterji.

Tretja tabela: Države bi vsebovala polja:
- (ID, ID-DRŽAVNEGA AKTERJA, IME DRŽAVE) vnosi v tabelo: 1 ─ id, 2 ─ id-državnega akterja, 3 ─ ime države.

Četrta tabela: Grožnje bi vsebovala polja:
- (ZAPOREDNI ID, ID-GROŽNJE, ID-INDIKATORSKEGA POLJA, ID-DRŽAVNEGA AKTERJA, ID-DRŽAVE, DATUM, ČAS, NASLOV GROŽNJE, OPIS GROŽNJE, STOPNJA, ID-SEKTORJA ZA OBVEŠČANJE).

Peta tabela: Aktivnost bi vsebovala polja:
- (ZAPOREDNI ID, ID-KONVENCIONALNE GROŽNJE, ID-NEKONVENCIONALNE GROŽNJE, DATUM, ČAS, NASLOV, OPIS, STOPNJA, ID-OBVEŠČENEGA SEKTORJA)

Šesta tabela: Sektorji bi vsebovala polja:
- (ID-SEKTORJA, NASLOV, OPIS, OSEBA ZA STIKE ...).

Pri vnosu posamezne grožnje v sistem bi izpolnili vnosna polja za tabelo Grožnje.

Po vnosu bi sistem sprožil funkcijo, ki bi preverila povezave vnesene grožnje s trenutnimi. Pri funkciji bi se določili izbrani algoritmi za prepoznavanje medsebojnih povezav med grožnjami, ki bi nato sprožili aktivnost, če bi glede na prednastavljeni algoritem prišlo do ujemanja. Algoritmi bi preverili, ali pride do ujemanja obveščevalnega podatka konvencionalne grožnje z nekonvencionalno grožnjo za posameznega državnega akterja. Ob ujemanju se sproži obvestilo ID-sektorju, ki je pristojen za posamezno grožnjo.

Za večjo varnost bi to temeljilo na decentralizirani »blockchain« tehnologiji, pri čemer bi bili podatki porazdeljeni medmrežno, saj bi bila tako ranljivost najmanjša. Mreža bi uporabljala javni in zasebni ključ kriptografije za dostop in pretakanje informacij digitalnih sredstev.

Sklep

Z obravnavo teoretičnih vsebin smo izpostavili indikatorje konvencionalnih in nekonvencionalnih ogrožanj. Dokazali smo, da so indikatorji hibridnega ogrožanja le kombinacija indikatorjev konvencionalnega in nekonvencionalnega ogrožanja in ne novo dejstvo. Prišli smo do pomembnega spoznanja, da so hibridne grožnje dokazljive, ter se distancirali od pojma hibridna vojna. Določili smo mogoče akterje hibridnega ogrožanja. Tako smo operacionalizirali hibridno ogrožanje in oblikovali model za prepoznavanje hibridnega ogrožanja nacionalne varnosti. V nadaljnjem raziskovanju se ta model lahko razvije v računalniško aplikacijo ob ustrezni določitvi algoritmov, ki bi obveščevalne podatke s pomočjo indikatorjev groženj povezali z enim ali več akterji. Aplikacija bi bila podlaga analitikom za izdelavo subjektivnih analiz hibridnega ogrožanja. Pomanjkljivost izdelanega modela je povezava kibernetskih groženj z akterji. Določanje akterjev pri kibernetskem ogrožanju je in bo velik izziv. Hibridne grožnje ne poznajo meja, ne razlikujejo med vojaškim in civilnim, kar pa je tudi razlog, da preučevanje in iskanje rešitev za prepoznavanje in preprečevanje hibridnih groženj ne more biti usmerjeno samo kot naloga vojaške organizacije, ampak se morajo s tem problemom spoprijeti vsi, ki so vključeni v nacionalnovarnostni sistem. Prav tako je to naloga prav vsakega varnostno osveščenega državljana. Zavedati se namreč moramo, da živimo v časih, ko se vojne ne odvijajo na oddaljenih bojiščih, ampak med nami. Zato bo vedno več pozornosti in finančnih sredstev treba namenjati tudi oboroženim silam, njihovi opremi, kadru, oborožitvi in usposabljanju. Že skoraj zgodovinsko dejstvo je, da ljudstvo, ki ne hrani svoje vojske, hrani tujo.

Z narejenim modelom bomo lažje prepoznali hibridne grožnje. Nato bo treba okrepiti ustrezno nacionalno odpornost in zagotoviti, da bomo pripravljeni odgovoriti s hitro oceno in učinkovitim odločanjem. S krepitvijo konvencionalnih zmogljivosti brez ustreznih nekonvencionalnih mehanizmov ne bomo mogli vzpostaviti kredibilnega odziva. Ob zgodnjem prepoznavanju groženj bo potrebna krepitev sinergije med strategijami in delovanjem resorjev. Ker je krepitev nacionalnih odpornosti ena izmed pomembnih komponent uspešnega odvračanja in obrambe pred hibridnimi grožnjami in izzivi, morajo države poglobiti trenutno veljavne in vzpostaviti nove mehanizme ter koordinacijo na nacionalni ravni.

