AKADEMIA E FORCAVE TË ARMATOSURA
INSTITUTI KËRKIMOR SHKENCOR USHTARAK
REVISTË TEORIKO-SHKENCORE
MARS 2025

REVISTA
USHTARAKE
(edicioni i parë)

Botim i Akademisë së Forcave të Armatosura
Miratuar me vendim nr. 1 datë 03.03.2025
të Bordit Drejtues të Revistës Ushtarake

Përgatiti për botim: Grupi i Redaktimit dhe i Publikimit

Art design: Engjellushe Llulla

ISSN 2227-8133 (Print), ISSN 2227-8141 (Online)

Akademia e Forcave të Armatosura
Instituti Kërkimor Shkencor Ushtarak
Shtypur: Mars 2025

PARATHËNIE

I nderuar lexues,

Mirë se vini në edicionin e parë të Revistës Ushtarake, për vitin 2025, një botim që synon të sjellë në vëmendje zhvillimet më të fundit dhe risitë shkencore që ndikojnë në fushën e mbrojtjes, sigurisë dhe strategjisë ushtarake.

Në këtë numër, kemi përmbledhur shkrime dhe studime që mbulojnë një gamë të gjerë temash - nga karakteri dhe strategjitë e luftës së ardhshme, instrumentet ligjore kombëtare dhe ndërkombëtare në luftën kundër terrorizmit, e ardhmja e logjistikës ushtarake drejt përdorimit të inteligjencës artificiale, risitë teknologjike në fushën e mbrojtjes, deri tek analiza e vlerësime mbi evoluimin e konceptit të mbrojtjes në Shqipëri nga qasja tradicionale drejt konceptit të ri të përdorimit, një proces që ka kërkuar adaptimin e strategjive dhe politikave për të përballuar sfidat e reja të sigurisë, si dhe për të siguruar një zhvillim të qëndrueshëm për të ardhmen, apo çështje që prekin balancën e sigurisë ndërkombëtare dhe ndikimin e politikave globale në strategjitë ushtarake. Gjithashtu, kemi përfshirë shkrime historike, të cilat mund të ofrojnë një pasqyrë të thelluar mbi zhvillimet dhe ngjarjet ushtarake që kanë ndodhur në të kaluarën, por edhe për të kuptuar pasojat që lufta ka mbi shoqëritë dhe individët, duke kontribuar në krijimin e një ndërgjegjësimi për nevojën e ruajtjes së paqes dhe stabilitetit.

Revista jonë e shpreh me krenari angazhimin për t'u bërë një burim i besueshëm i informacionit dhe analizës për të gjithë ata që kanë interes në zhvillimin e politikave ushtarake dhe mbrojtëse, si dhe për të gjithë ata që kontribuojnë në avancimin e njohurive të fushës.

Me besimin se shkenca dhe kërkimi janë thelbësorë për forcimin e kapaciteteve ushtarake dhe përballimin e sfidave të sigurisë botërore, ne jemi të përkushtuar t'ju ofrojmë materiale të rëndësishme që mbështesin përparimin dhe zhvillimin në këtë sektor kyç.

Faleminderit për mbështetjen dhe angazhimin tuaj në këtë iniciativë të rëndësishme.

Drejtori i IKSHU

Mars 2025

PËRMBAJTJA E REVISTËS USHTARAKE

RUBRIKA E PARË
Vlerësime dhe analiza në mjedisin e sigurisë

RUBRIKA E DYTË
Zhvillimi i teknologjisë dhe inovacionit në fushën e mbrojtjes

RUBRIKA E TRETË
Studime historike

RUBRIKA E PARË

VLERËSIME DHE ANALIZA NË MJEDISIN E SIGURISË

KARAKTERI DHE STRATEGJITË E LUFTËS SË ARDHSHME,PËRTEJ MBIVLERËSIMIT TË TEKNOLOGJISË

Kolonel Msc. Hysni GJERGJI
Shef Departamenti në IKSHU

Trajtesë e shkurtuar.

Diskutimet se si Forcat e Armatosura duhet të përgatiten për një luftë të ardhshme përtej vitit 2035 aktualisht, janë fokusuar në mënyrë të njëanshme; vetëm në ndryshimin teknologjik, duke shmangur analizën për një transformim të gjerë të karakterit të luftës. Këto argumente vetëm teknologjike injorojnë kontekstin dhe mendimin teorik të konfliktit të armatosur. Për t'u përgatitur efektivisht për konfliktin e ardhshëm, FA-të duhet të pranojnë se çdo luftë ka një karakter unik dhe të ndryshueshëm, i cili drejtohet dhe ndikohet pikë së pari nga faktorë politikë, shoqërorë, ekonomikë gjeografikë, por edhe nga teknologjia. Gjatë gjithë historisë shekullore, forcave të armatosura iu është dashur të përshtatin qasjet e tyre ndaj luftërave që kanë ndodhur dhe kanë pasur karaktere të ndryshme nga njëra-tjetra.

Në këtë punim, duke përdorur një analizë për karakterin e një lufte të mundshme të NATO-s kundër Kinës ose Rusinë, mund të parashikojmë se si ata do të ndjekin dhe përdorin befasinë, fuqinë e zjarrit, dezinformacionin, komplotin, burimet njerëzore, padyshim të mbështetur nga teknologjia smart dhe inteligjenca artificiale, që disponojnë me shumicë. Forcat e Armatosura Shqiptare dhe të aleancës ku ne jemi pjesë, duhet të jenë të gatshme të ndjekin strategji fituese për të mposhtur shpejt dhe me vendosmëri forcat e një kundërshtari, përpara se ata të mund të krijojnë një mbrojtje në thellësi, e cila do ta zgjaste konfliktin dhe do të rrezikonte përshkallëzimin deri në atë bërthamor.

Fjalët kyçe: lufta e ardhshme, konflikt i armatosur, forcë e armatosur, mbrojtja aktive, strategji.

1. Histori e evoluimit të parimeve dhe teknologjisë së luftës

Pesëdhjetë vjet më parë, Lufta e Yom Kipurit[1] solli "zhvlerësimin" e armëve të reja dhe dukej se zbuloi një ndryshim në karakterin e luftës. Komandanti i Komandës së Trajnimit dhe Doktrinës së Ushtrisë së SHBA, gjenerali William DePuy, dërgoi gjeneralmajor Donn Starry[2], për të studiuar atë luftë. Qëllimi i tij ishte të nxirrte mësime dhe, nëse ishte e nevojshme, për të luftuar vendet që ishin anëtare me Paktin e Varshavës në Evropë. Nga analiza e detajuar e efektivitetit të teknologjive të reja në atë luftë, në 1976, TRADOC publikoi Doktrinën e Mbrojtjes Aktive për SHBA.

Pasi drejtoi studimin, gjenerali Donn Starry mori komandën e Korpusit V në Gjermani dhe filloi testimin e koncepteve në Mbrojtjen Aktive, kundër një sulmi nga forcat e Traktatit të Varshavës të vendosura përpara tij. Pasi u zbatua në praktikë, ai zbuloi se doktrina që ai vetë kishte ndihmuar të krijonte, në fakt, nuk funksionoi. Fakt është se ai nuk ishte i vetmi kritik i "Mbrojtjes Aktive".

Kritikët vunë në dukje se efektiviteti i raketave të drejtuara antitank në shkretëtirën e hapur të Sinait nuk përshtatej për pyjet dhe kodrat kufizuese të Evropës Qendrore. Përveç kësaj, ata vunë re se sovjetikët kishin kaluar nga përparimi i përqendruar të përshkruar në "Mbrojtjen Aktive" në një sulm të shpërndarë, të fokusuar në krijimin e mundësive për shfrytëzimin e skalioneve të dyta. Mbrojtja aktive nuk i plotësonte kërkesat strategjike të Ushtrisë Amerikane për të kërcënuar me një sulm që mund të çlironte vendet e Traktatit të Varshavës apo të pengonte Bashkimin Sovjetik nga kërcënimi i luftës. Mbrojtja aktive u fokusua më shumë në teknologjinë e shfaqur në Yom Kippur dhe jo sa duhet në kontekstin operacional dhe strategjik të një lufte me Bashkimin Sovjetik. Sot, shumë analistë ushtarakë po bëjnë rekomandime se si ushtria amerikane duhet të luftojë, bazuar në vëzhgimet dhe mësimet e luftës Ruso-Ukrainase. Ashtu si me studimin e Ushtrisë për Luftën e Yom Kipurit, këta studiues shpesh fokusohen në teknologjinë e përdorur në Ukrainë. Ata e kanalizojnë dhe e sjellin idenë e Carl von Clausewitz-it në kontekstin e luftës së 2022-2025 për të arritur në përfundimin se si kjo teknologji e re, e përdorur këto tre vite, tregon "karakterin në ndryshim të luftës".

Karakteri i luftës – si, ku, me çfarë armësh dhe teknologjish zhvillohen luftërat, - po ndryshon me shpejtësi. Ndryshimi i fundit thelbësor në karakterin e luftës ndodhi midis Luftës së Parë Botërore dhe Luftës së Dytë Botërore. Përparimet teknologjike transformuan rrënjësisht karakterin e luftës. Një numër autorësh argumentojnë në mbështetje të ndryshimeve për 2030 se "Sensorë të lirë dhe të

[1] https://telegrafi.com/lufta-arabo-izraelite-e-vitit-1973-krejt-cfare-ndodhi-ne-luften-qe-coi-ne-nje-realitet-te-ri-ne-boten-arabe/

[2] https://www.nytimes.com/2011/09/22/us/gen-donn-a-starry-cold-war-strategist-dies-at-86.html

bollshëm, të mbështetur me armë zjarri gjithnjë e më të sakta me rreze të gjatë, luftë elektronike dhe aftësi kibernetike, po ndryshojnë karakterin e luftës". Të dyja këto argumente dhe shumë të tilla si ato, në fakt, janë të paplota. Për shkak se fokusohen vetëm në ndryshimin teknologjik, ato nuk përputhen me përdorimin e termit të karakterit të luftës të cituar nga Clausewitz. Në vend që të diskutonte teknologjinë, Clausewitz shpjegoi karakterin e bashkëkohor të luftës kryesisht në kontekstin e ndryshimeve politike dhe shoqërore. Ai paralajmëroi me një gjuhë të tillë, duke shpjeguar se "Luftërat duhet të ndryshojnë në varësi të natyrës së motiveve të tyre dhe të situatave që i shkaktojnë ato".

Këto argumente "teknologjike" injorojnë kontekstin i cili ka shumë rëndësi, pasi bazuar në palët ndërluftuese, objektivat e tyre politikë, strategjitë e tyre ushtarake, ekonomitë e tyre, shoqëritë e tyre dhe terreni ku ata luftojnë, secila luftë ka karakterin e saj. Edhe brenda një lufte, beteje dhe fronti të ndryshëm mund të kenë karaktere të ndara. Për më tepër, periudha fillestare e luftës shpesh ka një karakter të dallueshëm nga mënyra se si duket pasi palët janë të mobilizuara plotësisht. Ndërsa ushtria përgatitet për të luftuar një konflikt të mundshëm në të ardhmen, ajo nuk duhet të analizojë vetëm armatimet, teknologjitë dhe konfliktet bashkëkohore, por duhet të kujtojë gjithashtu të kaluarën dhe përvojën e saj për të kuptuar se si resurset e luftërave të saj kanë ndikuar në strategjitë fituese (ose humbëse) që ajo ka ndjekur.

Ukraina vendos një pikë shtesë për parashikimin e karakterit të ardhshëm të luftërave të mundshme, por ne nuk duhet të bëjmë përgjithësime gjithëpërfshirëse rreth ndryshimit të karakterit të luftës bazuar në vëzhgimet e ngushta të ndryshimeve teknologjike. Për të mësuar prej kësaj lufte që vazhdon në vitin 2025, ne duhet të marrim në konsideratë edhe qasjen e rekomanduar të Michael Howard ndaj historisë ushtarake. Duke e bazuar punimin në një studim të gjerë dhe hollësishëm të konfliktit, duhen njohur si ngjashmëritë, ashtu edhe defektet në luftën Ruso-Ukrainase në krahasim me luftërat e tjera. Duke përdorur një perspektivë të gjerë historike, ne duhet të kuptojmë se si konteksti i kësaj lufte është i ndryshëm nga konteksti i një lufte të mundshme midis Shteteve të Bashkuara apo NATO-s kundër Rusisë ose Kinës. Ne duhet të përpiqemi të parashikojmë karakterin e një lufte të tillë të mundshme dhe ta përdorim atë për të parashikuar një strategji optimale për të penguar ose mposhtur kundërshtarët.

2. Mbivlerësimi i teknologjisë është në dëm të parimeve

Duke shkruar mbi "Rrugën e Luftës" amerikane, Russell Weigley paralajmëroi gjysmëshekulli më parë se "Kërkimi për një doktrinë të re nuk duhet të ngatërrohet me kërkimin për një teknologji më të mirë të armëve. Të kërkosh

justifikim në teknologji për problemet e strategjisë dhe politikës është tendencë e rrezikshme, e nxitur nga cilësitë pragmatike të karakterit amerikan dhe nga kompleksiteti i teknologjisë së epokës bërthamore".

Në vend që të nxjerrin mësime të përshtatshme për një kontekst specifik, analistët theksojnë se ndryshimi teknologjik nxit karakterin e luftës dhe shpesh i drejtohen mitit teknologjik. Ky mit e përforcon kulturën strategjike të Amerikës, e cila ka kërkuar zgjidhje teknologjike për luftën. Për dekada, teoricienët ushtarakë kanë pretenduar teknologji që mund të eliminojnë «mjegullën e luftës» duke u fokusuar te dronët dhe inteligjenca artificiale. Studiuesit që e mbitheksojnë teknologjinë, rrezikojnë të mendojnë se gjithçka që duhet të bëjmë është të sinkronizojmë (ose konvergojmë) aftësitë e duhura për të fituar luftën.

Teknologjia ka rëndësi, por përqendrimi vetëm në të, çon në një fokus tepër të ngushtë të karakterit të luftës. Disa nga përparimet më të rëndësishme teknologjike të shekullit të 19-të janë përdorimi i pushkëve i cili çoi në një fushë beteje me front gjithnjë e më të gjerë. Trenat më vonë lejuan mobilizimin dhe vendosjen më të shpejtë të rezervave operative. Në vitet e fundit, Shtetet e Bashkuara dominuan forcat irakiane duke përdorur armë superiore dhe me një avantazh teknologjik, por nga ana tjetër ShBA-të nuk ishin në gjendje të mposhtnin as Viet Kongun dhe më vonë as talebanët, me gjithë teknologjinë e sofistikuar që kishin. Nuk mund të mendojmë se vetëm një teknologji do të sigurojë avantazh vendimtar të NATO-s apo vetëm të SHBA-ve ndaj Rusisë ose Kinës. Sot, teknologjitë e reja përhapen me shpejtësi dhe Rusia dhe Kina i kanë gjithashtu aftësitë shkencore dhe industriale për përditësuar shpejt, si dhe për t'u përshtatur me përparimet çka e tregoi edhe Deepseek i lançuar në janar 2025.

Me gjithë fokusin në teknologjinë në Ukrainë, armët kryesore në atë konflikt kanë qenë artileria e rëndë, raketat dhe sistemet ajrore pa pilot (UAS) të disponueshme në tregun e lirë. Nëse do të vendosim një UAS me skuadrone avionësh luftarakë, atëherë karakteri i konfliktit aktual do të analizohej lehtësisht edhe nga një oficer i Luftës së Parë Botërore. UAS e kanë bërë të vështirë arritjen e befasisë në Ukrainë, por e njëjta gjë ka ndodhur edhe në ofensivën e pranverës në 1918, kur gjermanët gjithashtu duhej të fshihnin forcat e tyre nga vëzhgimi ajror për të ruajtur befasinë.

Ka disa autorë që përshkruajnë karakterin e luftës dhe fokusohen në sfidën e minave të teknologjisë së ulët, por këto mina e ndalën kundërsulmin e Ukrainës në 2023 në Mala Tokmachka. Oficerët ukrainas deklaruan se ata kishin zgjidhje për shumë nga sfidat e tjera në luftë, por jo për minat e konsideruara si të tejkaluara. Rusët i vendosin fushat e minuara shumë thellë për t'u depërtuar lehtësisht pavarësisht nga pajisjet anti-minë ukrainase. Rusët dyfishuan dhe trefishuan minat antitank duke çaktivizuar pajisjet e depërtimit ukrainas,

pasi rusët kanë mjete të ndryshme për të rimbjellë fushat e minuara. Lufta Ruso-Ukrainase na lejon gjithashtu të rishqyrtojmë deklaratat e mëparshme të ndryshimeve të nxitura teknologjikisht në karakterin e luftës. Para luftës, shumë analistë kishin dyshime nga ardhja e luftës hibride dhe kibernetike dhe Ukraina ka treguar kufijtë e të dyjave.

Për më shumë se një dekadë, ekspertët kanë frikë nga një Pearl Harbor kibernetik. Në potencialin e sulmeve kibernetike, ne pamë që diçka po e ndryshonte karakterin e luftës. Cyber madje u bë një domen i ri në operacionet me shumë domene (MDO). Përpara luftës, disa ekspertë ushtarakë, duke ndjekur gjurmët e karakterit të drejtuar teknologjikisht të luftës, parashikuan se pushtimi rus i Ukrainës "mund t'i jepte botës shembullin e parë të një lufte të vërtetë kibernetike". Rusia zotëronte aftësi të avancuara kibernetike dhe kishte vite duke u përgatitur për të zhvilluar sulme të tilla ndaj Ukrainës. Megjithatë, sulmet kibernetike ruse bënë pak për të gjunjëzuar Ukrainën. Një analizë e efekteve të sulmeve kibernetike ruse raportoi se "tendencat tregojnë se operacionet kibernetike nuk kanë pasur një ndikim të madh material në fushën e betejës". Një dekadë më parë, ishte pranuar nga profesionistët se sulmuesit kanë avantazhin e befasisë dhe përzgjedhjes së objektivit në hapësirën kibernetike. Ukraina ka treguar se pala mbrojtëse kishte sukses pasi "përparimet e inteligjencës për zbulimin e kërcënimit, duke përfshirë përdorimin e inteligjencës artificiale, kanë ndihmuar në zbulimin më efektiv të sulmeve ruse.

Zhvillimi i suksesshëm i teknikave të mbrojtjes kibernetike tregon rëndësinë e të kuptuarit dhe përshtatjes me teknologjinë, por nuk duhet të supozojmë se teknologjia e re do të ndryshojë karakterin e luftës. Ushtritë e NATO-s mund të ketë mbivlerësuar rëndësinë e operacioneve kibernetike në doktrinën e tyre të re të MDO[3]. Pjesa më e madhe e MDO mbështetet në sulmet kibernetike të trupave me domene të tjera. A duhet ta bazojmë të gjithë qasjen tonë ndaj luftës, rreth teknologjisë?

Në vend që të përqendrohemi në mënyrë "të verbër" te teknologjia, duhet të kujtojmë se si Clausewitz analizoi karakterin e luftës. Kur Clausewitz diskutoi për "Karakterin e Luftës Bashkëkohore", ai nuk e përmendi zhvillimin e pushkëve apo topave, as nuk e përmendi fare teknologjinë. Në vend të kësaj, ai u fokusua në kontekstin politik të luftës. Clausewitz diskutoi rëndësinë e nacionalizmit dhe kombit dhe kontributit të madh që mund ti japë zemra dhe temperamenti i një kombi, forcës së tij luftarake. Nëse ndjekim Clausewitz-in, duhet të analizojmë faktorët strategjikë bashkëkohorë në luftërat e ardhshme të mundshme me kundërshtarë të ndryshëm. Ne duhet të shqyrtojmë se si karakteri i një lufte të mundshme do të ndikonte në natyrën e asaj lufte,

[3] Operacionet me shumë domene.

veçanërisht në trekëndëshin e dhunës, rastësisë dhe arsyes. Ky trekëndësh shkruan Antulio J. Echevarria II, përshtatet me karakterin e çdo lufte dhe "përfaqëson shtrirjen e mundshme të qëndrimeve dhe ndjenjave luftarake në dimensionet socio-kulturore, ushtarake dhe politike të konfliktit të armatosur". Kryesore është të gjemë se cilat janë objektivat politikë të kundërshtarëve tanë dhe potenciali për t'u mobilizuar për një luftë? A do të përballemi me një luftë të kufizuar apo totale?

- Kthimi në Luftërat e Kufizuara.

Por, ndërsa Shtetet e Bashkuara hynë në Luftën e Ftohtë, armët bërthamore do të zbusin përshkallëzimin. Vetëm pesë vjet pas përfundimit të Luftës së Dytë Botërore, ushtria amerikane do ta gjente veten të përfshirë në një luftë të kufizuar në Kore. Edhe pse brutale për ushtarët e përfshirë, lufta u kufizua nga mjetet e mobilizuara për të, nga metodat e përdorura (pa armë bërthamore dhe pa bombardim të Kinës) dhe nga qëllimet politike të kërkuara. Shtetet e Bashkuara ishin fokusuar në kërcënimin e një sulmi gjithëpërfshirës sovjetik, por nuk e kishin përgatitur atë për t'u marrë me konflikte të kufizuara.

Megjithëse Akti i Shërbimit Selektiv i vitit 1948 krijoi rekrutim në kohë paqeje, ushtria amerikane nuk ishte gati për të luftuar një luftë të kufizuar, por intensive. Forcat e saj në Paqësor ishin në një gjendje veçanërisht të mjerueshme, të përqendruara ose në detyrat e pushtimit në Japoni ose në këshillimin e krijimit të një policie në Republikën e Koresë. Në qershor 1950, duke vëzhguar mungesën e angazhimit të Shteteve të Bashkuara ndaj Koresë dhe mungesën e gatishmërisë së saj për të ndërhyrë, (DPRK[4]) filloi një pushtim të befasishëm. E udhëhequr nga ushtarë me përvojë dhe tanke T-34 të siguruara nga sovjetikët, ajo shpejt pushtoi Ushtrinë e Republikës së Koresë të pajisur keq, pushtoi Seulin, la mënjanë Task Forcën Smith të mbledhur me nxitim të Ushtrisë Amerikane dhe mbërtheu forcat e mbetura në Perimetrin e Pusanit.

Ushtria amerikane u hodh në një luftë të kufizuar bazuar në një urdhër ekzekutiv dhe një rezolutë të Këshillit të Sigurimit të Kombeve të Bashkuara (OKB). Megjithëse ushtria amerikane kishte luftuar më parë luftëra të kufizuara, kjo ishte e një karakteri të ri. Ajo luftoi me një ushtri të vogël, për shkak se Shtetet e Bashkuara kishin prioritet parandalimin e një sulmi sovjetik në Evropë, kështu që forcat në Kore morën mbështetje të kufizuar. Edhe me forca të kufizuara, gjenerali Douglas MacArthur pa një mundësi për të mposhtur DPRK-në duke përdorur një strategji asgjësimi duke zbarkuar në Inchon, duke rrethuar forcat e tyre në jug dhe duke ndjekur pjesën tjetër drejt kufirit kinez. Duke injoruar kërcënimet e Kinës për të hyrë në luftë nëse Shtetet e Bashkuara i afroheshin

[4] Republika Demokratike e Koresë.

lumit Yalu, MacArthur kishte arritur një fitore spektakolare. Por ndërsa trupat e tij të tepërta iu afruan Yalu, Kina kaloi kufirin dhe i çoi forcat e MacArthur-it në jug të Seulit.

Presidenti Harry S. Truman e shkarkoi MacArthur-in në prill 1951. MacArthur e shihte luftën si totale, ndërsa Truman u përpoq ta mbante atë të kufizuar. Ai nuk donte të përfshinte Shtetet e Bashkuara ndaj Koresë përballë agresionit të mundshëm komunist në Evropë. Lufta ishte bërë gjithnjë e më e papëlqyeshme në vend. Dyzet për qind e amerikanëve në vitin 1951 u penduan që hynë në luftë dhe në vitin 1952 ky numër u rrit në pesëdhjetë për qind. Truman zëvendësoi MacArthurin me gjeneralin Matthew Ridgway, i cili ndante idenë e Trumanit për ta mbajtur luftën të kufizuar. Duke hequr dorë nga një mundësi për fitore përmes asgjësimit, Shtetet e Bashkuara do të ndiqnin një strategji rraskapitjeje. Ai mbështetej në sulme dhe bombardime të kufizuara e të pakëndshme për të rraskapitur komunistët. Strategjisë iu deshën edhe dy vjet të tjera për të çuar në një armëpushim. Në fund, vdekja e Jozef Stalinit dhe mosinteresimi i Bashkimit Sovjetik për të vazhduar mbështetjen e luftës ishte me gjasë faktori vendimtar në pranimin e komunistëve për një armëpushim.

Rikthimi në luftën e parregullt COIN[5]. Në Luftën e Gjirit Persik, ushtria do të zhvillonte një luftë me karakter krejtësisht të ndryshëm. Përballë ushtrisë irakiane që kishte kryer një sulm të kufizuar për të pushtuar Kuvajtin, Shtetet e Bashkuara, me një koalicion dërrmues, mund të zhvillonin një luftë të kufizuar duke përdorur një strategji asgjësimi për të mposhtur me vendosmëri ushtrinë e Irakut dhe për të çliruar Kuvajtin. Me kalimin e kohës në anën e tij, koalicioni arriti dominimin ajror, i cili fiksoi dhe shkatërroi forcat irakiane, përpara se koalicioni të niste një kundërofensivë me një sulm që depërtoi forcat e përhapura të Irakut në krahun e tyre perëndimor në shkretëtirën e hapur.

Lufta e Gjirit Persik ofroi karakterin ideal të luftës për ushtrinë amerikane të dalë nga Lufta e Ftohtë. Ai shkëlqeu në fushat e betejës që imitonin terrenin e Korridorit Qendror të Qendrës Kombëtare të Stërvitjes, në të cilin ishte trajnuar gjatë gjithë viteve 1980. Fatkeqësisht, ishte aq i suksesshëm sa ushtria filloi të shpresonte se luftërat e ardhshme do të kishin një karakter të ngjashëm. Deri më sot, simulimet e luftëtarëve në përgjithësi ndjekin një skenar të një sulmi të kufizuar armik, një ngritje të fuqisë dërrmuese luftarake dhe dominimit ajror, dhe një ofensivë të kufizuar për të mposhtur me vendosmëri armikun dhe për të rivendosur kufijtë ndërkombëtarë. Në vitet 2000, Shtetet e Bashkuara në dukje fillimisht do të kishin sukses në luftëra të kufizuara në Afganistan dhe Irak. Ajo përdori një strategji të asgjësimit kundër talebanëve dhe regjimit të Sadam Huseinit. Megjithatë, karakteri i atyre luftërave ndryshoi me shfaqjen

[5] Kundër kryengritje.

e kryengritjeve dhe i ktheu ato në luftëra rraskapitjeje. Në Irak, shoqëria përfundimisht mobilizoi mjetet për të mposhtur kryengritjen, veçanërisht në Zgjimin Sunit. Në Afganistan, një qeveri gjithnjë e më e izoluar dhe e korruptuar vazhdoi të mbështetej në mbështetjen e jashtme për ta izoluar atë nga kryengritja. Pasi mbështetja e jashtme mori fund, popullsia nuk donte të luftonte për të ruajtur qeverinë.

- Një ushtri e gatshme dhe jo një ushtri masive.

Bazuar në vëzhgimet e Ukrainës, komentuesit kanë shtyrë që ushtria amerikane të fokusohet në përgatitjen për një konflikt më total dhe të zgjatur. Këta komentues humbasin karakterin e mundshëm të kufizuar të një lufte të ardhshme. Rekomandimet e tyre do të prishnin gatishmërinë e forcave tona. Nëse Ushtria do të zhvillonte një forcë për një luftë të zgjatur, ajo do të duhej të devijonte burimet drejt grumbullimit të pajisjeve dhe të ricaktonte personelin drejt krijimit të njësive të kuadrit për të trajnuar dhe integruar ushtarët e mobilizuar. Në vitin 1934, nënkoloneli i atëhershëm Charles de Gaulle argumentoi se ushtria franceze ishte shumë e përqendruar në mobilizimin masiv për një luftë të zgjatur. Franca mbështetej te rekrutët për të fituar një luftë rraskapitjeje. Ai propozoi zhvillimin e divizioneve të mekanizuara profesionale për të siguruar një forcë të lëvizshme dhe të gatishmërisë së lartë në shpërthimin e luftës. Propozimi i tij u kundërshtua nga mbrojtësit e kombit në armë. Kur Franca më pas hyri në Luftën e Dytë Botërore me një ushtri të optimizuar për një konflikt të zgjatur, nuk shkoi mirë.

Gjatë Luftës së Ftohtë, Morris Janowitz shkroi: "Për të penguar aktet e agresionit, të kufizuara apo të pakufizuara, përvoja koreane sugjeroi se nuk ishte kapaciteti për mobilizim ai që kishte më shumë rëndësi, por gjendja e gatishmërisë. Komunistët luanin "kumar" në Kore për fatin e luftës sepse besonin se mund të arrinin një *fakt të kryer* përpara se Amerika të përgjigjej bazuar në mungesën e gatishmërisë së Amerikës. Por, gatishmëria nuk do të thotë matjet e përgjithshme që duhet të raportojnë njësitë. Për të penguar Rusinë ose Kinën dhe, nëse është e nevojshme, për të arritur një fitore vendimtare të asgjësimit, ushtria amerikane duhet t'i japë përparësi përgatitjes së njësive për të luftuar karakterin e mundshëm të një lufte në Baltik ose në Tajvan.

Për ta bërë këtë, ne duhet të reformojmë sistemin tonë të rekrutimit të personelit për të theksuar ndërtimin dhe mirëmbajtjen e njësive kohezive me efektivitet të lartë luftarak për të mposhtur kundërshtarët tanë. Edhe pse kanë kaluar dekada që nga kalimi në forcën vullnetare, sistemi ynë i personelit ruan proceset e Ushtrisë të mesit të shekullit të 20-të. Sistemi i personelit të ushtrisë i jep përparësi efikasitetit burokratik mbi kohezionin. Që nga Lufta Koreane, ky sistem ka zhvlerësuar efektivitetin luftarak. Çdo dy vjet, personeli në

njësitë tona ndryshon plotësisht. Njësitë janë ngecur në një përpjekje sizifiane të trajnimit dhe certifikimit të të ardhurve të rinj që i pengon ata të zhvillojnë teknika për të luftuar dhe për të fituar në kontekstin specifik të mbrojtjes së Tajvanit ose të Baltikut. Edhe nëse vjen në kurriz të efikasitetit burokratik, Ushtria duhet t'i japë përparësi shërbimit afatgjatë në njësi për t'i lejuar ato të zhvillojnë ato teknika dhe të ruajnë gatishmërinë e nevojshme për të arritur një fitore të shpejtë dhe vendimtare ndaj kundërshtarëve tanë.

Përfundime për (pa) parashikimin e karakterit të një lufte të ardhshme

Për të mbizotëruar në konfliktet e mundshme të ardhshme, Ushtria duhet të bëjë plane të llogaritura për karakterin e atyre konflikteve. Nëse vizioni ynë turbullohet nga një fokusim i verbër vetëm në teknologji, ne do ta lexojmë gabim të ardhmen me pasoja potencialisht katastrofike. Përpara se një theksim i tepërt i teknologjisë të fillonte të mjegullonte mendimin tonë në mesin e shekullit të 20-të, Ushtria kishte nxjerrë liderë si Grant dhe Scott të cilët e perceptonin qartë karakterin e luftërave që bënin, zhvilluan një strategji efektive për dinamikën e atyre luftërave dhe përshtati ushtrinë për të fituar. Me analizën e duhur për të ekzaminuar paparashikueshmërinë e çdo lufte , ne mund ta kthejmë atë në planifikim për një luftë të mundshme të ardhme.

Duke vëzhguar se si lufta Ruso-Ukrainase është e zhytur në një fushatë rraskapitjeje, një numër analistësh kanë bërë thirrje që Shtetet e Bashkuara të përgatiten për luftëra të zgjatura të mobilizimit masiv kundër Rusisë ose Kinës. Këta autorë supozojnë se një luftë e tillë do të ngjasonte me luftërat totale të Luftës së Parë ose të Dytë Botërore, por karakteri i një lufte të ardhshme nuk do të jetë si luftërat totale të shekullit të 20-të. Ashtu si lufta Ruso-Ukrainase ka qenë e kufizuar, një luftë e ardhshme me Rusinë mbi Baltikun ose Kinën për Tajvanin gjithashtu do të ishte e kufizuar. Një luftë e tillë do të ndante një sërë ngjashmërish politike si me luftërat evropiane të shekullit të 18-të ashtu edhe me luftën koreane.

- Armët bërthamore do të vazhdojnë të kufizojnë luftën. Si në Luftën Koreane ashtu edhe në Luftën Ruso-Ukrainase, armët bërthamore po e zbusin përshkallëzimin. Nëse Shtetet e Bashkuara do të hynin në luftë me Kinën ose Rusinë, të dyja palët do të zhvillonin një kërcim të rrezikshëm dhe koreografik të ngushtë për të luftuar në një mënyrë që nuk rrezikon një përgjigje bërthamore. Ashtu si në Kore, të dyja palët ka të ngjarë ta mbanin konfliktin të kufizuar në terrenin e kontestuar. Sulmet me rreze të gjatë kundër atdheut armik do të ishin shumë të rrezikshme. Kundërshtari nuk mund ta dinte nëse municionet e ardhura ishin konvencionale apo bërthamore - gjë që duhet të na bëjë të rishqyrtojmë investimet në goditje me precizion me rreze të gjatë.

- Si monarkitë në Evropën e shekullit të 18-të, autoritarët e sotëm janë të shqetësuar kryesisht për ruajtjen e rendit politik. Ashtu si në regjimin *e vjetër,* diktatorët modernë i frikësohen një popullsie politikisht aktive. Siç shihet me Rusinë, kundërshtarët tanë do të dëshironin të luftonin një luftë të kufizuar që nuk përpiqet të mobilizojë popullsinë ose të nxjerrë taksa tepër të rënda. Kina dhe Rusia bashkëkohore nuk janë regjime totalitare të mesit të shekullit të 20-të, të cilat mblodhën popullsinë e tyre në një zjarr fanatik. Në vend të kësaj, ata kanë qetësuar popullsinë e tyre përmes premtimeve për stabilitet dhe rritje ekonomike në këmbim të rendit politik.

- Ashtu si ato fuqi të shekullit të 18-të, Kina dhe Rusia kanë reformuar ushtritë e tyre drejt forcave të vogla dhe profesionale të optimizuara për të luftuar luftëra të kufizuara. Një shekull më parë, shtetet mbanin miliona rezervistë të cilët mund t›i mobilizonin, t›i dorëzonin pushkët dhe t›i vinin trenat për në front. Vendet sot nuk mbajnë sisteme të tilla për mobilizim masiv dhe forcat moderne kërkojnë shumë më tepër investime për të qenë efektive në betejë. Pas humbjeve të saj fillestare në Ukrainë, Rusia ka luftuar me cilësinë e forcës së saj, ka zbrazur burgjet e saj për fuqi punëtore dhe është drejtuar drejt tërheqjes së tankeve të kategorisë muzeale nga një rezervë në rënie e pajisjeve sovjetike.

- Luftërat ka të ngjarë të jenë të kufizuara; Ne marrim një tregues për këtë kur vërejmë se Rusia dhe Kina kanë ambicie të kufizuara territoriale. Kur luftërat janë për qëllime të kufizuara, armiqtë në përgjithësi do të mobilizojnë vetëm mjete të kufizuara. Siç vërejti Clausewitz, "Nëse politika drejtohet vetëm drejt objektivave të vogla, emocionet e masave do të trazohen më pak". Rusia synon të rimarrë tokat e humbura "ruse". Kina kërkon t'i japë fund përfundimisht luftës së saj civile duke pushtuar Tajvanin. Këto nuk janë regjimet fashiste të shekullit të 21-të me vizione të riformësimit të botës përmes pushtimit. Epoka e ndërtimit të perandorive ka kaluar prej kohësh. Normat ndërkombëtare tani respektojnë sovranitetin kombëtar. Vendet janë bërë të vështira për t›u gëlltitur me fuqinë e provuar të kryengritjes. Edhe nëse një pushtim do të kishte sukses, do të kishte pak vlerë të shtuar. Fuqia e një vendi nuk mbështetet më shumë në kapjen e territorit, popullsisë apo burimeve natyrore.

- Nëse do të fillonin një konflikt, Rusia dhe Kina do të fillonin një sulm vetëm kur mendonin se mund të arrinin befasi strategjike. Me mbikëqyrjen moderne, do të ishte e vështirë për ta të mobilizonin një forcë të madhe të pazbuluar; kështu, kundërshtarët tanë ka të ngjarë të përdorin një forcë të kufizuar. Që nga Lufta e Dytë Botërore, gjatë ndërhyrjeve në Ukrainë, Gjeorgji, Kosovë, Çeçeni, Afganistan dhe Çekosllovaki, Rusia ka përdorur forca të kufizuara që mbështeten "në elan, befasi dhe gatishmëri për të bërë blof". Për të pushtuar Tajvanin, Kina do të kufizohej nga anijet e saj zbarkuese amfibe, me një

analizë që vlerëson se ato kanë një kapacitet prej vetëm 20,000 trupash.

- Për të penguar në mënyrë të besueshme dhe, nëse është e nevojshme, për të mposhtur një sulm të tillë, Shtetet e Bashkuara duhet të jenë të gatshme për të kryer një strategji asgjësimi. Ajo duhet të përgatitet për të mposhtur me vendosmëri forcat e kufizuara të përfshira në një *fakt të kryer* përpara se ato të mund të nguliten. Ukraina kishte një mundësi të tillë në mars dhe prill të 2022, por asaj i mungonin aftësitë për ta bërë këtë. Me përgatitjen, trajnimin dhe doktrinën e duhur, Shtetet e Bashkuara dhe partnerët e tyre mund të zbehin një sulm rus në Baltik. Linja e Mbrojtjes Baltike, me qindra bunkerë dhe mina të grumbulluara, është një hap i saktë drejt mohimit të Rusisë për mundësinë e një *fakti të kryer*. Në mënyrë të ngjashme, Tajvani, me strategjinë e tij është në rrugën e duhur për t'u bërë i vështirë për Kina që ta gëlltisë lehtë. Ajo po ndjek aftësitë asimetrike për të mposhtur një ulje amfibe kineze. Ne duhet t'i përforcojmë këto përpjekje.

- Ukraina shfaq rreziqet e një strategjie lodhje dhe rraskapitjeje. Nëse ajo ndjek rraskapitjen, Shtetet e Bashkuara rrezikojnë një luftë të zgjatur, të përgjakshme, të pa fituara dhe një përshkallëzim të mundshëm bërthamor. Për më tepër, Shtetet e Bashkuara nuk janë të vendosura për të ndjekur një strategji rraskapitjeje. Ajo ka një numër minimal rezervash individuale të gatshme për t'u mobilizuar si zëvendësim për humbjet luftarake, baza e saj industriale nuk mund të kalojë lehtësisht në prodhimin e armatimeve dhe popullsia e saj është e ndarë politikisht dhe mund të ketë angazhim të kufizuar ndaj luftërave jashtë vendit.

- Në një luftë të ardhshme, veçanërisht duke marrë parasysh kontekstin e saj të mundshëm të kufizuar, Shtetet e Bashkuara do ta kishin të vështirë të ndiqnin një strategji rraskapitjeje kundër Rusisë ose Kinës. Siç ka treguar ndikimi i kufizuar i sanksioneve ndaj Rusisë, fuqitë e mëdha kontinentale janë të vështira për t'u bllokuar ekonomikisht. Njëkohësisht, siç kanë treguar sulmet e Rusisë ndaj Ukrainës, sulmet strategjike jo-bërthamore nuk mund të degradojnë në mënyrë vendimtare aftësinë e një vendi për të zhvilluar luftë ose vullnetin e popullsisë së tij për të luftuar.

- Një strategji rraskapitjeje luan gjithashtu në pikat e forta të perceptuara të Rusisë. Vladimir Putin, dhe ultranacionalistët që kanë ardhur për të ndikuar në të menduarit e tij, besojnë se forca e Rusisë vjen nga, "kapaciteti i saj për vuajtje". Putini nuk ndjen keqardhje për dërgimin e mijëra ushtarëve rusë në vdekje në sulme të pashpresë për të rraskapitur mbrojtësit ukrainas. Putini e ka heshtur kundërshtimin ndaj luftës dhe ndjen pak presion për të pushuar luftimet edhe tani që në SHBA është presidenti Trump. Perceptimi i tij se Rusia mund të durojë më gjatë se armiqtë e saj në një konflikt, do të thotë se ai nuk do të pengohet nga një strategji rraskapitjeje, por përkundrazi do ta shohë atë si një mundësi për të shfrytëzuar atë që ai e percepton si pikat e forta të Rusisë.

Literatura e shfrytëzuar:

1. John Nisser, "Konceptualizimi i refuzimit doktrinar: një krahasim midis Mbrojtjes Aktive dhe Betejës Ajrore", *Studime të Mbrojtjes*, 23 nr. 2 (2023), 280. https://doi.org/10.1080/14702436.2022.2132232 .
2. *Joint Force Quarterly* 110 (korrik 2023), https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-110/Article/article/3447159/strategic-inflection-point-the-most-historically-significant-and-fundamental-ch/ .
3. James Rainey dhe Laura Potter, "Delivering the Army of 2030", *War on the Rocks* , 6 gusht 2023. https://warontherocks.com/2023/08/delivering-the-army-of-2030/ .
4. Robert Rose, "Biting Off What It Can Chew: Ukraine Understands It Attritional Context," *War on the Rocks*, 26 shtator 2023. https://www.nytimes.com/2012/10/12/world/panetta-warns-of-rreth-kërcënimi-of-cyberattack.html
5. FM 3-0, *Operacionet* (Uashington, DC: Zyra e shtypit e qeverisë së SHBA, tetor 2022), ix, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000 -web-2.pdf .
6. Grace B. Mueller et al., "Operacionet kibernetike gjatë Luftës Ruso-Ukrainase nga modele të çuditshme në të ardhme alternative", Qendra për Studime Strategjike dhe Ndërkombëtare, 13 korrik 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-07/230713_Mueller_CyberOps_RussiaUkraine.pdf .
7. Brad Smith, "Mbrojtja e Ukrainës: Mësime të hershme nga Lufta Kibernetike", *Microsoft On the Issues* , 22 qershor 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending -Ukrainë-mësimet-e-hershme-nga-lufta-kibernetike/ .
8. Robert G. Rose, "All Power is Local", *Military Review*, janar–shkurt 2023,https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JF-23 /Rose/rose-all-power-is-local-v1.pdf .
9. Anton Troianovski, "Rusia e merr censurën në ekstreme të reja, duke mbytur mbulimin e luftës", *New York Times* , 4 mars 2022. https://www.nytimes.com/2022/03/04/world/europe/russia-censorship -media-crackdown.html.
10. Anne Applebaum, "Putin is Caught in His Own Trap", *The Atlantic*, 25 qershor 2023, https://www.theatlantic.com/ideas/archive/2023/06/putin-caught-in-his-own -kurth/674524/ .

11. "Sulmet e dronëve ukrainas mbi rafineritë dhe infrastrukturën ruse të naftës", *Reuters*, 18 qershor 2024, https://www.reuters.com/world/europe/ukrainian-drone-attacks-russian-oil-refineries-infrastructure-2024 -06-18/

12. Mark Galeotti, *Luftërat e Putinit* (Nju Jork, NY: Osprey Publishing, 2022), 77.

13. Joel Wuthnow et al., *Kalimi i ngushticës: Ushtria e Kinës përgatitet për luftë me Tajvanin* (Washington, DC: National Defense University Press, 2022), 175, https://ndupress.ndu.edu/Portals/68/Documents /Books/crossing-the-strait/crossing-the-strait.pdf .

14. Michael C. DiCianna, "Baltikët për të luftuar Rusinë nga milja e parë", Qendra për Analizën e Politikave Evropiane, 19 mars 2024, https://cepa.org/article/baltics-to-fight-russia-from-the -milje e parë/ .

15. James O. Ellis Jr. dhe James Timbie , "Një numër i madh gjërash të vogla: një strategji porcupine për Tajvanin», *Rishikimi i Sigurisë Kombëtare të Teksasit* 5, nr. 1 (Winter 2021/2022), https://tnsr.org/2021/12/a-large-number-of-small-things-a-porcupine-strategy-for-taiwan/#article .

16. Yuriy Gorodnichenko , Iikka Korhonen dhe Elina Ribakova , "Ekonomia ruse në një bazë lufte: Një realitet i ri i financuar nga eksportet e mallrave," *Qendra për Kërkimin e Politikave Ekonomike*, 24 maj 2024, https://cepr.org/voxeu/columns/russian-economy-war-footing- re-reality-finance-commodity-exports .

17. Amos Fox, "Manovra është e vdekur? Kuptimi i kushteve dhe komponentëve të luftimeve, "*Royal United Services Institute*, 11 Prill 2022),https://rusi.org/explore-our-research/publications/rusi-journal/manoeuvre-dead-understanding-conditions-and-components -luftim .

18. Stephen Biddle, "Si Rusia ndaloi momentin e Ukrainës: Një mbrojtje e thellë është e vështirë të mposhtet," *Foreign Affairs*, 29 janar 2024, https://www.foreignaffairs.com/ukraine/how-russia-stopped-ukraines-momentum .

19. Paul Sonne et al., "Beteja për Kievin: trimëria ukrainase, gabimet ruse të kombinuara për të shpëtuar kryeqytetin", *Washington Post*, 24 gusht 2024. https://www.washingtonpost.com/national-security/interactive/2022/kyiv-battle-ukraine-survival/.

20. Robert G. Rose, "Biting Off What It Can Chew: Ukraine Understands It Attritional Context", *War on the Rocks*, 26 shtator 2023, https://warontherocks.com/2023/09/biting-off-what- ajo-mund-përtypet-ukraina-kupton-kontekstin e saj-lidhjes/.

21. Mykhaylo Zabrodskyi et al., "Mësime paraprake në luftimet konvencionale

nga pushtimi rus i Ukrainës", *Instituti Mbretëror i Shërbimeve të Bashkuara*, nëntor 2022, https://www.rusi.org/explore-our-research/publications/special- burimet/mësimet-preliminare-konvencionale-lufta luftarake-rusia-pushtimi-ukrainë-shkurt-korrik-2022

22. John B. Bradley III, "Fires," në *A Call to Action: Lessons from Ukraine for the Future Force* , eds. John A. Nagl dhe Katie Crombe (Carlisle Barracks, PA: United States Army War College Press, 2024), 101, https://press.armywarcollege.edu/monographs/968/

23. Robert G. Rose, "Parandalimi i një kërcimi të shkurtër nëpër një kanal të gjerë: Përqafimi i plotë i komandës së misionit për të shmangur një fatkeqësi me shumë domene", *Rishikimi Ushtarak* , Mars–Prill 2022, https://www.armyupress.army.mil/Journals/Military-Revieë/English-Edition-Archives/Mars-April-2022/Rose/

24. Andrey J. Forney, "Davy Crockett dhe Boy Scouts: Lufta Koreane dhe Keqmenaxhimi i Konfliktit të Zgjatur" *Rishikimi i Sigurisë Kombëtare të Teksasit* 8, nr. 1 (Winter 2024/2025), https://tnsr.org/2024/10/davy-crockett-and-the-boy-scouts-the-korean-war-and-mismanaging-protracted-conflict/

NDRYSHIMET KLIMATIKE NË SIGURINË E ALEANCËS DHE ALEATËVE TË SAJ

Nënkolonel Dr. Fitim KARASANI
Pedagog në AFA
Dr. Edlira TITINI
Pedagoge në AFA

Trajtesë e shkurtuar

Situata aktuale ka krijuar një akumulim sfidash dhe kërcënimesh të cilat shtrihen nga dimensioni klasik i ri i aktualizimit të mbrojtjes ushtarake të integritetit territorial, deri në ndryshime klimatike e rreziqe të tjera. Ndërthurja e kërcënimeve konvencionale me ato jo konvencionale ka ndryshuar konceptin e marrjes së masave për të qenë i sigurt, pasi kërkon edhe trajtimin e të ashtuquajturve kërcënime të padukshme, siç janë ndryshimet klimatike. Si kërcënime të tilla, ato sjellin me vete një paparashikueshmëri të lartë, vështirësi objektive për përballimin e tyre në nivel kombëtar e më gjerë, duke u klasifikuar si sfida të reja për sigurinë.

NATO ka ndërgjegjësuar rritjen e ndikimit të ndryshimeve klimatike në siguri dhe ka ndërmarrë hapa konkretë për t'iu përgjigjur kësaj sfide. Ajo adoptoi Planin e Veprimtarisë për Ndryshimet Klimatike dhe Sigurinë, që përfshin qëllime dhe veprime për të përfshirë ndryshimet klimatike në agjendën politike dhe ushtarake. Në raportet dhe dokumentet e NATO-s theksohet ndikimi domethënës që ndryshimet klimatike kanë për sigurinë e aleatëve, si pjesë përbërëse tashmë e mjedisit kompleks.

Ndryshimet klimatike, krahas ndikimeve të saj në paqëndrueshmërinë e zhvillimit ekonomik të vendeve, stabilitetit politik, cenimit të sigurisë njerëzore

e më gjerë, gama e ndikimit së saj prek edhe vetë detyrat e aleancës. Forcat e saj operacionale, mjetet apo instalimet ushtarake të aleancës janë nën trysninë e vazhdueshme të ndryshimeve klimatike, si në periudhën përgatitore të tyre, ashtu edhe gjatë realizimit të misionit.

Fjalë kyçe: ndryshim klimatik, mjedis sigurie, mjedis operacional, aleancë, kërcënim.

Hyrje

Tashmë, mjedisi strategjik karakterizohet nga një kompleksitet në rritje dhe një nivel parashikueshmërie në ulje. Rreziqet e tanishme ndaj sigurisë kombëtare janë më të ndërlikuara dhe të ndërvarura se në të kaluarën. Ato ndërthurin kërcënimet tradicionale konvencionale dhe ato jokonvencionale. Alan Collins[1] specifikon që, krahas masave dhe parashikimeve për mbrojtjen e shtetasve, sistemit politik, ekonomik etj., duhet të fokusohemi edhe te "*kërcënimet e padukshme, si ndryshimet klimatike"*[2].

Sikurse fusha më e gjerë e studimeve të sigurisë, qasjet ndaj ndryshimeve klimatike janë diverse dhe reflektojnë disa perspektiva teorike. Perceptimi i sigurisë për vende të ndryshme ka natyra të ndryshme. Vendet e zhvilluara, krahas sigurisë klasike të rigjallëruar së fundmi, kanë edhe rritjen e vazhdueshme të sigurisë ekonomike për të mbështetur një zhvillim të qëndrueshëm. Vendet që janë në zhvillim po përdorin gjithnjë e më shumë burimet e tyre natyrore për mbështetjen e zhvillimit ekonomik. Këto mënyra veprimi ndikojnë direkt në atë që tashmë e quajmë ndryshime klimatike, të cilat, në mënyrë të drejtpërdrejtë, të çojnë në kërcënime për shkak të ndryshimit të variablave natyrorë.

Studimet mbi ndryshimet klimatike kanë evoluar gjatë 30 viteve të fundit dhe roli i kësaj sigurie është rritur përherë e më shumë. Domethënia e saj ka të bëjë me kushtet e jashtme që rrethojnë një entitet dhe shtrin efektin e saj jashtë integritetit territorial të një vendi. Kjo do të thotë që grupe vendesh me probleme të ngjashme nuk mund të arrijnë dot objektivat përkatës në mënyrë të njëanshme, reagimi kërkon përgjigje multilaterale. Ky është shpjegimi i shumë takimeve dhe traktateve rajonale apo globale, i koncepteve strategjikë të aleancës, i strategjive të sigurisë kombëtare, ushtarake apo sektoriale.

Shqetësimet legjitime në disa raste janë anashkaluar, duke mos marrë parasysh se për shumë prej tyre ndryshimet klimatike përbëjnë kërcënim për sigurinë. Në tërësi, sigurimi i ekosisteme të shëndetshme e të qëndrueshme, në mbështetje

[1] Alan Collins, profesor i shkencave politike në Universitetin e Wellsit.

[2] Collins, Alan. *Escaping a Security Dilemma: anarchy, certainty and embedded norms Inter national Politics*, 2014 faqe 176.

të jetës së gjallë, mund të sjellë si pasojë që gjeneratat e sotme dhe ato të ardhshme të përballen me probleme që eventualisht mund të jenë burim konfliktesh në nivelin global, rajonal apo kombëtar. Kanë ekzistuar një sërë përpjekjesh për të vlerësuar shkallën në të cilën ndryshimet klimatike ndikojnë në shkaktimin e konflikteve të dhunshme brenda dhe midis shteteve. Ka shpjegime të ndryshme rreth mënyrave në të cilat ndryshimet klimatike mund të dobësojnë sigurinë kombëtare. Vërehet një rritje e vëmendjes kërkimore për lidhjet midis ndryshimeve klimatike/sigurisë mjedisore dhe çështjeve të zhvillimit, si varfëria dhe siguria njerëzore. Këto përsiatje kërkimore kanë influencuar zhvillimet politike në disa vende dhe në organizata ndërkombëtare.

Ndryshimet klimatike mund të kërcënojnë elementet bazë të sigurisë si: sigurinë e ushqimit dhe shëndetin e njeriut; stabilitetin e shteteve duke ngadalësuar ose përmbysur zhvillimin; rritjen e gjasave të konfliktit të brendshëm për shkak të migracionit; zhdukjen e territorit si një çështje të sovranitetit; konfliktin ndërkombëtar mbi burimet e përbashkëta, etj. Në aspektin e forcave të armatosura (FA), siç do e trajtojmë në vazhdimësi të këtij shkrimi, ato po shndërrohen në një kërcënim ndaj të cilit nëse nuk trajtohen që tashmë me frekuencën e duhur, pasojat e saj do të ndikojnë në realizimin e misionit apo detyrave specifike të tyre.

Ndryshimet klimatike dhe mjedisi sigurisë i NATO-s

Ndryshimet klimatike janë një sfidë përcaktuese me ndikim të thellë në sigurinë e aleancës. Në samitin e vitit 2021 në Bruksel, krerët e shteteve dhe qeverive të NATO-s (HOSG)[3] miratuan një Plan Veprimi për Ndryshimin e Klimës dhe Sigurinë, duke rënë dakord se NATO duhet të synojë të bëhet organizata kryesore kur bëhet fjalë për të kuptuar dhe përshtatur me ndikimin e ndryshimeve klimatike mbi sigurinë. Në vija të përgjithshme, ndryshimet klimatike paraqesin rrezikshmërinë e tyre në mjedisin strategjik të NATO-s, në asetet dhe instalimet ushtarake, në operacionet, si dhe në përgatitjen e forcave të vendeve anëtare të NATO-s. Në këtë fushë janë disa organizma të cilët bëjnë studimet përkatëse në NATO, si: Autoriteti Ushtarak i NATO-s (NMA-s)[4], Qendra e Shkencës dhe Teknologjisë për Kërkimin dhe Eksperimentimin Detar (STOCMRE),[5] si dhe Qendra e Ndryshimeve Klimatike për Sigurinë (CCASCOE)[6].

---

[3] Heads of State and Government.

[4] NATO Military Authorities.

[5] NATO Science & Technology Organization Centre for Maritime Research and Experimentation.

[6] Climate Change and Security Centre of Excellence. Kjo qendër ka në mision të saj që të jetë një qendër ekselence e njohur ndërkombëtarisht mbi ndryshimet klimatike dhe sigurinë për ekspertët ushtarakë, civilë dhe vendimmarrësit.

Kontributi i mekanizmave të mësipërm ndjehet në Konceptin Strategjik të NATO-s 2022, ku në parathënien e tij përcakton "*rëndësinë ndërsektoriale të investimit në inovacionin teknologjik dhe integrimin e ndryshimeve klimatike*"[7], për të garantuar qëndrueshmërinë kombëtare dhe kolektive duke mbështetur përpjekjet e aleancës për të mbrojtur kombet dhe shoqëritë e aleatëve, paqes dhe të sigurisë. Për të përmbushur detyrat kryesore të Aleancës, koncepti thekson se "*Ne do të promovojmë ....integrimin e ndryshimeve klimatike"*[8] në të gjitha detyrat tona. Gjatë vitit të kaluar, njësitë/strukturat e klimës të cilat informojnë në vazhdimësi NATO-n, paraqesin si shumë problematike faktin e shpejtësisë dhe shkallës të ndryshimeve klimatike.[9] Në mënyrë të ngjashme, janë zhvilluar vëzhgime mbi humbjen e akullit të Arktikut, rritjen e nivelit të ujit, degradimin e tokës, pakësimin e disponueshmërisë së ujit të freskët, si dhe mbi rritjen e numrit të ditëve jashtëzakonisht të nxehta[10].

Mjedisi i sigurisë në kufijtë lindorë dhe jugorë të NATO-s është shoqëruar me ndryshueshmëri në rritje ku, krahas ndikimeve të tjera, dy ishin më domethënës: i ashtuquajturi Operacion Special ndaj Ukrainës nga Rusia, i cili po shoqërohet me pasoja shkatërruese humanitare, sociale, ekonomike dhe mjedisore; dhe shpërthimi i konfliktit në Lindjen e Mesme. Përpos këtyre konflikteve të armatosura, NATO po përballet me konkurrencën në rritje të shteteve autoritare duke përfshirë edhe Kinën. Sfidat "*jo tradicionale të sigurisë dhe ndryshimet klimatike po testojnë gjithnjë e më shumë elasticitetin e NATO-s, me efekte të përshkallëzuara në sigurinë dhe mbrojtjen e aleatëve në nivelet strategjike, operacionale dhe taktike*"[11].

Për aleatët e NATO-s, ndikimi i rritjes së temperaturave të ajrit dhe ujit të deteve konstatohet lehtësisht në ngjarjet ekstreme të motit: përmbytjet katastrofike dhe zjarret shkatërruan zona të mëdha të Evropës dhe Amerikës së Veriut, duke rezultuar në dëme të rënda ekonomike. Këto dhe të tjera ngjarje të tilla ekstreme të motit kanë bërë presion mbi infrastrukturën kritike ushtarake dhe atë civile dhe kanë kërkuar forca ushtarake shtesë për të mbështetur autoritetet civile. Duke parë përpara, forcave ushtarake të aleancës do t'u kërkohet të përshtaten me mjedise operative gjithnjë e më sfiduese, ekstreme dhe të paparashikueshme, si dhe të përgatiten për një kërkesë në rritje për të ndihmuar autoritetet civile.

---

[7] NATO 2022 - Strategic Concept, page 1.

[8] Po këtu, faqe 3.

[9] Sipas Organizatës Botërore Meteorologjike, viti 2023 ishte viti më i nxehtë, ndërsa periudha 2015-2023 kanë qenë vitet më të ngrohta të regjistruar mbi të dhënat 174-vjeçare. Homepage |World Meteorological Organization WMO.

[10] Akulli i Groenlandës po humbet më shumë seç mendohej më parë. Niveli i detit është rritur me 9.4 cm që nga viti 1993. Home | UNCCD, "*The Global Land Outlook - Second Edition*," April 27, 2022

[11] Timothy Clack, Z., *Climate Change, Conflict and (In)Security | Hot War.*

Kjo prirje duket që tashmë do të jetë në rritje për FA-të, duke pasur parasysh frekuencën në rritje të ngjarjeve ekstreme dhe pasigurinë lidhur me shtrirjen e ndikimeve të ardhshme. Përveç ndikimeve të mësipërme të ndryshimeve klimatike, FA duhet të jenë të përgatitura edhe për pasojat indirekte të ndryshimeve klimatike si të atyre që ndodhin brenda territorit të aleancës dhe të atyre në kufijtë e jashtëm të saj. Edhe pse marrëdhënia në mes konfliktit të armatosur dhe ndryshimeve klimatike është komplekse, kjo e fundit ka potencialin të kontribuojë për një nivel më të lartë konflikti, paqëndrueshmërie dhe dhune, me anë të pasojave indirekte të saj. Pasoja të tilla si: paqëndrueshmëria e shkaktuar nga klima, lëvizjet në shkallë të gjerë të popullsisë nga ndërprerja e zinxhirëve të furnizimit global ka të ngjarë të ndryshojë mjedisin strategjik në afatmesëm dhe afatgjatë. Ndryshimet e papritura të rrymave oqeanike ose kolapsi që mund të shkaktohet në prodhimet bujqësore, mund të ushqejë një përshkallëzim të shpejtë të paqëndrueshmërisë dhe zhvendosjes në rajonet që tashmë përjetojnë një stres klimatik.

Ka dallime të rëndësishme rajonale në vulnerabilitetin e klimës. Rajonet e Lindjes së Mesme, Afrikës së Veriut dhe Sahelit[12] janë shfaqur si pika të nxehta të ndryshimit të klimës. Vendet e Sahelit janë veçanërisht të prekshme, për shkak të kushteve ekstreme klimatike dhe të një varësie të lartë nga bujqësia dhe blegtoria, gërshetuar kjo edhe me pamundësinë e adoptimit të tyre, për shkak të kostove të papërballueshme për ekonominë e këtyre vendeve. Koncepti strategjik i NATO-s 2022 evidenton se "*konflikti, brishtësia dhe paqëndrueshmëria në Afrikë dhe Lindjen e Mesme ndikojnë drejtpërdrejt në sigurinë tonë dhe në sigurinë e partnerëve tanë*[13]".

Ndikimet rajonale të ndryshimeve klimatike do të ndihen gjithnjë e më shumë edhe në rajonin e Indo-Paqësorit. Nga rritja e rrezikut të zjarreve në vende si Australia dhe Zelanda e Re, deri te ngjarjet ekstreme të motit dhe rritja e nivelit të detit që prekin vendet ishullore, ndryshimet klimatike përbëjnë tashmë një kërcënim të madh për sigurinë dhe mirëqenien e banorëve të indo-paqësorit. Ndryshimi i klimës ndikon shumë në mjedisin operacional dhe strategjik në zonën veriore, pasi "*Arktiku po ndjen,* më shumë se kudo në botë, të tilla ndryshime, duke *impaktuar* në mjedis, komunitet lokal dhe në sigurinë e rajonit"[14]. Ndryshimi i klimës po përkeqëson konkurrencën strategjike.

---

[12] Vendet e Sahelit përfshijnë një rajon të gjerë në Afrikë që shtrihet nga Oqeani Atlantik në Perëndim deri në Detin e Kuq në Lindje, si: Burkina Faso, Kamerun, Çad, Eritrea, Gambia, Guineja, Mali, Mauritania, Senegal, Sudan etj.

[13] NATO 2022 - Strategic Concept , pika11, p. 4.

[14] Rachael Gosnell and Joseph Thomas, *European Security Seminar North: A Cooperative Future; Opportunities for the Arctic - 7*, GCMC, September 23, 2023.

Mungesa e burimeve dhe përpjekja globale për të "*përdorur*" këto pritet të intensifikohen dhe të nxisin paqëndrueshmëri të mëtejshme, konkurrencë dhe konflikt, me pasoja të tërthorta për elasticitetin rajonal, sigurinë dhe për operacionet e NATO-s. Paqëndrueshmëria dhe konflikti përkeqësojnë në mënyrë graduale sigurinë njerëzore, konsideracionet për paqen dhe sigurinë, duke i sjellë ato në ballë të diskutimit të sigurisë klimatike.

Kundërshtarët e mundshëm dhe konkurrentët strategjikë të NATO-s po shfrytëzojnë edhe këtë kërcënim global kundër saj. Kjo është e dukshme në rritjen e dezinformimit lidhur me klimën, duke ulur në këtë mënyrë si reagimin publik ashtu dhe vullnetin politik që është i nevojshëm për një veprim më ambicioz ndaj ndryshimeve klimatike. Ndryshimi i klimës jo vetëm që do të ndikojë në sigurinë e aleatëve të NATO-s por edhe të Rusisë dhe konkurrentëve strategjikë si Kina. Kapaciteti adaptues i Rusisë dhe Kinës dhe përgjigjet e mundshme ndaj një bote që ngrohet, përfshirë edhe FA, janë konsiderata të rëndësishme për planifikuesit e sigurisë dhe mbrojtjes në të gjithë NATO-n.

Sa i përket Rusisë, efektet e ndryshimit të klimës kanë qenë veçanërisht të dukshme në zonat e saj të Arktikut dhe zonat bujqësore të jugut të saj dhe përfshijnë "*zonat me ngrirje të përhershme, rritjen e përmbytjeve, thatësirë të zgjatur, valët e të nxehtit, si dhe një numër në rritje të fatkeqësive natyrore*"[15]. Kushtet ekstreme mjedisore mund të ndikojnë negativisht në shëndetin e popullsisë dhe produktivitetin e punës, të nxisin migrimin dhe zhvendosjen, të prishin ofrimin e shërbimeve thelbësore dhe të përkeqësojnë kushtet e jetesës në përgjithësi. Këto sfida të brendshme mund të ndikojnë në marrjen e vendimeve të politikës së jashtme dhe të sigurisë. Megjithëse Rusia pranon se ngrohja globale paraqet një problem serioz, reagimi i saj ndaj ndryshimeve klimatike deri më sot është bazuar në një peshim të kujdesshëm të kostove dhe përfitimeve. Fokusi ka qenë "*në përshtatjen me ndikimet fizike të ndryshimeve klimatike, në vend të strategjive të zbutjes që trajtojnë shkaqet rrënjësore*"[16].

Mendojmë që përshtatja e FA-ve ruse është më konstatuese te forcat që ajo ka dislokuar në Arktik, duke zhvilluar aftësi të konsiderueshme për të mbështetur operacionet ushtarake në zonat e largëta të mbuluara me akull. Kina "*përballet me kërcënime nga rritja e nivelit të detit, ngjarjet ekstreme të motit, intensifikimi i valëve të nxehtësisë dhe thatësirës, të lëvizjes së popullsisë dhe shkrirjes së akujve*"[17]. Përveç ndikimeve të mundshme ekonomike dhe socio-politike në të

[15] Thane Gustafson, *Klimat: Russia in the Age of Climate Change*, Harvard University Press, 2021, ISBN 9780674247437

[16] Bobo Lo, *The Adaptation Game: Russia and Climate Change*, pdf. The French Institute of International Relations, March 2021.

[17] Erin Sikorsky, China's Climate Security Vulnerabilities, Center for Climate and Security, Council on Strategic Risks, November 2022, p. 9.

gjithë vendin, efektet e ndryshimeve klimatike në Kinë mund të kenë pasoja për pjesën tjetër të globit. Ndërsa ndryshimet klimatike ndikojnë gjithnjë e më shumë në sistemet ushqimore globale, disa vende (përfshirë edhe Kinën) po punojnë për të blerë sasi të mëdha të tokës bujqësore jashtë vendit, si dhe për të zhvilluar korridore të efektshme tregtare. Prodhimi bujqësor i Kinës luan një rol kritik në zinxhirin botëror të furnizimit dhe çdo ndikim thelbësor i klimës në të do të ketë pasoja globale, pasi Kina ushqen rreth 20% të popullsisë globale.[18] Në drejtim të FA-ve, raportet e kufizuara sugjerojnë "*përmirësime të efektshmërisë së energjisë dhe përdorim alternativ të karburantit, si dhe zhvillimin e aftësive që mund të ofrojnë njëkohësisht lehtësim nga katastrofat, duke ruajtur gatishmërinë ushtarake*"[19].

Ndikimi i ndryshimeve klimatike në operacionalitetin e NATO-s

Rreziqet e ndryshimit të klimës përbëjnë një stres operacional në rritje mbi personelin ushtarak. Ndikimet e drejtpërdrejta shëndetësore përfshijnë një incidencë në rritje nga ndryshimet klimatike, që mund të kufizojnë trajnimin dhe operacionet. Ndikimet indirekte variojnë nga efektet psikologjike mbi ushtarët që reagojnë ndaj katastrofave natyrore deri në një kurbë më të lartë të sëmundjeve infektive në kontekste të ndryshme operative. Rreziqet e dukshme përfshijnë problematikën mbi zinxhirët e furnizimit; qasje më të pakta ndaj ujit të freskët; dhe një frekuencë më të lartë të ndërhyrjeve mjekësore që kryhen në kushte ekstreme mjedisore.

Rreziqet e drejtpërdrejta, që lidhen me ndryshimet klimatike, ka të ngjarë të ndikojnë në pajisjet ushtarake dhe sistemet e armëve, mjetet e blinduara dhe ato të pa blinduara, avionët luftarakë dhe ato të transportit, anijet sipërfaqësore dhe ato nënujore, pajisjet mbrojtëse, armatimin dhe municionin, etj. Krahas armatimit në përgjithësi, instalimet e ndryshme ushtarake, si dhe zonat e trajnimit janë gjithashtu të prekshme ndaj efekteve të ndryshimeve klimatike. Këto ndikime janë të ndryshme sipas zonave të ndryshme gjeografike. Kështu, strukturat ushtarake në gjerësitë më veriore të NATO-s janë në rrezik nga shkrirja e sipërfaqeve të tokës që kanë qenë historikisht të ngrira, e cila komprometon integritetin strukturor, ndërsa zonat e ulëta në Evropë përballen me rrezik në rritje të përmbytjeve. Në Jug të Aleancës, forcat dhe instalimet e gjejnë veten në rrezik nga nxehtësia ekstreme. Rreziqet e ndryshimit të klimës të çojnë në kosto më të larta të mirëmbajtjes dhe riparimit, përbëjnë rrezik për sigurinë e personelit ushtarak dhe në fund, të ndikojnë në operacionalitetin dhe gatishmërinë e forcave.

---

[18] Sipas UN (World Population Prospects 2024). Popullsia e Kinës është rreth 1.4 miliard njerëz, janar 2025.

[19] Michael Brzoska, Climate Change and the Military in China, Russia, the United Kingdom, and the United States, Bulletin of the Atomic Scientists 68, no. 2 March 2012.

Për të parandaluar dhe reaguar në mënyrë efektive ndaj krizave që mund të ndikojnë në sigurinë e aleatëve, është vendimtare të ruhet aftësia ushtarake për të kryer një gamë të gjerë operacionesh dhe misionesh në nivel global, edhe mes një klime në ndryshim. Shembujt aktualë të operacioneve dhe misioneve të tilla përfshijnë trajnimin shumëkombësh të NATO-s dhe përpjekjet për ngritjen e kapaciteteve në Irak, operacionet dhe aktivitetet në domenin detar (Operacioni Sea Guardian), policimin ajror në disa vende aleate ose në misionin KFOR.

Shumë nga misionet dhe veprimtaritë e NATO-s zhvillohen në rajone të cilat tashmë janë të prekshme nga nxehtësia ekstreme, reshjet e dendura, stuhitë e pluhurit dhe ekstreme të tjera. *Ngjarjet e motit.* Misioni i NATO-s në Irak (NMI) është veçanërisht i prekur nga valët e nxehtësisë. Vitet e fundit, personeli i vendosur u përball me periudha të shpeshta të nxehtësisë ekstreme, duke shtyrë pajisjet dhe personelin përtej kufijve të tyre. Situata është shtuar edhe më shumë nga rritja e njëkohshme e shpeshtësisë së stuhive të pluhurit, të cilat zvogëlojnë shikueshmërinë, prishin si transportin ajror ashtu edhe atë rrugor, duke bllokuar pajisjet dhe ndikojnë negativisht në shëndetin e personelit ushtarak. Numri i "*ditëve të motit me flamur të zi*"[20] vazhdojnë të rriten, gjë që shkakton ndërprerje operacionale dhe komprometon trajnimin dhe gatishmërinë[21].

Evropa Juglindore, duke përfshirë Kosovën, është identifikuar si një nga "*pikat e nxehta ngrohëse*"[22] të planetit. Sipas sistemit evropian të informacionit për zjarret në pyje, Kosova "bën pjesë në vendet me nivel ekstrem rreziku për zjarret në pyje"[23]. Ngrohja e atmosferës në rajon po çon në ngjarje ekstreme të motit dhe së bashku me dobësinë social-ekonomike të Kosovës dhe mjedisin sfidues të sigurisë, ndryshimi i klimës mund të ketë pasoja të dëmshme si për Kosovën, ashtu edhe për praninë e NATO-s në terren. KFOR-i është përfshirë në monitorimin e krimeve mjedisore, ndihma e ofruar nga forcat ka qenë vendimtar në dhënien e ndihmës pas ngjarjeve ekstreme të motit por edhe mbështetje inxhinierike dhe ndërtimore për të vlerësuar urat, rrugët dhe ndërhyrjet pas përmbytjeve. Në një nga detyrat kryesore të NATO-s, "Parandalimi dhe Menaxhimi i Krizave", ashtu siç theksohet në Konceptin Strategjik të saj, NATO thekson se "*do ta zhvillojmë më tej aftësitë e Aleancës për të mbështetur menaxhimin e krizave civile dhe operacionet e ndihmës dhe*

[20] Ditë kur temperaturat kalojnë 35°C dhe operacionet janë të kufizuara ose ndërpriten krejtësisht për arsye shëndetësore dhe sigurie.

[21] NATO Mission Iraq, NATO Climate Change and Security Impact Assessment: Second Edition 2023.

[22] OSCE, "*Regional Assessment for South-Eastern Europe Security Implications of Climate Change*," 2021.

[23] European Forest Fire Information System dhe Copernicus Atmosphere Monitoring Service

*për përgatitjen për efektet e ndryshimeve klimatike, pasigurisë ushqimore, emergjencave shëndetësore. Kjo do të na lejojë t'i përgjigjemi çdo emergjence në një kohë të shkurt*ër.*"*[24]

Përveç përmbytjeve, nxehtësia ekstreme dhe grimcat në atmosferë kanë paraqitur sfida me ndikim të gjithanshëm. Ditët me temperatura ekstreme (*ditëve të motit me flamur të zi*) do fillojnë të rriten megjithëse rritja e parashikuar e temperaturës nuk është aq ekstreme sa në disa zona të tjera gjeografike ku vepron NATO. Parashikimet e temperaturave më të larta dhe rritjes së rreziqeve të zjarreve, "*zvogëlimit të reshjeve .....mund të ndikojnë në furnizimet me ujë si për popullsinë vendase, ashtu edhe për personelin e KFOR-it*"[25].

Impakti i ndryshimeve klimatike duhet analizuar në përputhje me ndikimin e saj në dy gjera thelbësore: në ndikimin e saj në arritjen e plotësimit të detyrave kryesore të forcave të NATO-si dhe në ndikimin e saj në forcat/mjetet operacionale të NATO-s si në rajonet e bazimit të tyre dhe rajonet e realizimit të misionit përkatës. Ndryshimi i klimës është një sfidë përcaktuese e kohës sonë, me një ndikim të thellë te siguria aleatëve. Është një shumëfishues krize dhe kërcënimi. Mund të përkeqësojë konfliktin, brishtësinë dhe konkurrencën gjeopolitike. Ndryshimi i klimës ndikon edhe në mënyrën se si funksionojnë Forcat tona të Armatosura. Infrastruktura, asetet dhe bazat tona janë të prekshme ndaj efekteve të saj. Forcat tona duhet të operojnë në klimë me kushte ekstreme; ato thirren më shpesh për të ndihmuar në lehtësimin e fatkeqësive natyrore[26].

Në hapësirën detare, forcat detare dhe aftësitë e tyre ndikohen gjithnjë e më shumë nga efektet e ndryshimeve klimatike duke përfshirë *"temperatura e ajrit dhe oqeanit, shpejtësinë e erës, rrymat sipërfaqësore dhe nënujore, etj."*[27]. Efekte të tilla po sfidojnë operacionet dhe aftësitë detare në disa mënyra. Valët e stuhive dhe ngritja e nivelit të detit rrezikojnë infrastrukturën ushtarake bregdetare, rritja e acidifikimit të ujit përshpejton korrozionin e mjeteve detare, rritja e temperaturave të ujit ndikon direkt në mirë funksionimin e mjeteve të tilla, etj. Ndryshimi i temperaturës së ujit dhe acidifikimi ndikojnë në funksionimin normal të mjeteve të vrojtimit, sensorëve të ndryshëm, me pasoja të mundshme në operacionalitetin e tyre. Ndryshimet klimatike kanë zgjeruar territorin e përgjegjësive të mëparshme, pasi hapja e rrugëve të reja

[24] NATO 2022 - Strategic concept , page 9
[25] USAID, "Climate Change Risk Profile: Kosovo" January 2017
[26] NATO 2022 - Strategic Concept , page 6.
[27] Contribution from NATO's Science & Technology Organization Centre for Maritime Research and Experimentation (CMRE).

të qarkullimit detar në Arktik ka shtuar nevojën si të rritjes së prezencës, ashtu edhe të emergjencave të mundshme.

Ndikimet e përshkallëzuara të ndryshimeve klimatike po paraqesin sfida komplekse taktike dhe operacionale në operacionet tokësore. Zjarret në Kanada, Greqi, etj., në vitin 2023 treguan për nevoja urgjente në rritje ndaj burimeve ushtarake. Këto burime ishin të pamjaftueshme si ndaj mbështetjes së popullsisë ashtu dhe në mbrojtjen e vetë infrastrukturës ushtarake. Përveç rreziqeve për sigurinë, "*zjarret transformojnë zona të gjera, duke paraqitur sfida të tjera në fushën tokësore ku bimësia është vendimtare për mbulimin natyror, manovrueshmërinë taktike, etj., duke ndikuar në vendimet strategjike dhe taktike*"[28]. Ndryshimet e mundshme ne terren brenda një periudhe të shkurtër kohore, kërkojnë që FA në mënyrë të vazhdueshme të bëjnë rivlerësimin e tij, i cili në mënyrë direkte të çon në ndryshime të mundshme në vendimmarrjen ushtarake. Sa i përket faktorëve njerëzorë, ekspozimi ndaj temperaturave ekstreme shkakton një rritje të sëmundjeve të lidhura me ndryshimet mbi normalen të temperaturave. Forcat speciale, forcat në operacionet e mbrojtjes kimike, biologjike etj., me pajisjet e tyre, ndjehen në vështirësi për t'i përdorur në kushte ekstreme. Një rivlerësim i "*modeleve të trajnimit, uniformave, pajimeve mbrojtëse mund të jetë i nevojshëm për të minimizuar këto rreziqe*"[29]. Në të njëjtën shkallë rrezikshmërie paraqiten edhe ekuipazhet në mjetet e blinduara, të cilat i kanë të shumëfishuara ndryshimet klimatike për shkak të materialeve përbërëse të këtyre mjeteve.

Ndryshimi i klimës ndikon ndjeshëm në të gjitha aspektet e hapësirës ajrore, që nga performanca fizike e avionëve, në sigurinë e pajisjeve dhe infrastrukturës, deri te struktura dhe planifikimi i operacioneve të fluturimit. Duke filluar nga hapësira ajrore, ndryshimi i klimës shkakton ndryshime të ndjeshme në kushtet mjedisore, duke çuar në paqëndrueshmëri më të madhe të motit dhe paparashikueshmëri, turbullira të intensifikuara dhe një frekuencë më të lartë të ngjarjeve ekstreme të motit. Këto sfida kërkojnë që avionët të operojnë në kushte më të vështira, duke komplikuar planifikimin e fluturimit dhe duke rritur rreziqet e fluturimit. Në veçanti, "*rritja e temperaturave zvogëlon dendësinë e ajrit, ndoshta faktori fizik më i rëndësishëm që ndikon në performancën e avionëve*"[30].

---

[28] Gerhard Herda, *Climate Change and International Security: Challenges for the Austrian Military Geoservices,* No. 04, 2024. Book_climate_12_climate_change_and_international_security.pdf.

[29] Daniel S Moran et al., *Beating the Heat: Military Training and Operations in the Era of Global Warming. pdf*. 2023, p. 60–67.

[30] NATO - News: NATO releases its Climate Change and Security Impact Assessment , 28-Jun.-2022

Efektet e lidhura me ndryshimet klimatike sfidojnë gjithnjë e më shumë aftësinë e anëtarëve të NATO-s për të vepruar në mënyrë efektive në hapësirë dhe kufizojnë vlerën potenciale që aftësitë hapësinore mund të shtojnë në misionet dhe operacionet e NATO-s. Ndryshimi i klimës mund të ndikojë në infrastrukturën tokësore që është kritike për operacionet hapësinore, të tilla si stacionet tokësore, kullat e komunikimit, platformat e lëshimit të hapësirës ose satelitët që ende nuk janë nisur. Shumë nga infrastruktura përkatëse mund të dëmtohet si rezultat i rritjes së nivelit të detit apo erozioni tokës. Duke studiuar infrastrukturën përkatëse, ndikimet e lidhura me klimën janë shqetësim më i madh për aftësitë hapësinore aleate sesa ato për Rusinë dhe Kinën, sepse "*shumica e vendeve të lëshimit të operuara nga këto dy vende janë të vendosura në brendësi, duke përfituar nga kushtet më të qëndrueshme të motit*"[31].

Kryqëzimi i mbrojtjes kibernetike dhe ndryshimeve klimatike përbën një fushë shqetësimi komplekse dhe gjithnjë e më kritike. Ndërsa bota bëhet më e ndërlidhur dhe e varur nga teknologjitë digjitale, rritet mundësia për veprimtari keqdashëse kibernetike për të përkeqësuar çështjet e ndryshimeve klimatike. Që nga sulmet kibernetike në sistemet e monitorimit të mjedisit, deri te manipulimi i të dhënave dhe fushatat e dezinformimit lidhur me klimën, mënyrat se si ndërlidhen rreziku kibernetik dhe ndryshimet klimatike janë të gjera dhe të larmishme.

Ndryshimet klimatike në dokumentet strategjike të vendit

Gjatë dy dekadave të fundit, Shqipëria i ka kushtuar vëmendje të veçantë mbrojtjes së mjedisit në përgjithësi dhe ndryshimeve klimatike në veçanti. Vetë Kushtetuta e Shqipërisë ka përfshirë "*një mjedis të shëndetshëm dhe ekologjikisht të përshtatshëm për brezin e tanishëm dhe atë të ardhshëm*"[32] si një prej objektivave socialë që duhet të merren në konsideratë nga të gjitha institucionet shtetërore. Interesat kryesore strategjike të Shqipërisë gërshetohen me interesat që mund të quhen klasikë me "*angazhimin global kundër ndryshimeve klimatike, rritjen e sigurisë energjetike dhe asaj ushqimore, etj.,*"[33] dhe duke vazhduar me "*menaxhimin e duhur të fatkeqësive natyrore*"[34].

Shqipëria është palë nënshkruese e Konventës në kuadër të Kombeve të Bashkuara për *Ndryshimet Klimatike* dhe e ratifikuar nga Parlamenti Shqiptar, e cila ka përcaktuar objektivin për luftën kundër ndryshimeve klimatike

[31] NATO Review - The climate-space nexus: new approaches for strengthening NATO's resilience, 2022

[32] Kushtetuta e Republikës së Shqipërisë, neni 59, pika d.

[33] SSK, faqe 2

[34] Po këtu, faqe 3

përmes stabilizimit të përqendrimeve të gazrave serë në atmosferë dhe kufizimit të rritjes së temperaturave mesatare globale për të përkrahur zhvillimin e qëndrueshëm[35]. Duke pasur parasysh statusin aktual të Shqipërisë si vend kandidat që ka hapur negociatat për anëtarësim në BE, ka gjasa që ajo të anëtarësohet në BE gjatë periudhës së mbuluar nga kjo strategji. Për këtë arsye, është me rëndësi thelbësore që strategjia për energjinë të jetë në përputhje edhe me Politikën e BE-së për Ndryshimet Klimatike, "*duke garantuar që objektivat e politikave të energjisë dhe planet përkatëse të veprimit për energjinë të identifikuara të jenë në një linjë me ambiciet e shprehura në pikësynimet e BE, lidhur me ndryshimet klimatike*"[36].

Në shtjellimin e mjedisit strategjik në SSK, ritheksohet se tashmë kërcënimeve të tjera i shtohet ndryshimi i kushteve klimatike, të cilat kanë potencial të sjellin implikime të reja social-ekonomike për sigurinë. Ato po shkaktojnë një efekt zinxhir, i cili shkon nga ngrohja globale dhe degradimi i mjedisit te rivaliteti për burime, emigracioni në rritje, përhapja e sëmundjeve dhe pandemive me impakt global në sigurinë shëndetësore dhe atë ushqimore nëpërmjet pakësimit të burimeve jetike, dhe rritja e forcës shkatërruese të fatkeqësive natyrore, çka ka sjellë si pasojë lëvizjet e pakontrolluara të njerëzve, si drejt zonave urbane ashtu dhe në emigracion. Ndryshimet klimatike po ndikojnë gjithnjë e më shumë në ndryshimin e "*mjedisit gjeopolitik duke shkaktuar paqëndrueshmëri dhe fërkim më të madh politik brenda dhe ndërmjet vendeve.... Gjithashtu, ato mund të ndikojnë në rritjen e konkurrencës dhe kërcënimeve ekzistuese, si dhe në balancat gjeopolitike*"[37].

Dukuria globale e ndryshimit të klimës ndikon negativisht në ekuilibrat natyrorë të vendit tonë. Si pasojë, vendi mund të përballet me temperatura të larta që kanë një ndikim domethënës në florën dhe faunën, thatësira të zgjatura dhe rrezik të shtuar për përmbytje, me kosto të konsiderueshme për dimensionin njerëzor dhe ekonominë kombëtare. Elementi i sigurisë ushqimore si element mjaft i rëndësishëm i sigurisë njerëzore, me ndikim në shëndetin e popullatës, merr një rëndësi të veçantë në kushtet e krizës ekonomike, si dhe të "*kushteve klimatike në ndryshim....*"[38].

Ngjarjet e viteve të fundit kanë treguar se ekziston një nevojë urgjente për të forcuar gatishmërinë ndaj fatkeqësive dhe aftësitë e menaxhimit të riskut, për të miratuar sisteme dhe procedura të përshtatshme reagimi dhe për të përmirësuar kapacitetin institucional për koordinimin dhe menaxhimin e

[35] Plani Kombëtar i Energjisë dhe Klimës (NECP) 2020-2030, f. 10 NECP-Albania_drafti-shqip.pdf
[36] Po këtu, faqe 12
[37] Po këtu, faqe 5.
[38] Po këtu, faqe 10.

reduktimit të risqeve nga fatkeqësitë për bashkëveprimin midis niveleve publike të qeverisë, si dhe me aktorët privatë dhe ata të shoqërisë civile. Prioritet është "*parandalimi i degradimit mjedisor dhe reduktimi i pasojave të ndryshimeve klimatike, duke menaxhuar me efektivitet basenet ujore, shtuar sipërfaqet pyjore, trajtuar në mënyrë të integruar mbetjet urbane, si dhe duke bashkëpunuar me shoqërinë civile për ndërgjegjësimin e opinionit publik për ruajtjen e mjedisit dhe garantimi i sigurisë së digave të rezervuarëve*"[39].

Sistemi i mbrojtjes civile u ridimensionua dhe është përmirësuar kuadri i zvogëlimit të riskut nga fatkeqësitë nëpërmjet identifikimit, vlerësimit periodik të riskut dhe monitorimit të tij, duke zbutur pasojat negative të fatkeqësive, si edhe krijimit të bazës së të dhënave të humbjeve nga emergjencat natyrore dhe fatkeqësitë. Në zbatim të Strategjisë Kombëtare të Energjisë dhe referuar rekomandimit të BE-së, në vitin 2021 u miratua Plani Kombëtar i Energjisë dhe Klimës (NECP) 2020-2030. Ky Plan plotëson Strategjinë Kombëtare të Energjisë dhe "*vendos objektiva të rinj dhe më ambiciozë* për efiçencën e energjisë, përdorimin të burimeve të *rinovueshme* të energjisë dhe de karbonizimit"[40].