Literatura

1. *Alderman, R. (2015). Sixth generation warfare: manipulating space and time. Dostopno na: http://mil-embedded.com/guest-blogs/sixth-generation-warfare-manipulating-space-and-time/. 5. 4. 2017.*
2. *Ancker, J. C. in Burke, M. D., 2003. Doctrine for asymmetric warfare. Dostopno na: http://www.au.af.mil/au/awc/awcgate/milreview/ancker.pdf. 7. 4. 2017.*
3. *Bowers, O. C., 2012. Identifying Emerging Hybrid Adversaries. U.S. Army War College. http://indianstrategicknowledgeonline.com/web/hybrid%20Bowers.pdf. 28. 3. 2017.*
4. *Cigler, M. 2016. Hibridna varnost. V Konvencionalna in hibridna varnost: Vzorci (dis) kontinuitete, ur. Marjan Malešič, str. 75–95. Ljubljana: Fakulteta za družbene vede.*
5. *Department of Defense. Quadrennial defense review 2014. Dostopno na: http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf. 10. 4. 2017.*

6. *Eikenberry, W. K., 2014. Thoughts on unconventional threats and terrorism. Hoover institution. http://www.hoover.org/sites/default/files/fw_hoover_foreign_policy_working_group_unconventional_threat_essay_series/201411%20-%20Eikenberry.pdf. 17. 6. 2017.*
7. *European Commission, 2016. Joint communication to the European parliament and the Council, Joint Framework on countering hybrid threats a European Union response. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN. 1. 9. 2018.*
8. *Fleming, P. B., 2011. The hybrid threat concept: Contemporary war, military planning and the advent of unrestricted operational art. Monograph. Kansas: School of advanced Military studies. United States army command and General Staff College.*
9. *Gologranc, G. 2015. Statistična ocena faltorjev prevlade šibkejšega nad močnejšim v slovenski osamosvojitveni vojni. Magistrsko delo. Ljubljana: FDV.*
10. *Hoffman, F., 2006. Lessons from Lebanon: Hezbollah and Hybrid Wars. http://www.fpri.org/article/2006/08/lessons-from-lebanon-hezbollah-and-hybrid-wars/. 1. 3. 2107.*
11. *Liang, Q. and Wang X., 1999. Unrestricted Warfare. Beijing: PLA Literature and Arts Publishing House.*
12. *Lind, S. W., Nightengale H., Schmitt, J. F., Sutton, J. W. And Wilson H. I., 1989. The Changing Face of War: into the Fourth Generation. Marine Corps Gazette 73 (10). https://www.mca-marines.org/files/The%20Changing%20Face%20of%20War%20-%20Into%20the%20Fourth%20Generation.pdf. 20. 3. 2017.*
13. *Malešič, M. in Žabkar A., 2016. Konvencionalno ali hibridno vojskovanje? 1. part. Vloga Ruske federacije v sirski vojni. Revija Obramba. Ljubljana: Založba Defensor, d. o. o.*
14. *Mažeikis, E., 2017. Hybrid threats: overcoming ambiguity, building resilience. http://www.tspmi.vu.lt/doc/1554-edvardas-mazeikis-hybrid-threatsdocx. 29. 5. 2017.*
15. *Prezelj, I., ed., Svete U., Kopač E., Meško G. in Dobovšek B., Kraigher A. in Berger T., Grošelj K., 2007. Model celovitega ocenjevanja ogrožanja nacionalne varnosti Republike Slovenije. Ljubljana: Ministrstvo za obrambo, Direktorat za obrambne zadeve, Sektor za civilno obrambo.*
16. *Svete, U., 2016. Hibridni konflikti v omrežni družbi. V Konvencionalna in hibridna varnost: Vzorci (dis)kontinuitete, ed. Malešič, M., str. 97─112. Ljubljana: FDV.*
17. *Svete, U., 2002. Vloga in pomen informacijske tehnologije v sodobnem asimetričnem vojskovanju. Magistrsko delo. Ljubljana: FDV.*
18. *Svete, U., Guštin D. IN Prebilič, V., 2010. Asimetrija in vojaška organiziranost: slovenske izkušnje. V Mednarodne razsežnosti varnosti Slovenije, ed. Malešič, M., str. 247─280. Ljubljana: FDV.*
19. *Stonič, D., 2017. Oblikovanje modela za prepoznavanje hibridnih groženj nacionalno varnostnega sistema: Primer Sloveija. Magistrsko delo. Ljubljana: FDV.*
20. *Škerbinc, M., 2015. KAJ JE TO: hibridno vojskovanje. Revija Obramba. Ljubljana: Založba Defensor, d. o. o.*
21. *Theile, D. R., 2016. Hybrid Threats – And how to counter them. ISPSW Strategy Series: Focus on Defense and International Security 448. Berlin.*