Impakti i ndryshimeve klimatike në trajtimin në tërësi që jepet në SSK shërben si tregues për fokusimin më tej të saj nga institucionet e tjera shtetërore, që në misionin e tyre trajtojnë problematikat përkatëse. Krahas këtyre institucioneve, të cilat hartojnë strategjitë sektoriale, gjejnë veten të përfshirë në këtë proces edhe forcat e armatosura, të cilat në misionin e tyre, krahas ruajtjes së pavarësisë, sovranitetit dhe tërësisë territoriale të vendit, *"mbrojtja dhe mbështetja e popullsisë në kohë paqeje, krize e lufte...."*[41] është pjesë e rëndësishme e misionit. Strategjisë Ushtarake të Republikës së Shqipërisë, 2024, në kreun e dytë "Mjedisi strategjik i sigurisë në nivelin global", në vazhdimësi të kërcënimeve të tjera, "*i shtohet edhe ndryshimi i kushteve klimatike, me implikime të reja social-ekonomike dhe krizave humanitare me ndikime negative për sigurinë*"[42].

Ndikimi i ndryshimeve klimatike në SU trajtohet si një kërcënim, i cili ka ndikim të drejtpërdrejtë në sigurimin e elementeve jetike bazë të popullsisë, "*siguria ushqimore si element mjaft i rëndësishëm i sigurisë njerëzore, me ndikim në shëndetin e popullatës, merr një rëndësi të veçantë në kushtet e krizës ekonomike, kushteve klimatike, etj*."[43] Dukuria globale e ndryshimit të klimës ndikon negativisht në ekuilibrat natyrorë dhe vendi ynë mund të përballet me temperatura të larta që kanë një ndikim domethënës në shumë

[39] Po këtu, faqe 20.
[40] Po këtu, faqe 23-24.
[41] SU të RSH-2024, faqe 22.
[42] SU të RSH-2024, faqe 10.
[43] SU të RSH-2024, faqe 12.

fusha, me kosto të konsiderueshme për dimensionin njerëzor dhe ekonominë kombëtare. Qasja jonë brenda NATO-s, në kuadrin e zhvillimit të një force të përbashkët, ku një nga detyrat e saj do të jetë edhe pjesëmarrje në operacione apo për menaxhimin e krizave, Forca jonë e Armatosur do të jetë e dislokuar në rajone të ndryshme të globit.

Shpërndarja aktuale e misioneve të ndërmarrë nga NATO ose e atyre që mund të ndërmerren në të ardhmen është në zona gjeografike të ndryshme. Kështu, krahas ndryshimeve aktuale të klimës të ndodhura brenda territorit të vendit tonë, FA-të duhet të jenë të përgatitura për të zhvilluar misione edhe në rajone ku ndryshimet klimatike janë edhe më shumë të theksuara.

Përfundime

Mjedisi strategjik është në evoluim të vazhdueshëm. Kalimi nga kërcënime konvencionale të në atë jo konvencionale, ishte një periudhë e caktuar kohore. Më tej, mjedisi i sigurisë kaloi në një periudhë të gërshetimit të këtyre kërcënimeve dhe rreziqeve, fazë në të cilën nuk mund të përcaktosh se cili nga këto kërcënime mbizotëron mbi tjetrin. Cenimi i integritetit territorial, pasuar me retorikën e përdorimit të armës bërthamore, deri te kërcënimet e ndryshimeve klimatike, i vendosin forcat e armatosura përpara zgjidhjeve gjithnjë e më komplekse.

Ndryshimi i klimës është një çështje që kërkon një përgjigje botërore. Ndjekja e politikave të drejta do të thotë që kostoja e veprimeve mund të jetë më e vogël se sa dëmi që shmanget. Duke pranuar tashmë faktin që ndryshimet klimatike janë të prekshme, duke konstatuar që ndikimi i saj ka efekte të nivelit të parë dhe më tej, mjedisi i sigurisë do të formësohet tashmë edhe nga ky kërcënim.

Nëse shkaktarët e ndryshimeve klimatike janë të shumëllojtë dhe që kanë të bëjnë në tërësi me veprimet politike të shteteve apo organizatave të ndryshme, pasojat e tyre do të përkthehen në cenim sigurie. Kompleksiteti i ndryshimeve klimatike rritet më tej kur aktorët kryesorë të shkaktimit të saj, kanë shpesh herë këndvështrime të ndryshme.

Parë në këtë këndvështrim, Forcat e Armatosura kombëtare dhe ato të aleancës do të ndeshen gjithnjë e më shumë me cenimin e sigurisë në forma nga më të ndryshmet. Nëse për parandalimin e ndryshimeve klimatike forca e armatosura ka një ndikim minimal, vetë forca e armatosur do jetë nën ndikimin e tyre. Trajtimi si duhet i këtij kërcënimi, do të mundësonte që FA-të të kenë aftësinë e fleksibilitetit si për të minimizuar këto pasoja, ashtu edhe për të mos cenuar operacionalitetin e tyre.

Literatura e shfrytëzuar:

1. Bobo Lo, *The Adaptation Game: Russia and Climate Change*, pdf. 2021.
2. Daniel S Moran et al., *Beating the Heat: Military Training and Operations in the Era of Global Warming.* pdf. 2023.
3. Erin Sikorsky, *China's Climate Security Vulnerabilities*, Center for Climate and Security, Council on Strategic Risks, November 2022.
4. Kushtetuta e Republikës së Shqipërisë.
5. Michael Brzoska, *Climate Change and the Military in China, Russia, the United Kingdom, and the United States*, Bulletin of the Atomic Scientists.
6. NATO 2022 - Strategic Concept.
7. OSCE, *Regional Assessment for South-Eastern Europe Security Implications of Climate Change*, 2021.
8. Plani Kombëtar i Energjisë dhe Klimës (NECP) 2020-2030.
9. Rachael Gosnell and Joseph Thomas, *European Security Seminar North: A Cooperative Future; Opportunities for the Arctic - 7*, GCMC.
10. Strategjia e Sigurisë Kombëtare, 2024.
11. Strategjia Ushtarake e Republikës së Shqipërisë, 2024.
12. Thane Gustafson, *Klimat: Russia in the Age of Climate Change*, Harvard University Press, 2021, ISBN 9780674247437.

Evoluimi i konceptit tradicional të mbrojtjes drejt ekonomizimit të burimeve në Shqipëri

Nënkolonel Msc. Pëllumb HIDRI
Komandant i Batalionit Komando
Prof. Asoc. Dr. Blendi LAMI
Lektor në UET

Trajtesë e shkurtuar.

Në këtë material analizohet evolucioni i konceptit të mbrojtjes nga qasja tradicionale drejt konceptit të ri të përdorimit në mënyrë të efektshme. Fillimisht, kumtesa shqyrton bazat e mbrojtjes tradicionale, e cila është fokusuar kryesisht në sovranitetin kombëtar dhe forcën ushtarake si mbrojtëse kryesore ndaj kërcënimeve të jashtme. Duke u nisur nga analiza e historisë dhe doktrinave ushtarake klasike, tregohen kufizimet e kësaj qasjeje përballë mjedisit të ri të sigurisë, ku kërcënimet janë gjithnjë e më komplekse dhe asimetrike.

Më tej, shkrimi shqyrton faktorët kryesorë që kanë ndikuar në ndryshimin e mjedisit të sigurisë ndërkombëtare, përfshirë këtu avancimin teknologjik, kërcënimet kibernetike, terrorizmin global, dhe transformimet gjeopolitike. Në këtë kontekst, shtjellohet koncepti i ekonomizimit të burimeve, i promovuar kryesisht nga NATO si një qasje e re ndaj mbrojtjes kolektive. Përmes bashkëpunimit të ngushtë midis aleatëve dhe përdorimit më të efektshëm të burimeve ushtarake dhe teknologjike, efektiviteti i kapaciteteve paraqet një alternativë të nevojshme për përballimin e kërcënimeve të reja dhe përmirësimin e mbrojtjes.

Shkrimi bën gjithashtu një krahasim të detajuar midis qasjes tradicionale të

mbrojtjes dhe përdorimit kolektiv, duke nxjerrë në pah avantazhet e saj në aspektin e efektivitetit dhe bashkëpunimit. Përmes analizës së rasteve konkrete nga vende të ndryshme, diskutohen aplikimet praktike dhe rezultatet e kësaj strategjie. Në përfundim, kumtesa përqendrohet në sfidat që hasin vendet dhe organizatat ndërkombëtare në adoptimin e plotë të konceptit të përdorim eficient dhe ofron rekomandime për të ardhmen, për të siguruar që mbrojtja të përshtatet me kërkesat e mjedisit bashkëkohor të sigurisë.

Fjalët kyçe: qasje tradicionale e mbrojtjes, ekonomizim i burimeve, mbrojtje kolektive, mjedis i sigurisë, sovranitet kombëtar mbrojtje territoriale, ndryshimet gjeopolitike dhe teknologjike, Shqipëri, NATO.

Koncepti tradicional i mbrojtjes në Shqipëri: historia, sovraniteti dhe roli i Forcave të Armatosura

Mbrojtja kombëtare ka qenë gjithmonë një aspekt thelbësor i politikave shtetërore, veçanërisht për vendet që kanë përjetuar kërcënime të vazhdueshme ndaj sovranitetit të tyre. Në Shqipëri, koncepti i mbrojtjes ka pësuar transformime të thella për shkak të konteksteve historike dhe gjeopolitike të vendit. Qasja tradicionale e mbrojtjes, e bazuar kryesisht në sovranitetin kombëtar dhe mbrojtjen territoriale, ka evoluar në përputhje me ndryshimet ndërkombëtare dhe rajonale. Ky artikull do të shqyrtojë historinë dhe zhvillimin e konceptit të mbrojtjes kombëtare në Shqipëri, me një fokus të veçantë në mbrojtjen e sovranitetit dhe rolin e forcave të armatosura. Gjithashtu, do të trajtohen doktrinat kryesore të mbrojtjes dhe mësimet e nxjerra nga shembuj historikë. "Bashkëpunimi ndërkombëtar dhe ndarja e burimeve është thelbësore në një botë ku asnjë shtet nuk mund të garantojë sigurinë vetëm." Bjola, C., & Kornprobst, M. (2013).

Historia dhe zhvillimi i konceptit të mbrojtjes kombëtare në Shqipëri

Koncepti i mbrojtjes kombëtare në Shqipëri është formësuar nga pozita gjeopolitike e vendit dhe sfidat historike që ai ka përjetuar. Që nga periudha e themelimit të shtetit shqiptar më 1912, mbrojtja ka qenë një prioritet për qeveritë shqiptare, për shkak të kërcënimeve të vazhdueshme nga fqinjët dhe të pushtimeve të huaja (Duka, 2012). Luftërat Ballkanike dhe Lufta e Parë Botërore ishin periudha të vështira për Shqipërinë, duke treguar dobësinë e institucioneve të reja shtetërore dhe mungesën e një ushtrie të mirëorganizuar për të mbrojtur integritetin territorial. Pas Luftës së Dytë Botërore, Shqipëria u bë një shtet komunist nën drejtimin e Enver Hoxhës. Gjatë kësaj periudhe, koncepti i mbrojtjes kombëtare mori një drejtim të ri, duke u fokusuar kryesisht

në mbrojtjen nga fuqitë perëndimore dhe lindore. Mbrojtja kombëtare u kthye në një ideologji sovrane, ku shteti i vogël dhe i izoluar duhej të mbrohej nga çdo kërcënim i jashtëm. Shqipëria filloi një politikë të fortë të militarizimit dhe ndërtimit të bunkerëve në të gjithë territorin, duke ndjekur doktrinën e "mbrojtjes me forcat e veta" (Fischer, 2009). Kjo periudhë përfaqëson një nga fazat më ekstreme të sovranitetit dhe mbrojtjes territoriale në historinë moderne të vendit.

Mbrojtja e sovranitetit dhe roli i Forcave të Armatosura. Në qasjen tradicionale të mbrojtjes kombëtare, sovraniteti ka luajtur një rol kyç, duke e bërë mbrojtjen e kufijve dhe të integritetit territorial një prioritet absolut. Në Shqipëri, ky koncept ka qenë veçanërisht i theksuar gjatë periudhës komuniste, kur vendi ishte në izolim ndërkombëtar dhe përballej me kërcënime reale dhe të perceptuara nga fqinjët dhe fuqitë e mëdha. Sovraniteti kombëtar u shndërrua në një element kryesor të politikave të sigurisë, duke ndikuar në doktrinat ushtarake dhe strategjitë mbrojtëse të vendit. Dhe kjo në një kohë kur "Teknologjia moderne ka ndryshuar rrënjësisht natyrën e luftës, duke nxitur nevojën për bashkëpunim dhe inovacion në mbrojtje." Boot, M. (2006).

Forcat e armatosura shqiptare kanë luajtur një rol qendror në ruajtjen e sovranitetit dhe mbrojtjes së integritetit territorial. Gjatë periudhës komuniste, ushtria shqiptare ishte një nga sektorët më të rëndësishëm të shtetit, duke pasur një numër të madh të rekrutëve dhe një organizim të gjerë të rezervave (Duka, 2012). Kjo strukturë ushtarake, e bazuar kryesisht në mbrojtjen territoriale dhe strategjitë e rezistencës popullore, ishte në përputhje me doktrinën e mbrojtjes kombëtare që përqendrohej në një mbrojtje të decentralizuar, ku çdo qytetar do të merrte pjesë në mbrojtjen e vendit.

Sipas kësaj doktrine, mbrojtja e vendit nuk varej vetëm nga ushtria profesioniste, por nga përfshirja e të gjithë popullit në një luftë të përgjithshme të rezistencës. Kjo ide përkonte me zhvillimet e epokës komuniste në vendet e tjera të Evropës Lindore, por në Shqipëri ishte veçanërisht e fortë për shkak të izolimit dhe mungesës së aleatëve të jashtëm. Kjo doktrinë përfshinte gjithashtu ndërtimin e bunkerëve dhe strukturave të mbrojtjes që mundësonin një rezistencë të gjatë ndaj një pushtimi të mundshëm (Fischer, 2009).

Doktrinat kryesore dhe mësimet nga e kaluara

Doktrinat ushtarake shqiptare kanë qenë të ndikuara nga një sërë faktorësh, duke përfshirë rrethanat historike, gjeopolitikën dhe ideologjinë politike të regjimeve të ndryshme. Gjatë periudhës komuniste, doktrina kryesore e mbrojtjes ishte "mbrojtja me forcat e veta", e cila synonte të minimizonte varësinë e vendit nga aleatët ndërkombëtarë dhe të garantonte mbrojtjen e tij përmes forcave të brendshme. Kjo doktrinë kishte një bazë ideologjike të

fortë, pasi regjimi i E. Hoxhës promovonte autarkinë dhe besimin te forcat kombëtare, si një element kyç për mbijetesën e shtetit socialist (Kaplan, 2015).

Një shembull historik që pasqyron fuqinë dhe kufizimet e kësaj doktrine është periudha e izolimit të Shqipërisë pas prishjes së marrëdhënieve me Bashkimin Sovjetik dhe Kinën. Shqipëria ishte një nga vendet e pakta në botë që ndiqte një politikë të jashtme të izolimit të plotë, duke mbështetur doktrinën e mbrojtjes kombëtare për të garantuar mbijetesën e regjimit (Fischer, 2009). Megjithatë, ndërsa kjo doktrinë mund të siguronte një farë stabiliteti të brendshëm në afat të shkurtër, ajo ishte e paqëndrueshme në planin afatgjatë, për shkak të kufizimeve ekonomike dhe teknologjike të vendit. Pas përmbysjes së regjimit komunist në fillim të viteve 1990, Shqipëria ndryshoi qasjen e saj ndaj mbrojtjes dhe sigurisë. Anëtarësimi në organizata ndërkombëtare si NATO dhe bashkëpunimi me vende të tjera për të garantuar sigurinë kombëtare përfaqësonin një largim të madh nga doktrina tradicionale e mbrojtjes sovrane (Duka, 2012). Shqipëria filloi të adoptojë doktrina të reja që theksonin bashkëpunimin ndërkombëtar dhe integrimin në struktura të sigurisë kolektive.

Pra, koncepti tradicional i mbrojtjes në Shqipëri ka evoluar nga një qasje sovrane dhe e bazuar në izolim drejt një modeli më të hapur dhe të integruar të mbrojtjes kolektive. Historia e mbrojtjes kombëtare të Shqipërisë tregon rëndësinë e sovranitetit dhe mbrojtjes territoriale në periudha të ndryshme të historisë së vendit, veçanërisht gjatë periudhës komuniste. Megjithatë, mësimet e nxjerra nga shembujt historikë tregojnë se qasja tradicionale e mbrojtjes mund të jetë e kufizuar në përballimin e sfidave të reja të sigurisë. Ndërsa Shqipëria ecën drejt integrimit në arkitekturën ndërkombëtare të sigurisë, është e qartë se doktrinat e reja dhe qasjet bashkëpunuese janë thelbësore për mbrojtjen e vendit në mjedisin e sotëm global.

Ndryshimet në mjedisin e sigurisë ndërkombëtare dhe ndikimi i tyre në Shqipëri

Mjedisi i sigurisë ndërkombëtare ka përjetuar ndryshime të thella në dekadat e fundit për shkak të zhvillimeve gjeopolitike dhe teknologjike. Shqipëria, si një vend i vogël në rajonin e Ballkanit dhe anëtare e NATO-s që nga viti 2009, është ndikuar ndjeshëm nga këto transformime, të cilat kanë ndryshuar mënyrën se si ajo qaset ndaj sigurisë kombëtare dhe rajonale. Ndryshimet në mjedisin e sigurisë përfshijnë jo vetëm avancimin teknologjik dhe shfaqjen e kërcënimeve të reja, si sulmet kibernetike dhe terrorizmi global, por edhe kërcënime të asimetrike, të cilat kanë ndryshuar strategjitë mbrojtëse të shteteve. Shqipëria, si një vend në tranzicion drejt modernizimit dhe integrimit euroatlantik, është sfiduar të adoptojë qasje të reja për të përballuar kërcënimet e reja në epokën e globalizimit. “Mbrojtja inteligjente kërkon një

qasje të integruar që kombinon mbrojtjen tradicionale me elemente të rinj si kibernetika dhe operacionet për paqe." Collins, A. (2016).

Ndryshimet gjeopolitike dhe teknologjike. Ndryshimet gjeopolitike kanë pasur një ndikim të thellë në strukturën e sigurisë ndërkombëtare dhe në strategjitë e vendeve të vogla si Shqipëria. Pas përfundimit të Luftës së Ftohtë, botëkuptimi i sigurisë ka ndryshuar nga ai bipolar, ku superfuqitë dominonin në rajone të caktuara, drejt një sistemi multipolar, ku aktorët rajonalë dhe joshtetërorë luajnë rol të rëndësishëm (Kaplan, 2015). Rajoni i Ballkanit, i cili ka qenë tradicionalisht një qendër tensioni për fuqitë e mëdha, është integruar gjithnjë e më shumë në strukturat e sigurisë perëndimore, duke përfshirë anëtarësimin e vendeve si Shqipëria në NATO dhe përpjekjet për anëtarësim në Bashkimin Evropian. Ky transformim gjeopolitik ka ofruar mundësi të reja për stabilizimin e rajonit, por gjithashtu ka sjellë sfida të reja për sigurinë, veçanërisht në lidhje me ndërhyrjet e aktorëve të jashtëm si Rusia dhe Kina, të cilat kanë rritur ndikimin e tyre në rajon (Duka, 2012).

Ndryshimet teknologjike kanë qenë një tjetër faktor kyç që ka ndikuar në mjedisin e sigurisë. Teknologjia kibernetike, zhvillimet në inteligjencën artificiale dhe rritja e kapaciteteve të mbikëqyrjes globale kanë transformuar mënyrën se si shtetet menaxhojnë dhe përgjigjen ndaj kërcënimeve. Në këtë kontekst, Shqipëria ka filluar të forcojë kapacitetet e saj në mbrojtjen kibernetike dhe të përmirësojë infrastrukturën e saj teknologjike për të përballuar sfidat e reja. Ndërhyrjet kibernetike që Shqipëria ka përjetuar në vitet e fundit kanë theksuar nevojën për investime në këtë fushë, veçanërisht pas sulmit të madh kibernetik që goditi institucionet shtetërore në vitin 2022 (Fischer, 2009).

Evolucioni i kërcënimeve: kibernetike, terrorizmi, kërcënime asimetrike. Evolucioni i kërcënimeve të sigurisë ka ndikuar në mënyrë të ndjeshme në politikën mbrojtëse të Shqipërisë. Në të kaluarën, kërcënimet ishin kryesisht të natyrës territoriale dhe përqendroheshin në mbrojtjen e kufijve nga sulmet e mundshme ushtarake. Megjithatë, në epokën moderne, kërcënimet kibernetike janë shfaqur si një ndër sfidat më të mëdha për sigurinë kombëtare. Sulmet kibernetike, të cilat mund të kryhen nga aktorë shtetërorë dhe joshtetërorë, kanë aftësinë të paralizojnë infrastrukturën kritike të një shteti, duke përfshirë sistemet financiare, energjetike dhe të komunikimit (Weiss, 2018). Sulmi kibernetik ndaj Shqipërisë në vitin 2022, i cili mendohet të jetë kryer nga një aktor i jashtëm, theksoi dobësitë në mbrojtjen kibernetike të vendit dhe nënvizoi nevojën për modernizim dhe bashkëpunim më të madh ndërkombëtar në këtë fushë.

Një tjetër kërcënim i rëndësishëm për Shqipërinë dhe rajonin është terrorizmi ndërkombëtar. Megjithëse Shqipëria nuk është përballur me sulme të mëdha terroriste, rajoni i Ballkanit ka qenë një burim rekrutimi për grupe terroriste ndërkombëtare si ISIS, duke krijuar shqetësime për stabilitetin e brendshëm

dhe përfshirjen e qytetarëve shqiptarë në veprimtari terroriste jashtë vendit (Orford, 2016). Për të përballuar këto sfida, Shqipëria ka bashkëpunuar ngushtë me NATO-n dhe partnerët e tjerë ndërkombëtarë për të forcuar sigurinë dhe për të luftuar financimin dhe rekrutimin e terrorizmit. Kërcënimet asimetrike, të cilat përfshijnë taktika që sfidojnë fuqitë tradicionale ushtarake, janë bërë gjithashtu më të shpeshta. "Kërcënimet hibride kërkojnë një qasje fleksibël dhe inteligjente ndaj mbrojtjes, ku vendet të ndajnë burimet dhe përvojat për të përballuar sfidat e përbashkëta." Hoffman, F. G. (2007). Kërcënime të tilla përfshijnë veprimtari të krimit të organizuar, kontrabandën e drogës dhe armëve dhe migracionin e paligjshëm, të cilat prekin drejtpërdrejt Shqipërinë për shkak të pozitës së saj strategjike në rrugët e Ballkanit. Për të përballuar këto kërcënime, Shqipëria ka përforcuar bashkëpunimin rajonal dhe ka ndërtuar kapacitete më të mëdha për monitorimin e kufijve dhe luftimin e krimit të organizuar (Duka, 2012).

Qasja e mbrojtjes në epokën e globalizimit. "Kostot e larta të armatimeve moderne nënkuptojnë se vetëm përmes ndarjes së burimeve dhe bashkëpunimit mund të arrihet një mbrojtje efektive." Cordesman, A. H. (2014). Në epokën e globalizimit, koncepti i sigurisë dhe mbrojtjes ka ndryshuar thellësisht. Mbrojtja nuk shihet më si një çështje ekskluzive e territorit kombëtar, por si një komponent i integruar në sigurinë ndërkombëtare dhe rajonale. Shqipëria, si anëtare e NATO-s, është përfshirë në një sistem të mbrojtjes kolektive që synon të garantojë sigurinë e të gjithë aleancës përballë kërcënimeve globale (Weiss, 2018). Qasja e re e mbrojtjes përfshin një kombinim të forcave tradicionale ushtarake dhe teknologjive të avancuara, duke përfshirë kapacitetet kibernetike, mbrojtjen e hapësirës ajrore dhe detare, dhe bashkëpunimin në fushat e inteligjencës dhe sigurisë. Globalizimi ka sjellë edhe nevojën për një rishikim të strategjive të mbrojtjes, duke vendosur theksin te bashkëpunimi ndërkombëtar dhe ndarjen e burimeve. Smart Defense, një koncept promovuar nga NATO, synon të maksimizojë përdorimin e burimeve të kufizuara përmes bashkëpunimit dhe koordinimit të ngushtë midis aleatëve (Kaplan, 2015). Shqipëria ka filluar të adoptojë këtë qasje, duke integruar forcat e saj të armatosura në operacionet e përbashkëta të NATO-s dhe duke kontribuar në misionet paqeruajtëse ndërkombëtare. Pra, mjedisi i sigurisë ndërkombëtare ka ndryshuar ndjeshëm për shkak të zhvillimeve gjeopolitike dhe teknologjike, dhe këto ndryshime kanë pasur një ndikim të madh në politikat e sigurisë të Shqipërisë. "Luftërat e reja kërkojnë strategji të reja dhe Smart Defense është një përgjigje ndaj sfidave që nuk mund të përballohen vetëm me forca ushtarake tradicionale." Kaldor, M. (2013).

Evolucioni i kërcënimeve kibernetike, terrorizmi dhe kërcënimet asimetrike kanë sfiduar strategjitë tradicionale të mbrojtjes dhe kanë detyruar Shqipërinë të adaptojë qasje më të sofistikuara dhe bashkëpunuese. Në epokën e

globalizimit, mbrojtja nuk mund të kufizohet më vetëm në kufijtë kombëtarë, por kërkon një integrim të thelluar në strukturat ndërkombëtare të sigurisë, të cilat Shqipëria ka filluar t'i adoptojë me sukses.

Përdorimi i aseteve në kushtet e Shqipërisë: Koncepti dhe zhvillimi i tij

Në botën e sotme, ku kërcënimet ndaj sigurisë janë gjithnjë e më komplekse dhe të ndërlidhura, strategjitë tradicionale të mbrojtjes kombëtare nuk janë më të mjaftueshme për të garantuar sigurinë e vendeve të vogla si Shqipëria. Kërcënimet moderne, si sulmet kibernetike, terrorizmi ndërkombëtar dhe veprimet asimetrike, kërkojnë qasje më të koordinuara dhe më të efektshme për të menaxhuar burimet e kufizuara. Në këtë kontekst, koncepti i ekonomizimit të aseteve ka marrë një rëndësi të veçantë, sidomos për vendet që janë pjesë e aleancave ndërkombëtare si NATO. Ky artikull shqyrton origjinën e konceptit të Smart Defense, elementet e tij kryesore dhe mënyrën se si ky koncept po zbatohet në Shqipëri në kuadrin e strategjive mbrojtëse të aleancës.

Origjina e Konceptit të ekonomizimit. Ky koncept u promovua për herë të parë nga NATO në vitin 2012, në përgjigje të nevojës për një qasje më të efektshme ndaj mbrojtjes kolektive. Pas krizës financiare globale të vitit 2008, shumë vende aleate të NATO-s filluan të përjetonin presione të mëdha buxhetore që kufizuan investimet e tyre në mbrojtje. Për t'u përballur me këto sfida, nisma synoi të maksimizonte efikasitetin e burimeve të mbrojtjes përmes bashkëpunimit ndërmjet aleatëve dhe përdorimit më efektiv të teknologjive të reja (Kaplan, 2015). Në vend që secili shtet të investonte veçmas në kapacitete të shtrenjta mbrojtëse, përqendrimi i tyre ofroi një platformë për ndarjen e përgjegjësive dhe burimeve përmes projekteve të përbashkëta të NATO-s, duke rritur kështu kapacitetin e mbrojtjes kolektive.

Në kontekstin e Shqipërisë, ky koncept është veçanërisht i rëndësishëm, pasi vendi përballet me sfida të mëdha për shkak të buxhetit të kufizuar ushtarak dhe nevojës për të modernizuar forcat e saj të armatosura. Anëtarësimi i Shqipërisë në NATO i ka mundësuar vendit të përfitojë nga avantazhet e kësaj qasjeje, duke kontribuar në projekte kolektive dhe duke përmirësuar kapacitetet mbrojtëse përmes bashkëpunimit me partnerët aleatë (Duka, 2012). Zbatimi i tij ka bërë të mundur që Shqipëria të luajë një rol më të madh në sigurinë rajonale dhe ndërkombëtare, pa pasur nevojën për shpenzime të mëdha në armatim të shtrenjtë. "Pushteti i butë dhe kapacitetet teknologjike janë dy elementë që duhet të kombinohen në mënyrë të zgjuar për një mbrojtje më efektive dhe të përballueshme." Nye, J. S. (2011).

Elementet kryesore të ekonomizimit të burimeve bazohet në tre drejtime kryesore: *mbrojtjen kolektive, koordinimin ndërmjet aleatëve, dhe përdorimin*

me efiçencë të burimeve. Të tre këto elemente janë thelbësore për të garantuar që vendet anëtare të NATO-s të mund të përballojnë sfidat e sigurisë globale në mënyrë të koordinuar dhe të suksesshme.

- **Mbrojtja kolektive**: Në thelb të ekonomizimit të burimeve qëndron parimi i mbrojtjes kolektive, i cili nënkupton që një sulm kundër një vendi anëtar të NATO-s konsiderohet një sulm kundër të gjithë aleancës. Ky parim është thelbësor për sigurinë e vendeve të vogla si Shqipëria, të cilat nuk kanë kapacitete të mjaftueshme për t'u mbrojtur të vetme kundër kërcënimeve të mëdha. Përmes tij, Shqipëria mund të mbështetet tek aleatët e saj për të garantuar sigurinë kombëtare, duke kontribuar njëkohësisht në operacionet kolektive të mbrojtjes (Fischer, 2009).
- **Koordinimi ndërmjet aleatëve**: Një nga sfidat kryesore me të cilat përballen vendet aleate është mungesa e koordinimit në investimet ushtarake. Investimi në modernizim kërkon të zgjidhë këtë problem duke inkurajuar vendet aleate të koordinojnë përpjekjet e tyre mbrojtëse dhe të ndajnë burimet. Për shembull, në vend që çdo vend të ndërtojë kapacitete të plota ushtarake në fusha të ndryshme, vendet aleate mund të specializohen në fusha të veçanta dhe të mbështeten tek njëra-tjetra për kapacitetet që u mungojnë (Kaplan, 2015). Në këtë mënyrë, Shqipëria mund të përqendrojë burimet e saj në fushat ku ka përparësi, ndërkohë që përfiton nga kapacitetet e vendeve të tjera aleate.
- **Përdorimi me efiçencë i burimeve**: Në vetvete ky parim synon të maksimizojë përdorimin e burimeve të kufizuara përmes optimizimit të teknologjisë dhe ndarjes së përgjegjësive. Teknologjia luan një rol të rëndësishëm në këtë drejtim, duke i mundësuar vendeve të përdorin pajisje dhe sisteme më të avancuara për të përballuar kërcënimet moderne. Shqipëria, si një vend me burime të kufizuara, ka përfituar nga kjo qasje duke përmirësuar kapacitetet e saj teknologjike dhe duke përdorur burimet e saj në mënyrë më efektive përmes pjesëmarrjes në projekte të përbashkëta të NATO-s (Duka, 2012).

Efikasiteti i përdorimit të burimeve dhe Shqipëria: Sfida dhe perspektivat për të ardhmen

Për Shqipërinë, përqendrimi i burimeve paraqet një mundësi të madhe për të përmirësuar kapacitetet e saj mbrojtëse dhe për të kontribuar në sigurinë rajonale dhe ndërkombëtare. Ndërsa vendi vazhdon të integrohet në strukturat euroatlantike, efikasiteti i përdorimit ofron një platformë për bashkëpunim të ngushtë me aleatët dhe për ndarjen e përgjegjësive në mbrojtjen kolektive. Megjithatë, për zbatimin e suksesshëm të tij në Shqipëri, ka disa sfida që duhen adresuar. Një nga sfidat kryesore për Shqipërinë është **kufizimi i burimeve**

financiare dhe teknologjike. Ndërsa efiçenca e investimit synon të optimizojë përdorimin e burimeve përmes bashkëpunimit, Shqipëria ka nevojë për investime të mëtejshme për të përmirësuar kapacitetet teknologjike të saj, sidomos në fushat e mbrojtjes kibernetike dhe teknologjive të mbikëqyrjes (Fischer, 2009). Rritja e buxhetit të mbrojtjes dhe bashkëpunimi me partnerët ndërkombëtarë do të jetë vendimtar për përmirësimin e kapacitetit mbrojtës të vendit.

Një tjetër sfidë është **rritja e kapaciteteve të personelit ushtarak**. Për të zbatuar strategjitë e burimeve të mbrojtjes, Shqipëria duhet të investojë në trajnim dhe aftësim të personelit të saj ushtarak, sidomos në fushën e teknologjisë dhe mbrojtjes kibernetike. Përmes programeve të trajnimit të NATO-s dhe bashkëpunimeve dypalëshe me vendet e tjera anëtare, Shqipëria mund të rrisë kapacitetet e saj në këto fusha dhe të përmirësojë gatishmërinë e saj për t'u përballur me kërcënimet e reja. **Perspektivat për të ardhmen** janë pozitive, megjithatë. Përmes zbatimit të kësaj qasje, Shqipëria ka filluar të integrohet më ngushtë në arkitekturën e mbrojtjes kolektive të NATO-s dhe të përfitojë nga ndarja e burimeve dhe përvojave me aleatët e saj. Vendi ka një potencial të madh për të luajtur një rol më të madh në sigurinë rajonale dhe për të kontribuar në operacionet e përbashkëta të NATO-s, duke u bazuar në parimin e ndarjes së barrës dhe ndihmës reciproke. "Forca ushtarake tradicionale ka kufizime në një botë të ndërlidhur, dhe vetëm përmes një qasjeje inteligjente dhe të përbashkët mund të arrihet siguria e qëndrueshme." Smith, R. (2007).

Pra, përmes parimeve të mbrojtjes kolektive, koordinimit ndërmjet aleatëve dhe përdorimit më të efektshëm të burimeve, Shqipëria ka arritur të rrisë kapacitetet e saj mbrojtëse dhe të kontribuojë në sigurinë rajonale. Megjithëse sfidat janë të mëdha, veçanërisht në aspektin e financimit dhe kapaciteteve teknologjike, Shqipëria ka treguar angazhim të fortë për të përmbushur detyrimet e saj ndaj NATO-s dhe për të përmirësuar sigurinë kombëtare. Në të ardhmen, zhvillimi i mëtejshëm i ekonomizimit të përdorimit të burimeve në Shqipëri do të kërkojë investime të qëndrueshme, bashkëpunim të ngushtë me partnerët ndërkombëtarë dhe përkushtim për të përballuar sfidat që lidhen me teknologjinë dhe personelin. Vetëm përmes një qasjeje të tillë, Shqipëria mund të sigurojë që të jetë e gatshme për të përballuar kërcënimet e reja dhe të mbrojë sovranitetin e saj në një botë gjithnjë e më të ndërlidhur.

Krahasimi midis konceptit tradicional dhe ekonomizimit të burimeve në kushtet e Shqipërisë

Siguria kombëtare ka qenë gjithmonë një aspekt thelbësor për çdo shtet, veçanërisht për vendet e vogla si Shqipëria. Tradicionalisht, koncepti i mbrojtjes ishte i përqendruar në ruajtjen e sovranitetit dhe integritetit territorial

përmes forcave të armatosura. Ky koncept, i quajtur **mbrojtja tradicionale**, u formua gjatë periudhës së Luftës së Ftohtë, kur kërcënimet ndaj sigurisë kombëtare ishin kryesisht të natyrës ushtarake dhe territoriale. Megjithatë, me zhvillimet globale dhe ndryshimet në natyrën e kërcënimeve u paraqit koncepti i **përafrimit të aseteve**, veçanërisht në kuadër të NATO-s. Kjo ese do të shqyrtojë avantazhet dhe dizavantazhet e këtyre dy koncepteve në Shqipëri, evoluimin e strategjive kombëtare dhe ndërkombëtare dhe shembuj të implementimit të njehsimit të burimeve në vende të ndryshme.

Avantazhet dhe dizavantazhet e konceptit tradicional dhe ekonomizimit të burimeve. Mbrojtja tradicionale është e përqendruar kryesisht në ruajtjen e integritetit territorial përmes forcave ushtarake dhe mobilizimit të brendshëm të shtetit. Avantazhi kryesor i kësaj qasjeje është qartësia dhe kontrolli i drejtpërdrejtë që një shtet ka mbi mbrojtjen e tij. Shqipëria, veçanërisht gjatë periudhës komuniste, mbështetej tek kjo qasje, ku çdo qytetar ishte i përfshirë në mbrojtjen e vendit përmes një strategjie të rezistencës popullore (Duka, 2012). Kjo qasje theksonte rëndësinë e një mbrojtjeje të decentralizuar, duke garantuar që forcat e brendshme mund të reagojnë ndaj çdo kërcënimi ushtarak.

Megjithatë, **dizavantazhi kryesor i mbrojtjes tradicionale** është varësia e saj nga burimet e brendshme, të cilat në raste të caktuara, siç është rasti i Shqipërisë, mund të jenë të kufizuara. Shqipëria ka përballuar vështirësi të mëdha për të modernizuar forcat e saj ushtarake dhe për të siguruar burime të mjaftueshme për një mbrojtje efektive gjatë tranzicionit pas-komunist (Fischer, 2009). Ky model është gjithashtu i kufizuar për t'u përballur me kërcënimet e reja që nuk janë vetëm ushtarake, por përfshijnë sulme kibernetike, terrorizëm dhe kërcënime asimetrike.

Nga ana tjetër, **unifikimi i pajisjeve dhe teknikës** është një qasje që promovon bashkëpunimin ndërkombëtar dhe përdorimin më efikas të burimeve përmes projekteve kolektive. Ky koncept u prezantua nga NATO në vitin 2012 për të përmirësuar mënyrën se si vendet aleate menaxhojnë mbrojtjen e tyre, veçanërisht në kontekstin e presioneve buxhetore dhe kërcënimeve të reja (Kaplan, 2015). Avantazhi kryesor i implementimit të teknologjive të njëjta është që i lejon vendeve me burime të kufizuara, si Shqipëria, të përfitojnë nga teknologjitë dhe kapacitetet e aleatëve të saj. Përmes këtij koncepti, Shqipëria mund të kontribuojë në projekte kolektive të mbrojtjes pa pasur nevojë të ndërtojë të gjitha kapacitetet vetë. "NATO përfaqëson një shembull të unifikimit të burimeve dhe ideve, ku vendet anëtare mund të ndajnë përgjegjësitë për të arritur një mbrojtje më të koordinuar dhe më të fuqishme." Sloan, S. (2016). Megjithatë, *dizavantazhi kryesor i unifikimit teknologjik* është varësia e shtuar nga aleatët. Ndërsa unifikimi teknologjik nënkupton

ndarjen e barrës midis vendeve anëtare, kjo qasje mund të krijojë një ndjenjë pasigurie për shtetet që ndihen më të ekspozuara ndaj kërcënimeve rajonale ose globale. Shqipëria, si një vend i vogël në Ballkan, mund të ndiejë presione të jashtme nga aktorë të fuqishëm si Rusia apo Kina, të cilët kanë interes strategjik në rajon (Orford, 2016).

Evolucioni i strategjive kombëtare dhe ndërkombëtare në drejtim të mbrojtjes inteligjente

Me kalimin e kohës, strategjitë e sigurisë dhe mbrojtjes kanë pësuar ndryshime të thella për të përballuar sfidat e reja globale. Mbrojtja tradicionale, e fokusuar në ruajtjen e kufijve dhe mbrojtjen nga kërcënimet ushtarake, ka evoluar për të përfshirë një qasje më holistike, e cila përfshin kërcënimet jokonvencionale. Kërcënimet si terrorizmi, krimi i organizuar dhe sulmet kibernetike kanë nxitur nevojën për një **mbrojtje inteligjente** dhe një qasje më bashkëpunuese në fushën e sigurisë.

Në Shqipëri, ky evolucion ka qenë i dukshëm që pas anëtarësimit të vendit në NATO. Anëtarësimi ka detyruar Shqipërinë të modernizojë dhe përmirësojë kapacitetet e saj mbrojtëse për t'u përputhur me standardet e aleancës. **Strategjia Kombëtare e Mbrojtjes** e Shqipërisë tani përqendrohet në forcimin e mbrojtjes kolektive, modernizimin e forcave të armatosura dhe forcimin e kapaciteteve kibernetike për të përballuar kërcënimet moderne (Duka, 2012).

Në kuadrin ndërkombëtar, njehsimi teknologjik ka qenë një mjet i rëndësishëm për të menaxhuar burimet e kufizuara të vendeve anëtare dhe për të garantuar një **mbrojtje më efikase dhe të koordinuar**. NATO ka inkurajuar vendet e saj anëtare të investojnë në teknologji dhe projekte të përbashkëta që ndihmojnë në përmirësimin e kapaciteteve të përgjithshme të aleancës pa pasur nevojë për shpenzime të mëdha individuale (Weiss, 2018). Ky ndryshim në strategjitë ndërkombëtare ka mundësuar një qasje më të përballueshme dhe më të sofistikuar ndaj mbrojtjes.

Shembuj praktikë të implementimit të unifikimit teknologjik në vende të ndryshme. Ky investim ka treguar sukses në disa vende që kanë përfituar nga bashkëpunimi ndërkombëtar dhe ndarja e burimeve. Një nga shembujt më të njohur është programi **NATO Airborne Warning and Control System (AWACS)**, ku disa vende aleate ndajnë avionët e mbikëqyrjes ajrore. Ky program ka lejuar vende të vogla si Shqipëria të përfitojnë nga kapacitetet ajrore të NATO-s pa pasur nevojën për të investuar në avionë të shtrenjtë vetjakë (Kaplan, 2015). Ky model është një shembull i qartë i suksesit të këtij modeli, pasi ndihmon në mbulimin e boshllëqeve në mbrojtjen kombëtare përmes bashkëpunimit me aleatët.

Një tjetër shembull i suksesshëm i investimit me bazë të njëjtë është **përdorimi i teknologjive të reja** për të përmirësuar kapacitetet kibernetike të vendeve anëtare. Shqipëria ka filluar të ndërtojë kapacitete më të fuqishme në mbrojtjen kibernetike, veçanërisht pas sulmeve kibernetike që goditën institucionet e saj në vitin 2022. Përmes ndihmës së NATO-s dhe partnerëve të saj ndërkombëtarë, Shqipëria ka filluar të forcojë infrastrukturën e saj kibernetike për të përballuar kërcënimet e reja (Fischer, 2009). Gjithashtu kjo praktikë ka ndihmuar vendet me burime të kufizuara të investojnë në projekte të përbashkëta të **mbrojtjes detare**. Për shembull, disa vende aleate kanë ndërtuar një flotë të përbashkët për mbrojtjen detare në Mesdhe, duke ndarë burimet e tyre dhe duke përmirësuar sigurinë e përgjithshme të rajonit (Orford, 2016). Këto praktika kanë treguar se janë një zgjidhje e qëndrueshme dhe efektive për të përballuar sfidat e përbashkëta të mbrojtjes, veçanërisht për vendet me burime të kufizuara si Shqipëria. Ky bashkëpunim ndërmjet vendeve anëtare të NATO-s lejon që kapacitetet e mbrojtjes të maksimizohen përmes ndarjes së burimeve dhe teknologjive, duke krijuar një sistem më të fortë dhe më të përgjegjshëm ndaj kërcënimeve rajonale dhe globale.

Shqipëria ka filluar të përfitojë nga koncepti i Smart Defense përmes pjesëmarrjes në operacione dhe misione të përbashkëta të NATO-s dhe bashkëpunimeve rajonale me vendet e Ballkanit. **Pjesëmarrja në operacionet e përbashkëta paqeruajtëse** dhe në mbrojtjen e hapësirës ajrore në kuadër të NATO-s ka forcuar ndjeshëm rolin e Shqipërisë në arkitekturën e sigurisë rajonale (Weiss, 2018). Ky është një shembull i qartë se si Smart Defense ka lejuar Shqipërinë të rrisë kapacitetet e saj mbrojtëse pa kërkuar burime të mëdha financiare të brendshme.

Në përfundim, **Smart Defense** ofron një qasje moderne dhe më efikase ndaj sfidave të sigurisë për vendet me burime të kufizuara si Shqipëria. Ndërsa **mbrojtja tradicionale** ofronte avantazhe të caktuara në ruajtjen e sovranitetit dhe kontrollit të drejtpërdrejtë mbi forcat mbrojtëse, ajo është bërë e pamjaftueshme për të përballuar kërcënimet e reja të epokës moderne, siç janë sulmet kibernetike dhe terrorizmi ndërkombëtar. Smart Defense, nga ana tjetër, promovon bashkëpunimin ndërkombëtar dhe ndarjen e burimeve, duke lejuar Shqipërinë të rrisë kapacitetet e saj përmes integrimit me aleatët e NATO-s.

Megjithëse ka disa dizavantazhe, si varësia e shtuar nga aleatët, Smart Defense ofron një zgjidhje më të qëndrueshme për sfidat e sigurisë në epokën e globalizimit. Përmes investimeve të mëtejshme në teknologji dhe përfshirjes në projekte të përbashkëta, Shqipëria ka potencialin për të përmirësuar mbrojtjen e saj dhe për të kontribuar në sigurinë rajonale dhe ndërkombëtare. Evolucioni i strategjive të mbrojtjes nga një qasje tradicionale në një model inteligjent është një hap i rëndësishëm për Shqipërinë dhe vendet e tjera të

vogla, të cilat kërkojnë të sigurojnë sovranitetin dhe stabilitetin e tyre në një botë gjithnjë e më të ndërlidhur.

Sfida dhe perspektivat për të ardhmen në kushtet e Shqipërisë

Në kontekstin e Shqipërisë, koncepti i **ekonomizimit të burimeve** përfaqëson një hap të rëndësishëm për modernizimin e mbrojtjes kombëtare dhe përfshirjen e vendit në sistemet e sigurisë ndërkombëtare, sidomos në kuadrin e NATO-s. Megjithatë, ka disa sfida të rëndësishme që duhen tejkaluar për të garantuar zbatimin e plotë dhe efektiv të kësaj qasjeje. Vështirësitë përfshijnë mungesën e burimeve financiare, të teknologjisë së avancuar dhe mungesën e koordinimit të duhur midis aktorëve kombëtarë dhe ndërkombëtarë. Përkundër këtyre sfidave, ekzistojnë mundësi të konsiderueshme për përmirësim dhe zhvillim të mëtejshëm të zhvillimit teknologjik në Shqipëri, veçanërisht përmes bashkëpunimit rajonal dhe përmirësimit të kapaciteteve teknologjike dhe njerëzore. "Luftërat e së ardhmes do të kërkojnë një përzierje të fuqisë ushtarake tradicionale dhe kapacitetit teknologjik, dhe njehsimit teknologjik është rruga drejt kësaj përzierje." Thompson, L. (2013).

Vështirësitë e adoptimit të investimit teknologjik në Shqipëri

Një nga sfidat kryesore me të cilat përballet Shqipëria në adoptimin e **teknologjisë së njëjtë me aleatët** është **mungesa e burimeve financiare**. Shqipëria, si një vend me ekonomi të vogël, ka kufizime të mëdha në buxhetin e saj të mbrojtjes, gjë që e bën të vështirë modernizimin e forcave të saj të armatosura dhe investimin në teknologji të avancuara. Për të qenë në gjendje të përfitojë plotësisht nga teknologjia, vendi duhet të investojë në sisteme të mbrojtjes kibernetike, inteligjencë artificiale dhe dronë, por mungesa e fondeve të nevojshme kufizon aftësinë për të zbatuar këto strategji (Kaplan, 2015).

Një tjetër sfidë është **mungesa e koordinimit** midis institucioneve kombëtare dhe partnerëve ndërkombëtarë. Për të zbatuar ekonomizimin e aseteve në mënyrë efektive, është e nevojshme që të ketë një koordinim të ngushtë midis institucioneve shqiptare dhe aleatëve të NATO-s. Për shembull, ndërkohë që Shqipëria ka përparuar në përfshirjen e saj në operacione të përbashkëta të NATO-s, mbetet nevoja për një bashkëpunim më të mirë në shkëmbimin e inteligjencës dhe integrimin e teknologjive të përbashkëta (Weiss, 2018). Mungesa e këtij koordinimi çon në përçarje dhe vështirësi në arritjen e rezultateve efektive.

Mundësitë për përmirësimin dhe zhvillimin e mëtejshëm

Përkundër sfidave, Shqipëria ka disa mundësi të rëndësishme për të përmirësuar dhe zhvilluar më tej kapacitetet e saj në kuadrin e **efikasitetit të burimeve**.

Një nga mundësitë më të mëdha është **bashkëpunimi rajonal**. Ballkani është një rajon që përballet me sfida të përbashkëta të sigurisë, si krimi i organizuar, kërcënimet kibernetike dhe terrorizmi. Përmes përpjekjeve të përbashkëta me vendet e tjera të Ballkanit dhe me partnerët rajonalë, Shqipëria mund të përmirësojë mbrojtjen e saj dhe të ndajë burimet me vendet e tjera të rajonit (Duka, 2012). Krijimi i një platforme të përbashkët për mbrojtjen kibernetike dhe mbikëqyrjen ajrore mund të jetë një hap i rëndësishëm në këtë drejtim. Po kështu rivitalizimi i industrisë ushtarake është një bazë e mirë për implementimin e teknologjisë së njëjtë me ato të aleancës.

Një tjetër mundësi për zhvillim është **modernizimi i kapaciteteve teknologjike** të Shqipërisë. Ndërsa teknologjia luan një rol thelbësor në konceptin e njehsimit teknologjik, Shqipëria duhet të investojë më shumë në teknologji të avancuara dhe infrastrukturën e saj kibernetike dhe atë të industrisë së mbrojtjes. Në këtë drejtim, NATO dhe partnerët e tjerë ndërkombëtarë mund të luajnë një rol të rëndësishëm në mbështetjen e Shqipërisë për të forcuar kapacitetet teknologjike dhe për të zhvilluar infrastrukturën e nevojshme për t›u përballur me kërcënimet moderne (Fischer, 2009).

Pra, ndërsa Shqipëria përballet me sfida të mëdha në zbatimin e modernizimit, përfshirë kufizimet financiare dhe mungesën e koordinimit, ekzistojnë mundësi të mëdha për përmirësim dhe zhvillim të mëtejshëm të kësaj qasjeje. Përmes bashkëpunimit rajonal dhe përmirësimit të kapaciteteve teknologjike, Shqipëria mund të përfitojë plotësisht nga përparësitë që ofron ekonomizimi i aseteve dhe të përforcojë mbrojtjen e saj kombëtare në një botë gjithnjë e më të ndërlidhur dhe të sfiduar nga kërcënimet moderne.

Përfundime dhe rekomandime

Në botën e sotme, ku kërcënimet ndaj sigurisë kombëtare dhe globale janë gjithnjë e më komplekse dhe të larmishme, Shqipëria po përballet me sfida të reja që kërkojnë një qasje të re dhe më të sofistikuar ndaj mbrojtjes. Në këtë kuadër, koncepti i **unifikimit të burimeve të mbrojtjes**, i promovuar nga NATO, ofron një mundësi të jashtëzakonshme për të përmirësuar kapacitetet e mbrojtjes të vendeve me burime të kufizuara, siç është Shqipëria. Megjithatë, për të arritur këto qëllime, është e domosdoshme që Shqipëria të zgjidhë disa sfida kryesore, përfshirë koordinimin më të mirë midis partnerëve ndërkombëtarë dhe sigurimin e burimeve të nevojshme financiare dhe teknologjike.

Në këtë analizë, kemi shqyrtuar si konceptin **tradicional të mbrojtjes**, i cili përqendrohet në mbrojtjen e kufijve kombëtarë përmes forcave të armatosura dhe mobilizimit të burimeve të brendshme, ashtu edhe konceptin më të avancuar të **ekonomizimit të aseteve**, që thekson bashkëpunimin ndërkombëtar dhe përdorimin më efikas të burimeve të kufizuara përmes ndarjes dhe koordinimit

ndërmjet vendeve anëtare të NATO-s. Mbrojtja tradicionale ka qenë thelbësore për Shqipërinë në të kaluarën, veçanërisht gjatë periudhës së komunizmit, kur çdo qytetar dhe pjesë e territorit ishte pjesë e strategjisë mbrojtëse. Megjithatë, kjo qasje është e kufizuar për t'u përballuar me kërcënimet moderne si sulmet kibernetike dhe terrorizmi ndërkombëtar.

Nga ana tjetër, **infrastruktura e përbashkët** ofron një zgjidhje më të qëndrueshme për Shqipërinë në kontekstin e kërcënimeve të reja globale. Përmes ndarjes së përgjegjësive dhe burimeve, Shqipëria mund të përfitojë nga teknologjitë dhe kapacitetet e vendeve të tjera aleate të NATO-s, duke përmirësuar mbrojtjen e saj me kosto më të ulët dhe më të përballueshme. Megjithatë, kjo qasje sjell edhe varësinë e shtuar nga aleatët dhe kërkon një bashkëpunim më të thellë dhe më të organizuar në kuadrin e strategjive të mbrojtjes.

Rekomandimet për politikat e mbrojtjes dhe bashkëpunimin ndërkombëtar

- **Rritja e investimeve në teknologji të avancuara**: Teknologjia është thelbësore për integrimin e resurseve ushtarake, veçanërisht për vendet si Shqipëria që kanë burime të kufizuara financiare. Investimi në sisteme mbrojtëse kibernetike, inteligjencë artificiale dhe pajisje të sofistikuara mbrojtëse mund të përmirësojë ndjeshëm kapacitetet mbrojtëse të vendit. Qeveria shqiptare duhet të vendosë teknologjinë si prioritet të lartë në buxhetin e mbrojtjes, duke kërkuar gjithashtu mbështetje financiare dhe teknike nga NATO dhe partnerët ndërkombëtarë.
- **Përmirësimi i koordinimit ndërkombëtar**: Bashkëpunimi me aleatët e NATO-s është thelbësor për zbatimin e suksesshëm të integrimit të kapaciteteve. Shqipëria duhet të intensifikojë përpjekjet për të bashkëpunuar me vendet e tjera anëtare të NATO-s në fushat e shkëmbimit të inteligjencës, trajnimeve të përbashkëta dhe operacioneve paqeruajtëse. Një koordinim më i ngushtë do të ndihmojë Shqipërinë të përmirësojë kapacitetet e saj dhe të përfitojë më shumë nga përvojat dhe burimet e partnerëve të saj ndërkombëtarë.
- **Zhvillimi i kapaciteteve njerëzore**: Një nga aspektet më të rëndësishme për implementimin e suksesshëm të burimeve njerëzore është trajnimi dhe aftësimi i personelit ushtarak. Shqipëria duhet të investojë më shumë në edukimin dhe specializimin e forcave të saj të armatosura në teknologji dhe taktika moderne. Trajnimet e ofruara nga NATO dhe programet ndërkombëtare të mbrojtjes janë thelbësore për rritjen e kapaciteteve të personelit ushtarak shqiptar.
- **Bashkëpunimi rajonal**: Shqipëria duhet të forcojë bashkëpunimin me

vendet e tjera të Ballkanit për të përballuar kërcënimet e përbashkëta të sigurisë. Ballkani përballet me sfida të tilla si krimi i organizuar, kërcënimet kibernetike dhe migracioni i paligjshëm. Duke krijuar aleanca dhe partneritete rajonale, Shqipëria mund të ndihmojë në ndarjen e burimeve dhe të përmirësojë mbrojtjen e përbashkët të rajonit. Kjo do të zvogëlonte presionin mbi burimet e brendshme të Shqipërisë dhe do të siguronte një mbrojtje më të koordinuar ndaj kërcënimeve rajonale.

- **Politikat për rritjen e buxhetit të mbrojtjes**: Për të përmbushur standardet e NATO-s dhe për të zbatuar me sukses ekonomizimin e burimeve, Shqipëria duhet të rrisë buxhetin e saj të mbrojtjes. Edhe pse vendi përballet me kufizime ekonomike, një përqindje më e lartë e buxhetit shtetëror duhet t'i kushtohet forcimit të kapaciteteve të mbrojtjes. Një politikë e tillë do të ndihmojë Shqipërinë të forcojë pavarësinë e saj mbrojtëse, ndërsa përfiton nga bashkëpunimi ndërkombëtar.

Përfundime

Në një mjedis të sigurisë që ndryshon me shpejtësi, Shqipëria duhet të jetë gati për të përballuar kërcënimet moderne që variojnë nga sulmet kibernetike deri te sfidat gjeopolitike rajonale. Integrimi i burimeve të mbrojtjes ofron një qasje më bashkëkohore dhe të përballueshme për vendet e vogla, por kërkon një përkushtim të madh nga ana e Shqipërisë për të rritur investimet në teknologji dhe për të forcuar bashkëpunimin me aleatët e saj ndërkombëtarë. Me një planifikim të duhur dhe përkushtim politik, Shqipëria ka mundësinë të forcojë mbrojtjen e saj dhe të kontribuojë në sigurinë rajonale dhe ndërkombëtare.

Literatura e shfrytëzuar:

1. Bjola, C., & Kornprobst, M. (2013). *Understanding International Diplomacy: Theory, Practice, and Ethics*. London: Routledge.
2. Boot, M. (2006). *War Made New: Technology, Warfare, and the Course of History, 1500 to Today*. New York: Gotham Books.
3. Collins, A. (Ed.). (2016). *Contemporary Security Studies*. Oxford: Oxford University Press.
4. Cordesman, A. H. (2014). *The Middle East in Transition: The New Regional Dynamics*. Washington, DC: Center for Strategic and International Studies.
5. Duka, F. (2012). *Historia e Ushtrisë Shqiptare*. Tiranë: Botimet Albania.
6. Fischer, B. (2009). *Shqipëria gjatë Luftës së Dytë Botërore*. Tiranë: Toena.

7. Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies.
8. Kaldor, M. (2013). *New and Old Wars: Organised Violence in a Global Era* (3rd ed.). Stanford: Stanford University Press.
9. Kaplan, R. D. (2015). *The Revenge of Geography: What the Map Tells Us About Coming Conflicts and the Battle Against Fate*. New York: Random House.
10. Nye, J. S. (2011). *The Future of Power*. New York: PublicAffairs.
11. Orford, A. (2016). *International Authority and the Responsibility to Protect*. Cambridge: Cambridge University Press.
12. Smith, R. (2007). *The Utility of Force: The Art of War in the Modern World*. New York: Knopf.
13. Sloan, S. (2016). *Defense of the West: NATO, the European Union and the Transatlantic Bargain*. Manchester: Manchester University Press.
14. Thompson, L. (2013). *The New Face of War: How War Will Be Fought in the 21st Century*. New York: Free Press.
15. Weiss, T. G. (2018). *Humanitarian Intervention*. Malden: Polity Press.

Direktiva Gjithëpërfshirëse e Planizimit të Operacioneve dhe risitë në Procesin e Planizimit të Operacioneve

Nënkolonel Msc. Mazllum ALLA
Specialist në IKSHU

Trajtesë e shkurtuar.

Direktiva Gjithëpërfshirëse e Planizimit të Operacioneve (COPD), versioni 2.0, për gati një dekadë ka qenë dokumenti kryesor i planizimit të operacioneve në nivelet strategjik dhe operacional. E përdorur në mënyrë të vazhdueshme nga strukturat e NATO-s dhe pjesërisht nga vendet anëtare të Aleancës, kjo Direktivë arriti në fazën ku mësimet e identifikuara nxorën në pah nevojën për rishikimin e saj, me synimin për ta përmirësuar dhe përafruar me kërkesat e reja dhe ndryshimet në mjedisin e veprimit. Bazuar në versionin e mëparshëm, versioni i ri i COPD-së përshkruan në detaje proceset e planizimit përkatësisht për nivelet strategjik dhe operacional, duke mbetur një dokument bazë për procesin e planizimit të operacioneve të përbashkëta të aleancës. Nëpërmjet këtij shkrimi, synohet të theksohen elementet e reja dhe të nënvizohen ndryshimet në procesin e planizimit të operacioneve. Si rrjedhojë, publikimi i dokumentit të ri të COPD-së, kërkon përshtatjen e arsyeshme dhe maturimin e planizimit të operacioneve të FA-ve, në nivelet strategjik dhe operacional.

Fjalë kyçe: COPD; planizimi i operacioneve; procesi i planizimit; niveli strategjik; niveli operacional.

Hyrje

Direktiva Gjithëpërfshirëse e Planizimit të Operacioneve të Komandës së Operacioneve të Aleancës, Versioni 3.0, e njohur shkurt si COPD[1], u publikua zyrtarisht më 15 janar 2021 dhe zëvendësoi botimin e mëparshëm të vitit 2013 (ACO COPD Interim Version 2.0), që për gati një dekadë ka qenë dokumenti kryesor i planizimit të operacioneve në nivelet strategjik dhe operacional. E përdorur në mënyrë të vazhdueshme nga strukturat e NATO-s dhe pjesërisht nga vendet anëtare të Aleancës, kjo Direktivë arriti në fazën ku mësimet e identifikuara pas zhvillimit të stërvitjeve, përdorimit në operacione si dhe ndryshimeve në strukturat e NATO-s, nxorën në pah nevojën për rishikimin e saj.

Nga ana tjetër, ndryshimet në mjedisin e sigurisë dhe efektet që i pasuan ato sollën nevojën për reflektimin e ketyre ndryshimeve duke zëvëndësuar versionin 3.0, me version 3.1 që u publikua zyrtarisht më 12 Tetor 2023, me synimin për ta përafruar me kërkesat e reja të Komandës së Operacioneve (ACO). Duhet theksuar se COPD v3.1 *nuk* është një përditësim themelor dhe nuk paraqet asnjë ndryshim në Procesin e Planizimit të Operacioneve. Ajo paraqet ndryshime të vogla nga versioni i vitit 2021, për të korrigjuar disa pasaktësi dhe paqartësi të vogla gjuhësore, si rezultat i vëzhgimeve dhe reagimeve të marra gjatë zhvillimit të Kurseve të Planizimit të Operacioneve.[2]

Vitet e fundit mjedisi i veprimit ka ndryshuar dhe është bërë më kompleks me shumë aktorë, si dhe me interesat dhe axhendat e tyre përkatëse, politike dhe ushtarake. Prandaj, NATO e ka përshtatur procesin e planizimit të operacioneve me zhvillimet dhe kërkesat e reja, të cilat rezultuan në një Direktivë të re të Planizimit të Operacioneve si dokumenti bazë për planizimin e operacioneve në nivelin strategjik dhe operacional.

Procesi aktual i planizimit të NATO-s bazohet në planizimin paralel dhe një qasje gjithëpërfshirëse. Fazat e ndryshme të planizimit janë të lidhura me njëra-tjetrën si horizontalisht (fazë pas faze) ashtu edhe vertikalisht (planizimi paralel në të gjitha nivelet). Brenda këtij procesi kompleks ka faza dhe produkte që janë kritike edhe për planizimin e operacioneve nga FA-të. Prandaj, komandantët dhe shtabet e forcave duhet ta kuptojnë dhe të jenë të familjarizuar me këtë proces planizimi, i cili me botimin e Direktivës së Planizimit të Operacioneve të FARSH do të shtrihet në përdorim në të gjitha strukturat e saj.

---

[1] COPD – **C**omprehensive **O**perations **P**lanning **D**irective.

[2] COPD v.3.1, 2023, fq. 1

Vlen të theksohet se Direktiva e re e Planizimit të Operacioneve të NATO-s vijon qasjen e botimit të mëparshëm, përkatësisht duke dhënë udhëzime të qarta për planizimin e operacioneve, duke ofruar procese, procedura, metoda dhe modele por *pa dhënë recetën magjike,* për suksesin në operacionet ushtarake.

Direktiva e Planizimit të Operacioneve përshkruan procedurat dhe përgjegjësitë që rregullojnë përgatitjen, miratimin, zbatimin dhe rishikimin e planeve të operacionit për të mundësuar një qasje të përbashkët për planizimin e operacioneve.[3] Ashtu si publikimi i mëparshëm edhe COPD v3.1 *përshkruan planizimin e operacioneve në nivelet operacional dhe strategjik brenda strukturave të NATO-s* dhe nuk trajton nivelin taktik, *ku planizimi i operacioneve kryhet në bazë të procedurave dhe proceseve kombëtare të secilit vend*. [4] Megjithatë, metodologjia e kësaj direktive duhet të kuptohet edhe nga strukturat përkatëse të nivelit taktik, për të qenë në gjendje të kryejnë planizim paralel, pasi produktet e nivelit taktik ndikojnë në shkallën me të cilën ato zhvillohen në nivelet më të larta.

Metodologjia e procesit të planizimit mbetet e njëjtë, një qasje nga lart poshtë, në kuptimin që udhëzimet dhe produktet e nivelit strategjik dhe strukturat/ komandat në nivel operacional janë në bashkëveprim të vazhdueshëm me strukturat vartëse. Për më tepër, *fazat e procesit të planizimit* në nivel operacional mbeten të pandryshuara, të strukturuara për të zhvilluar si propozimet dhe produktet e kërkuara nga niveli strategjik, ashtu edhe udhëzimet, direktivat dhe urdhrat e nevojshëm për nivelin taktik. Gjithashtu renditja dhe detajet e procesit të planizimit ruajnë të njëjtën linjë me versionin e mëparshëm, ndryshimet e bëra janë të vogla dhe vetëm me qëllim të sistemimit të informacionit. Këto ndryshime i përkasin organizimit të paragrafëve, prezantimit të termave të rinj të përdorur në strukturat e NATO-s, nxjerrjen në pah të aktiviteteve ose proceseve, riemërtimin e strukturave ose grupeve të punës jo të përhershme, të cilat kanë sjellë qartësi dhe përmirësim nga dokumenti i COPD v2.0.

Nga pikëpamja e elementeve të përmbajtjes së dokumenteve të planizimit, nuk ka ndryshime në krahasim me versionin e mëparshëm. Për më tepër, është ruajtur formati standard për dokumentet kryesore të planizimit, që mundëson njohjen dhe kuptimin më të lehtë të aspekteve që lidhen me planizimin dhe zhvillimin e operacioneve, duke lehtësuar kështu procesin e vendimmarrjes. Gjithashtu nuk ka ndryshime në përmbajtjen dhe emërtimin e planeve të operacioneve.

Analiza krahasuese e dy dokumenteve (COPD v2.0 dhe COPD v3.1) e cila është baza e këtij punimi, nuk do të pasqyrojë asnjë ndryshim apo rinumërim

[3] COPD v.3.1, 2023, fq. 1.1.
[4] Po aty, fq. 1.2.

të paragrafëve. Nëpërmjet këtij shkrimi, synohet të theksohen elementet e reja të COPD v3.1 dhe të nënvizohen ndryshimet dhe shtesat në procesin e planizimit të operacioneve në një kontekst të gjerë analitik. Megjithatë, ky punim nuk ka për qëllim të ofrojë një analizë shteruese të të gjitha ndryshimeve, ju mbetet strukturave përkatëse t'i identifikojnë, analizojnë dhe pasqyrojnë ato në dokumentat e planizimit të operacioneve të FA-ve (veçanërisht në Direktivën e Planizimit të Operacioneve të FARSH).

Në përputhje me objektin e këtij hulumtimi është e nevojshme që fillimisht të qartësohen termat: "*planëzim*" dhe "*planizim*", që do të përdoret gjatë gjithë këtij punimi. Termi i parë përdoret shpesh dhe jam munduar ta diskutoj me shumë kolegë, madje edhe me gjuhtarë të cilët mund të më jepnin një përgjigje shteruese nga ekspertiza e tyre. Ky term ka një përdorim të gjerë vetëm në veprimtarinë ushtarake. Gjithsesi fjala e saktë është "*planizim*" dhe jo "planëzim", sepse sipas drejtshkrimit të gjuhës shqipe[5] fjala plan si rrënja e saj në të gjitha mënyrat, trajta, numri, rasa, lakimi etj. shkruhet pa 'ë 'fundore: plan – plani – plane - planet- planeve dhe jo "planë". Një argument tjetër është se, në pajtim me parimet themelore të drejtshkrimit të shqipes të gjitha fjalët e prejardhura apo të formuara nga rrënja "plan", me anë prapashtesash si p.sh planifikoj, planifikim, planoj, planim, planimetri, plandos, etj. shkruhen pa "ë".[6] Pra nuk shkruhen planëfikim, planëfikoj apo planëmetri. Kështu që në termin planëzim kemi shkelje të parimit morfologjik dhe fjalëformues. Si rrjedhojë duhet shkruajtur: planizim!

Risitë kryesore të Direktivës së Planizimit të Operacioneve (COPD v3.1)

Analiza krahasuese e dokumentit të COPD tregon ndryshimet dhe shtesat si në kapitujt specifikë që detajojnë proceset e planizimit përkatësisht për nivelet strategjik dhe operacional, ashtu edhe në kapitullin hyrës, ku paraqitet korniza për planizimin e operacioneve. Më poshtë do të shtjellohen në mënyrë të përmbledhur elementët kryesorë, të identifikuar në COPD v3.1, të cilët ofrojnë kuadrin e nevojshëm për planizimin e operacioneve dhe i referohen drejtpërdrejt procesit të planizimit në nivel operacional dhe startegjik.

Theksimi i rolit të komandantit gjatë procesit të planizimit që në faqet e para të Direktivës,[7] është i rëndësishëm për të kuptuar më tej se si ata drejtojnë shtabin e planizimit dhe marrin vendimin e duhur, brenda kornizës kohore të përshtatshme për secilën fazë të procesit të planizimit.

[5] Drejtshkrimi i gjuhës shqipe, 1973, fq. 170
[6] Drejtshkrimi i gjuhës shqipe, 1973, fq. 40
[7] COPD v.3.1, 2023, fq.1-2.

Për më tepër, *qasja e re ndaj rolit të komandantit në aspektin e ndërveprimit me shtabin tregon se ai mbetet figura qendrore në drejtimin e të gjithë procesit*. Vështrimi i përgjithshëm i ndërveprimit të komandantit me shtabin/grupin e planizimit i paraqitur grafikisht[8] nga COPD v3 tregon se prania e tij gjatë gjithë procesit siguron përafrimin e masave të planizimit me synimin e tij për të përmbushur objektivat e operacionit. Në të njëjtën mënyrë, përcaktimi dhe paraqitja në kapitullin e parë i koncepteve dhe nocioneve mbi *artin operativ, rrezikun dhe mundësitë, sinkronizimin e fushatës dhe veçanërisht nivelet e komandimit*, ka rolin e parashtrimit dhe shpjegimit të thelbit të këtyre nocioneve, duke u përdorur më pas në të gjithë Direktivën, ku detajohen proceset e planizimit specifike për nivelet strategjik dhe operacional.

Kështu, një nga risitë kryesore është zëvendësimi i frazës mjedis operacional (*operational environment*) me *mjedis veprimi* (operating environment) për të përshkruar "një përbërje të kushteve, rrethanave dhe faktorëve që ndikojnë në përdorimin e aftësive dhe në vendimet e komandantit".[9] Ky ndryshim përputhet me termin e paraqitur dhe të detajuar në Terminologjinë Zyrtare të NATO-s (NATO Term[10] 2022) dhe i pranuar prej të gjithë shteteve anëtare të Aleancës.

Në fakt, vetë termi ka përdorur dy fraza të ndryshme që i bashkëngjiten fjalës operacional: mjedis operacional (*operational environment*) dhe mjedis veprimi (*operating environment*). Për më tepër, ky term është përdorur me kuptim të dyfishtë për të përshkruar mjedisin e operacionit dhe nivelin e operacioneve diktuar nga gjuha angleze. Edhe pse në dukje të ndryshëm, doktrina e NATO-s i referohet termit të parë si mjedis i kryerjes së një operacioni dhe jo mjedisit që i përket nivelit operacional. *Keqkuptimi* për këtë term vlen edhe për FA-*të*, pothuajse të gjitha botimet tona doktrinare, përdorin termin mjedis operacional dhe jo mjedis veprimi, duke përfshirë edhe Direktivën e Planizimit të Operacioneve të FARSH.[11]

Është e rëndësishme të theksohet se ka një dallim të madh ndërmjet këtyre dy termave. Ndërsa në gjuhën angleze këta dy terma janë qartësisht të dallueshëm, në gjuhën shqipe janë përkthyer dhe përdorur me të njëjtin term, mjedis operacional. Për të bërë dallimin në shqip të këtyre dy termave të ndryshëm e konsideroj të përshtatshëm përdorimin e termit "*mjedis veprimi*" në dokumentet doktrinat dhe strukturat tona, jo vetëm për të kuptuar dallimin por në të njëjtën kohë për të shmangur keqkuptimet e tyre.

---

[8] Po aty, fq.4-6.

[9] COPD v.3.1, fq. K-7.

[10] NATO Term, është baza zyrtare e terminologjisë së NATO-s, në https://nso.nato.int/natoterm/content/nato/pages/ntp.html?lg=en.

[11] Direktiva e Planëzimit Operacional të FARSH, Dhjetor 2024, fq 311,

Një tjetër risi është zëvendësimi i frazës *planizim operacional* (operational planning) me *planizim operacioni* (operations planning). Për shumë vite ky ka qenë një nga termat më të keqkuptuara për sa i përket planizimit të operacioneve ushtarake. Për vite me radhë, edhe në botimet tona doktrinare ky term është përdorur me kuptim të dyfishtë për të përshkruar planizimin e operacionit dhe nivelin e planizimit. Doktrina e NATO-s i referohet termit të parë, si proces i planizimit të një operacioni dhe jo planizimit që i përket nivelit operacional. Për më tepër e ka përkufizuar termin "Planizimi i Operacioneve" si: "*Planizimi i operacioneve ushtarake në nivelet strategjik, operacional dhe taktik*". Ndaj, termi i duhur për të përcaktuar planizimin e operacioneve ushtarake në të gjitha nivelet është "*planizimi i operacioneve*". Është e nevojshme të përmendet se, termi "*planizim operacional*" nuk duhet të përdoret më për të parandaluar konfuzionin me planizimin në nivel operacional.[12]

Por, ndryshe nga botimet doktrinore të NATO-s dhe dokumenti i COPD që përdorin këtë "term të ri", Direktiva e Planizimit të Operacioneve të FARSH përdor gjerësisht dhe ka përkufizuar termin "Planëzim Operacional".[13] Madje edhe emërtimi i këtij dokumenti është "Direktiva e Planëzimit Operacional". Siç ka thënë Kenneth Allard (pedagog në National Defense University), "është më e rëndësishme t›i bësh gjërat me të njëjtën mënyrë sesa t›i bësh ato me mënyrën më të mirë.»[14] Ndaj, për të shmangur paqartësinë në të kuptuarit e shprehjeve të ndërlidhura, dhe në bazë të përkufizimeve të miratuara nga NATO, të pranuara (ratifikuara) nga ana jonë, si dhe për të udhëzuar dhe përdorur termin e duhur për strukturat planizuese mendoj se ky dokument duhet emërtuar "*Direktiva e Planizimit të Operacioneve*".

Një aspekt për t'u përmendur është se diferenca thelbësore me Doktrinën për Planizimin e Operacioneve AJP – 5, qëndron në faktin se sipas COPD, Kuptimi i Situatës (*Situational Awareness*) paraqitet si një Fazë e veçantë në kundërshtim me AJP-5, që e paraqet si *një proces të vazhdueshëm të mbledhjes së informacionit gjatë gjithë operacionit*, gjë që është logjike. Kjo do të thotë, nuk është renditur si një fazë e veçantë ose i ashtuquajturi "HAP". Vlen të përmendet se procesi i vlerësimit të situatës ka mbetur si një fazë më vete edhe në nivelin strategjik. Ndërsa, përmbajtja e hapave të tjerë në AJP - 5 është në thelb e njejtë me aktivitetet në faza të veçanta të COPD. Duhet theksuar se Doktrina AJP - 5 është STANAG *dhe qëndron më lart në arkitekturën e planizimit të operacioneve* të Aleancës *sesa* COPD.

Një tjetër aspekt që nuk ndryshon domosdoshmërisht, por vetëm shkakton

[12] COPD v.3.1, fq. 1.7.

[13] Direktiva e Planëzimit Operacional të FARSH, Dhjetor 2024, fq 19.

[14] Kenneth Allard, *Somalia Operations:Lessons Learned*, National Defense University, në http://www.dodccrp.org/files/Allard_Somalia.pdf

paqartësi është përdorimi i termave të ndryshëm për të njëjtat procese ose produkte. Kështu, termi projekt operacional (*operational design*)[15] në COPD v3.1 përdoret si term i dyfishtë si projekt i operacionit (*operations design*) ashtu edhe projekt operacional (*operational design*). Në fakt, një projekt operacioni është kuadri konceptual që mbështet planizimin e operacioneve, një shprehje e vizionit të komandantit, përfytyrim për një operacion të caktuar duke përdorur artin operativ, *nuk është e lidhur vetëm me nivelin operacional, por përdoret në të gjitha nivelet*.

Për më tepër, Doktrina për Planizimin e Operacioneve AJP - 5 (2019) thekson se "*asnjë nivel i caktuar komandimi nuk ka të bëjë vetëm me artin operacional*",[16] ndërsa versioni i ri i COPD nuk është aq i qartë kur thekson: "*Arti operativ ka kuptime të ndryshme gjatë procesit të planizimit të nivelit operacional, veçanërisht në zhvillimin e projektit të operacionit... Zbatimi i artit operativ më së shpeshti lidhet me komandantët dhe shtabet e larta*.."[17] Nga ky këndvështrim, mund të ketë përshtjellime për rolin dhe vendin tradicional të artit operativ. Por, sipas ish-Gjeneralit amerikan James N. Mattis, "projekti i operacionit nuk zëvendëson planizimin, por planizimi është i paplotë pa projektin e operacionit…të dy proceset janë gjithmonë plotësuese, të mbivendosura, sinergjike dhe të vazhdueshme.".[18] Ndërsa, planizimi është një proces, projekti i operacionit është edhe proces edhe një produkt i rëndësishëm i shtabit, që kërkon përdorimin e artit operativ. Sidoqoftë, arti operativ mbetet lidhja kritike midis strategjisë dhe taktikës.

Nga ana tjetër, përdoret edhe termi korniza e operacionit (*operations framework)* dhe korniza operacionale *(operational framework*). Këta terma, edhe pse në dukje të ndryshëm, përdoren në fakt të këmbyeshëm edhe tek doktrinat tona, pavarësisht planizimit në nivel strategjik, operacional apo taktik. Megjithatë, duhet theksuar se kjo paqartësi është zgjidhur në dokumentin e Doktrinës së Përbashkët për Planizimin e Operacioneve (AJP 5) botimi 2019, e cila përdor termin projekt i operacionit (*operations design*).[19] Mendoj se ky term, duhet të përdoret edhe në doktrinat dhe dokumentet tona si dhe gjatë planizimit të operacioneve ushtarake në të gjitha nivelet.

Sa i përket *projektit të operacionit* një tjetër ndryshim është se COPD v3.1 paraqet një mënyrë logjike për ta zhvilluar atë, së bashku me pikëpamjen se

---

[15] COPD v.3.1, fq.1-18 dhe fq. 4-60.

[16] AJP-5 *Allied Joint Doctrine for the Planning of Operations*, (Doktrina e Përbashkët e Aleancës për Planëzim e Operacioneve)" 2019, p. 3-3.

[17] COPD v.3.1, fq. 1.11.

[18] James N. Mattis, *Vision for a Joint Approach to Operational Design*. Norfolk, VA: U.S. Joint Forces Command, October 6, 2009, fq.6.

[19] Allied Doctrine Joint for Operations Planning (AJP 5), 2019, fq. 3-1.

qasja e përdorur nga grupi i planizimit mund të ndryshojë, në varësi të situatës, udhëzimeve të ofruara nga komandanti dhe përvojës së shtabit/grupit të planizimit. Kështu, *elementi i parë i projektit të operacionit janë linjat e operacioneve*, sepse zhvillimi i tyre do të formësojnë zhvillimin e planit dhe kryerjen e operacioneve, dhe për rrjedhojë, qasja e nënkuptuar e COPD v3.1 është që duhet të ketë një linjë operacioni për çdo objektiv. Nga ana tjetër, futja, përcaktimi dhe detajimi *i pikave të vendimmarrjes* në projektin e operacionit synon të optimizojë përdorimin dhe sinkronizimin e burimeve të disponueshme, pas çdo vendimi të komandantit.[20] Megjithatë, duhet theksuar se *projekti i operacionit trajtohet më në detaje në kapitullin 3 të* AJP-5 *sesa në* COPD.

Një tjetër ndryshim në dokumentin e COPD *ka të bëjë me katër instrumentet e fuqisë*. Versioni i mëparshëm i COPD 2.0 shtjellonte instrumentet e fuqisë në bazë të konstruktit PMEC[21] (Politike, Ushtarake, Ekonomike dhe Civile). Ndërsa, tani *instrumentet e fuqisë shtjellohen në bazë të konstruktit* DIME[22]*, (Diplomatike, Informative, Ushtarake dhe Ekonomike),* duke qenë se NATO, si Aleancë e Sigurisë, ushtron kontroll vetëm mbi instrumentet diplomatike/politike (pjesërisht) dhe ushtarake (parësore).[23] Renditja e fazave të Procesit të Reagimit ndaj Krizave të NATO-s (i referuar më parë si Procesi i Menaxhimit të Krizave të NATO-s) e përforcon këtë ndryshim, pasi të kuptuarit sesi vendimmarrja strategjike në nivelin e NAC-ut[24] siguron, brenda një afati kohor të arsyeshëm, udhëzime dhe këshilla në nivel strategjik të nevojshme për të planëzuar dhe zbatuar një operacion.

Ndër risitë kryesore është, *kalimi nga planizimi* në një mjedis shumëdimensional në *planizimin* në një *mjedis me shumë fusha,* që do të jetë një nga sfidat e planizimit të operacioneve, si për strukturat e NATO-s edhe për vendet anëtare. Duke pasur parasysh angazhimin e konsiderueshëm të personelit që kërkohet për të integruar, sinkronizuar dhe konverguar aftësitë në të gjithë fushat ajrore, tokësore, detare, hapësinore dhe kibernetike, është i nevojshëm një staf profesional që mund të përballojë planizimin e këtyre operacioneve. *Operacionet me shumë fusha (multi-domain operations) përfaqësojnë një ndryshim thelbësor në Konceptin e Luftimit të NATO-s*.[25] Ky koncept transformues do të mundësojë ndikimin strategjik dhe do të sinkronizojë

[20] COPD v.3.1, fq. 4-65, 4-66.

[21] PMEC – **P**olitical, **M**ilitary, **E**conomic, and **C**ivil.

[22] DIME – **D**iplomatic, **I**nformation, **M**ilitary, and **E**conomic.

[23] COPD v.3.1, fq. 1.14.

[24] NAC – **N**orth **A**tlantic **C**ouncil. (*Këshilli i Atlantikut të Veriut*).

[25] Faqja e Komandës së ACT, *NATO Warfighting Capstone Concept: An Adaptive 20-year Strategy for NATO and its Allies*, Prill 2023, në https://www.act.nato.int/article/nato-warfighting-capstone-concept-an-adaptive-20-year-strategy-for-nato-and-its-allies/

aftësitë e të gjithë aleatëve. Forcat ushtarake të vendeve anëtare në fusha të caktuara luajnë një rol vendimtar; por po aq i rëndësishëm është sinkronizimi i aftësive ushtarake me Instrumentet e Fuqisë të integruara në nivel kombëtar. Për shembull, veprimet nga disa vende anëtare të NATO-s ndaj aktorëve malinj janë përqendruar në sanksionet ekonomike, fushatat e informimit dhe veprimtarinë diplomatike. Këto aktivitete kryhen kryesisht në nivel kombëtar, si Ministria e Jashtme ose institucione financiare, dhe janë shembuj kryesorë të rolit që luajnë Instrumentet Kombëtare të Fuqisë në Operacionet me Shumë Fusha.[26] Në këtë kontekst, për të përgatitur dhe kryer operacione me shumë fusha (*multi-domain operations*), është e nevojshme të zhvillohet një proces planizimi i detajuar, duke përfshirë të gjithë faktorët dhe aktorët përkatës për kryerjen efikase të këtyre operacioneve.

Është e rëndësishme të theksohet se *operacionet e përbashkëta karakterizohen me një fokus kolektiv* dhe *bashkëpunimi ndërmjet forcave ushtarake*. Kjo do të thotë se, strukturat e komandës së bashkuar promovojnë koordinimin me forcat e tjera të armatosura, ndërsa *koncepti i operacioneve me shumë fusha shkon përtej kësaj qasje duke përfshirë mjetet ushtarake dhe jo ushtarake*,[27] - që është një nga tiparet kryesore dallues ndërmjet "operacioneve të përbashkëta" dhe "operacioneve me shumë fusha".

Në mbështetje të procesit të planizimit, COPD v3.1 *prezanton shkurtimisht tre platforma planizimi* të zhvilluara në bazë të aplikacioneve/shërbime funksionale në internet dhe të përdorura nga NATO: INTEL FS[28], TOPFAS[29] and LOGFAS[30], përkatësisht zbulimi, operacionet dhe logjistika. Qëllimi i këtyre platformave, është mbështetja e shtabit të përfshirë në planizimin dhe zhvillimin e operacioneve, në nivel politik, strategjik dhe operacional. Megjithatë, në varësi të rolit të nivelit taktik dhe veçorive të procesit të planizimit, këto platforma mund të përdoren edhe në këtë nivel. Krahasuar me versionin e mëparshëm, në të cilin bëheshin vetëm referenca për këto platforma, në varësi të mënyrës se si mund të mbështesnin procese ose produkte të ndryshme, COPD v3.1 i paraqet ato në një pjesë të veçantë, me përkatësitë, komponentët dhe opsionet e tyre specifike.[31]

Një tjetër risi është *integrimi i elementit ndërlidhës/koordinues i planizimit* të

---

[26] Faqja e Komandës së ACT, *Multi-Domain Operations in NATO – Explained*, tetor 2023, në https://www.act.nato.int/article/mdo-in-nato-explained/

[27] Po aty

[28] INTEL FS – **Intel**ligence **F**unctional **S**upport (*Mbështetje Funksionale e Zbulimit*).

[29] TOPFAS – Tool for Operations Planning Functional Area Services (*Mjet për Shërbimet Funksionale të Planizimit* të Operacioneve)

[30] LOGFAS – **L**ogistic **F**unctional **A**rea **S**ervices (*Shërbimet Funksionale të Logjistikës*)

[31] COPD V3.1, fq 1-24.

operacioneve (OPLE)[32] në nivel strategjik, i cili siguron jo vetëm marrëdhënien e grupeve të planizimit në të dy nivelet, por edhe mbështetjen në zhvillimin e produkteve të tyre. I përbërë nga staf me përvojë në planizimin e nivelit operacional dhe që ka ndërvepruar me grupin e planizimit (JOPG)[33], OPLE është i familjarizuar me procesin e planizimit të komandës që përfaqëson, si dhe me veçoritë e nivelit strategjik dhe, *në versionin e ri të COPD*, siguron koordinimin e veprimeve ndërmjet dy niveleve.[34]

Ndërsa termi Përgatitja Gjithëpërfshirëse e Mjedisit të Veprimit (CPOE)[35] është përdorur në COPD v2.0 për të përshkruar vlerësimin e mjedisit të veprimit, COPD v3.1 sjell në vëmendjen e planëzuesve termin *Kuptimi Gjithëpërfshirës i Mjedisit të Veprimit* (CUOE)[36], duke theksuar kështu nevojën për të marrë njohuri, interpretim dhe të kuptimit të tyre në kontekstin e një krize. I paraqitur si një proces ndërmjet strukturave të një komande, CUOE mbështetet nga funksione dhe specialitete të veçanta të shtabit, disa prej të cilave kanë procesin e tyre për të kontribuar në CUOE, siç është Përgatitja e Përbashkët me Zbulim e Mjedisit të Veprimit (JIPOE),[37] e detajuar në doktrinën e NATO-s AJP-2.[38]

Po aq i rëndësishëm është specifikimi në fazën 1[39] të procesit të planizimit, në të cilin, shefi i J2 drejton procesin e përgatitjes me zbulim (JIPOE) për të zhvilluar dhe monitoruar kuptimin fillestar të krizës, ndërsa grupi i planizimit ndërvepron me stafin e zbulimit për të identifikuar kërkesat për informacion, si pjesë e zhvillimit të CUOE. Kjo kufizon, përgjegjësitë për zhvillimin e JIPOE dhe CUOE, si dhe faktin që të *dy proceset nuk janë identike, por vetëm plotësuese*. Për të kuptuar mjedisin e veprimit dhe ndikimin e tij në planizimin dhe zhvillimin e një operacioni të përbashkët, grupi i planizimit në fillim të fazës 3[40] të procesit të planizimit kryen, një *analizë të faktorëve të kohës, hapësirës, forcës, informacionit dhe marrëdhëniet e tyre specifike*. Kjo analizë, që nuk përshkruhej në COPD v2.0, do të ndihmojë planëzuesit e nivelit operacional në analizën e mëtejshme të faktorëve kryesorë dhe qendrave të rëndesës. Duke detajuar faktorët e kohës, hapësirës, forcës dhe informacionit dhe marrëdhëniet specifike midis tyre, COPD v3.1 siguron linjëzimin me dispozitat e AJP-5, Doktrina e Përbashkët për Planizimin e Operacioneve.[41]

---

[32] OPLE – **O**perational **P**lanning and **L**iaison **E**lement.
[33] JOPG – **J**oint **O**perations **P**lanning **G**roup.
[34] COPD V3.1, fq.3-22.
[35] CPOE – **C**omprehensive **P**reparation of **O**perational **E**nvironment.
[36] CUOE – **C**omprehensive **U**nderstanding of the **O**perating **E**nvironment.
[37] JIPOE – **J**oint **I**ntelligence **P**reparation of the **O**perating **E**nvironment.
[38] COPD V3.1, fq.4-13
[39] Faza 1 – Vlerësimi fillister i situates për një krizë aktuale ose në zhvillim.
[40] Faza 3 – Vlerësimi Operacional
[41] AJP-5, 2019, fq. A-1.

Një element kyç i artit operativ është *identifikimi i qendrave të rëndesës të aktorëve kry*esorë me qëllim që të mund të realizohen objektivat e caktuara. Për shkak se *analiza dhe identifikimi i qendrave të rëndesës është një proces i vazhdueshëm*, COPD v3.1 *sjell një qasje të re*, të dobishme në të njëjtën kohë, për konceptin e qendrës së rëndesës, duke plotësuar kështu informacionin e pakët në botimin e mëparshëm. Në lidhje me këtë ndryshimet parësore janë:

- Është përditësuar përkufizimi i qendrës së rëndesës, si «*burimi kryesor i fuqisë që i siguron një aktori forcën, lirinë e veprimit dhe/ose vullnetin për të luftuar*"[42], duke e njësuar me përkufizimin e terminologjisë së NATO-s (NATO Term).
- Është shprehur qartë se, *në nivel operacional, qendra e rëndesës do të jetë gjithmonë një entitet*[43], duke shmangur kështu diskutimet se ku mund të identifikohet ajo. Gjithashtu është e rëndësishme të theksohet se, kur zhvillohen kurset e veprimit, njësia/forca që do të jetë përgjigja e pyetjes *kush do ta kryejë operacionin*? bëhet qendra e rëndesës për atë kurs veprimi.[44]
- Në këtë dokument *janë dhënë më shumë detaje mbi qendrën e rëndesës*, duke i dhënë këtij koncepti rëndësinë e duhur për nivelin operacional.
- Analiza e qendrës së rëndesës fokusohet në karakteristikat/elementet kyçe të secilit aktor, duke filluar me vlerësimin e qëllimeve dhe objektivave, aftësive kritike, kërkesave kritike dhe dobësive kritike dhe duke kulmuar me përcaktimin e qendrës së rëndesës. Sipas versionit të ri të COPD-së, *hapi kryesor në analizën e qendrës së rëndesës është nxjerrja e përfundimeve*,[45] ku mund të përcaktohen objektivat dhe efektet e mundshme, në mënyrë që të shfrytëzohen dobësitë, boshllëqet ose mangësitë në elementët e identifikuar më parë të kundërshtarit ose të forcave tona;
- Informacioni i dhënë në këtë dokument siguron një qasje të unifikuar për identifikimin e qendrës së rëndesës në nivel operacional. Për më tepër, *detajet e paraqitura në Aneksin B* të AJP-5, *së bashku me elementët e* COPD v3.0 *sigurojnë njohuritë e nevojshme për të kuptuar konceptin e qendrës së rëndesës*.

Një tjetër ndryshim i rëndësishëm, është bërë për të kuptuar rëndësinë e *rrezikut të operacionit*[46] (si gjasat e shfaqjes, peshës së ndikimit, masat zbutëse) dhe

[42] COPD V3.1, fq. 4-53.
[43] Po aty, fq. 4-54.
[44] Po aty, fq. 4-75.
[45] Po aty, fq. 4-55, d.(6)
[46] Po aty, fq. 4-57.

nevoja për të përfshirë komandantin në përcaktimin e nivelit të pranueshmërisë së rrezikut. Në të njëjtin mënyrë, *koncepti i mundësive operacionale paraqitet si një risi në nivel operacional* dhe zakonisht lidhet me pranimin e rrezikut në analizën e faktorëve të kohës, hapësirës, forcave/aktorëve dhe të informacionit në zonën e operacionit[47]. Kështu, formatet e produkteve të planizimit në nivel operacional janë plotësuar nga ky koncept i ri, dhe në paraqitjen e analizës së misionit dhe kornizës së operacionit, komandantit *duhet t'i paraqitet edhe analiza e rrezikut dhe e mundësive* të bëra nga shtabi/grupi i planizimit.

Pas përpunimit të planit të operacionit në nivel strategjik dhe miratimit të planit/planeve të nivelit operacional, kërkohet rregullimi, koordinimi dhe drejtimi i aktiviteteve të mëpasshme, në nivel strategjik dhe operacional, në kohë dhe hapësirë, në varësi të evolimit të mjedisit të veprimit. Për këtë, COPD V3.1 paraqet si zgjidhje Urdhrin e Koordinimit Strategjik (SCO[48]). Pra, *ky urdhër është mekanizmi dhe, në të njëjtën kohë, produkti, i cili jep udhëzime për komandat vartëse për sinkronizimin e planeve dhe operacioneve në nivel operacional*, si pjesë e fushatës së përgjithshme ushtarake. Nga ana tjetër, ndërsa sinkronizimi i fushatës ushtarake në nivel strategjik kryhet, nëpërmjet Urdhrit të Koordinimit Strategjik (SCO), në nivel operacional sinkronizimi, udhëzimet e detajuara dhe orientimi i vartësve arrihet me përdorimin e Urdhrit të Përbashkët të Koordinimit[49] (JCO[50]). Formati i një Urdhri Koordinimi nuk është dhënë, por me shumë gjasa do të ndjekë formatin standard të një urdhri operacioni.[51]

Në mbështetje të komunikimit në çdo nivel dhe, në mënyrë të veçantë, të planëzuesve, *COPD v2.0 paraqiste në Shtojcën A*, elementet përcaktues në lidhje me objektivat, efektet dhe kushtet vendimtare dhe, më e rëndësishmja, një qasje praktike në lidhje me hartimin e tyre.[52] Kjo siguronte një standardizim të mënyrës së të menduarit dhe të përshkruarit të këtyre elementeve, por edhe një gjuhë të përbashkët ndërmjet grupeve të planizimit në nivele të ndryshme, me përparësi në harkun kohor të disponueshëm. *COPD v3.1 e ka hequr këtë aneks* për faktin se këto elementë janë miratuar më parë dhe duhet vetëm të përpunohen ose për faktin se ato do të rifuten në procedura të tjera ose udhëzime funksionale.

---

[47] Po aty, fq. 4-57.
[48] SCO – **S**trategic **C**oordination **O**rder.
[49] COPD V3.1, fq. 1-13
[50] JCO – **J**oint **C**oordination **O**rder.
[51] COPD V3.1, fq. 3-128. Pika d.
[52] COPD V2.0 2013, A-1÷A-5.

Përfundime

Direktiva e Planizimit të Operacioneve mbetet dokumenti bazë i planizimit të strukturave të NATO-s të përfshira në planizimin e operacioneve në nivelet strategjik dhe operacional dhe një udhëzues i nevojshëm për drejtimin e planizimit të operacioneve për nivelin taktik. Planizimi dhe zhvillimi i operacioneve të përbashkëta janë veprimtari të udhëhequra nga komandanti dhe të kryera nga shtabi/grupi i planizimit. Ndërsa proceset dhe mjetet për kryerjen e këtyre aktiviteteve përshkruhen nga kjo direktivë. Me një numër më të madh faqesh krahasuar me versionin e mëparshëm, versioni i ri bashkon nocionet e teorisë dhe praktikës mbi planizimin e operacioneve duke përshkruar proceset dhe produktet e nevojshme.

Analiza e dokumentit, e cila shpreh disa pikëpamje të bazuara në përvojën personale, ka evidentuar disa elementë, të cilët janë ndryshuar në versionin e ri, dhe mund të keqinterpretohen nga planizuesit e operacioneve në strukturat e FA-ve. Dihet se *planizimi i operacioneve përfshin zhvillimin e produkteve të ndryshme, në nivele të ndryshme, në mënyrë bashkëpunuese dhe shpesh nën presionin e pamëshirshëm të kohës*. Proceset e planizimit të përdorura për çdo nivel sigurojnë si pasqyrimin e propozimeve të bëra në nivele të larta, ashtu edhe përpunimin e urdhrave apo udhëzimeve të dërguara strukturave vartëse, në përputhje me vizionin dhe synimet e komandantit.

Logjikisht, ky dokument do të ndryshohet më tej si rezultat i rishikimit të rregullt të doktrinave dhe publikimeve në nivel të Aleancës, ose si rezultat i mësimeve të nxjerra nga përdorimi i këtij varianti, që do të ndikohet në mënyrë të pashmangshme nga veprime, fenomene apo koncepte të reja.

COPD ka normuar disa terma, për këtë arsye edhe në dokumentat e planizimit në FA duhet të përdoren terma të sakta doktrinore për të përcaktuar qartë kuptimin e tyre. Njohja, kuptimi dhe përdorimi i kësaj direktive është jo vetëm e domosdoshme por edhe e detyrueshme (edhe pse shtetet anëtare mund të zgjedhin nëse do ta zbatojnë atë apo jo) për strukturat e FA, veçanërisht shtabin e përgjithshëm, si strukturë e nivelit strategjik dhe personelin që përfaqsohemi në strukturat e NATO-s.

Së fundmi, është e rëndësishme të theksohet se, si një vend anëtar me aftësi të kufizuara, ne nuk mund të planizojmë me një dokument që përshkruan struktura gjigande, si komandat e operacioneve të NATO-s. Megjithatë, elementi kryesor i një dokumenti të çdo lloji janë të dhënat dhe jo strukturat. Ndaj, është e domosdoshme një ***"përshtatje e arsyeshme"*** e këtij dokumenti në përputhje me strukturën aktuale të FA-së. *Në fakt, është për tu theksuar se pas më shumë se një dekade me botimin e mëparshëm të COPD, ne kemi tashmë një dokument të planizimit* të operacioneve të FARSH *të lidhur me*

këtë direktivë! Por, në fund të fundit, koha do ta tregojë sesa praktik dhe i përdorshëm do jetë ky dokument i ri për strukturat tona.

Për më tepër, Forcat tona duhet të përgatiten për të vepruar në të tre nivelet (strategjik, operacional dhe taktik) por që *në të vërtetë ne na mungon niveli operacional*; ndaj përshtatja e COPD-së duhet të jetë zgjedhja numër një për një proces planizimi operacionesh në nivel strategjik. Nga ana tjetër edhe pse COPD, është një dokument i vështirë për t'u përtypur nga strukturat tona, përdorimi në anglisht në kurset e ndryshme në AFA, terminologjia dhe qasja e përgjithshme e saj do të kishin shumë përfitim për personelin përfaqësues në strukturat e NATO-s dhe stërvitjet e përbashkëta shumëkombëshe. Mbi të gjitha, sfida më e madhe do të jetë gjithmonë zbatimi praktik i saj. Duke cituar Klauseviçin që thoshte "*Dituria duhet të transferohet në aftësi*", ne duhet të përshtatim jo vetëm procesin e planizimit, por edhe aftësitë për ta përdorur atë në stërvitje dhe operacione pa marrë parasysh nivelin e komandës.//

Literaturë e shfrytëzuar

1. AJP-5. *Allied Joint Doctrine for the Planning Of Operations, Edition A Version 2, Maj 2019.*
2. COPD V2.0. *Allied Command Operations Comprehensive Operations Planning Directive, 4 Tetor* 2013.
3. COPD V3.0. *Allied Command Operations Comprehensive Operations Planning Directive,* 15 Janar 2021.
4. COPD V 3.1 *Allied Command Operations Comprehensive Operations Planning Directive 13 Tetor 2023.*
5. *Direktiva e Planëzimit Operacional të FARSH,* dhjetor 2024*,*
6. NATO Term*, The Official NATO Terminology Database.* 20 Janar 2025, në https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en.
7. *NATO Warfighting Capstone Concept* (NWCC), Allied Command Transformation, 2021.

INSTRUMENTET LIGJORE KOMBËTARE DHE NDËRKOMBËTARE NË LUFTËN KUNDËR TERRORIZMIT: CENIMI I SIGURISË KOMBËTARE

Msc. Jurgert ZAVALANI
Jurist në Akademinë e Forcave të Armatosura

Trajtesë e shkurtuar.

Krimi dhe terrorizmi janë dy fenomene që kanë shoqëruar historinë e njerëzimit për shekuj me radhë, duke ndikuar në mënyrën si shtetet, shoqëritë dhe individët e shohin sigurinë dhe drejtësinë. Ata shpesh shërbejnë si katalizatorë për ndryshime sociale dhe politike dhe janë një reflektim i luftës dhe tensioneve që ndodhin në shoqëritë e ndryshme.

Krimi shoqërohej me luftëra dhe përpjekje për pushtet, ku individë ose grupe të caktuara përfitonin nga situata të caktuara për të arritur qëllimet e tyre. Më vonë, me krijimin e shtetit të fortë dhe të centralizuar, krimi mori një formë më të strukturuar. Krijimi i forcave të rendit dhe agjencive ligjzbatuese, si policia, ka ndihmuar në ndalimin e veprimeve kriminale, por gjithashtu ka nxitur zhvillimin e krimit të organizuar dhe korrupsionit. Nga sa më sipër, ditët e sotme del si domosdoshmëri ballafaqimi i eksperiencave në luftën kundër krimit dhe terrorizmit në fushën e jurisprudencës, pasi terrorizmi sot nuk është vetëm një e keqe më ngjyrime rajonale dhe nacionale, por përmasat janë globale ndaj kërkon jo vetëm shkëmbim informacioni, por edhe veprim në bllok për të parandaluar dhe luftuar këtë fenomen që rrezikon jo vetëm bashkëjetesën por gjithashtu edhe cenon rëndë sigurinë kombëtare.

Ky shkrim synon të nxitë mendimin për të rritur ndërgjegjësimin e organeve ligjvënëse në rëndësinë dhe domosdoshmërinë e miratimit të paketave ligjore, të cilat duhet t'i shërbejnë shtetit për parandalimin dhe luftimin e terrorizmit,

duke pasur parasysh që është një nga faktorët kryesore që cenon sigurinë kombëtare dhe atë ndërkombëtare.

Për përgatitjen e këtij punimi janë studiuar dhe ofruar shembuj kombëtarë, ndërkombëtarë e rajonalë në përgatitjen e konventave, akteve ligjore dhe nënligjore, si dhe praktikave të veçanta për luftën kundër terrorizmit, duke hulumtuar boshllëqet, mangësitë dhe përmirësimet që mund të rekomandohen për modelin e luftës kundër terrorizmit të shtetit shqiptar, në aspektin e cenimit të sigurisë kombëtare.

Fjalë kyçe: terrorizëm, krim, cenim i sigurisë, akte ligjore dhe nënligjore, lufta kundër terrorizmit, agjenci ligjzbatuese, konventë.

Hyrje

Historia e njerëzimit ka qenë gjithmonë e shoqëruar nga dy aspekte: krimi dhe terrorizmi. Disa prej ngjarjeve më të rëndësishme, që kanë ndodhur në periudha të ndryshme, në lidhje me këto dy fenomene, kanë ndikuar në zhvillimin e shoqërive dhe në ndërtimin e shteteve moderne.

Këto dy fenomene kanë evoluar për të marrë forma gjithnjë e më të sofistikuara dhe shkatërruese dhe janë përdorur si një mjet për të arritur qëllime politike ose ideologjike, duke shkaktuar frikë dhe panik në mesin e civilëve. Terrorizmi është përdorur nga individë, grupe të armatosura dhe shtete të ndryshme për të destabilizuar shoqëritë dhe për të pasur ndikim të drejtpërdrejtë në politikat e brendshme dhe ndërkombëtare.

Bota perëndimore, popujt e Afrikës dhe Lindja e Mesme tashmë po tronditen vazhdimisht nga fenomene terroriste, të cilat vënë në rrezik rregullat e bashkëjetesës dhe janë kërcënim i vazhdueshëm për sigurinë mbarëbotërore. Ky fakt shqetësues ka shtyrë komunitetin ndërkombëtar drejt një pune të koordinuar për të ndërtuar një paketë të plotë ligjore në përballjen dhe luftën kundër terrorizmit.

Organizata e Kombeve të Bashkuara (OKB), Bashkimi Europian (BE), si dhe organizata të tjera rajonale të shumë vendeve të botës, veçanërisht pas shtatorit 2001, hodhën një hap të rëndësishëm në përpilimin e Konventave dhe paketave ligjore, që do të disiplinonin masat parandaluese dhe bashkëvepruese të luftës kundër terrorizmit ndërkombëtar dhe mos-cenimit të sigurisë kombëtare, rajonale e botërore. Kjo është arsyeja pse terrorizmi ndërkombëtar dhe lufta kundër tij me instrumente ligjore është shndërruar në një fushë të re studimi dhe analize që po tërheq gjithnjë e më tepër vëmendjen, jo vetëm të organeve përgjegjëse të sigurisë kombëtare në mbarë botën, por është bërë dhe një fushë ku ka shumë debate të shumë në fushën juridike. Studiuesi Luigi Bonanate shprehet se: *"Neoterrorizmi, kjo armë brutale, efikase dhe e jashtëzakonshme,*

vuri në vëmendje të veçantë ngjarjet politike të këtij shekulli, duke iu përshtatur situatave më të ndryshme, një galaktikë në lëvizje që është e vështirë, por jo e pamundur për ta hetuar".[1]

Terrorizmi në të gjitha format dhe mënyrën e shfaqjes së tij përbën një kërcënim të përgjithshëm për paqen dhe sigurinë botërore. Fenomeni i terrorizmit në nivel kombëtar dhe ndërkombëtar është një ndër sfidat më të vështira për të sotmen dhe për të ardhmen. Siguria kombëtare e Republikës së Shqipërisë përfaqëson tërësinë e mjeteve dhe instrumenteve shtetërore që sigurojnë mbrojtjen e qytetarëve, të shoqërisë dhe të shtetit shqiptar nga kërcënimet dhe rreziqet e jashtme e të brendshme.

Shqipëria është ndër vendet e para të renditura në koalicionin kundër terrorizmit, e cila, përgjatë viteve, ka përmirësuar legjislacionin si dhe ka ngritur kapacitete të reja të specializuara për të adresuar këtë fenomen. Shqipëria është pjesëmarrëse aktive në përpjekjet e koordinuara të partnerëve të saj strategjikë SHBA dhe BE kundër fenomenit të ekstremizmit të dhunshëm dhe terrorizmit. Që prej vitit 2013,[2] vendi ynë ka miratuar strategjinë kundër terrorizmit, e cila përveçse ka krijuar mekanizmat e nevojshëm, ajo ka ofruar edhe një qasje gjithëpërfshirëse për parandalimin dhe goditjen e terrorizmit. Ky është dokumenti strategjik kryesor kundër terrorizmit. Ai garanton vazhdimësinë në menaxhimin e këtij fenomeni dhe ka për qëllim fuqizimin e mëtejshëm të mekanizmave ekzistues, ndaj situatave dhe dinamikave aktuale të kërcënimeve nga terrorizmi.

1. Terrorizmi dhe e drejta ndërkombëtare. Konventa e Këshillit të Evropës për Parandalimin e Terrorizmit

Konventa për Parandalimin e Terrorizmit përbën një bazë solide dhe një instrument shumë të rëndësishëm ligjor. Qëllimi i hartimit të kësaj Konvente është zgjerimi i përpjekjeve të të gjitha shteteve palë në parandalimin e terrorizmit dhe efekteve të tij, duke përcaktuar masa që duhet të merren në nivel kombëtar dhe nëpërmjet bashkëpunimit ndërkombëtar, duke pasur parasysh zbatimin e marrëveshjeve ose traktateve dypalëshe ose shumëpalëshe, midis palëve.[3] Konventa i referohet politikave kombëtare të parandalimit dhe veçanërisht përfshin katër aspekte që lidhen me parandalimin: trajnimi, edukimi, kultura, media dhe ndërgjegjësimi i publikut; bashkëpunimi ndërmjet autoriteteve shtetërore; promovimi i tolerancës dhe bashkëpunimi i qytetarëve me

---

[1] Luigi Bonanate, *Le terrorisme international*. Casterman,1994.

[2] Vendim i Këshillit të Ministrave nr. 663, datë 17.07.2023 "Për miratimin e strategjisë ndërsektoriale të luftës kundër krimit të organizuar, trafiqeve të paligjshme dhe terrorizmit, 2013-2020 dhe planit të veprimit për vitet 2013 - 2016".

[3] Konventa e Këshillit të Evropës për Parandalimin e Terrorizmit, Varshavë, 2005, neni 2.

autoritetet shtetërore[4]. Konventa parashikon bashkëpunimin ndërkombëtar, që synon zgjerimin e kapaciteteve të shteteve palë, në përpjekjet për parandalimin e terrorizmit. Konventa u bën thirrje shteteve palë të asistojnë dhe mbështesin njëri-tjetrin, duke përfshirë shkëmbimin e informacionit, trajnime dhe përpjekje të përbashkëta si skuadra të përbashkëta për analiza dhe investigime në luftë kundër terrorizmit[5].

Shprehimisht në këtë Konventë kërkohet nga shtetet palë të saj që të përjashtohen masa ligjore në legjislacionin e brendshëm, duke parashikuar figura të reja të veprave penale, sidomos ato vepra penale të cilat parashikohen edhe nga dispozitat e Konventës, sidomos të neneve 5, 6, 7 të saj. Po ashtu, Konventa parashikon shprehimisht si vepër penale provokimin publik për kryerjen e një akti terrorist në bazë të të cilit: *provokim publik për kryerjen e një akti terrorist,* do të thotë shpërndarja e mesazheve publikut ose bërja e ditur e këtyre mesazheve me qëllim nxitjen e kryerjes së një akti terrorist. Në bazë të kësaj dispozite nuk kërkohet që të ketë ardhur pasoja kriminale, domethënë kryerja e aktit terrorist, por nga ana objektive do të mjaftonin veprimet kriminale të shpërndarjes së mesazheve publikut me qëllim për të provokuar kryerjen e një akti terrorist[6]. Konventa përcakton detyrimin që çdo shtet të parashikojë në legjislacionin e brendshëm penal si figure të re krimi, veprën penale të provokimit publik për kryerjen e një akti terrorist.[7]

Konventa parashikon si vepër penale rekrutimin për qëllime terroriste në bazë të të cilit: *rekrutimi për qëllime terrorizmi,* do të thotë që t'i kërkohet një personi tjetër që të marrë pjesë ose t'i bashkohet një grupi me qëllim për të marrë pjesë në kryerjen e një ose më shumë akteve terroriste[8]. Në Konventë, përsëri kërkohet që shtetet palë të saj të përshtatin masa të tilla në legjislacionin e brendshëm penal, në mënyrë që kjo figurë krimi të parashikohet si vepër penale[9]. Konventa parashikon një figurë të re krimi, pikërisht atë të trajnimit për qëllime terroriste. *Trajnimi për qëllime terroriste*, do të thotë dhënia e instruksioneve lidhur me përdorimin e eksplozivëve, armëve të zjarrit, armëve të tjera ose dhënia e instruksioneve për përdorimin e substancave të rrezikshme, metodave të posaçme ose teknikave të tjera, me qëllim përdorimin e tyre për kryerjen e akteve terroriste[10]. Konventa kërkon që nga shtetet palë të saj të parashikohet në legjislacionin e brendshëm kjo figurë krimi si vepër penale[11].

[4] Po aty, neni 3.
[5] Po aty, neni 4.
[6] Po aty, neni 5, parag. 1.
[7] Po aty, neni 5, parag. 2.
[8] Po aty, neni 6, parag. 1
[9] Po aty, neni 6, parag. 2.
[10] Po aty, neni 7, parag. 1
[11] Po aty, neni 7, parag. 1.

Konventa përcakton që shtetet palë të Konventës të marrin masa në legjislacionin e brendshëm që të parashikohen si veprime kriminale të dënueshme edhe format e bashkëpunimit, të veprave penale të mësipërme e konkretisht, pjesëmarrjen e një personi si bashkëpunëtor për kryerjen e veprave të mësipërme, organizimin ose drejtimin e personave të tjerë, me qëllim për të kryer veprat penale të mësipërme, dhënien e ndihmës për kryerjen e këtyre veprave e bërë me qëllimin për të vazhduar veprimtarinë kriminale të mëtejshme, si dhe e bërë duke e ditur se personat e mësipërm kanë dijeni dhe me vetëdije do të kryejnë akte terroriste. Duke vëzhguar Ligjin Penal, parashikohet bashkëpunimi i personave për kryerjen e një vepre penale, si institucion i përgjithshëm i të drejtës penale. Megjithatë mendojmë që bashkëpunimi i personave që kanë kryer veprat penale të parashikuara nga Konventa, të cilësohet si i veçantë, pra, si rrethanë cilësuese për kryerjen e akteve terroriste, kur këto vepra penale janë kryer sipas neneve 5, 6, 7 të Konventës[12].

Në Konventë parashikohet detyrimi, që të përcaktohet në legjislacionin e brendshëm përgjegjësia penale, civile dhe administrative e personave juridike, duke mos përjashtuar përgjegjësinë individuale, lidhur me pjesëmarrjen në veprat terroriste. Lidhur me këtë nen të Konventës theksojmë se ligji për përgjegjësinë penale, të personit juridik pritet të miratohet së shpejti nga Kuvendi[13]. Po ashtu, Konventa përcaktohet se çdo shtet palë duhet të marrë masat e nevojshme, për të parashikuar veprat e përcaktuara në nenet 5, 6, 7 dhe 9 të kësaj Konvente, si të dënueshme, duke vendosur dënime efektive, proporcionale në raport me rrezikshmërinë e veprës, njëkohësisht edhe parandaluese[14]. Në Konventë parashikohet që çdo shtet duhet të sigurojë që parashikimi dhe zbatimi i veprave penale të neneve 5, 6, 7 dhe 9 të kësaj Konvente duhet të bëhet në përputhje me respektimin e detyrimeve të Konventës Europiane për Liritë dhe të Drejtat Themelore të Njeriut, veçanërisht të së drejtës së shprehjes, të drejtës për t'u organizuar, lirisë fetare, Konventës Ndërkombëtare për të Drejtat Civile dhe Politike, si dhe detyrimeve të tjera të së drejtës ndërkombëtare[15].

Konventa kërkon që shtetet pjesëmarrëse në të, të marrin masa të brendshme legjislative, për të siguruar mbrojtjen, kompensimin dhe ndihmën e viktimave të terrorizmit dhe të familjeve të tyre[16]. Pasi studiuam legjislacionin penal, vërejtëm se këto detyrime nuk janë të parashikuara. Për këto arsye mendojmë që kjo mbrojtje do të bëhej e mundur efektivisht me anë të një ligji të veçantë

[12] Po aty, neni 9.
[13] Po aty, neni 10
[14] Po aty, neni 11.
[15] Po aty, neni 12.
[16] Po aty, neni 13.

për mbrojtjen, kompensimin dhe ndihmën e viktimave të terrorizmit, pasi një ligj i tillë do të plotësonte edhe më mirë legjislacionin tonë penal.

Konventa përcakton masat e çdo shteti për të vendosur juridiksionin mbi veprat penale të parashikuara në këtë konventë[17]. Pasi studiuam legjislacionin penal dhe veçanërisht Ligjin Penal, vërejtëm se nuk parashikohen këto detyrime. Nga krahasimi që kemi ndërmarrë, lidhur me legjislacionin penal spanjoll, italian, anglez dhe francez, rezulton që asnjë nga këto shtete nuk e parashikon këtë detyrim të Konventës. Gjithsesi, jemi të mendimit që edhe për këtë detyrim të Konventës të bëhen ndryshime në Kodin Penal. Në nenet 15 deri në 23 të Konventës kemi të bëjmë me dispozita të karakterit procedural penal. Kështu, nisur që nga përcaktimi i procedurave që duhet të ndiqen lidhur me detyrimin e shteteve palë për të hetuar; ekstradimin dhe ndjekjen penale të personave, duke përfshirë edhe bashkëpunimin gjyqësor ndërkombëtar.

Në Konventë përcaktohet detyrimi që shtetet duhet t'u ofrojnë ndihmë të ndërsjellë juridike për hetimin, procedimin penal për veprat e parashikuara në nenet 5, 6, 7 dhe 9 të kësaj Konvente. Ky detyrim i shteteve do të realizohet nëpërmjet traktateve ose marrëveshjeve të ndërsjella; në mungesë të tyre do të zbatohet legjislacioni i brendshëm penal[18]. Konventa parashikohet që çdo shtet, në territorin e të cilit ndodhet personi i akuzuar si autor i veprës penale, i cili ka juridiksion, sipas kësaj Konvente, për veprat penale të parashikuara në të, pavarësisht nëse vepra penale është kryer ose jo në territorin e këtij shteti, ky shtet ka detyrimin që këtë çështje t'ia parashtrojë pa vonesë organeve të tij të brendshme, me qëllim nisjen e procedimit penal të personit të akuzuar si autor të veprës penale[19].

Në Konventë parashikohet se veprat e përcaktuara në nenet 5, 6, 7 dhe 9 të jenë të ekstradueshme, duke përcaktuar në çdo traktat ose marrëveshje, këto vepra si të ekstradueshme. Edhe në rast se nuk janë parashikuar në traktate si të ekstradueshme, ato duhet të jenë të ekstradueshme. Kur midis palëve nuk ekziston një traktat ekstradimi, lidhur me veprat e neneve 5, 6, 7 dhe 9, kjo Konventë do të shërbejë si bazë ligjore për ekstradimin. Çdo shtet duhet të modifikojë traktatet dhe marrëveshjet e ekstradimit që kanë nënshkruar ndërmjet tyre, me qëllim që këto të jenë në përputhje me detyrimet e Konventës, pra veprat e parashikuara të jenë të ekstradueshme[20]. Po ashtu, në Konventë përcaktohet detyrimi i shteteve që veprat penale të parashikuara nga Konventa nuk do të konsiderohen si politike për qëllime ekstradimi ose ndihme juridike të

[17] Po aty, neni 14.
[18] Po aty, neni 17.
[19] Po aty, neni 18.
[20] Po aty, neni 19.

ndërsjellë, kur përbëjnë akte terroriste. Në këtë rast ekstradimi duhet të lejohet. Nisur nga Ligji Procedural Penal, veprat e kryera me karakter politik ose kur kryen për qëllime politike përbëjnë një nga rastet për moslejimin e ekstradimit. Për këtë arsye, sugjerojmë që kjo dispozitë të ndryshohet, duke pasqyruar këtë detyrim të Konventës[21]. Në nenin 22 të Konventës parashikohet që autoritetet kompetente të një shteti, pa ndonjë kërkesë paraprake, t'i dërgojnë autoriteteve kompetente të një shteti tjetër informacion lidhur me hetimet dhe ndjekjen penale, kur çmohet se shpërndarja e një informacioni të tillë do t'i ndihmojë shtetet në vazhdimësinë e mëtejshme të hetimit ose të ndjekjes penale[22]. Ky nen i Konventës forcon më shumë bashkëpunimin ndërmjet shteteve në luftën kundër terrorizmit. Duke ditur se sovraniteti i shteteve kufizon veprimet e një shteti të vetëm ose të një organizate ndërkombëtare të zgjidhë problemin e terrorizmit, shtetet duhet të reagojnë efektivisht, nëpërmjet bashkëpunimit midis tyre, ndaj terrorizmit. Me qëllim që të sigurohet mbrojtja nga terrorizmi dhe të ndiqen penalisht terroristët, lind nevoja e zgjerimit të bashkëpunimit ndërkombëtar midis shteteve.

2. NATO dhe lufta kundër terrorizmit

Në përpjekjet për t'iu kundërvënë kërcënimit në rritje dhe drejtpërdrejt terrorizmit ndërkombëtar, qeveritë e vendeve aleate kanë ndërmarrë nisma të tjera, me qëllim që të zvogëlojnë veprimtarinë terroriste në rajonin e Ballkanit e më gjerë. Modernizimi i aftësive ushtarake të NATO-s dhe shtrirja e gjerë e operacioneve ushtarake të saj, i ka ndryshuar rrënjësisht kërkesat ushtarake të Aleancës. Forcat e mëdha të mbrojtjes të së kaluarës tashmë duhej të zëvendësoheshin me trupa që ishin në gjendje për t'iu përshtatur pak a shumë veprimeve luftarake në shkallë të vogël, në përgjigje të krizave. Në të tilla veprime duhet të mbizotërojë elasticiteti, lëvizshmëria dhe aftësia për t'u përhapur me largësi të konsiderueshme, prej bazave të tyre të zakonshme operative[23].

Në takimin e Pragës, qeveritë e vendeve anëtare hodhën idenë e fillimit të një procesi modernizimi të përcaktuar, për t'i mundësuar NATO-s marrjen e masave më të frytshme për përballimin e sfidave të shekullit XXI.[24] Aty u miratua një paketë masash që fuqizonte aftësi operative ushtarake të Aleancës. Në të përfshiheshin:

- Nisma e aftësive të reja, me emërtimin "Zotësimi për aftësitë në Pragë".
- Krijimi i forcës kundërvepruese të NATO-s.

[21] Po aty, neni 20, paragrafi 1.
[22] Po aty, neni 22.
[23] https://rm.coe.int/1680483a8c
[24] https://www.balkanweb.com/lideret-e-be-u-bene-bashke-ne-prage-cfare-u-arrit-ne-takimin-e-pare-te-bashkesise-politike-evropiane/#gsc.tab=0

- Përmirësimi i strukturës komanduese ushtarake të Aleancës.

Këto janë tri nismat kryesore të transformimit ushtarak, më rëndësi të veçantë për përshtatjen e aftësive ushtarake të NATO-s. Veç kësaj, kryesuesit e shteteve anëtare të NATO-s bënë thirrje për t'i shtuar përpjekjet në fushat e shkëmbimit të informacionit, të zbulimit dhe të parapërgatitjeve në përgjigje të krizave, por edhe për ngritjen në një nivel më të lartë të bashkëpunimit me vendet partnere. E gjithë kjo u realizua përmes *Planit të veprimit kundër terrorizmit* dhe në fushën e administrimit të ndihmës për pasojat nga terrorizmi, krahas zbatimit të një plani veprimi për planëzimin e çështjeve civile në situatë të jashtëzakonshme, për përgatitjen civile kundër sulmeve të mundshme, përfshirë përdorimin e agjentëve kimikë, biologjikë dhe radiologjikë.

Njësia e zbulimit të kërcënimeve terroriste, e krijuar fill pas goditjeve terroriste të 11 shtatorit, u zgjerua duke kryer analiza më të gjera kundër kërcënimeve terroriste në aspektin e NATO-s. Për më tepër, ndaj kësaj njësie u miratuan fonde të shumta për dhënien e ndihmës në luftën kundër terrorizmit në aspektin doktrinar por gjithashtu me mjete dhe aftësi luftarake. Njësia e zbulimit të kërcënimeve terroriste përfshin përdorimin efektiv të diplomacisë, organeve të zbatimit të ligjit, kontrollet financiare si dhe grumbullimin e të dhënave të zbulimit[25]. Kundërterrorizmi, nëpërmjet njësisë së sipërcituar e krijuar nga NATO, përfshin shumë më tepër veprimtari sesa mbart vetë emërtimi "kundër-terrorizëm". Përpara sulmeve të 11 shtatorit terrorizmi ishte i lokalizuar në agjenci të vogla ligjzbatuese të shpërndara në disa aparate drejtuese, por mbas sulmeve ajo u bë gjithëpërfshirëse për SHBA, duke bashkuar përpjekjet e ministrive, institucioneve dhe agjencive të ndryshme, madje duke përfshirë edhe diplomacinë në të.

3. Legjislacioni shqiptar në luftën kundër terrorizmit

Legjislacioni shqiptar në fushën e luftës kundër terrorizmit është mjaft i gjerë dhe ka pësuar ndryshime e përmirësime të dukshme, bazuar në legjislacionin ndërkombëtar dhe diktuar nga situata e terrorizmit në aspektin kombëtar e ndërkombëtar. Në fushën e terrorizmit, Republika e Shqipërisë ka në zbatim një kuadër të plotë ligjor dhe mekanizma institucionalë efektivë, të cilët përfshijnë, edhe pse jo shteruese, aktet e mëposhtme:

- Kushtetuta e Republikës së Shqipërisë.
- Kodi Penal i Republikës së Shqipërisë (ndryshuar me ligjin nr. 36/2017, ligjin 89/2017) ku në nenin 28 të të cilit "Forma të veçanta të bashkëpunimit", në pikën 2, jepet përkufizimi i organizatës terroriste dhe në vijim parashikohen veprat penale të kryera me qëllime terroriste,

[25] Citim i Paul R. Pillar

parashikuar në kreun VII të këtij kodi, si dhe nenet 265/a,265/b dhe 265/c që parashikojnë sanksione për pjesëmarrësit në veprime luftarake në një shtet të huaj (ndryshime sipas ligjit nr. 98,datë 31.07.2014).

- Kodi i Procedurës Penale të Republikës së Shqipërisë, i ndryshuar, ku përcaktohet kompetenca e hetimit të veprave penale që lidhen me terrorizmin, si dhe ligji nr. 95/2016 "Për organizimin dhe funksionimin e institucioneve për të luftuar korrupsionin dhe krimin e organizuar", në bazë të të cilit është krijuar Prokuroria e Posaçme, që ka në kompetencë hetimin e veprave të kryera nga grupet terroriste.
- Ligji nr. 9917, datë 19.05.2008 "Për parandalimin e pastrimit të parave dhe financimit të terrorizmit", i ndryshuar. Ky ligj ka për qëllim të parandalojë pastrimin e parave dhe të produkteve që burojnë nga veprat penale, si dhe parandalimin e financimit të terrorizmit. Ky ligj gjithashtu parashikon detyrime dhe procedura për raportimin për subjektet e ligjit te strukturat përgjegjëse në funksion të zbatimit të tij, kompetencat e autoriteteve mbikëqyrëse dhe autoritetit përgjegjës.
- Ligji nr. 10192, datë 03.12.2009 "Për eliminimin dhe goditjen e krimit të organizuar dhe trafikimin, nëpërmjet masave ndaluese kundër pasurisë", zbatohet edhe për pasuritë e personave mbi të cilët ekziston një dyshim i arsyeshëm, bazuar në indicie, edhe për pjesëmarrje në organizata terroriste ose në banda të armatosura.
- Ligji nr. 157/2013 "Për masat kundër financimit të terrorizmit". Ky ligj është në përputhje me kërkesat e rezolutës 1373 (2001) të Këshillit të Sigurimit të Kombeve të Bashkuara. Zbatimi i këtij ligji bëhet nga një sërë institucionesh dhe agjencish si Ministria e Drejtësisë, Banka e Shqipërisë, Drejtoria e Përgjithshme e Parandalimit të Pastrimit të Parave (DPPP) dhe Autoriteti i Mbikëqyrjes Financiare, ndërsa administrimi i llogarive dhe aseteve të ngrira/sekuestruara/konfiskuara bëhet nga Agjencia për Administrimin e Pasurive të Sekuestruara dhe Konfiskuara.
- Vendimi i Këshillit Mbikëqyrës të Bankës së Shqipërisë nr. 44, datë 10.06.2009 "Për miratimin e rregullores "Për parandalimin e pastrimin e parave dhe financimit të terrorizmit"".
- VKM nr. 140, datë 13.02.2008 "Për mënyrën e administrimit të pasurive të paluajtshme të sekuestruara, në kuadër të masave kundër financimit të terrorizmit".
- Ligji nr. 10173, datë 22.10.2009 "Për mbrojtjen e dëshmitarëve dhe bashkëpunëtorëve të drejtësisë".
- Ligji nr. 108/2013 "Për të huajt" (ndryshuar me ligjin nr.74/2016, datë

14.7.2016 dhe ligjin nr.13/2020), i cili rregullon regjimin e hyrjes, të qëndrimit, të punësimit dhe të daljes së të huajve në/nga Republika e Shqipërisë.

- Ligji nr. 10193, datë 03.12.2009 "Për marrëdhëniet juridiksionale me autoritetet e huaja në çështjet penale".
- Ligji nr. 79/2020 "Për ekzekutimin e vendimeve penale".
- Ligji nr. 45/2019 "Për mbrojtjen civile".
- Plani i Përbashkët i Veprimit Kundër Terrorizmit për Ballkanin Perëndimor ndërmjet Shqipërisë dhe Komisionit Evropian[26].

4. Instrumentet ligjore ndërkombëtare

Lufta kundër terrorizmit është një çështje shumë e rëndësishme dhe e ndërlikuar, e cila kërkon një bashkëpunim të ngushtë ndërkombëtar, si dhe zbatimin e instrumenteve ligjore për të parandaluar dhe ndaluar aktivitete të tilla të dëmshme. Këtu do të përmendim disa nga instrumentet ligjore më të rëndësishme kombëtare dhe ndërkombëtare që përdoren për të luftuar terrorizmin.

Marrëveshjet ndërkombëtare, ku Republika e Shqipërisë është palë dhe në veçanti:

- Plani i Përbashkët i Veprimit kundër Terrorizmit për Ballkanin Perëndimor ndërmjet Shqipërisë dhe Komisionit Evropian.
- Marrëveshje me EUROPOL, INTERPOL.
- Konventa kundër krimit të organizuar ndërkombëtar.
- Prioritetet e Shqipërisë në Këshillin e Sigurimit, 2022-2023.
- Strategjia Globale e Kombeve të Bashkuara, Konventat dhe protokollet e Kombeve të Bashkuara kundër terrorizmit.
- Konventa e Këshillit të Evropës për parandalimin e Terrorizmit për parandalimin e Terrorizmit.
- Protokolli i bashkëpunimit me Maqedoninë e Veriut (2019) dhe Plani i Përbashkët i Veprimit në Luftën kundër Terrorizmit.

Republika e Shqipërisë në kuadër të bashkëpunimit në luftën kundër terrorizmit ka nënshkruar dhe ratifikuar konventat dhe protokollet ndërkombëtare që përbëjnë instrumentet e së drejtës ndërkombëtare në fushën e antiterrorizmit. Shqipëria u është bashkuar iniciativave të OKB-së për të luftuar terrorizmin dhe ka ratifikuar tashmë 12 prej tyre. Krahas tyre ekzistojnë edhe një sërë rezolutash të Këshillit të Sigurimit të OKB-së më vlerë detyruese për shtetet

[26] Vendim i Këshillit të Ministrave nr. 1137, date 16.12.2020 " Për miratimin e strategjisë ndërsektoriale të luftës kundër terrorizmit, 2021 - 2025 dhe të planit të veprimit 2021 – 2023."

anëtare, si edhe konventa dhe protokolle të ashtuquajtura rajonale. Në këtë kuadër, Shqipëria aderon në të gjitha konventat dhe protokollet e Këshillit të Evropës kundër krimit të organizuar dhe terrorizmit (aktualisht 16 të tilla) dhe konkretisht:

- "Konventa mbi Veprat Penale dhe Aktet e tjera të Kryera në Bordin Avionit", Tokio, 14.09.1963, ratifikuar me ligjin nr. 8197, datë 06.3.1999, Fletore Zyrtare nr. 3, datë 28.3.1997.
- "Konventa mbi Shtypjen e Akteve të Paligjshme të Rrëmbimit të Avionit", Hagë, 16.12.1970, ratifikuar me ligjin nr. 8197, datë 06.03.1997. Fletore Zyrtare nr. 3, datë 28.03.1997.
- "Konventa mbi Shtypjen e Akteve të Paligjshme kundër Sigurisë së Aviacionit Civil", Montreal, datë 23.09.1971, ratifikuar me ligjin nr. 8191, datë 06.03.1997. Fletore Zyrtare nr. 3, datë 28.03.1997.
- "Konventa mbi Parandalimin dhe Ndëshkimin e Krimeve kundër Personave me Imunitet Ndërkombëtar, përfshirë Agjentët Diplomatikë", Nju Jork, 14.12.1973, ratifikuar me ligjin nr. 8832, datë 22.11.2001. Fletore Zyrtare nr. 56, datë 21.12.2001.
- "Konventa Evropiane mbi Shtypjen e Terrorizmit", Strasburg, 27.01.1979 ratifikuar me ligjin nr. 8642, datë 13.7.2000. Fletore Zyrtare nr. 22, datë 19.07.2000.
- "Konventa ndërkombëtare Kundër Marrjes së Pengjeve", Nju Jork 17.12.1979, ratifikuar me ligjin nr. 8837, datë 22.11.2001. Fletore Zyrtare 22, datë 19.07.2000,
- "Konventa mbi Mbrojtjen Fizike të Materialit Bërthamor", Vjenë më datë 03.03.1980, ratifikuar me ligjin nr. 8853, datë 31.01.2002. Fletore Zyrtare 12, datë 08.02.2002.
- "Protokolli Mbi Shtypjen e Akteve të Paligjshme të Dhunës në Aeroport që i shërbejnë Aviacionit Civil Ndërkombëtar", Montreal, 24.02.1991 ratifikuar me ligjin nr. 8835, datë 22.11.2001.
- "Konventa mbi Shtypjen e Akteve të Paligjshme kundër Sigurisë së Lundrimit Detar", Romë, 10.03.1998, ratifikuar me ligjin nr. 8850, datë 27.12.2001. Fletore Zyrtare nr. 60, datë 31.12.2001.
- "Protokolli mbi Shtypjen e Akteve të Paligjshme kundër Sigurisë së Platformave Fikse, të Vendosura në Platformën Kontinental", Romë, 10.03.1988, ratifikuar me ligjin nr. 8850, datë 27.12.2001. Fletore Zyrtare nr. 60, datë 31.12.2001.
- "Konventa mbi Etiketimin e Eksploziveve Plastik për Qëllim Zbulimi", Montreal, 01.03.1991, ratifikuar me ligjin nr. 9020, datë 06.3.2003. Fletore

Zyrtare nr. 21, datë 28.03.2003.

- "Konventa Ndërkombëtare mbi Ndalimin e Bombardimeve Terroriste", Nju Jork, 15.12.1997, ratifikuar me ligjin nr. 8836, datë 22.11.2001. Fletore Zyrtare nr. 57, datë 21.12.2001.
- "Konventa ndërkombëtare për luftën kundër financimit të terrorizmit" Nju Jork, 10.01.2000, ratifikuar nga parlamenti Shqiptar me ligjin nr. 8865, datë 14.03.2002.
- "Konventa Europiane (Strasburgut), për pastrimin, depistimin, kapjen dhe konfiskimin e produkteve të krimit", ratifikuar me ligjin nr. 8646, datë 20.7.2000. fletore Zyrtare, nr. 23, datë 04.08.2000.
- "Konventa e Këshillit të Europës, mbi pastrimin, kërkimin dhe konfiskimin e procedurave të krimit të organizuar dhe financimit të terrorizmit", datë 6.5.2005, nënshkruar me 22 dhjetor 2005, hyrë në fuqi me 1 Maj 2008.
- "Konventa e Këshillit të Europës për pastrimin, kërkimin, kapjen dhe konfiskimin e produkteve të krimit dhe për financimin e terrorizmit", ratifikuar me ligjin nr. 9646, datë 27.11.2006. Fletore Zyrtare nr. 134, datë 22.12.2006.
- Ratifikimi i "Protokollit ndryshues i konventës europiane për shtypjen e terrorizmit", ratifikuar me ligjin nr. 9230, datë 13.5.2004. Fletore Zyrtare nr. 38, datë 16.06.2004.
- Për ratifikimin e "Konventës europiane për kompensimin e viktimave të krimeve të dhunshme" me ligjin nr. 9265, datë 29.7.2004.
- "Konventa Ndërkombëtare për Shtypjen e Akteve të Terrorizmit Nuklear (Bërthamor) (2005)."[27]

Planifikimi dhe kryerja e aktiviteteve terroriste është një proces i vështirë që rrallë herë ndodh brenda territorit të një vendi dhe në zbatim të Strategjisë Globale të OKB-së për Terrorizmin, e cila kërkon bashkëpunim në nivel global, rajonal dhe kombëtar, në zbatim të rekomandimit të rezolutës së Asamblesë së Përgjithshme të OKB-së 49/60 (1995). Shqipëria ka nënshkruar dhe po zbaton 21 marrëveshje bashkëpunimi me vende të rajonit, Europës dhe SHBA-së, në fushën e sigurisë dhe shkëmbimit të informacionit për verifikimin dhe luftën kundër terrorizmit, konkretisht[28]:

- Me Sllovenine - Mbi bashkëpunimin në luftën kundër terrorizmit, trafikut të paligjshëm të drogës dhe krimit të organizuar, nënshkruar më 24.11.1993, në Tiranë.

[27] www.qbz.al

[28] Strategjia Ndërsektoriale për Parandalimin e Ekstremizmit të Dhunshëm dhe Luftën Kundër Terrorizmit.

- Me Kroacinë - Për bashkëpunimin policor, 20 janar 2014.
- Me Egjiptin - Protokoll mbi bashkëpunimi në fushën e luftës kundër terrorizmit, nënshkruar në Kajro, më 24.10.1995.
- Me Hungarinë - Mbi bashkëpunimin në luftën kundër terrorizmit, trafikut të drogës dhe krimit të organizuar, nënshkruar në shkurt 1999 dhe ratifikuar me ligjin nr. 8623, datë 15.06.2000.
- Me Rumaninë - Mbi bashkëpunimin në fushën e luftës kundër terrorizmit, të luftës kundër krimit të organizuar, të trafikut të paligjshëm të substancave narkotike e psikotrope, si edhe aktivitete të tjera ilegale, nënshkruar më 07.06.2002, në Bukuresht.
- Me Malin e Zi - Mbi bashkëpunimin në fushën e luftës kundër krimit të organizuar, terrorizmit, trafikut të paligjshëm si dhe veprimtarive të tjera të paligjshme", nënshkruar në Podgoricë, Mal i Zi, më 31 tetor 2003.
- Me Maqedoninë - Mbi bashkëpunimin në luftën ndaj terrorizmit, krimit të organizuar, trafikut të paligjshëm të drogave narkotike, substancave psikotrope e prekursoreve, migracionit të paligjshëm dhe veprimtarive të tjera të paligjshme, nënshkruar në Shkup, Maqedoni, më 17.06.2004.
- Në kuadër të bashkëpunimit rajonal në luftën kundër terrorizmit, Protokolli ndërmjet Ministrisë së Punëve të Brendshme të Republikës së Shqipërisë dhe Ministrisë së Punëve të Brendshme të Republikës së Maqedonisë "Për bashkëpunimin në luftën kundër terrorizmit", në Ohër, Maqedoni, më 3 shkurt 2018.
- Me Bullgarinë - Mbi bashkëpunimin në fushën e luftës kundër terrorizmit, krimit të organizuar, trafikimit të paligjshëm dhe akteve të tjera kriminale, nënshkruar në Tiranë, më 29 janar 2007.
- Me Francën - Mbi bashkëpunimin në fushën e sigurisë së brendshme, nënshkruar në Paris, me 15.05.2008.
- Me Gjermaninë - Mbi bashkëpunimin në fushën e sigurisë, nënshkruar më 31 Maj 2013 dhe ratifikuar me ligj më 23 janar 2014.
- Me Bosnjë-Hercegovinën - Mbi bashkëpunimin në luftën kundër krimit veçanërisht terrorizmit, trafikimit të paligjshëm të drogave dhe krimit të organizuar, nënshkruar me 24.03.2009, hyrë në fuqi më 04.03.2010.
- Me Kosovën - Mbi bashkëpunim të ndërsjellë në fushën e sigurisë. Miratuar me VKM nr. 429, datë 20.05.2015.
- Me Sllovakinë - Mbi bashkëpunimin në luftën kundër terrorizmit, krimit të organizuar, trafikut të paligjshëm të lëndëve narkotike, substancave psikotrope e prekursorëve të drogës dhe krimeve të tjera. Miratuar me

VKM nr. 485, datë 10.06.2015.

- Me SHBA - Marrëveshja e bashkëpunimit midis Këshillit të Ministrave të Republikës së Shqipërisë dhe Qeverisë së SHBA, "Për shkëmbimin e informacionit për verifikimin e terrorizmit", si dhe Protokollit Operacional, të Ratifikuara me ligjin nr. 72, datë 07.07.2016 Memorandumi i bashkëpunimit ndërmjet Qeverisë të Shteteve të Bashkuara të Amerikës dhe Këshillit të Ministrave të Republikës së Shqipërisë, "Për rritjen e bashkëpunimit për të parandaluar udhëtimin e terroristëve dhe për të luftuar migracionin e paligjshëm dhe krimet e rënda që lidhen me to", miratuar në parim me VKM nr.153, datë 01.03.2017.
- Me Serbinë - Mbi bashkëpunimin në fushën e luftës kundër krimit të organizuar, trafikimit të paligjshëm ndërkombëtar të drogës dhe terrorizmit ndërkombëtar, nënshkruar më 11.03.2010, hyrë në fuqi më 01.03.2012.
- Me Letoninë - Mbi bashkëpunimin në luftën kundër terrorizmit, krimit të organizuar, trafikimit të paligjshëm të drogave narkotike, substancave psikotrope dhe prekursorëve, nënshkruar më 16.12.2009.
- Me Italinë - Protokolli mes Ministrisë së Brendshme të Republikës së Shqipërisë dhe Ministrisë së Brendshme të Republikës Italiane "Mbi forcimin e bashkëpunimit dypalësh në luftën kundër terrorizmit dhe trafikimit të qenieve njerëzore", nënshkruar më 3 nëntor 2017 në Tiranë, hyrë në fuqi datën e nënshkrimit.

5. Kuadri institucional

Përpjekjet për parandalimin e ekstremizmit të dhunshëm që çojnë në terrorizëm kërkojnë përfshirjen dhe bashkëpunimin e aktorëve publikë e privatë nga niveli qendror tek ai vendor, me qëllim garantimin e ndërveprimit, koordinimit dhe ndarjes së informacionit midis aktorëve të përfshirë në këtë proces. Institucionet, që kanë një rol thelbësor në parandalimin e ekstremizmit të dhunshëm[29] që çojnë në terrorizëm, janë:

Qendra e Koordinimit kundër Ekstremizmit të Dhunshëm (QKEDH), e cila ka për mision parandalimin me sukses të përhapjes së radikalizimit dhe ekstremizmit të dhunshëm nëpërmjet realizimit të përpjekjeve të lokalizuara, fuqizimit të të rinjve, familjes, grave dhe pakicave, duke i kanalizuar këto përpjekje drejt rrjeteve fetare, kulturore dhe arsimore si dhe përfshirjes së medias dhe shoqërisë civile. QKEDH-ja luan një rol kryesor në monitorimin dhe zbatimin e Strategjisë Kombëtare për Parandalimin e Ekstremizmit të

[29] Roli i shoqërisë civile për parandalimin dhe luftën kundër ekstremizmit të dhunshëm dhe radikalizimit që të çon në terrorizëm në Evropën Juglindore- Organizata për siguri dhe bashkëpunim në Europë.

Dhunshëm dhe Luftën kundër terrorizmit, duke bashkëpunuar me institucionet përgjegjëse në drejtim të përmbushjes së përgjegjësive të tyre. Ndër të tjera, me rëndësi konsiderohet edhe zhvillimi i kapaciteteve të aktorëve të përfshirë në identifikimin dhe parandalimin e radikalizimit dhe ekstremizmit të dhunshëm që çojnë në terrorizëm. Gjithashtu, ky institucion dizajnon, zbaton dhe monitoron vetë ose në bashkëpunim me institucione të tjera projekte dhe veprimtari që kanë në fokus kundërshtimin e radikalizimit dhe parandalimin e ekstremizmit të dhunshëm që çon në terrorizëm.

Ministria e Drejtësisë (MD), nëpërmjet Drejtorisë së Përgjithshme të Burgjeve dhe Shërbimit të Provës, luajnë një rol të rëndësishëm në kundërshtimin dhe parandalimin e radikalizimit dhe ekstremizmit të dhunshëm që çon në terrorizëm, duke qenë se ky fenomen gjen terren të favorshëm tek të dënuarit që vuajnë masën e dënimit në këto institucione.

Policia e Shtetit, nëpërmjet të cilës funksionon Drejtoria e Antiterrorit, me shtrirje strukturore në të gjithë territorin e vendit. Funksionet kryesore të Drejtorisë janë parandalimi, identifikimi, gjurmimi dhe hetimi i personave të dyshuar si të përfshirë në vepra terroriste. *Agjencia e Administrimit të Aseteve Kriminale (AAPSK),* për administrimin e fondeve dhe të pasurive të sekuestruara e konfiskuara.

Shërbimi Informativ Shtetëror, i krijuar me ligjin nr. 8391, datë 28.10.1998, mbledh informacion nga jashtë në funksion të sigurimit kombëtar, kryen veprimtari kundërzbulimi për ruajtjen e integritetit, të pavarësisë e të rendit kushtetues. SHISH mbledh informacion për terrorizmin, për prodhimin dhe trafikun e narkotikëve, për prodhimin e armëve të dëmtimit në masë, për krimet kundër mjedisit, mbledh informacion për krimin e organizuar, krime që cenojnë sigurinë kombëtare.

Prokuroria e Posaçme Kundër Korrupsionit dhe Krimit të Organizuar. Prokuroria e Posaçme dhe Njësia e Posaçme Hetimore për ndjekjen penale dhe hetimin e veprave penale të korrupsionit, krimit të organizuar dhe çështjeve penale sipas nenit 135, paragrafi 2, të Kushtetutës janë të pavarura nga Prokurori i Përgjithshëm. Njësia e Posaçme Hetimore është në vartësi të Prokurorisë së Posaçme. Prokuroria e Posaçme ushtron ndjekjen penale dhe përfaqëson akuzën në emër të shtetit para Gjykata vetë posaçme për veprat penale. Çdo vepër penale e kryer nga grupi i strukturuar kriminal, organizata kriminale, organizata terroriste dhe banda e armatosur, sipas përcaktime vetë Kodit Penal.

Prokuroria e Përgjithshme, ushtron ndjekjen penale dhe përfaqëson akuzën në gjyq në emër të shtetit për veprat penale në lidhje me terrorizmin. Gjithashtu, në Prokurorinë e Përgjithshme funksionon edhe Zyra e Përgjimeve të Komunikimeve Elektronike. Me memorandum të përbashkët ndërinstitucional,

funksionojnë strukturat e hetimit të krimit financiar në Prokuroritë e Rretheve Gjyqësore - 8 njësitë e përbashkëta hetimore - të ngritura në Tiranë, Durrës, Shkodër, Fier, Vlorë, Korçë, Elbasan e Gjirokastër.

Agjencia e Inteligjencës dhe Sigurisë së Mbrojtjes, në vartësi të ministrit të Mbrojtjes dhe funksionon bazuar në ligjin nr. 65/2014 "Për Agjencinë e Inteligjencës dhe Sigurisë së Mbrojtjes". Ligji përcakton mënyrat e marrjes, administrimit dhe shpërndarjes së informacionit të klasifikuar kundër terrorizmit.

Drejtoria e Përgjithshme e Parandalimit të Pastrimit të Parave (DPPPP), shërben si njësi e specializuar financiare për parandalimin dhe luftën kundër pastrimit të parave dhe financimit të terrorizmit. Kjo drejtori funksionon si qendër kombëtare e ngarkuar me mbledhjen, analizimin dhe shpërndarjen tek agjencitë e zbatimit të ligjit të të dhënave për veprimtaritë e mundshme të pastrimit të parave të financimit të terrorizmit. Në kuadër të ushtrimit të funksioneve mbikëqyrëse, të kontrollojë zbatimin e programeve të luftës kundër pastrimit të parave dhe financimit të terrorizmit.

Drejtoria e Përgjithshme e Doganave (DPD), bashkëvepron me strukturat e tjera të zbatimit të ligjit në funksion të realizimit të misionit të saj për garantimin e sigurisë dhe të rendit publik në porte dhe aeroporte, duke përfshirë dhe masat në kuadër të luftës kundër terrorizmit.

Banka e Shqipërisë, në kuadër të ushtrimit të funksioneve si autoritet mbikëqyrës, për subjektet nën juridiksionin e saj, të kontrollojë zbatimin e programeve të luftës kundër pastrimit të parave dhe financimit të terrorizmit.

Ministria e Drejtësisë, nëpërmjet strukturave të saj, siguron bashkëpunimin e nevojshëm mes Prokurorisë, Interpolit dhe autoriteteve të huaja të drejtësisë në çështje që lidhen me luftën 24 kundër krimit të organizuara po kundër terrorizmit dhe financimit të tij, në zbatim të ligjit nr.10193, datë 3.12.2009 "Për marrëdhëniet juridiksionale me autoritetet e huaja në çështjet penale". Drejtoria e Përgjithshme e Burgjeve dhe ajo e Shërbimit të Provës kanë një rol të rëndësishëm për parandalimin dhe kundërshtimin e ekstremizmit të dhunshëm dhe radikalizimit edhe për faktin që këto fenomene janë shpesh të pranishme në mjediset apo shërbimet e këtyre institucioneve. Përveç institucioneve të sipërcituara, janë edhe Ministria e Shëndetësisë dhe Mbrojtjes Sociale (MSHMS), Ministria e Arsimit dhe Sportit (MAS), Ministria e Financave dhe Ekonomisë (MFE) dhe Njësitë e Vetëqeverisjes Vendore, që luajnë një rol të rëndësishëm në adresimin e faktorëve nxitës e shtytës dhe në identifikimin e hershëm të shenjave të radikalizmit dhe ekstremizmit të dhunshëm që çojnë në terrorizëm, duke mundësuar kështu parandalimin dhe rehabilitimin/ riintegrimin e individëve të prekur nga ky fenomen.

Përfundime dhe mësime të nxjerra

Në luftën kundër terrorizmit, institucionet mbështetin idenë e veprimit të gjithë bashkë, me një qasje gjithëpërfshirëse dhe të balancuar, në nivel global, rajonal dhe kombëtar.

Qeveria shqiptare e ka vlerësuar luftën kundër terrorizmit si një prioritet kombëtar, duke qenë ndër vendet e para që në zbatim të Rezolutës 2178 (2014)[30] ndërmori hapa konkretë të reflektuara në legjislacionin kombëtar. Duke ndryshuar Kodin e Procedurës Penale, u synua forcimi i aftësisë së adresimit të problemit të luftëtarëve të huaj terroristë, duke e konsideruar të paligjshme dhe të ndëshkueshme pjesëmarrjen, organizmin apo çdo nxitje për pjesëmarrje në veprime ushtarake të një vendi të huaj. Të vendosur për të arritur rezultate të prekshme dhe për të treguar progres real, janë marrë masa për rishikimin, forcimin dhe ndryshimin e mekanizmave aktualë të kontrollit të financimit të terrorizmit dhe ngrirjes së aseteve për individë dhe subjekte të përfshirë në aktivitet terrorist. Bazuar në studimet dhe raportet e riskut rezulton se kërcënimi real prej terrorizmit në Shqipëri është në nivel të ulët me përjashtim të disa rasteve kur niveli i kërcënimit është rritur në "mesatar". Shqipëria nuk ka regjistruar akte e viktima terroriste të mirëfillta por është prekur nga fenomeni i pjesëmarrjes së luftëtarëve terroristë, zhvendosur së bashku me familjet e tyre në zonat në konflikt.

Aktualisht, evidentohen shtetas shqiptarë, kryesisht gra dhe fëmijë, të strehuar në qendrat e pritjes për t'u riatdhesuar. Për Policinë e Shtetit, parandalimi dhe lufta kundër terrorizmit mbetet një fushë kyçe për bashkëpunimin operacional dhe shkëmbimin e informacionit me shërbimet antiterror në vendet e rajonit, Itali, Kosovë, Mal i Zi, Maqedoni, me INTERPOL, EUROPOL, Qendrën Europiane Antiterrorizëm, Oficerët Ndërlidhës, Qendrën për Verifikimin e Terrorizmit (TSCSHBA), agjencitë ligjzbatuese dhe shërbimet partnere në BE.

Shqipëria ka nënshkruar dhe ratifikuar të gjitha rezolutat, konventat dhe protokollet kundër terrorizmit, të Këshillit të Sigurimit të OKB-së dhe Protokollin shtesë të Konventës së Këshillit të Europës për Parandalimin e Terrorizmit.

Shqipëria merr pjesë dhe përfaqësohet me kontribut konkrete në të gjitha aktivitetet, grupet e punës së Koalicionit Global D-ISIS, dhe forumet e organizatave ndërkombëtare, ku vendet anëtare shkëmbejnë praktikat më të mira që lidhen me zbatimin e Strategjisë Globale të luftës kundër terrorizmit (UNGCTS)[31] të OKB-së dhe Planin e Veprimit të Parandalimit të Ekstremizmit të Dhunshëm.Shqipëria radhitet në ato vende që e kanë mbështetur fuqimisht

[30] https://main.un.org/securitycouncil/en/s/res/2178-%282014%29

[31] https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy

UNGCTS dhe Planin e Veprimit, me bindjen se do të shërbente si një udhëzues i suksesshëm në përpjekjet tona të përbashkëta të luftës kundër terrorizmit dhe ekstremizmit të dhunshëm.

Vendi ynë ka bërë analizën totale, nen për nen, të legjislacionit për luftën kundër terrorizmit dhe po punon për përputhjen plotësisht të Kuadrit Ligjor për Luftën Kundër Terrorizmit dhe parandalimin e Ekstremizmit të Dhunshëm, me "Acquis" të Bashkimit Evropian.

Literatura e shfrytëzuar

1. Luigi Bonanate – La terrorisme international
2. Vendim i Këshillit të Ministrave nr. 663, datë 17.07.2023 "Për miratimin e strategjisë ndërsektoriale të luftës kundër krimit të organizuar, trafiqeve të paligjshme dhe terrorizmit, 2013-2020 dhe planit të veprimit për vitet 2013 - 2016"
3. Tim Pat Coogan, The IRA, Palgrave, New York, viti 2002.
4. Demolli, Terrorizmi, Prishtinë, viti 2002.
5. (https://telegrafi.com/historia-e-terrorizmithovi-keq-shekulli-xix-dhe-shekullit-xx/)
6. Konventa e Këshillit të Evropës për parandalimin e Terrorizmit, Varshavë, viti 2005
7. Sulejmani, Dukuria e terrorizmit,-studim krahasues juridik penal, 2014
8. Marevci, Luftimi i terrorizmit bashkëkohor, viti 2014
9. https://rm.coe.int/1680483a8c
10. (https://www.balkanweb.com/lideret-e-be-u-bene-bashke-ne-prage-cfare-u-arrit-ne-takimin-e-pare-te-bashkesise-politike-evropiane/#gsc.tab=0)
11. Vendim i Këshillimit të Ministrave nr. 1137, date 16.12.2020 " Për miratmin e strategjisë ndërsektoriale të luftës kundër terrorizmit,
    2021 – 2025 dhe të planit të veprimit 2021 - 2023"
12. www.qbz.al
13. Strategjia Ndërsektoriale për parandalimin e ekstremizmit të dhunshëm dhe luftën kundër terrorizmit
14. Roli i shoqërisë civile për parandalimin dhe luftën kundër ekstremizmit të dhunshëm dhe radikalizimit që të con në terrorizëm në Evropën Juglindore - Organizata për siguri dhe bashkëpunim në Europë.
15. https://main.un.org/securitycouncil/en/s/res/2178-%282014%29

Lufta Rusi-Ukrainë, roli i armëve bërthamore dhe i energjisë bërthamore

Msc. Alqi NIKOLLA
Specialist në IKSHU
Msc. Enxhi HETI
Studiuese

Trajtesë e shkurtuar.

Lufta midis Rusisë dhe Ukrainës ka pasur ndikime të thella në rolin e armëve bërthamore dhe energjisë bërthamore në botë. Ky konflikt ka rikthyer vëmendjen ndërkombëtare te rreziku i përdorimit të armëve bërthamore, duke nxjerrë në pah dobësitë e mekanizmave ekzistues të kontrollit të armëve dhe duke theksuar nevojën për masa më të forta për parandalimin e përhapjes së tyre. Përveç kësaj, konflikti ka ndikuar në tregjet globale të energjisë, duke theksuar varësinë nga energjia bërthamore si një burim alternativ për të zëvendësuar gazin dhe naftën nga rajonet e prekura nga lufta. Ky punim shqyrton dimensionin bërthamor të luftës në Ukrainë nëpërmjet dy arsyetimeve: së pari, njohuritë tona për botën bërthamore janë shumë të kufizuara dhe çdo përfundim që nxjerrim nga lufta në Ukrainë duhet të jetë i bazuar në prova, së dyti, ajo që po vëzhgojmë në Ukrainë duket, të paktën në përputhje me njohuritë teorike bazë dhe të mirëpërcaktuara rreth armëve bërthamore, që: a) armët bërthamore pengojnë; b) armët bërthamore mundësojnë; dhe c) efektet politike të armëve bërthamore lindin nga rreziqe të vërteta bërthamore. Ky artikull parashtron këto njohuri dhe demonstron përputhshmërinë e tyre me provat ekzistuese të dëshmuara nga lufta në Ukrainë. Në përgjithësi, nuk duket se lufta në Ukrainë duhet të na bëjë të rimendojmë në mënyrë thelbësore kuptimin tonë mbi armët bërthamore. Gjithashtu, në pjesën e fundit të këtij punimi, jepen disa reflektime mbi ndikimin e kësaj lufte në rolin e armëve bërthamore dhe energjisë bërthamore në botë.

Fjalët kyçe: konflikti Rusi-Ukrainë, armë bërthamore, rrezik botëror, rendi botëror bërthamor.

Hyrje

Sulmi i Rusisë ndaj Ukrainës në shkurt të vitit 2022 dhe rezistenca e mëvonshme e Ukrainës ndaj agresionit rus kanë qenë subjekt i shumë analizave. Ndoshta asnjë aspekt i luftës në Ukrainë nuk ka shkaktuar më shumë diskutime sesa dimensioni bërthamor i konfliktit dhe në çfarë mase armët bërthamore ruse dhe amerikane po ndikojnë në llogaritjet e aktorëve të ndryshëm të përfshirë në të. "Bomba në sfond"[1] e konfliktit nuk ka qenë asnjëherë larg nga qendra e analizës. Kjo nuk është e habitshme, duke marrë parasysh mundësinë që konflikti të përshkallëzohet në mënyra të paparashikueshme, pasojat potencialisht shkatërrimtare të përdorimit bërthamor dhe kërcënimet e rregullta bërthamore të bëra nga Rusia.

Me shpalljen e pushtimit, Vladimir Putin paralajmëroi shtetet perëndimore se çdo përpjekje për të ndërhyrë do të çonte në "pasoja të papara në histori", një kërcënim i theksuar vetëm tre ditë më vonë kur ai vendosi forcat bërthamore të Rusisë në "gatishmëri të lartë luftarake". Në fillim të vjeshtës të vitit 2022, një grup gjeneralësh të lartë rusë rritën më tej tensionet globale, duke diskutuar mbi përdorimin e mundshëm të armëve bërthamore taktike në territorin ukrainas[2]. Deri në maj 2024, situata ishte përshkallëzuar me Moskën duke njoftuar manovra të menjëhershme pranë kufirit ukrainas, të dizajnuara në mënyrë të qartë për të trajnuar procedurat për vendosjen e armëve bërthamore taktike, të cilat justifikoheshin si një përgjigje e nevojshme ndaj "deklaratave provokuese dhe kërcënimeve nga disa zyrtarë perëndimorë" ndaj Moskës. Më 19 dhjetor 2024, Presidenti Vladimir Putin njoftoi për ndryshime në doktrinën bërthamore, duke ulur pragun për përdorimin e armëve bërthamore. Këto ndryshime parashikojnë përdorimin e armëve bërthamore jo vetëm në përgjigje të një sulmi bërthamor, por edhe në rast të një sulmi masiv ajror ndaj Rusisë, duke zgjeruar kështu kushtet për përdorimin e tyre[3].

Shumë analiza mbi rolin e armëve bërthamore në konflikt kanë theksuar dinamikën e re bërthamore brenda luftës dhe kanë bërë vlerësime të implikimeve të luftës për aspekte të ndryshme të politikës bërthamore, përfshirë rendin botëror bërthamor; përdorimin e armëve bërthamore në konflikt; efektivitetin e shantazhit bërthamor; modelet e ardhshme të përhapjes; teoritë më të gjera mbi armët bërthamore dhe politikën ndërkombëtare; ose mësimet që mund të marrin shtete të tjera si Kina nga konflikti duke u bërë kontribute të vlefshme në kuptimin tonë të dimensioneve potencialisht kyçe të luftës në Ukrainë.

---

[1] Nina Tannenwald, *The Bomb in the Background,* February 24, 2023, Foreign Affairs.

[2] Cooper, Helene, Barnes, Julian & Schmitt, Eric, *2022: Russian Military Leaders Discussed Use of Nuclear Weapons:* New York Times. https://www.nytimes. com/2022/11/02/us/politics/russia-ukraine-nuclear-weapons.html (Accessed 23 May 2024).

[3] https://www.armscontrol.org/act/2024-12/news/russia-revises-nuclear-use-doctrine

Njohuritë tona për botën bërthamore janë të kufizuara, prandaj çdo përfundim që nxjerrim nga lufta në Ukrainë duhet të jetë i kujdesshëm. Thënë kështu, është veçanërisht i vlefshëm vlerësimi i teorive ekzistuese me prova të reja, pikërisht kur përballemi me tema të rëndësishme për të cilat na mungon siguria. Prandaj, është i rëndësishëm shqyrtimi i konfliktit të vazhdueshëm në Ukrainë për prova që lidhen me teoritë ekzistuese rreth armëve bërthamore. Ajo që ne po shohim në Ukrainë aktualisht duket të paktën në përputhje me njohuritë teorike bazë dhe të mirëpërcaktuara rreth armëve bërthamore. Ky artikull parashtron këto njohuri dhe demonstron përputhjen e tyre me provat ekzistuese empirike nga Ukraina.

1. Pasiguria është e pashmangshme

Konfliktet e kohës së sotme të mbështetura nga armët bërthamore, teknologjitë e avancuara dhe dinamika komplekse globale krijojnë një realitet ku pasiguria është e pashmangshme. Kjo pasiguri lind nga disa faktorë të ndërlidhur me njëri-tjetrin:

- Paaftësia për të parashikuar veprimet e aktorëve kryesorë. Edhe nëse fuqitë e mëdha ruajnë statusin ekzistues të armëve bërthamore, faktorët e paparashikueshëm politikë ose ekonomikë mund të ndryshojnë krejtësisht rrethanat.
- Kompleksiteti i sistemeve të aleancave. NATO dhe aleancat e tjera rajonale dhe ndërkombëtare mund të përfshijnë interesa të ndryshme, të cilat në situata krizash mund të ndërlikojnë përpjekjet për zgjidhje.
- Kërcënimi i konflikteve hibride. Përdorimi i mjeteve hibride, si sulmet kibernetike dhe propaganda, krijon një pasiguri të vazhdueshme, pasi sulmet mund të vijnë nga aktorë të ndryshëm dhe shpesh pa një autor të qartë.

Si rrjedhojë, strategjia më e mirë për të adresuar këtë pasiguri është përqendrimi në krijimin e mekanizmave elastikë të komunikimit dhe të parandalimit të krizave, duke përfshirë si fuqitë bërthamore, ashtu edhe aktorët rajonalë. Ne jemi të kufizuar në mënyrë të pashmangshme nga provat që kemi për të kuptuar dinamikën e epokës bërthamore, gjë që e bën të vështirë nxjerrjen e përfundimeve të qarta dhe të sigurta. Siç thekson Francis Gavin, "Është e rëndësishme të pranojmë se sa pak dimë në të vërtetë si për dinamikën bërthamore në përgjithësi, ashtu edhe për rolin e tyre në luftën Rusi-Ukrainë, dhe sa nga ato që vijojnë janë, në rastin më të mirë, supozime të dokumentuara"[4].

[4] Gavin, F. J., *Nuclear Lessons and Dilemmas from the War in Ukraine, 2024.* https://muse.jhu.edu/pub/1/oa_edited_volume/chapter/3881924

Në të njëjtën linjë, Robert Jervis thekson se "Ne kemi mbetur të pasigurt"[5] për shumë nga pyetjet kyçe që ka ngritur epoka bërthamore dhe kjo pasiguri është një pasojë e pashmangshme e natyrës dhe objektit të shkrimit për disa arsye:

Mungesa e të dhënave: Deri më sot, ka pasur vetëm dy raste të përdorimit të drejtpërdrejtë të armëve bërthamore për qëllime ushtarake[6]. Nuk ka pasur asnjë luftë termonukleare, dhe ka pasur një numër relativisht të vogël krizash bërthamore vërtet të rrezikshme. Vetëm dhjetë vende kanë zhvilluar armë bërthamore dhe ekziston vetëm një shembull i qartë i një vendi që ka prodhuar armë bërthamore dhe më pas ka vendosur të çarmatoset vullnetarisht[7]. Kjo do të thotë se ne kemi shumë pak prova faktike, dhe nganjëherë jo të drejtpërdrejta, që mund të na ndihmojnë t'u përgjigjemi disa prej pyetjeve më të rëndësishme në lidhje me armët bërthamore. Këto përfshijnë mënyrën se si mund të ndodhë përshkallëzimi bërthamor përtej pragut të përdorimit të armëve bërthamore, veprimet që mund të shkaktojnë përdorimin e armëve bërthamore në raste të caktuara, dinamika e një bote pa armë bërthamore, ose sa efektiv mund të jetë ndalimi normative (moral dhe ligjor) i përdorimit të armëve bërthamore pas përdorimit të tyre.

***Natyra sekrete e informacionit bërthamor*:** Shumë informacione rreth strategjive bërthamore, zhvillimit të armëve dhe teknologjisë bërthamore janë të klasifikuara. Shtetet që zotërojnë armë bërthamore kanë një interes të lartë për të ruajtur sekretin e këtyre aftësive për arsye sigurie kombëtare.

***Ndikimi i kufizuar i të dhënave historike*:** Dinamika e epokës bërthamore është në ndryshim të vazhdueshëm. Përvojat dhe provat e kaluara nuk mund të ofrojnë gjithmonë udhëzime të sakta për të ardhmen, pasi zhvillimet teknologjike, ndryshimet në strategjitë ushtarake dhe ndryshimet në politikën ndërkombëtare vazhdojnë të evoluojnë.

***Pasiguria e qëllimshme në politikën bërthamore*:** Shtetet shpesh krijojnë paqartësi rreth qëllimeve dhe kapaciteteve të tyre bërthamore për të ruajtur një

[5] Jervis, R., *The Nuclear Age: During and After the Cold War,* 2021.

[6] Këto ishin bombat atomike të hedhura nga Shtetet e Bashkuara mbi qytetet japoneze të Hiroshimës dhe Nagasakit gjatë Luftës së Dytë Botërore, më 6 dhe 9 gusht 1945. Këto sulme çuan në shkatërrime masive dhe humbje të mëdha jetësh njerëzore, duke ndihmuar në përfundimin e luftës. Që atëherë, armët bërthamore nuk janë përdorur në konfliktet ushtarake, edhe pse disa vende i kanë zhvilluar dhe mbajnë arsenale bërthamore për qëllime parandalimi dhe mbrojtjeje.

[7] Vetëm dhjetë vende kanë zhvilluar armë bërthamore: Shtetet e Bashkuara, Rusia, Mbretëria e Bashkuar, Franca, Kina, India, Pakistani, Izraeli (ndonëse nuk e ka pranuar publikisht), Koreja e Veriut dhe Afrika e Jugut. Afrika e Jugut është shembulli i vetëm i qartë i një vendi që ka zhvilluar armë bërthamore dhe më pas ka vendosur të çarmatoset vullnetarisht. Në vitet 1980, Afrika e Jugut ndërtoi disa armë bërthamore, por në fillim të viteve 1990, ajo vendosi të heqë dorë nga arsenali i saj bërthamor dhe të shkatërrojë armët ekzistuese. Kjo vendimmarrje u bë në një kontekst të ndryshimeve politike të brendshme dhe pas fund të aparteidit. Ky rast është unik dhe përbën një precedent të rëndësishëm për çarmatimin bërthamor në skenën ndërkombëtare.

avantazh strategjik. Kjo e bën të vështirë të kuptohet plotësisht balanca e fuqisë bërthamore.

***Kufizimet shkencore dhe teknike*:** Edhe nëse informacioni shkencor është i disponueshëm, modelimi dhe parashikimi i sjelljes në një konflikt bërthamor mbetet kompleks dhe i pasigurt, pasi ka shumë faktorë të panjohur që ndikojnë në rezultat.

***Konteksti ndërkombëtar dhe faktorët politikë*:** Epoka bërthamore nuk mund të kuptohet pa analizuar kontekstin politik global. Megjithatë, ky kontekst është i ndërlikuar dhe shpesh i paqëndrueshëm, gjë që kufizon aftësinë për të bërë analiza të qëndrueshme afatgjata.

Konceptet thelbësore teorike si superioriteti bërthamor, ekuilibri i vendosmërisë, rendi bërthamor ose tabuja bërthamore janë të vështira për t'u konceptuar, përcaktuar, apo edhe vëzhguar me saktësi dhe mund të kuptohen ndryshe nga aktorë të ndryshëm[8]. Këto kufizime na detyrojnë të përdorim të dhënat që kemi në dispozicion dhe të pranojmë se çdo kuptim i dinamikës së epokës bërthamore mbetet i paplotë dhe subjekt i ndryshimeve të mëtejshme.

Kjo pasiguri ka dy pasoja të rëndësishme: *Së pari,* zvogëlon besimin në nxjerrjen e përfundimeve të sigurta rreth çështjeve bërthamore, veçanërisht rreth luftës së vazhdueshme në Ukrainë. Quinlan, argumenton se "kufizimet në njohuritë tona duhet të rrënjosen te të gjithë ata që bëjnë deklarata parashikuese rreth këtyre çështjeve"[9]. Kjo nuk do të thotë se nuk mund të nxjerrim përfundime, por (për të përdorur terminologjinë sasiore shkencore shoqërore) në mënyrë të pashmangshme, do të ketë ndryshime të mëdha besimi për vlerësimet që bëjmë. Në vlerësimin e rolit të armëve bërthamore në luftën në Ukrainë, duhet të jemi të kujdesshëm në përfundimet që nxjerrim. Pasiguria nuk është specifike për të kuptuarit tonë të çështjeve bërthamore ose në thelb shqetësuese. Siç ka vërejtur filozofi Bertrand Russell, "e gjithë njohuria jonë për të vërtetat është e infektuar me një shkallë dyshimi[10]." Si rezultat, çdo analizë e fenomeneve sociale duhet të pranojë pasigurinë dhe të marrë parasysh kualifikimin. Prandaj, përfundimet për rolin e armëve bërthamore duhet të bëhen me kujdes, duke njohur kufijtë e gjerë të gabimit në vlerësime të tilla komplekse.

Së dyti, njohuritë për botën sociale rrjedhin në mënyrë të pashmangshme nga një kombinim i teorisë dhe provave faktike. Në fushat ku provat faktike janë

---

[8] Logan, D. C., *The Nuclear Balance is What States Make of it,* 2022.

[9] Quinlan, M., *Thinking About Nuclear Weapons.* 1997. https://fisherp.scripts.mit.eduwordpress/wp-content/uploads/2017/03/Thinking-about-Nuclear-Weapons-RUSI-WHP41_QUINLAN1.pdf

[10] Bertrand Russell, *The Problems of Philosophy,* 1912.

më pak bindëse, ku dinamikat themelore sociale që ne kërkojmë të kuptojmë janë komplekse dhe heterogjene, dhe ku vendosja e standardeve të hulumtimit praktik (si eksperimentet e rastësishme) është e vështirë ose e pamundur, ne në mënyrë të pashmangshme do të anojmë më shumë mbi teoritë për të nxjerrë përfundimet[11]. Në lidhje me armët bërthamore, për shkak të rëndësisë së temës dhe provave faktike të kufizuara që kemi, nuk na mbetet gjë tjetër veçse të mbështetemi shumë në teori, koncepte, hipoteza dhe përfundime të pa testuara drejtpërdrejt ose plotësisht. Prandaj, në përgjithësi duhet të jemi të kujdesshëm në lidhje me hedhjen poshtë të teorive ekzistuese dhe të vërtetuara mirë e të bazuara në prova të pashmangshme. Këto mësime duhet të zbatohen për çdo përfundim që nxjerrim nga konflikti i vazhdueshëm në Ukrainë. Pasiguria është një aspekt i pashmangshëm në analizën e dinamikës bërthamore në luftën Rusi-Ukrainë.

Ndërsa disa studiues e kanë theksuar këtë pasiguri, shumë të tjerë paraqesin përfundime të sigurta, duke argumentuar shpesh se armët bërthamore kanë pasur ndikim minimal në konflikt. Shembujt përfshijnë pohimin e Snyder 'se lufta bërthamore nuk po ndodh', pretendimin e Gould-Davies 'se Rusia nuk ka linja të kuqe bërthamore' dhe pikëpamjen e Sauer 'se armët bërthamore ofrojnë pak përfitim përtej parandalimit'[12]. Po kështu Ramesh Thakur shprehet se: "Ajo që më duket më e habitshme në lidhje me armët bërthamore është mungesa pothuajse e plotë e dobisë së tyre. Prania e afro 6000 bombave në arsenalin e Rusisë.... nuk arriti të frikësonte Ukrainën që të dorëzohej. Kievi thjesht ka vazhduar të mbrojë trimërisht territorin e tij, i bindur se, pasi kanë dështuar si një mjet diplomacie shtrënguese, armët bërthamore nuk janë të përdorshme ushtarakisht... Reputacioni i Rusisë do të dëmtohej plotësisht nëse do të përdorte bombën"[13]. Megjithatë, duke pasur parasysh provat e kufizuara faktike, përfundime të tilla të sigurta duhet të priten me skepticizëm. Pavarësisht nga kjo pasiguri, analiza empirike mbetet vendimtare. Vlerësimi i provave në zhvillim ndihmon në përsosjen e të kuptuarit teorik, për shkak të mungesës së precedentit historik në çështjet bërthamore. Prandaj, duhet një përpjekje e kujdesshme por e vazhdueshme shkencore për të vlerësuar dinamikën bërthamore në konfliktet bashkëkohore. Duke pasur parasysh këto

[11] Snyder, J., *Richness, Rigor, and Relevance in the Study of Soviet Foreign Policy,* 1984-1985, https://muse.jhu.edu/article/446102.

[12] *"Nuclear War! Why it isn't Happening." Snyder, T. 2023. February 8, 2023. "Putin Has No Red Lines." Gould-Davies, N. 2023. New York Times, January 2, 2023. "How Useful Are Nuclear Weapons in Practice? Case-Study: The War in Ukraine." Sauer, T. 2024. Journal for Peace & Nuclear Disarmament 7 (1): 194–210.*

[13] *"How Much Damage Have Putin's Threats Done to the Nuclear Nonproliferation Regime?" Thakur, R. 2022. The Strategist. July 18, 2022. https://www.aspistrategist.org.au/howmuch-damage-have-putins-threats-done-to-the-nuclear-non-proliferation-regime*

kufizime, përfundimet nga lufta në Ukrainë nuk duhet të çojnë në ndryshime të ideve teorike të mëparshme për armët bërthamore, por duhet t'i mbështesin ato, sidomos sa i përket përdorimit të tyre si mjet frenimi dhe kërcënimi në kontekste strategjike.

2. Efektet dhe roli i armëve bërthamore

Duke marrë parasysh analizën e mësipërme, është e arsyeshme të ndjekim një qasje (në kuptimin e dijes) të kujdesshme kur nxjerrim përfundime mbi luftën në Ukrainë. Në këtë kontekst, çfarë përfundimesh mund të nxjerrim dhe me çfarë niveli pasigurie, lidhur me rolin e armëve bërthamore në këtë konflikt? Duke u mbështetur në tre ide të njohura teorike mbi armët bërthamore, mendoj se ajo që po ndodh në Ukrainë është kryesisht në përputhje me këto parime:

Armët bërthamore kanë efekt parandalues - Ato pengojnë aktorët të ndërmarrin veprime që mund të çojnë në përshkallëzim të madh.

Armët bërthamore mundësojnë njëfarë lirie veprimi - Fuqitë bërthamore ndihen më të sigurta në ndërmarrjen e veprimeve të caktuara, duke pasur si garanci arsenalin e tyre bërthamor.

Efektet politike të armëve bërthamore burojnë nga rreziku i shkatërrimit që ato paraqesin - Nuk është domosdoshmërisht përdorimi i tyre, por vetë kërcënimi dhe pasojat e mundshme që ndikojnë në vendimet strategjike.

Duke pasur parasysh rëndësinë e teorive në kushte pasigurie, provat faktike, nga lufta në Ukrainë nuk duhet të na shtyjë të rishikojmë apo të hedhim poshtë këto ide të njohura. Përkundrazi, ajo duket se i forcon ato edhe më shumë.

Armët bërthamore si parandalues

Kuptimi parësor teorik i armëve bërthamore është se ato shërbejnë si një parandalues i fuqishëm për shkak të shkatërrimit të madh dhe vështirësive teknike në mbrojtjen e besueshme kundër një sulmi bërthamor. Siç thotë John Mearsheimer, armët bërthamore janë parandaluesi i fundit për shkak të frikës që ngjallin[14]. Ky këndvështrim pranohet gjerësisht në qarqet politike dhe ushtarake. Megjithatë, parandalimi nuk është absolut dhe efektiviteti i parandalimit bërthamor në parandalimin e të gjitha veprimeve kundërshtare mbetet një temë debati. Studiues si Vipin Narang dhe Paul Avey kanë eksploruar aspekte të ndryshme të parandalimit bërthamor, duke përfshirë qëndrimet e nevojshme për parandalim efektiv dhe strategjitë për shtetet më të dobëta për t'u përballur me fuqitë e armatosura bërthamore pa u përshkallëzuar në konflikt bërthamor.

[14] Mearsheimer, J. J., *Nuclear Weapons and Deterrence in Europe,* 1984 - 1985.

Lufta e vazhdueshme në Ukrainë ofron prova të botës reale që mbështesin efektet parandaluese të armëve bërthamore. Pavarësisht viktimave dhe shkatërrimeve të larta në Ukrainë, si Rusia ashtu edhe Shtetet e Bashkuara kanë treguar përmbajtje të konsiderueshme. Rusia ka shmangur sulmin ndaj vendeve të NATO-s ose përdorimin e armëve bërthamore taktike, edhe pse veprime të tilla mund të ofrojnë avantazhe ushtarake afatshkurtra. Në mënyrë të ngjashme, Shtetet e Bashkuara kanë kufizuar përfshirjen e tyre duke u përmbajtur nga ndërhyrja e drejtpërdrejtë dhe duke i vendosur kufizime Ukrainës në përdorimin e disa kapaciteteve ushtarake, duke pasur frikë nga përshkallëzimi rus.

Ndërsa disa argumentojnë se parandalimi bërthamor nuk ka formësuar dinamikën thelbësore të konfliktit, të tjerë pretendojnë se kujdesi i ndërsjellë i vërejtur është në përputhje me teoritë e vendosura të parandalimit. Veçanërisht, studiues si Tannenwald, Lewis dhe Wellerstein kanë theksuar rolin e armëve bërthamore në kufizimin e fushës së luftës. Pavarësisht kritikave për parandalimin bërthamor, provat tregojnë se armët bërthamore luajnë një rol të rëndësishëm në formësimin e sjelljes si të Rusisë ashtu edhe të Perëndimit.

Përshkallëzimi gradual nga Shtetet e Bashkuara është në përputhje me teoritë e vendosura të parandalimit, ku shtetet i shtyjnë me kujdes kufijtë nën kufizimet e përshkallëzimit të mundshëm bërthamor. Natyra e kufizuar e ofensivës së Ukrainës në rajonin e Kurskut të Rusisë nuk e zhvlerëson efektin parandalues të armëve bërthamore, pasi operacioni nuk kishte gjasa të ndryshonte në mënyrë drastike trajektoren e konfliktit. Reagimi i përmbajtur i Rusisë mund t'i atribuohet ndikimit të kufizuar strategjik të inkursionit dhe dobësimit të mundshëm afatgjatë të aftësive mbrojtëse të Ukrainës.

Shpjegimi më i besueshëm për kujdesin perëndimor nuk është mungesa e guximit, por përkundrazi parandalimi i shkaktuar nga ekzistenca e armëve bërthamore ruse. Këto armë mund të shkaktojnë shkatërrim katastrofik dhe kontrolli i tyre nga një udhëheqës i paparashikueshëm shton pasigurinë. Ky realitet nënvizon efektin politik të kuptuar prej kohësh të armëve bërthamore - ato kërkojnë kujdes dhe përmbajtje. Sjellja e Rusisë, Shteteve të Bashkuara dhe aleatëve të tyre në konfliktin e Ukrainës duket kryesisht në përputhje me dinamikën e parandalimit bërthamor, duke e bërë të parakohshme hedhjen poshtë të këtij kuadri teorik të vendosur mirë në favor të konceptit më të ri të vetëparandalimit pa prova bindëse. Në fund të fundit, lufta në Ukrainë ripohon idenë themelore se armët bërthamore janë mjete të fuqishme parandaluese, duke ndikuar në llogaritjet strategjike të të gjitha palëve të përfshira në konflikt.

Armët bërthamore mundësojnë...

Një nga efektet më të njohura teorike të armëve bërthamore është fuqia e tyre për të penguar kundërshtarët nga veprime të caktuara. Por, nëse kjo

është e vërtetë, atëherë ato duhet gjithashtu të ndikojnë në mënyrën si shtetet bëjnë llogaritjet e tyre strategjike, duke mundësuar sjellje të tjera. Studiuesit kanë debatuar gjatë mbi mënyrën dhe rrethanat në të cilat armët bërthamore i japin një shteti liri veprimi, por është e pranuar gjerësisht se ato krijojnë një avantazh të caktuar strategjik. Kjo dinamikë, e mbështetur nga punime shkencore sugjeron që armët bërthamore reduktojnë rreziqet negative të veprimeve duke ndryshuar llogaritjet kosto-përfitim, duke i bërë disa veprime më të realizueshme[15].

Në histori, kjo dinamikë është vënë re në shumë raste. Për shembull, Pakistani ka përdorur arsenalin e tij bërthamor për të mbrojtur qëllimet e tij në Kashmir, Britania e Madhe gjatë Luftës së Ftohtë e ka përdorur fuqinë bërthamore për të vepruar më e pavarur nga Shtetet e Bashkuara, dhe SHBA-të i kanë përdorur armët bërthamore si garanci për një rrjet global aleancash pas Luftës së Dytë Botërore. Këta shembuj theksojnë se shtetet e armatosura bërthamore kanë njohur dhe shfrytëzuar efektet mundësuese të arsenaleve të tyre bërthamore për të çuar përpara objektivat e politikës së jashtme.

Në rastin e Ukrainës, ka të ngjarë që armët bërthamore të kenë ndihmuar Rusinë të ndërmarrë agresionin e saj. Lufta ka dëmtuar ndjeshëm forcat e saj konvencionale, por aftësia e saj për të penguar ndërhyrjen e drejtpërdrejtë të Perëndimit ka mbetur e paprekur, falë arsenalit të saj bërthamor. Kjo nuk do të thotë domosdoshmërisht se Putin synon të përdorë armët bërthamore në këtë luftë, por fakti që ato ekzistojnë mund të ketë reduktuar rreziqet strategjike me të cilat Rusia do të përballej nëse nuk do t'i kishte ato. Në këtë mënyrë, armët bërthamore kanë funksionuar si një mburojë për agresionin rus, një dinamikë e ngjashme me atë të Pakistanit apo Afrikës së Jugut në të kaluarën[16].

Por ky efekt nuk është i njëanshëm. Në të njëjtën mënyrë që armët bërthamore mundësojnë agresionin rus, ato gjithashtu kanë ndihmuar Perëndimin të mbështesë Ukrainën pa u përfshirë drejtpërdrejt në luftë. SHBA-ja ka dërguar dhjetëra miliarda dollarë ndihmë ushtarake në Ukrainë, si dhe ka transportuar pajisje ushtarake përmes aleatëve të NATO-s, pa frikën e një sulmi të drejtpërdrejtë rus. Ky veprim tregon se të dyja palët janë të vetëdijshme për efektin e dyfishtë të armëve bërthamore: si një faktor pengues, ashtu edhe si një mjet që lejon manovra strategjike brenda kufijve të vendosur nga kërcënimi i përshkallëzimit.

---

[15] "Beyond Emboldenment: How Acquiring Nuclear Weapons Can Change Foreign Policy." Bell, M. S. 2015. International Security 40 (1): 87–119. "Fear and Loathing: When Nuclear Proliferation Emboldens." Cohen, M. D. 2018. Journal of Global Security Studies 3 (1): 56–71. Dangerous Deterrent: Nuclear Weapons Proliferation and Conflict in South Asia. Kapur, S. P. 2009. Stanford: Stanford University Press.

[16] Nuclear Reactions: How Nuclear-Armed States Behave. Bell, M. S. 2021. Ithaca: Cornell University Press

Ajo që po ndodh në Ukrainë është vazhdimësi e kësaj logjike të vjetër të Luftës së Ftohtë: të dyja palët përpiqen të arrijnë objektivat e tyre strategjike, por pa kaluar vijat e kuqe që mund të çojnë në përshkallëzim të pakontrolluar. Në këtë kuptim, lufta në Ukrainë nuk po krijon një precedent të ri për mënyrën se si shtetet e armatosura bërthamorë e përdorin fuqinë e tyre. Përkundrazi, ajo thjesht po konfirmon një dinamikë të njohur dhe të dokumentuar historikisht.

Kjo dinamikë nuk është e re. Gjatë Luftës së Ftohtë, SHBA dhe Bashkimi Sovjetik shpesh rivalizonin njëri-tjetrin nëpër një sërë konfliktesh, krizash dhe luftërash ndërmjetëse si në Kore, Kubë, Gjermani, Angola, Afganistan apo gjetkë, por të dyja palët ruanin gjithmonë një vijë të qartë për të shmangur një përshkallëzim të pakontrolluar[17]. Në vend që të përballeshin drejtpërdrejt me përdorimin e forcës bërthamore, ato shpesh manovronin për të shmangur nevojën për veprime drastike. Ky kombinim i konkurrencës dhe bashkëpunimit ka qenë një tipar i rregullt i konkurrencës së fuqive të mëdha në epokën bërthamore. Ajo që po ndodh në Ukrainë duket kryesisht të përputhet me këto dinamika të njohura.

Efektet politike të armëve bërthamore burojnë nga rreziku

Efektet politike të armëve bërthamore janë të lidhura ngushtë me rrezikun që ato paraqesin për përshkallëzimin e konflikteve në nivel bërthamor. Ndryshe nga armët konvencionale, armët bërthamore kanë një fuqi shkatërruese të jashtëzakonshme dhe mund të çojnë në pasoja katastrofike globale në rast përdorimi. Kjo natyrë e tyre krijon një situatë të veçantë, ku shtetet mund të konkurrojnë politikisht dhe ushtarakisht, por gjithmonë nën hijen e këtij rreziku. Rreziku që gjërat mund të dalin jashtë kontrollit nuk është një pengesë, por një komponent i nevojshëm për të mbajtur parandalimin bërthamor funksional[18]. Kjo logjikë mbështetet edhe nga historiani Alex Wellerstein, i cili vëren se logjika e parandalimit gjithmonë përfundon duke u bazuar në një ndjenjë frike dhe terrori të pastër[19].

Thomas Schelling (1966) argumenton që, edhe pse nuk mund të kërcënojnë në mënyrë të besueshme se do të fillojnë një luftë bërthamore për çështje politike, shtetet bërthamore mund të manipulojnë rrezikun e përshkallëzimit për të

[17] "Advancing without Attacking: The Strategic Game Around the Use of Force." Altman, D. 2018. Security Studies 27 (1): 58–88.

[18] "Who is Deterring Whom? The Place of Nuclear Weapons in Modern War." War on the Rocks. Lewis, J., and A. Stein. 2022. June 16, 2022. https://warontherocks.com/2022/06/who-is-deterring-whom-the-place-of-nuclear-weapons-in-modern-war/

[19] "The Nuclear Dilemma: Deterrence Works, Up to a Point." Engelsberg Ideas. Wallenstein, A. 2022. June 7, 2022. Wilson, W. 2007. "The Winning Weapon? Rethinking Nuclear Weapons in Light of Hiroshima." International Security 31 (4): 162–179.

fituar avantazhe politike dhe ushtarake[20]. Procesi i këtij manipulimi të rrezikut është një pjesë thelbësore e dinamikave politike në epokën bërthamore dhe nuk mund të bëhet pa rrezik. Analogjia e Schelling me dy alpinistë të lidhur pranë një shkëmbi e ilustron këtë dinamikë: secili prej tyre mund të kërcënojë se do të hidhet nga shkëmbi për të detyruar tjetrin të bëjë lëshime, por nuk mund të kërcënojë bindshëm se do të hidhet, pasi një akt i tillë do të kishte pasoja fatale për të dy. Rreziku i rrëshqitjes aksidentale ose gabimit është pjesë e kërcënimit dhe rrit efektin e tij shtrëngues.

Në këtë kontekst, veprime që duken të parëndësishme strategjikisht mund të kenë efekt të fortë politik për shkak të rrezikut që krijojnë. Për shembull, dislokimi i armëve taktike bërthamore ruse në Bjellorusi, ndonëse nuk ndryshon domosdoshmërisht balancën strategjike, shton rrugët potenciale për përshkallëzim dhe aksidente. Nisur nga një analizë më e thellë kjo tregon se qëllimi i këtij veprimi nuk është të ndryshojë balancën, por të shtojë pasigurinë dhe rrezikun e përshkallëzimit, duke krijuar më shumë mundësi që një ngjarje aksidentale të çojë në konflikt bërthamor.

Një tjetër shembull i kësaj dinamike është vendimi i SHBA-së dhe aleatëve të saj për të pranuar Finlandën[21] dhe Suedinë në NATO, duke dyfishuar kufirin tokësor midis NATO-s dhe Rusisë. Kjo shton rrugë të reja për përshkallëzim dhe presion mbi Rusinë. Pranimi i Finlandës dhe Suedisë në NATO është një ilustrim i qartë i mënyrës se si shtetet bërthamore, duke krijuar rreziqe të reja, mund të ushtrojnë presion mbi kundërshtarët e tyre. Pra, shumë veprime dhe kërcënime që synojnë të ushtrojnë presion nuk do të kishin kuptim nëse do të ishte e sigurt që nuk do të ndodhte përshkallëzim. Po ashtu, nëse këto veprime do të çonin domosdoshmërisht në luftë, ato nuk do të ndërmerreshin fare. Vlera e tyre qëndron pikërisht në rrezikun e një përshkallëzimi të papritur, të shkaktuar nga gabime ose aksidente, dhe kjo i bën këto veprime të rëndësishme në politikën ndërkombëtare.

Përfundimisht, ndërsa shtetet mund të përpiqen të menaxhojnë ose të reduktojnë rreziqet e përshkallëzimit bërthamor, një menaxhim i tillë domosdoshmërisht kufizon fuqinë shtrënguese të armëve bërthamore dhe aftësinë e shtetit për të arritur objektivat e tij politike. Prandaj, rreziku nuk është një problem që mund të eliminohet pa humbur ndikimin politik të armëve bërthamore. Ky rrezik mbetet një mekanizëm thelbësor për mënyrën se si armët bërthamore ndikojnë në politikën ndërkombëtare dhe historia e krizave bërthamore gjatë Luftës së Ftohtë e deri te lufta në Ukrainë tregon qartë rëndësinë e tij. Dinamikat që vërejmë sot midis Rusisë dhe Perëndimit janë në përputhje me këto njohuri të mirënjohura.

[20] Arms and Influence. Schelling, T. C. 1966. Cambridge: Harvard University Press.

[21] Finlanda ka një kufi të gjatë (1,340 km) me Rusinë dhe ka një histori të tensionuar me Moskën, veçanërisht gjatë Luftës Dimërore (1939-1940).

3. Ndikimi në rolin e armëve bërthamore dhe energjisë bërthamore në botë

Nga sa u analizua më sipër mund të japim disa reflektime si më poshtë:

Rusia e ka bërë luftën e saj kundër Ukrainës një krizë bërthamore. Në këtë luftë, Ukraina jo vetëm që po i kundërvihet një kundërshtari më të madh, më të pasur dhe të armatosur më mirë, por është gjithashtu një shtet pa armë bërthamore që i kundërvihet një shteti me armë bërthamore. Lufta në Ukrainë është një luftë konvencionale. Deri më tani. Por kjo është një krizë bërthamore me pasoja të thella për parandalimin bërthamor, mospërhapjen dhe çarmatimin, si dhe për të ardhmen e energjisë paqësore bërthamore. Jo çdo luftë e zhvilluar nga një shtet i armatosur bërthamor është, sipas përkufizimit, një krizë bërthamore, por ajo mund të bëhet e tillë nëse një shtet bërthamor e zgjedh këtë. Rusia ka zgjedhur ta bëjë luftën e saj kundër Ukrainës një krizë bërthamore. Rusia është mbështetur shumë në kërcënimet dhe sinjalizimet bërthamore, qëllimi kryesor i të cilave ka qenë të projektojë fuqinë e saj, të pengojë çdo mbështetje perëndimore për Ukrainën, si dhe të frikësojë udhëheqjen dhe popullin ukrainas.

Në lidhje me mbrojtjen e integritetit territorial të Rusisë gjatë një fjalimi më 21 shtator 2022 Vladimir Putin u shpreh: "Dhe kur integriteti territorial i vendit tonë kërcënohet, ne me siguri do të përdorim të gjitha mjetet që kemi në dispozicion për të mbrojtur Rusinë dhe popullin tonë. Nuk është një blof[22]." Deklarata e Putinit ishte një mesazh strategjik për të frikësuar Perëndimin, për të justifikuar mobilizimin dhe për të ruajtur ndikimin në Ukrainë. Megjithatë, përdorimi i armëve bërthamore mbeti i paprovuar, duke treguar kufizimet e këtij kërcënimi në realitetin gjeopolitik.

Së fundi, ekziston një rrezik gjithnjë i pranishëm i përdorimit nga Rusia të një arme bërthamore taktike kundër Ukrainës, qoftë në fushën e betejës apo kundër një qyteti ukrainas. Në mënyrë shqetësuese, retorika bërthamore ruse nuk është e kufizuar në Kremlin, ajo ka depërtuar në disa cepa të komunitetit të ekspertëve të mbrojtjes dhe është e përhapur në mediat ruse dhe diskursin publik. Sergej Karaganov dhe Dmitriy Trenin, janë ndër analistët, dikur të konsideruar me respekt në Perëndim, të cilët kanë mbrojtur një sulm bërthamor kundër NATO-s, si një mënyrë për të treguar vendosmërinë ruse dhe për të fituar respektin perëndimor për interesat ruse[23][24].

---

[22] https://onlinelibrary.wiley.com/doi/10.1111/nana.12876

[23] https://economictimes.indiatimes.com/news/defence/russian-hawk-pushes-case-for-putin-to-toughen-policy-on-nuclear-weapons/articleshow/113286729.cms

[24] https://www.euractiv.com/section/global-europe/news/russian-hawk-pushes-case-for-putin-to-strike-west-with-nuclear-weapons/

Shfaqjet politike ruse rrallë kalojnë pa kërcënime se do të godasë Ukrainën apo Evropën ose të dyja. Ndërsa është joshëse të shpërfillësh një retorikë të tillë si shaka ose propagandë me pak ndikim në vendimmarrjen bërthamore, një bisedë e tillë e lirshme bërthamore kontribuon në gërryerjen e tabusë bërthamore. Dhe kështu, bota ka mbetur të hamendësojë se çfarë mund të jetë e gatshme dhe e aftë të bëjë Rusia me arsenalin e saj bërthamor në mes të një lufte të nxehtë konvencionale në shkallë të gjerë duke u përballur me realitetin e pasigurisë së pashmangshme.

Rendi i përcaktuar global bërthamor. Cilat janë pasojat e kësaj krize të vazhdueshme bërthamore për rendin bërthamor global? Rendi Global Bërthamor i referohet grupit të normave, rregullave, marrëveshjeve dhe praktikave që rregullojnë posedimin, zhvillimin dhe përdorimin e armëve bërthamore dhe të energjisë bërthamore në mbarë botën. Ai përfshin ndërveprimet midis shteteve, institucioneve ndërkombëtare dhe aktorëve joshtetërorë në lidhje me çështjet bërthamore, me qëllim ruajtjen e sigurisë globale, parandalimin e përhapjes së armëve bërthamore dhe promovimin e çarmatimit bërthamor. William Walker, një studiues britanik, e koncepton Rendin Bërthamor Global si të përbërë nga dy nënrende: Sistemi i Parandalimit dhe Sistemi i Abstinencës[25]. Ky kuadër ndihmon për të kuptuar dinamikën e armëve bërthamore dhe marrëdhëniet ndërkombëtare. Në këtë kuadër mund të shtojmë edhe Sistemin e Qeverisjes së Energjisë Bërthamore për përdorime paqësore, pasi ndan të njëjtën prejardhje dhe një pjesë të së njëjtës shkencë dhe teknologji, me përdorimin ushtarak duke mbartur me vete rreziqet e përhapjes si dhe dëmtimin e mjedisit.

Këta tre sisteme janë herë-herë të ndërlidhur, por në raste të tjera, ata janë në kundërshtim të drejtpërdrejtë me njëri-tjetrin[26]. Pavarësisht përpjekjeve

[25] William Walker, A Perpetual Menace Nuclear Weapons and International Order, 2012.

[26] Sistemi i Parandalimit bazohet në idenë e deterrencës bërthamore, ku shtetet që zotërojnë armë bërthamore i përdorin ato për të frenuar mundësinë e sulmeve nga shtete të tjera, përmes kërcënimit të një hakmarrjeje masive dhe të përgjakshme. Ky sistem ka mbajtur paqen mes fuqive bërthamore që nga fundi i Luftës së Ftohtë, përmes një ndarje të fuqishme mes vendeve me dhe pa armë bërthamore.

Sistemi i Abstinencës ka të bëjë me ndalimin e përvetësimit të armëve bërthamore, duke përfshirë Nismën Ndërkombëtare të Mos-Proliferimit (NPT), e cila përpiqet të kufizojë shpërndarjen e armëve bërthamore dhe të promovojë disarmimin bërthamor, duke inkurajuar shtetet të mos zhvillojnë armë bërthamore, përkundër mundësisë për të përdorur energjinë bërthamore për qëllime paqësore.

Përveç këtyre dy sistemeve, mund të shtojmë një Sistem të Qeverisjes së Energjisë Bërthamore për Përdorime Paqësore. Ky sistem mbikëqyr përdorimin e teknologjisë bërthamore për qëllime paqësore, si prodhimi i energjisë dhe aplikimet mjekësore, duke siguruar gjithashtu kontrollin dhe kufizimet e nevojshme për të parandaluar shpërndarjen e teknologjisë që mund të përdoret për zhvillimin e armëve bërthamore.

për të menaxhuar tensionet midis këtyre sistemeve, nëpërmjet NPT[27], tensionet mbeten të thella. NPT ka qenë përpjekja kryesore për të krijuar një rend global bërthamor, por ajo është diskriminuese, pasi lejon disa shtete të mbajnë armë bërthamore, ndërsa të tjerëve ua ndalon këtë mundësi. Në fund, tensionet e vazhdueshme brenda këtyre sistemeve kanë një përhapje të mëtejshme në rendin global bërthamor. Çdo këputje ose ndryshim në një prej këtyre sistemeve ka potencialin të shkaktojë pasoja të thella dhe të papritura për gjithë sistemin, duke ndikuar në marrëdhëniet ndërkombëtare, moralin ndërkombëtar dhe sigurinë globale.

Lufta në Ukrainë është një nxitje për Sistemin e Parandalimit. Putini ka llogaritur saktë se arsenali bërthamor i Rusisë do të parandalojë ndërhyrjen e drejtpërdrejtë perëndimore në Ukraine duke përdorur armët bërthamore si një mundësues i luftës së tij kundër Ukrainës. Në të vërtetë, parandalimi bërthamor midis Rusisë nga njëra anë dhe Shteteve të Bashkuara dhe NATO-s nga ana tjetër, duket se funksionon dhe shkakton përmbajtje. Ndërsa vendet perëndimore kanë vendosur sanksione ndëshkuese ndaj Rusisë dhe kanë furnizuar një pjesë të madhe armatimesh dhe ndihma të tjera për Ukrainën, udhëheqësit e SHBA-së dhe NATO-s kanë deklaruar vazhdimisht se nuk do të dërgojnë trupa në Ukrainë, kanë qenë të kujdesshëm me dispozitat e armëve dhe kanë vendosur kufizime në përdorim e tyre. Me pak fjalë, kërcënimet bërthamore ruse ishin pjesërisht të suksesshme për të ndikuar në kohën dhe llojin e ndihmës ushtarake për Ukrainën.

Ajo që duket e drejtë të supozohet është se nëse Rusia nuk do të ishte një fuqi bërthamore dhe nëse nuk mund të mbështetej në kërcënimet bërthamore për të shmangur mundësinë e një përfshirjeje të drejtpërdrejtë perëndimore, llogaritjet e saj për pushtimin e Ukrainës do të kishin qenë shumë të ndryshme. Nëse Rusia nuk do të ishte një fuqi bërthamore, reagimi perëndimor ndaj agresionit rus në Ukrainë gjithashtu do të kishte qenë i ndryshëm.

Kjo luftë zbuloi asimetrinë e tolerancës ndaj rrezikut midis Rusisë dhe Shteteve të Bashkuara dhe aleatëve të saj në NATO. Lufta gjithashtu ka ekspozuar kufijtë e detyrimit bërthamor – ka një aktor që nuk frenohet dhe nuk frikësohet nga kërcënimet bërthamore ruse dhe ai është Ukraina. Kjo tregon se parandalimi bërthamor nuk varet vetëm nga fuqia ushtarake, strategjitë dhe doktrinat, por edhe nga interesat e përfshira dhe vendosmëria politike e palëve. Nëse një shtet beson se rreziku i përshkallëzimit është shumë i lartë dhe kostoja e një konflikti bërthamor do të ishte katastrofike, ai mund të stepet nga përdorimi i armëve bërthamore, pavarësisht nga kapacitetet që zotëron.

[27]NPT (Treaty on the Non-Proliferation of Nuclear Weapons) është Traktati për Mospërhapjen e Armëve Bërthamore, i cili ka për qëllim të parandalojë përhapjen e armëve bërthamore, të promovojë çarmatimin bërthamor dhe të inkurajojë përdorimin paqësor të energjisë bërthamore.

Pra, faktorët politikë dhe rrethanat specifike janë po aq të rëndësishme sa fuqia ushtarake në përcaktimin e sjelljes së aktorëve bërthamorë.

***Lufta në Ukrainë është një goditje për Sistemin e Abstinencës Bërthamore**:* Lufta në Ukrainë ka goditur rëndë sistemin global të parandalimit të shpërndarjes bërthamore (NPT) dhe besimin te garancitë ndërkombëtare të sigurisë. Nëse kufizimi midis Rusisë dhe NATO-s mund të jetë një shembull pozitiv i mënyrës sesi funksionon parandalimi bërthamor, kryqëzimi i Ukrainës është një demonstrim i asaj që ndodh me një vend që nuk mbrohet nga një parandalues bërthamor, qoftë i tij apo nga një aleat.

Ukraina, e cila hoqi dorë nga arsenali bërthamor në 1994 në këmbim të garancive të sigurisë për sovranitetin e saj, u tradhtua nga një prej nënshkruesve të Memorandumit të Budapestit – Rusia – me aneksimin e Krimesë në 2014 dhe pushtimin e saj në 2022, shoqëruar me kërcënime bërthamore. Pjesë e marrëveshjes që Ukraina negocioi në këmbim të çarmatimit ishin garancitë e sigurisë për të respektuar sovranitetin e Ukrainës, paprekshmërinë e kufijve të saj dhe për të përmbajtur kërcënimin ose përdorimin e forcës, bërthamore ose ndryshe, kundër Ukrainës, të zotuara në të ashtuquajturin Memorandum të Budapestit nga tre fuqi bërthamore, depozitues të NPT - Shtetet e Bashkuara, Mbretëria e Bashkuar dhe Federata Ruse. Rezultati është dëmtimi i besueshmërisë së regjimit të mospërhapjes dhe vlerës së garancive të sigurisë si një mjet i politikës së mospërhapjes.

Kjo ka dëmtuar besimin në marrëveshjet e çarmatimit dhe ka thelluar ndarjen mes fuqive bërthamore dhe vendeve pa armë bërthamore, duke nxitur traktate të reja si TPNW[28], që kërkon ndalimin e plotë të armëve bërthamore. Ndërkohë, kontrolli i armëve mes SHBA-së dhe Rusisë është bllokuar, me traktatin e fundit të reduktimit të armëve strategjike New START[29] që skadon në shkurt 2026 dhe nuk ka perspektiva për të negociuar një marrëveshje pasuese. Nëse nuk arrihet një kompromis, bota mund të hyjë në një epokë të re pa kufizime mbi arsenalet bërthamore, duke rritur rrezikun e një gare të re armatimi dhe konflikteve të mundshme. Mungesa e përparimit në kontrollin e armëve do të ndikojë në tendosje të mëtejshme në Rendin Bërthamor Global.

[28] Traktati për Ndalimin e Armëve Bërthamore (Treaty on the Prohibition of Nuclear Weapons – TPNW) është një marrëveshje ndërkombëtare e miratuar nga Kombet e Bashkuara më 7 korrik 2017, e cila synon ndalimin e plotë të armëve bërthamore. Traktati hyri në fuqi më 22 janar 2021, pasi u ratifikua nga 50 shtete.

[29] New START (New Strategic Arms Reduction Treaty) është një traktat i kontrollit të armëve bërthamore midis Shteteve të Bashkuara dhe Rusisë, i nënshkruar më 8 prill 2010 në Pragë dhe që hyri në fuqi më 5 shkurt 2011. Traktati kishte një afat fillestar 10-vjeçar dhe u zgjat edhe për 5 vite të tjera në shkurt 2021, duke mbetur në fuqi deri më 5 shkurt 2026.

Lufta në Ukrainë është një sfidë e paprecedentë për Sistemin e Qeverisjes së Energjisë Bërthamore. Lufta në Ukrainë ka krijuar sfida të për sigurinë dhe menaxhimin global të energjisë bërthamore. Rusia ka përdorur centralet bërthamore si instrumente lufte, duke pushtuar **Çernobilin** dhe më pas Zaporizhzhian, centralin më të madh bërthamor në Evropë. Forcat ruse e kanë kthyer këtë impiant në një bazë ushtarake, duke rrezikuar sigurinë bërthamore dhe duke shkaktuar ndërprerje të energjisë, si dhe dëmtime nga bombardimet dhe sabotimet, përfshirë shkatërrimin e digës Kakhovka që furnizonte me ujë sistemin e ftohjes së reaktorëve. Një tjetër shkelje serioze ka qenë trajtimi çnjerëzor i stafit ukrainas, ku mijëra punonjës janë detyruar të punojnë nën trysni, disa janë arrestuar, torturuar ose detyruar të nënshkruajnë kontrata me kompaninë ruse Rosatom.

Të gjitha këto veprime krijuan sfida të paprecedenta për sigurinë dhe sigurinë bërthamore në Centralin Bërthamor të Zaporizhias, sfida për të cilat nuk ekzistojnë ende praktikat më të mira, asnjë konventë, asnjë rregullore. Megjithëse Agjencia Ndërkombëtare e Energjisë Atomike (IAEA) ka bërë përpjekje të mëdha për monitorimin e situatës, mungojnë mekanizmat ndërkombëtarë për të adresuar raste të tilla, ku një fuqi ushtarake përdor impiante bërthamore si armë strategjike. Në një botë që synon zgjerimin e energjisë bërthamore për zhvillim dhe luftën kundër ndryshimeve klimatike, duhet një rishikim urgjent i sigurisë bërthamore, duke përfshirë mbrojtjen e personelit dhe sigurinë ndaj kërcënimeve të luftës.

Përfundime

Pavarësisht se kanë kaluar 75 vjet në epokën bërthamore, ndikimi i armëve bërthamore në politikën ndërkombëtare mbetet ende i paqartë. Megjithatë, studiuesit bien dakord për disa parime bazë: armët bërthamore pengojnë sulmet, u japin fuqi shteteve që i zotërojnë dhe krijojnë rreziqe të mëdha përshkallëzimi, për shkak të shkatërrimit katastrofik që mund të shkaktojnë.

Lufta në Ukrainë deri tani ka konfirmuar këto parime, por nuk ka sjellë ndonjë ndryshim të madh në të kuptuarit e rolit të armëve bërthamore. Një përdorim real i armëve bërthamore nga Rusia do të hapte një epokë të re, me pasoja të paparashikueshme për politikën globale, për forcën e tabusë bërthamore, për regjimin e mos përhapjes bërthamore dhe për mënyrën sesi shtetet i përdorin këto armë për të ushtruar presion. Një botë pas përdorimit të armëve bërthamore do të sillte mësime krejtësisht të reja, por deri tani ky skenar është shmangur.

Lufta në Ukrainë ka pasoja që shkojnë përtej sigurisë dhe integritetit territorial të një shteti të vetëm. Mënyra se si zhvillohet dhe si përfundon kjo luftë do të ndikojë drejtpërdrejt rolin e armëve bërthamore në politikën ndërkombëtare.

Pasojat për Rendin Bërthamor Global janë shqetësuese, sidomos për ata që e shohin **çarmatimin bërthamor si një synim të domosdoshëm për njerëzimin**. Kjo luftë ka treguar rreziqet e mëdha të një fuqie bërthamore që shkel rregullat ndërkombëtare, duke vënë në pikëpyetje vlerën e garancive të sigurisë dhe sistemin e mos shpërndarjes bërthamore. E ardhmja e armëve bërthamore si mjete të politikës shtetërore do të varet nga përfundimi i kësaj lufte dhe mënyra se si do të trajtohet Rusia pas agresionit të saj.

Mësimet bërthamore nga lufta në Ukrainë ende po formohen dhe ka mundësi që ne – dhe këtu nënkuptoj Ukrainën, partnerët e saj perëndimorë, si dhe të gjithë ata që janë të shqetësuar për të ardhmen e armëve bërthamore dhe energjisë bërthamore në botë – mund të ndikojnë në formësimin e këtyre mësimeve për të siguruar që:

- Ukraina mund të mposhtë një fuqi bërthamore, duke treguar se armët bërthamore nuk janë vendimtare për fitoren, por vendosmëria, guximi dhe mbështetja e aleatëve janë thelbësore. Perëndimi, me aleancën e tij politike dhe ushtarake më të fuqishme në histori, mund ta ndihmojë këtë fitore.
- Vlera e armëve bërthamore si mjete shantazhi dhe kërcënimi nuk duhet të rritet, duke penguar kështu shtetet e tjera të kërkojnë zhvillimin e tyre.
- Keqpërdorimi i armëve bërthamore për agresion dhe shantazh nuk duhet të mbetet pa përgjigje ose ndëshkim, për të ruajtur rendin ndërkombëtar.
- Ligjet dhe rregullat ndërkombëtare për sigurinë bërthamore duhet të përfshijnë edhe dimensionin njerëzor, duke garantuar që një shtet që shkel çdo normë dhe praktikë të sigurisë bërthamore nuk mund të përfitojë më nga tregtia bërthamore ndërkombëtare.
- Evropa duhet të shmangë një tjetër "vakum sigurie" si ai i Ukrainës, i cili i dha mundësi Rusisë të ndërmerrte agresion. Pa garanci të qarta sigurie, do të ketë kriza të tjera, me rreziqe të vazhdueshme bërthamore.
- Zhvillimi i strategjive për mbrojtjen e objekteve bërthamore në kohë lufte nëpërmjet përmirësimit të normave ndërkombëtare për mbrojtjen e centraleve bërthamore gjatë konflikteve dhe të sanksionohet çdo shtet që i përdor ato si mjete lufte.

Lufta në Ukrainë ka nxjerrë në pah sfidat dhe rreziqet që lidhen me armët bërthamore dhe energjinë bërthamore në shekullin XXI. Për të shmangur një epokë të re të pasigurisë bërthamore, nevojiten reforma në arkitekturën e sigurisë globale, kontroll më i mirë mbi armët bërthamore dhe masa për mbrojtjen e infrastrukturës bërthamore në konflikte të ardhshme.

Literatura e shfrytëzuar:

1. Anderson, N. 2019. "Competitive Intervention, Protracted Conflict, and the Global Prevalence of Civil War." International Studies Quarterly 63 (3): 692–706.
2. Anonymous 2023: Slouching Towards a Nuclear Gomorrah, Survival, 65: 6, 137–158.
3. Applebaum, A. 2022. "The War Won't End Until Putin Loses." The Atlantic. May 23, 2022.
4. Arceneaux, G. D. 2023. "Whether to Worry: Nuclear Weapons in the Russia-Ukraine War." Contemporary Security Policy 44 (4): 561–575. Arceneaux, G. D. 2024. ""Russian Nuclear Thresholds After the Kursk Offensive." United States Air Force Academy Institute for Future Conflict." September 6, 2024.
5. Arceneaux, Giles David 2023: Whether to worry: Nuclear Weapons in the Russia-Ukraine war, in: Contemporary Security Policy 44: 4, 561–575.
6. Arndt, A. C., L. Horovitz, and M. Onderco. 2023. "Russia's Failed Nuclear Coercion Against Ukraine." Washington Quarterly 46 (3): 167–184.
7. Arndt, Anna Clara, Horovitz, Liviu & Onderco, Michal 2023: Russia's Failed Nuclear Coercion Against Ukraine, Washington Quarterly 46: 3, 167–184.
8. Avery, Paul C. 2019: Tempting Fate: Why Nonnuclear States Confront Nuclear Opponents, Ithaca: Cornell University Press. Beardsley, Kyle & Asal, Victor 2009: Winning with the Bomb, Journal of Conflict Resolution, 53: 2, 278–301.
9. Avey, P. C. 2019. Tempting Fate: Why Nonnuclear States Confront Nuclear Opponents. Ithaca: Cornell University Press.
10. Bell, M. S., and N. L. Miller. 2023. "The Limits of Nuclear Learning in the New Nuclear Age." In The Fragile Balance of Terror: Deterrence in the New Nuclear Age, edited by V. Narang and S. D. Sagan, 209–229. Ithaca: Cornell University Press.
11. Binnendijk, Hans & Gombert, David 2019: Decisive Response: A new Nuclear Strategy for NATO, in: Survival, 61: 5, 113–128.
12. Bollfrass, A. K. & Herzog, S. 2023: The war in Ukraine and global nuclear order. In Survival: August-September 2022 (pp. 7-31).
13. Bollfrass, A. K., and S. Herzog. 2022. "The War in Ukraine and Global Nuclear Order." Survival 64 (4): 7–32.

14. Brands, H., and D. Palkki. 2011. “Saddam, Israel, and the Bomb: Nuclear Alarmism Justified?” International Security 36 (1): 133–166.

15. Buckley, C. 2023. “China Draws Lessons from Russia’s Losses in Ukraine, and Its Gains.” New York Times, April 1, 2023.

16. Budjeryn, M. 2024. “Why Russia is More Likely to Go Nuclear in Ukraine if it’s Winning.” Bulletin of the Atomic Scientists. October 2, 2024.

17. Budjeryn, Mariana 2022: Distressing a system in distress: global nuclear order and Russia’s war against Ukraine, Bulletin of the Atomic Scientists, 78: 6, 339–346.

18. Carson, A. 2016. “Facing off and Saving Face: Covert Intervention and Escalation Management in the Korean War.” International Organization 70 (1): 103–131.

19. Chyba, Christopher F. 2020: New Technologies and Strategic Stability, in: Daedalus, 150–170.

20. Cooper, Helene, Barnes, Julian & Schmitt, Eric 2022: Russian Military Leaders Discussed Use of Nuclear Weapons: New York Times.

21. Kofman, Michael & Fink, Anya Loukianova 2020: Escalation Management and Nuclear Employment in Russian Military Strategy, War on the Rocks.

22. Kofman, Michael & Fink, Anya Loukianova 2022: Escalation Management and Nuclear Employment in Russian Military Strategy, War on the Rocks. Available from:

23. Kohv, M. “Why the West Should Not Be Afraid of Russian Nuclear Threats.” International Centre for Defence and Security. March 25, 2024.

24. Nuclear Lessons and Dilemmas from the War in Ukraine. Gavin, F. J. 2024.

25. The Bomb in the Background, Nina Tannenwald, February 24, 2023 Foreign Affairs.

26. The Nuclear Age: During and After the Cold War. Jervis, R. 2021.

RUBRIKA E DYTË

ZHVILLIMI I TEKNOLOGJISË DHE INOVACIONIT NË FUSHËN E MBROJTJES

Si po transformohet inteligjenca artificiale, lufta dhe strategjitë moderne

Kolonel Msc. David RROKU
Shef Departamenti në IKSHU

Trajtesë e shkurtuar.

Përparimet e fundit në inteligjencën artificiale (IA) dhe potenciali i kësaj teknologjie kanë çuar në zhvillimin dhe vendosjen e teknologjive që dikur konsideroheshin fantashkencë. Nga dronët autonomë te robotët ushtarakë, integrimi i inteligjencës artificiale në sektorë të ndryshëm po riformulon luftën, sigurinë kombëtare, diplomacinë, ekonominë, qeverisjen, shëndetin dhe më gjerë. IA i referohet aftësisë së makinave për të kryer detyra që do të kërkonin inteligjencë njerëzore, të tilla si: arsyetimi, perceptimi, vendimmarrja, njohja e modeleve, mësimi nga përvoja, nxjerrja e përfundimeve dhe parashikimet.

Aftësitë ushtarake të inteligjencës artificiale përfshijnë armë, si dhe sisteme të mbështetjes së vendimeve, që ndihmojnë liderët në të gjitha nivelet për të marrë vendime më të mira dhe në kohë, nga fusha e betejës në sallën e këshillimit, nga lufta në nivelin taktik në atë të nivelit operacional e strategjik.

Megjithëse format rudimentare të IA kanë ekzistuar për dekada, vitet e fundit kanë parë një hap të madh në aftësitë e teknologjisë. Rrënjët e zhvillimit të inteligjencës artificiale vijnë në vitet 1940 me krijimin e neuroneve artificiale nga Warren McCulloch dhe Walter Pitts. Alan Turing, babIA i shkencës moderne kompjuterike, prezantoi testin Turing në 1950 për të përcaktuar aftësinë e një makine për të shfaqur përgjigje dhe inteligjencë të ngjashme me njeriun. Japonia zhvilloi robotin e parë "inteligjent" humanoid WABOT-1 në 1972.

Në vitet 2000, zhvillimet kryesore të IA përfshinin shfaqjen e mësimit të makinerive, zgjerimin e robotikës dhe vizionit kompjuterik, si dhe rritjen e nxjerrjes së të dhënave dhe njohjes së modeleve. Vitet 2010 panë përparim të jashtëzakonshëm në inteligjencën artificiale në fusha të ndryshme, të nxitur nga zbulimet e thella të të mësuarit, nga bashkëpunimi me burim të hapur, rritja e fuqisë kompjuterike me më shumë financime dhe investime kërkimore. Në vitin 2015, themelimi i OpenIA hodhi bazat për bumin aktual të inteligjencës artificiale. Në vitin 2016, programi AlphaGo i Google DeepMind mundi lojtarin profesionist Go, duke demonstruar potencialin e të mësuarit përforcues të thellë për lojëra komplekse strategjike. Në vitin 2019, bota pa lançimin e asistentit të parë të astronautit me IA.

Pika e vërtetë e kthesës erdhi me lançimin e ChatGPT në fund të vitit 2022, i cili solli IA në qendër të vëmendjes së publikut, duke gjeneruar interes dhe investime të gjera. Epoka e pas vitit 2020 është shënuar nga zhvillime novatore në gjeneratën e IA me modele të mëdha gjuhësore si: ChatGPT-4 i OpenAI, Gemini i Google (ish-Bard), Bing AI i Microsoft dhe Mistral AI Mixtral 8x7B, duke shtyrë kufijtë e ndërveprimit njeri-makinë. IA gjeneruese i referohet programeve që mund të krijojnë tekst, imazhe dhe përmbajtje të tjera me cilësi të lartë bazuar në të dhënat mbi të cilat janë trajnuar.

Fjalët kyçe: inteligjenca artificiale, siguri kombëtare, luftë moderne, strategji, teknologji ushtarake autonome, sistem inteligjent, bashkëpunim ndërkombëtar, inovacion.

Inteligjenca artificiale që transformon luftën moderne

Me përparimet e vazhdueshme në teknologji, Shtetet e Bashkuara të Amerikës (SHBA), Mbretëria e Bashkuar (MB), Kina, Franca, Rusia, Koreja e Jugut dhe Izraeli po investojnë shumë në zhvillimin e armëve me autonomi në rritje, ndërsa shtetet e tjera po mendojnë se si t'i përgjigjen automatizimit të luftës.

Ndërsa më shumë vende kërkojnë ta përfshijnë këtë teknologji në ushtritë e tyre, këto makina kanë nxitur një debat rreth zhvillimit dhe vendosjes së armëve që mund të kryejnë funksione gjithnjë e më të avancuara, me pak ose aspak mbikëqyrje njerëzore. Kjo çoi në debatin e parë ndonjëherë mbi inteligjencën artificiale në takimin e Këshillit të Sigurimit të Kombeve të Bashkuara në korrik 2023, me fokus në mundësitë dhe rreziqet e paraqitura nga IA për paqen dhe sigurinë ndërkombëtare.

Përtej kësaj nisme, disa vende kanë filluar t'i kushtojnë vëmendje më të madhe rolit në rritje të IA për qëllime ushtarake. Kjo kulmoi me samitin për IA në

fushën ushtarake, të mbajtur në vitin 2023 në Hagë.[1] Samiti, të cilin Holanda e organizoi në bashkëpunim me Korenë e Jugut, nxori një deklaratë të titulluar "thirrje për veprim" mbi zhvillimin e përgjegjshëm, vendosjen dhe përdorimin e IA në fushën ushtarake. Kjo u miratua nga 57 shtete, duke përfshirë SHBA-në, Britaninë e Madhe, Kinën, Japoninë, Gjermaninë dhe Francën, me përjashtim të Rusisë. Samiti diskutoi aplikimet e përgjithshme ushtarake dhe të mbrojtjes të IA, si dhe sistemet vdekjeprurëse të armëve autonome.

Vendet gjithashtu kanë bërë përparim në inteligjencën artificiale në fushën ushtarake. Në shkurt 2020, Departamenti i Mbrojtjes i SHBA (DoD) u bë departamenti i parë ushtarak në botë që miratoi parimet etike për të gjitha aplikimet e tij ushtarake të IA.[2] Kjo bazohet në Direktivën 3000.09, të krijuar në vitin 2012 dhe të përditësuar në janar 2023, e cila rregullon zhvillimin dhe vënien në terren e sistemeve të armëve autonome dhe gjysmë autonome. Vende të tjera si Britania e Madhe dhe Franca kanë zhvilluar politika kombëtare për IA në fushën ushtarake. Për më tepër, NATO zbuloi strategjinë e saj të parë të inteligjencës artificiale në 2021 për përdorimin e përgjegjshëm të saj në të ardhmen.

Ambiciet e SHBA për t'u bërë një ushtri e fuqizuar nga inteligjenca artificiale

Shtetet e Bashkuara po udhëheqin rrugën në zhvillimin e teknologjisë së inteligjencës artificiale, të nxitura nga ambicia e tyre për t'u bërë një ushtri e fuqizuar nga IA. Në shtator 2018, Pentagoni u zotua të bënte investimin më të madh deri më tani në sistemet e inteligjencës artificiale për armatimin amerikan, duke u angazhuar për të shpenzuar 2 miliardë dollarë gjatë pesë viteve të ardhshme, përmes Agjencisë së saj të Projekteve të Kërkimit të Avancuar të Mbrojtjes (DARPA), për të "zhvilluar valën e ardhshme të teknologjive të IA".[3]

Kohët e fundit, ushtria amerikane kërkoi miliarda dollarë nga ligjvënësit për të përmirësuar aftësitë e saj të IA dhe rrjetëzimit në vitin fiskal 2024, duke synuar të bëhet një forcë më e shkathët dhe e ndërlidhur. Pentagoni synon të përdorë inteligjencën artificiale për përmirësimin e vendimmarrjes dhe për të përmirësuar platformat pa pilot dhe sistemet e tjera.

---

[1] Responsible AI in the Military Domain Summit 2023, Ministry of Foreign Affairs, Government of the Netherlands, January 24, 2024. https://www.government.nl/ministries/ministry-of-foreign-affairs/activiteiten/reaim/

[2] U.S. Department of Defense, DOD Adopts Ethical Principles for Artificial Intelligence, DOD Release, February 24, 2020. https:// www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/

[3] DARPA, AI Next Campaign (Archived), Defense Advanced Research Projects Agency, March 25, 2024. https://www.darpa.mil/work-with-us/ai-next-campaign/

Kërkesa buxhetore e 2024-ës përfshin 1.8 miliardë dollarë për inteligjencën artificiale dhe makineritë të mësuarit (IA/ML) për të ofruar aftësi të përgjegjshme të aktivizuara nga IA dhe për të mbështetur zhvillimin e fuqisë punëtore dhe përpjekjet për menaxhimin e të dhënave. Për më tepër, Departamenti i Mbrojtjes në vitin fiskal 2024 kërkoi 1.4 miliardë dollarë për iniciativat e komandës dhe kontrollit të përbashkët të gjithë domenit (JADC2) për të "transformuar aftësinë luftarake".

CJADC2 - e ardhmja e luftës së përbashkët: Komandimi dhe kontrolli i kombinuar i gjithë domenit (CJADC2) është një koncept luftarak i lidhjes digjitale të forcës së përbashkët në domenet e ajrit, tokës, detit, kibernetikës dhe hapësirës. Ky sistem ka për qëllim të lidhë informacione të përqendruara te të dhënat nga të gjitha degët e shërbimit, partnerët dhe aleatët, në një internet të gjërave ushtarake, duke e bërë informacionin dhe mjetet e fundit të mbështetjes së vendimeve të aksesueshme kudo, në çdo kohë, për vendime të shpejta në fushën e betejës. Interneti i Gjërave Ushtarake (IoMT) është një rrjet sensorësh, pajisjesh që vishen, robotëve, municioneve, armëve, automjeteve dhe pajisjeve IoT që përdorin kompjuterin *cloud* dhe *edge* për të rritur aftësitë dhe sigurinë ushtarake. Departamenti i Mbrojtjes u ka dhënë kontrata katër kompanive teknologjike, *Amazon Web Services, Google, Microsoft* dhe *Oracle*, për të ofruar shërbime në mbështetje të aftësisë së saj të përbashkët luftarake në rrjetet kompjuterike. Portofoli i Pentagonit përfshin më shumë se 800 projekte të paklasifikuara të lidhura me IA, shumë në fazën e testimit.[4]

Në tetor 2023, Presidenti i SHBA-së, Biden, lëshoi një urdhër ekzekutiv për të promovuar miratimin e standardeve të sigurisë së IA, për të shfrytëzuar aftësitë kibernetike të inteligjencës artificiale për ndryshimin e lojës dhe për të zvogëluar potencialin dhe rreziqet që mund të paraqesë. Për të vazhduar me teknologjinë gjithnjë në zhvillim, DoD po miraton këto risi dhe po integron IA në operacione për të «zhvilluar një ushtri më të modernizuar, të drejtuar nga të dhënat dhe të fuqizuar nga IA", për të përparuar në avantazhin e vendimit duke përmirësuar shpejtësinë, cilësinë dhe saktësinë e vendimeve që mund të jenë vendimtare në një luftë.

Strategjia e inteligjencës artificiale 2023: Në fund të vitit 2023, Pentagoni publikoi një strategji të re të të dhënave, analitikës dhe IA, për të përshpejtuar adoptimin e aftësive të IA nga departamenti për të siguruar që luftëtarët amerikanë të ruajnë avantazhin e vendimit në fushën e betejës. Dokumenti ofron një bazë për DoD për të përdorur teknologjinë në zhvillim në vitet në

[4] Frank Bajak, Pentagon's AI initiatives accelerate hard decisions on lethal autonomous weapons, The Associated Press, November 25, 2023. https://apnews.com/article/us-military-ai-projects-0773b4937801e7a0573f44b57a9a5942/

vijim.[5] E zhvilluar nga CDAO, strategjia përshkruan qasjen për përmirësimin e mjedisit organizativ brenda të cilit "udhëheqësit e DoD dhe luftëtarët e luftës do të jenë në gjendje të bëjnë të shpejtë, të mirë informuar duke shfrytëzuar me ekspertizë të dhëna me cilësi të lartë, analitikë të avancuar dhe IA për avantazh të qëndrueshëm të vendimit."[6]

Aleanca AUKUS: SHBA po bashkëpunon gjithashtu me partnerët e saj ndërkombëtarë në fushën e IA. Aleanca AUKUS, e përbërë nga Australia, Mbretëria e Bashkuar dhe Shtetet e Bashkuara, kreu provën e parë të përbashkët të IA dhe autonomisë të mbajtur në MB, në prill 2023. Ky test u pasua nga operacioni i besuar i automjeteve robotike në një mjedis të kontestuar *(Trusted Operation of Robotic Vehicles in a Contested Environment, TORVICE)* prova e kryer në vjeshtën e vitit 2023 në zonën e trajnimit Cultana, Australia e Jugut. Një ekip shkencëtarësh të AUKUS morën pjesë në provat e suksesshme të TORVICE për integrimin e autonomisë së avancuar dhe inteligjencës artificiale (IA) në mjete robotike për operacione ushtarake.[7]

TORVICE kishte për qëllim identifikimin dhe zgjidhjen e dobësive në sistemet autonome në mjediset e kontestuara të luftës elektronike. Automjetet tokësore nga SHBA dhe Britania e Madhe simuluan lëshuesit autonomë me shumë domene dhe kryen misione të ndryshme, duke përfshirë zjarre me saktësi me rreze të gjatë. Ky test tregoi përkushtimin e kombeve të AUKUS ndaj aftësive të avancuara në IA dhe autonomi, duke promovuar sigurinë dhe stabilitetin në rajonin Indo-Paqësor. Për më tepër, partnerët e AUKUS po avancojnë teknologjitë elastike dhe autonome të IA në forcat tokësore dhe detare për mbrojtjen e forcës, shënjestrimin e saktë, inteligjencën, mbikëqyrjen dhe zbulimin, me plane për t'i integruar këto teknologji në programet kombëtare deri në vitin 2025.

Duke besuar se teknologjia me ndikim global kërkon veprim kolektiv, SHBA po angazhohet gjithashtu me vende të tjera për përdorimin e përgjegjshëm ushtarak të aplikacioneve të IA. Zyrtarët e mbrojtjes amerikane planifikojnë të takohen me përfaqësues nga mbi 50 vende deri në mesin e vitit 2025 për të diskutuar një kornizë të sapokrijuar për zhvillimin dhe vendosjen e përgjegjshme të IA dhe teknologjive ushtarake autonome. "Deklarata Politike

[5] Jospeh Clark, DOD Releases AI Adoption Strategy, U.S. Department of Defense News, November 2, 2023. https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/

[6] U.S. Department of Defense, Data, Analytics, and Artificial Intelligence Adoption Strategy, DOD, June 27, 2023. https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/dod_data_analytics_ai_adoption_strategy.pdf

[7] IRIA, AUKUS conducts trials for advanced AI-controlled robotic vehicles, IRIA News, February 7, 2024. https://www.ir-ia.com/news/aukus-conducts-trials-for-advanced-ai-controlled-robotic-vehicles/

për Përdorimin e Përgjegjshëm Ushtarak të Inteligjencës Artificiale dhe Autonomisë", e iniciuar në fillim të vitit 2023, ka marrë miratime nga më shumë se 51 vende. Kjo deklaratë synon të krijojë konsensus ndërkombëtar dhe të ofrojë udhëzime për shtetet në fushën ushtarake të IA, duke nxitur shkëmbimin e praktikave më të mira dhe duke lehtësuar ndërtimin e kapaciteteve midis shteteve miratuese.[8]

Aplikimi i inteligjencës artificiale në ushtri nga Kina

Kina është gjithashtu në ballë, së bashku me Shtetet e Bashkuara, në avancimin e teknologjisë së IA për aplikime ushtarake. Vendi po ndjek në mënyrë agresive aftësitë e IA me ambicie për të udhëhequr botën në IA deri në vitin 2030.[9] Kina ka udhëhequr një rritje globale të investimeve në inteligjencën artificiale gjeneruese (IA) në gjysmën e parë të vitit, me vendin kryesues në numrin e *startup*-eve në sektori për të siguruar financim, sipas një raporti kërkimor të vitit 2023.[10] Në gjysmën e parë të vitit 2023, Kina kishte 22 *startup-e* gjeneruese të IA që morën fonde, të ndjekura nga SHBA me 21 dhe MB me 4, sipas një raporti nga Zhidongxi, një firmë kërkimore kineze e fokusuar në IA.[11]

Pavarësisht se kanë numrin më të madh të bizneseve fillestare gjeneruese të IA që sigurojnë fonde, firmat amerikane morën më shumë fonde totale, tregoi raporti. Firmat kryesore të teknologjisë dhe *startup*-et kineze po përpiqen të mbyllin hendekun me homologët e tyre amerikanë pas lançimit të *ChatGPT* nga *OpenAI* i mbështetur nga *Microsoft* vitin e kaluar. Gjigantët kinezë të teknologjisë duke përfshirë *Tencent Holdings, Baidu* dhe *Alibaba Group* po investojnë shumë në këtë fushë, me fokus në zhvillimin e modeleve të tyre të mëdha gjuhësore *(Large Language Models, LLM).* Kina po zgjeron gjithashtu epërsinë e saj ndaj SHBA-së në paraqitjet e patentave të IA, me institucionet kineze që dorëzojnë 29,853 patenta të lidhura me IA në 2022, krahasuar me një rënie në paraqitjet në SHBA. Tani ajo përbën mbi 40% të

[8] U.S. Department of State, Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, DOS Bureau of Arms Control, Deterrence, and Stability, November 9, 2023. https://www.state.gov/political-declaration-on-responsi-ble-military-use-of-artificial-intelligence-and-autonomy-2/

[9] Rabi Sankar Bosu, China's presence glorifies the AI Safety Summit 2023, CGTN News, November 2, 2023. https://news.cgtn.com/news/2023-11-02/China-s-presence-glorifies-the-AI-Safety-Summit-2023-1ooX4T0Iev6/index.html/

[10] Xinmei Shen, China leads world in number of generative AI start-ups to receive funding in first half of 2023, report finds, South China Morning Post, July 10, 2023. https://www.scmp.com/tech/tech-trends/article/3227197/china-leads-world-number-genera-tive-ai-start-ups-receive-funding-first-half-2023-report-finds/

[11] Global Times, Companies rush to launch LLMs amid global AI frenzy, GT, November 7, 2023. https://www.globaltimes.cn/page/202311/1301370.shtml/

aplikimeve globale për patentë të IA, sipas të dhënave nga Organizata Botërore e Pronësisë Intelektuale e lidhur me OKB-në.[12]

Kina po ndjek në mënyrë aktive supremacinë e IA, duke synuar të bëhet një lider botëror si në aplikimet ekonomike, ashtu edhe në ato ushtarake. Ndoshta ishte e para që hyri në radhët e vendeve të fuqizuara nga IA me lançimin e 'Planit të zhvillimit të inteligjencës artificiale të gjeneratës së re' në 2017, duke paraqitur një plan gjithëpërfshirës për zhvillimin e IA në sektorët privatë dhe publikë. Gjatë viteve, ka fuqizuar investimet në mënyrë aktive në aplikimin e IA në Ushtrinë Çlirimtare Popullore (People's Liberation Army, PLA), me implikime të rëndësishme për dinamikat e sigurisë ndërkombëtare dhe rajonale. Vizioni i udhëheqjes kineze përfshin përdorimin e IA për të forcuar konkurrencën ekonomike dhe aftësitë ushtarake. Qeveria kineze ka zbatuar një qasje të shumanshme që përfshin strategji të ndryshme si: 1) mobilizimin e burimeve për zhvillimin e IA, duke përfshirë investimet financiare dhe iniciativat kërkimore, 2) kultivimin e një fuqie punëtore të kualifikuar në fusha të lidhura me IA përmes programeve arsimore dhe akademike, 3) angazhimin me partnerët dhe institucionet ndërkombëtare për të marrë njohuri dhe ekspertizë në IA përmes bashkëpunimeve, nismave të përbashkëta kërkimore dhe marrëveshjeve të transferimit të teknologjisë.[13]

Në fushën e çështjeve ushtarake, PLA e sheh IA si një forcë transformuese që po riformëson natyrën e luftës. Strategët dhe akademikët e PLA i përshkruajnë tendencat aktuale si lajmëtarë të një revolucioni të ri ushtarak të drejtuar nga IA dhe teknologjitë e lidhura me to. Aplikimi i IA në operacionet ushtarake përfshin një gamë të gjerë aftësish, duke përfshirë:

- **Sistemet inteligjente luftarake pa pilot:** Kina po investon shumë në zhvillimin e automjeteve inteligjente pa pilot, platformave dhe sistemeve të armëve, duke shfrytëzuar IA për të përmirësuar zbulimin, vëzhgimin, komunikimin dhe vlerësimin luftarak të fushëbetejës. Këto sisteme të aktivizuara me IA pritet të prishin paradigmat tradicionale të luftës duke rritur shpejtësinë, saktësinë dhe efektivitetin operacional.
- **Sulmin dhe mbrojtjen me shumë domene:** IA është duke u integruar në aftësitë sulmuese dhe mbrojtëse në fusha të shumta, duke përfshirë ato bërthamore, kibernetike dhe hapësirë. PLA kërkon të përdorë analitikën e të dhënave të mëdha të drejtuara nga IA, mësimin e makinerive dhe

[12] Bloomberg News, China Widens Lead Over US in AI Patents After Beijing Tech Drive, Bloomberg, October 24, 2023. https://www.bloomberg.com/news/articles/2023-10-24/china-widens-lead-over-us-in-ai-patents-after-beijing-tech-drive

[13] Jiayu Zhang, China's Military Employment of Artificial Intelligence and Its Security Implications, The International Affairs Review, August 16, 2020. https://www.iar-gwu.org/print-archive/blog-post-title-four-xgtap/

automatizimin për të rritur ndërgjegjësimin e situatës, mbrojtjen e rrjeteve kritike dhe shkallëzimin e operacioneve sulmuese kibernetike.

- **Trajnimin, simulimin dhe lojën luftarake *(war gaming)*:** Teknologjitë e IA janë duke u përdorur për të përmirësuar sofistikimin e simulimeve ushtarake, lojërave të luftës. Me mundësi të kufizuara për përvojën aktuale luftarake, PLA vendos theks të madh në metodat e trajnimit të bazuara në simulim për të përgatitur komandantët dhe ushtarët për skenarë të ndryshëm operacionalë.

Lufta e Ukrainës - Një terren testimi për inteligjencën artificiale ushtarake

Pushtimi i vazhdueshëm i Rusisë në Ukrainë ka qenë një terren testimi për aplikime të reja. Disa zyrtarë të Pentagonit e shohin atë si një mundësi të vlefshme mësimore për ushtrinë amerikane në lidhje me përdorimin strategjik të dronëve dhe inteligjencës artificiale, veçanërisht të dukshme në rolin e rëndësishëm që luajnë dronët me aftësi gjysmë autonome.

Ndërsa sistemet pa pilot me kosto të ulët janë shfaqur në konfliktet e fundit, duke përfshirë luftën e vitit 2021 midis Armenisë dhe Azerbajxhanit, lufta në Ukrainë ofron një mundësi unike të të mësuarit rreth platformave të aktivizuara me IA. Ndërsa Ukraina integron gjithnjë e më shumë IA në sistemet e saj ushtarake, ka një theks në rritje për të kuptuar natyrën në zhvillim të luftës dhe shfrytëzimin e teknologjisë për avantazhe strategjike. Pentagoni po vëzhgon nga afër përparimet e Ukrainës në IA ndërsa zhvillon algoritmet e veta dhe platformat e aktivizuara me IA, duke njohur ndikimin transformues të teknologjisë në luftën moderne.

Përveç armëve autonome, ka pasur edhe përshtatje të tjera të rëndësishme të teknologjisë së IA. Për shembull, kompania ukrainase e IA *Primer* modifikoi shërbimin e saj komercial të transkriptimit dhe përkthimit të zërit të aktivizuar me IA, në mënyrë që të mund të përpunonte komunikimet e përgjuara ruse dhe të nxjerrë në pah automatikisht informacionin në lidhje me forcat ukrainase. Ukraina ka përdorur gjithashtu softuerin e teknologjisë së njohjes së fytyrës të *startup*-it me bazë në SHBA *Clearview AI* për të identifikuar personelin rus të vdekur përmes profileve të tyre në mediat sociale për të njoftuar të afërmit e tyre dhe për të transferuar trupat e tyre.

Baza e të dhënave *Clearview AI* ndihmoi Ukrainën të identifikonte të vdekurit lehtësisht pa pasur nevojë të përputhen me shenjat e gishtërinjve dhe funksionon edhe nëse ka dëmtime në fytyrë.Me shënjestrimin e drejtuar nga IA duke u bërë e zakonshme në luftë, rëndësia strategjike e teknologjive të IA është ngritur në krye të agjendave globale ushtarake dhe politike.

Aplikimet e inteligjencës artificiale në ushtri (mbrojtje)

Inteligjenca artificiale po revolucionarizon operacionet ushtarake dhe të mbrojtjes në tokë, ajër, hapësirë, det dhe në fushën kibernetike, duke rritur ndërgjegjësimin për situatën, vendimmarrjen dhe efikasitetin operacional. Aplikimet e saj shtrihen nga sistemet autonome të armëve dhe dronët tek analitika parashikuese, nga analiza e inteligjencës te zbulimi, siguria kibernetike dhe logjistika, duke shënuar një epokë të re të luftës së karakterizuar nga teknologjia e përparuar. Disa nga aplikacionet kryesore janë: trajnime dhe simulime; logjistika dhe transporti; mbështetje mjekësore dhe kujdes shëndetësor; siguria kibernetike; sistemet e mbështetjes së vendimeve; sistemet autonome të armëve dhe njohja dhe gjurmimi i objektivit.

- **Trajnime dhe simulime të mbështetura nga Inteligjenca Artificiale**

Integrimi i simulatorëve në stërvitjen ushtarake ka revolucionarizuar gatishmërinë e ushtarëve për luftime. Këta simulatorë ofrojnë një alternativë me kosto efektive, të sigurtë dhe gjithëpërfshirëse ndaj metodave tradicionale, duke ofruar skenarë realistë pa rrezikuar jetën. Teknologjitë e avancuara të IA dhe simulatorët zhytës të realitetit virtual (VR) dhe realitetit të shtuar (AR) janë kritike për t'i mbajtur ushtarët gati dhe për të përmirësuar aftësitë e tyre për një hapësirë beteje që ndryshon vazhdimisht.[14]

Simulatorët e rinj të trajnimit të ushtrisë amerikane, të vendosur për t'u dorëzuar në vitin 2024 e në vijim, do të bëhen një komponent thelbësor i përgatitjeve moderne të luftës. Këto mjete lejojnë ushtarët të koordinojnë helikopterët, tanket dhe këmbësorinë në mënyrë efektive. Testet e fundit treguan aftësitë e pajisjeve, me dronët që koordinojnë sulmet e artilerisë kundër forcave sulmuese, duke demonstruar efektivitetin e tyre në simulimet luftarake. Simulatorët mbulojnë një sërë automjetesh dhe avionësh, duke përfshirë tankun M1 Abrams, helikopterin Black Hawk, helikopterin transportues CH-47 Chinook, dronët RQ-7 Shadow dhe dronin MQ-1C Grey Eagle, duke rritur realizmin e stërvitjes dhe gatishmërinë për misionet e ardhshme.[15]

Lockheed Martin, një nga kontraktorët më të mëdhenj për hapësirën ajrore, sigurinë dhe sistemet e mbështetjes ushtarake, investon shumë në IA për të forcuar aftësitë ushtarake të SHBA. Krijimi i Qendrës së Inteligjencës Artificiale Lockheed (LAIC) tregon përkushtimin e saj ndaj zhvillimit të inteligjencës

[14]Aerospace and Defense Review, Military Simulations: The Power of AI, AR/VR, and Machine Learning, October 9, 2023. https:// www.aerospacedefensereview.com/news/military-simulations-the-power-of-ai-arvr-and-machine-learning-nwid-1389.html/

[15] Sam Skove, Army's new training simulators on track for 2024 delivery, Defense One, July 24, 2023. https://www.defenseone.com/technology/2023/07/armys-new-training-simulators-track-2024-delivery/388797/

artificiale, me iniciativa si fabrika e IA që synojnë shkallëzimin e zbatimit të saj. Kjo fabrikë standardizon mjetet dhe proceset në të gjitha divizionet, duke thjeshtuar aksesin në ML/IA dhe duke lehtësuar kompleksitetin në operacionet e infrastrukturës dhe të mësimit të makinerive. Nëpërmjet nismave si fabrika e IA, firma amerikane e hapësirës ajrore dhe e mbrojtjes Lockheed synon të demokratizojë zhvillimin e IA dhe të sigurojë përputhjen me standardet etike dhe të privatësisë duke nxitur partneritete me kompani inovative si RedHat, Microsoft dhe NVIDIA.[16]

- **Logjistika dhe transporti.**

Përparimet në teknologjitë në zhvillim si dronët autonome, printimi 3D dhe realiteti i përzier kanë revolucionarizuar industri të tëra. Mund të revolucionarizojë gjithashtu logjistikën e mbrojtjes. Inovacioni në logjistikë konsiderohet vendimtar për të penguar agresionin dhe kërcënimet e reja. Logjistika dhe mbështetja janë jetike për efektivitetin, gatishmërinë dhe qëndrueshmërinë ushtarake, duke shërbyer si shtylla kurrizore e fuqisë ushtarake. Duke e njohur këtë, Departamenti i Mbrojtjes po eksploron përdorimin e teknologjive IA/ML për të përmirësuar logjistikën dhe qëndrueshmërinë ushtarake, duke synuar ruajtjen e pajisjeve, uljen e kostove operacionale dhe rritjen e gatishmërisë. IA në logjistikën ushtarake ka potencialin për të rritur efikasitetin dhe aftësitë vendimmarrëse.

Në kontekstin e luftës moderne dhe logjistikës së kontestuar, organizatat e mbrojtjes mund të përdorin IA për të rritur elasticitetin dhe efikasitetin. Integrimi i IA në logjistikën ushtarake ka potencialin për të revolucionarizuar operacionet përmes optimizimit të procesit, automatizimit të detyrave dhe efektivitetit të përmirësuar. Ndërsa siguria kibernetike dhe shqetësimet etike mbeten, njohuri të vlefshme nga përdorimi i gjerë i inteligjencës artificiale të sektorit tregtar në logjistikë mund të informojnë zbatimin e zgjidhjeve të aktivizuara nga IA nga ushtria.

- **Mbështetje mjekësore dhe kujdes shëndetësor.**

Ndërsa IA tashmë po përdoret në teknologjinë e armëve, ajo ka një rol restaurues në mjekësinë ushtarake. Inteligjenca artificiale mund të vendoset nga mjekët ushtarakë për të përshpejtuar procesin e vendimmarrjes në përcaktimin e të plagosurve bazuar në atë se kush ka nevojë për kujdes mjekësor më parë. Inteligjenca artificiale është bërë një mjet gjithnjë e më i fuqishëm për vlerësimin e dhomës së urgjencës, duke ofruar kujdes kritik për personin e duhur në kohën e duhur. Një studim i fundit i publikuar nga

[16] Lockheed Martin News, Accelerating Artificial Intelligence (AI) at Scale, Lockheed Martin, May 05, 2022. https://www.lock-heedmartin.com/en-us/news/features/2022/accelerating-artificial-intelligence-ai-at-scale.html/

nga Kolegji Amerikan i Kirurgëve thekson rolin vendimtar të IA në mbështetjen e specialistëve në klasifikimin e pacientëve pas operacionit për kujdes intensiv. Në spitalin universitar të Brukselit, IA është integruar pa probleme në rrjedhën e përditshme të punës së departamentit të radiologjisë, duke ofruar mbështetje thelbësore në menaxhimin e vëllimeve të mëdha të imazheve. Me potencialin e tij për të lehtësuar barrën në dhomat e urgjencës dhe njësitë e kujdesit intensiv, IA është gati të bëhet më i besueshëm në mbështetjen e mjekëve në vitet e ardhshme.

Inteligjenca artificiale ka një potencial të jashtëzakonshëm për të rritur aftësinë për t'u kujdesur për viktimat luftarake gjatë operacioneve në shkallë të gjerë. Me infrastrukturën bazë të të dhënave në vend, ajo do të lehtësojë zhvillimin e aftësive të ndryshme mjekësore të IA. Përparësi duhet t'i jepet zhvillimit të një algoritmi të cilësisë së lartë të klasifikimit të viktimave masive, për të optimizuar ndikimin e kujdesit mjekësor dhe një strategjie të dedikuar për aftësitë e IA mjekësore për të përmirësuar kujdesin luftarak ndaj viktimave dhe për të zvogëluar rrezikun strategjik për forca e përbashkët.[17]

- **Siguria kibernetike.**

Në një peizazh gjithnjë në ndryshim të kërcënimit kibernetik, IA shfaqet si një mjet i fuqishëm për forcimin e mbrojtjes kibernetike të vendit dhe përpjekjeve ushtarake për sigurinë kibernetike. Duke monitoruar dhe analizuar vazhdimisht trafikun e rrjetit, sistemet e sigurisë kibernetike të fuqizuara nga IA mund të identifikojnë me shpejtësi anomalitë, të zbulojnë kërcënimet e mundshme kibernetike dhe t'u përgjigjen menjëherë atyre.

Ekspertët e industrisë kanë theksuar në mënyrë të përsëritur mundësitë dhe sfidat në rritje në përdorimin e IA për sigurinë kibernetike. Në maj 2023, Eric Horvitz, shefi Shkencor i Microsoft-it, dëshmoi para Komitetit të Shërbimeve të Armatosura të Senatit të SHBA-së për sigurinë kibernetike, duke theksuar rëndësinë në rritje të IA në mbrojtjen kibernetike. Ai theksoi nevojën për investime të rëndësishme në trajnimin e fuqisë punëtore të sigurisë kibernetike, monitorimin, inxhinierinë dhe kërkimin për të kundërshtuar sulmet kibernetike në zhvillim të fuqizuara nga AI.[18] "Metodat e IA janë duke u aplikuar në të gjitha fazat e sigurisë, duke përfshirë parandalimin, zbulimin, hetimin dhe riparimin, zbulimin dhe klasifikimin, inteligjencën e kërcënimeve

[17] Benjamin P. Donham, It's Not Just About the Algorithm: Development of a Joint Medical Artificial Intelligence Capability, Joint Force Quarterly 111, National Defense University Press, October 2023. https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-111/Article/Article/3569597/its-not-just-about-the-algorithm-development-of-a-joint-medical-artificial-inte/

[18] Microsoft Corporate Blogs, Applications for artificial intelligence in Department of Defense cyber missions, Microsoft, May 3, 2022. https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial-intelligence-department-of-defense-cyber-missions/

dhe kërcënimeve dhe trajnimin dhe simulimet e sigurisë", tha ai. Teknologjitë e IA mund të lehtësojnë ngarkesën e punës së ekspertëve të sigurisë kibernetike, duke mundësuar zbulimin, prioritizimin dhe reagimin e automatizuar dhe në shkallë të gjerë. Megjithatë, përparimet në IA ngrenë gjithashtu shqetësime, veçanërisht në lidhje me fabrikimin e falsifikimeve të thella, të cilat përbëjnë kërcënim për sigurinë kombëtare. Në mars të vitit 2022, u shfaq në mediat sociale një video e rreme e presidentit ukrainas Zelenskyy, duke u kërkuar ukrainasve të linin armët dhe të dorëzoheshin në Rusi. Për të adresuar këto dobësi në sistemet e IA, Horvitz rekomandoi sigurimin e zinxhirëve të furnizimit inxhinierik, rritjen e ndërgjegjësimit midis ekipeve të zhvillimit dhe sigurisë kibernetike, si dhe investimin në kërkime mbi sistemet e besueshme dhe të sigurta të IA.

- **Sistemet e mbështetjes së vendimeve.**

Një sistem IA mund të përsërisë proceset e vendimmarrjes njerëzore. Kjo do të thotë se mund të ofrojë mbështetje, të shtojë dhe potencialisht të zëvendësojë vendimmarrjen njerëzore në raste të caktuara. Disa nga aplikimet e tij në fushën e mbrojtjes përfshijnë ndihmën e vendimmarrjes në skenarë konflikti, njohjen e objekteve nga imazhet ose videot, analizën e të dhënave, parashikimin e dështimit të pajisjeve dhe përgjigjet e automatizuara mbrojtëse.

Vendimmarrja ushtarake ndodh në sfera komplekse dhe shpesh kërkon koordinim në të gjitha fushat: tokë, ajër, det, hapësirë dhe hapësirë kibernetike. Inteligjenca artificiale luan një rol vendimtar në përmirësimin e vendimmarrjes duke përpunuar sasi të mëdha të dhënash në mënyrë efektive. Sistemet e IA në ushtri mund të përpunojnë të dhënat në mënyrë më efikase sesa sistemet tradicionale, duke lehtësuar komandimin dhe kontrollin. IA mund të veprojë si një ndihmë e fuqishme për vendimmarrjen njerëzore, duke përmirësuar ndjeshëm sistemet e mbështetjes së vendimeve (DSS) për të përmirësuar vendimmarrjen në ushtri. Sistemet e mbështetjes së vendimeve përkufizohen gjithashtu si "sisteme ndërvepruese të bazuara në kompjuter që ndihmojnë përdoruesit në gjykimin dhe aktivitetet e zgjedhjes". Megjithatë, vendimmarrja duhet të jetë një përpjekje bashkëpunimi midis njerëzve dhe makinerive inteligjente, ku të dyja palët njohin pikat e forta, kufizimet dhe objektivat e njëra-tjetrës.

Përparimet më të fundit në teknologjitë e të dhënave, analitikës dhe inteligjencës artificiale fuqizojnë liderët të marrin vendime më të shpejta dhe më të mira, duke përmirësuar operacionet e mbrojtjes dhe aftësitë luftarake. Përshpejtimi i adoptimit të këtyre teknologjive paraqet një mundësi unike për të pajisur liderët në të gjitha nivelet me të dhënat e nevojshme dhe për të zhbllokuar potencialin e plotë të aftësive vendimmarrëse njerëzore.

• **Sistemet e komandës dhe kontrollit.**

Në sferën dinamike të operacioneve të mbrojtjes, sistemet efikase të komandës dhe kontrollit (C2) janë parësore. Integrimi i IA në sistemet C2 mund të sigurojë analiza të të dhënave në kohë reale, ndërgjegjësim për situatën dhe mbështetje për vendimet për komandantët, duke mundësuar reagime të shpejta ndaj kërcënimeve në zhvillim dhe koordinim më efektiv të forcave. Duke përmirësuar komunikimin dhe duke përmirësuar kohën e reagimit, IA ka potencial transformues në rritjen e efektivitetit të përgjithshëm të operacioneve ushtarake. Një raport kërkimor sugjeroi se "pala që zbaton me sukses IA në sistemin e saj të komandës dhe kontrollit mund të bëhet më e mira dhe më e shpejta në analizimin e informacionit dhe si rezultat mund të marrë vendime më të shpejta dhe të fitojë një avantazh operacional ndaj kundërshtarit të saj."[19]

• **Sistemi autonom i armëve.**

Nuk ka asnjë përkufizim të pranuar ndërkombëtarisht për armët autonome ose vdekjeprurëse, por Departamenti i Mbrojtjes i SHBA-së ofron një të tillë. IA përshkruan një sistem armësh autonome si "një sistem armësh që, pasi të aktivizohet, mund të zgjedhë dhe të përfshijë objektiva pa ndërhyrje të mëtejshme nga një operator". Kjo përfshin, por nuk kufizohet vetëm në sistemet autonome të armëve të mbikëqyrura nga operatori që janë krijuar për të lejuar operatorët të anashkalojnë funksionimin e sistemit të armëve, por mund të zgjedhin dhe angazhojnë objektiva pa të dhëna të mëtejshme të operatorit pas aktivizimit.

Dronët V-BAT: *Shield* AI është një nga *startup*-et e teknologjisë së mbrojtjes që punon me Pentagonin për të transformuar mjetet ushtarake duke përdorur teknologjinë më të fundit. Kompania po ndihmon në avancimin e qëllimit të vendosjes së mjeteve ajrore të fuqishme pa pilot dhe dronëve autonomë. Në dhjetor 2023, *Shield* AI njoftoi zgjerimin e financimit të saj në 500 milionë dollarë, gjë që do të përshpejtojë zhvillimin e pilotëve të inteligjencës artificiale (IA) pa nevojën për operatorë në distancë ose GPS. *Shield* AI është tani *startup*-i i katërt i vlerësuar në gamën e shumë miliardë dollarëve në 20 vitet e fundit, duke iu bashkuar SpaceX, Palantir dhe Anduril.

Piloti i inteligjencës artificiale të *startup*-it, Hivemind, ka fluturuar me një

[19] Johan Schubert, Joel Brynielsson, Mattias Nilsson, Peter Svenmarck, Artificial Intelligence for Decision Support in Command and Control Systems, Department of Decision Support Systems Division of Defence and Security, Systems and Technology, Swedish Defence Research Agency, 23rd International Command and Control Research & Technology Symposium "Multi-Domain C2", 2018. https://www.foi.se/download/18.41db20b3168815026e010/1548412090368/Artificial-intelligence-decision_FOI-S-5904--SE.pdf

avion luftarak (F-16), një dron vertikal të ngritjes dhe uljes (V-BAT) dhe një kuadrokopter (Nova). Ekipet V-BAT i mundësojnë një operatori njerëzor të komandojë së paku katër V-BATS, të gjenerojë shtigje fluturimi të drejtuara nga IA në kohë reale dhe të shfaqë sjellje dinamike leximi dhe reagimi në mënyrë autonome. Në dhjetor 2022, *Shield* AI bëri historinë e aviacionit duke manovruar në mënyrë autonome një F-16 të modifikuar në skenarët e luftimeve ajrore të botës reale, duke hedhur bazat që avionët të pilotohen nga kompjuterët.

- **Njohja dhe gjurmimi i objektivit.**

Sistemet e drejtuara nga IA përmirësojnë saktësinë dhe minimizojnë dëmtimin kolateral duke zbuluar, gjurmuar dhe identifikuar objektivat e mundshëm. Këto sisteme integrojnë të dhëna nga burime të ndryshme për të ofruar ndërgjegjësim gjithëpërfshirës të situatës, duke lejuar analiza të shpejta, vendime në kohë dhe njohuri të zbatueshme. Aftësitë e analizës së imazhit dhe videove të IA mund të revolucionarizojnë identifikimin e objektivit, siç tregohet nga integrimi i një prototipi të njohjes së objektivit të aktivizuar me IA me një tank të Ushtrisë Amerikane M1 Abrams. Ky prototip, i njohur si ATLAS (Advanced Targeting & Lethality Aided System), i ndihmon ushtarët në gjetjen dhe klasifikimin e automjeteve të armikut në mënyrë më efikase.

Një nga detyrat më të vështira në fushën e betejës është parashikimi se ku do të sulmojë armiku më pas. Ky program përdor dronët, IA dhe mësimin e makinerive për të parashikuar sulmet e armikut dhe për të përmirësuar operacionet në fushën e betejës. Dronët identifikojnë sistemet e armatimit të armikut, të tilla si tanket, më pas i kalojnë shikimet e kërcënimeve të identifikuara në IA, të cilat "identifikojnë, klasifikojnë dhe gjeo-lokalizojnë entitetet, pengesat dhe kërcënimet e mundshme, duke gjeneruar një "pamje të përbashkët operative" (COP) të zonës së betejës për ushtarin.[20] Ky COP më pas përpunohet nga një agjent mbështetës vendimesh i aktivizuar nga IA për rekomandime. Kjo qasje dinamike përmirëson ndërveprimin midis sistemeve tokësore dhe ajrore, duke rritur ndërgjegjësimin e situatës dhe aftësitë vendimmarrëse të luftëtarëve në fushën e betejës dhe duke i mbajtur ata më të sigurt dhe më të zgjuar në fushën e betejës.

[20]Patrick Ferraris, Aided Detection on the Future Battlefield, Army Artificial Intelligence Task Force, DVIDS, January 24, 2020. https://www.dvidshub.net/news/360225/aided-detection-future-battlefield/

Përfundime

Inteligjenca artificiale si faktor katalizator për luftën moderne. Inteligjenca artificiale po transformon natyrën e luftës duke rritur automatizimin, efikasitetin dhe aftësinë për të marrë vendime të informuara në kohë reale. Përdorimi i saj në survejim, automatizim të armëve dhe luftë kibernetike po krijon mundësi dhe sfida të reja.

Strategji të reja në epokën digjitale. Strategjitë moderne po përqendrohen gjithnjë e më shumë në integrimin e teknologjive të avancuara, duke përfshirë luftën kibernetike dhe hibridizimin e operacioneve. Kjo ka ndryshuar mënyrën e planifikimit dhe zbatimit të operacioneve ushtarake.

Rritja e kompleksitetit në luftën asimetrike. IA ka fuqizuar forcat joshtetërore dhe aktorët e vegjël, duke rritur rrezikun e sulmeve të sofistikuara nga këta aktorë. Teknologjia është bërë më e arritshme dhe më e përshtatshme për përdorime të qëllimshme keqdashëse.

Rreziqet dhe sfidat e etikës. Automatizimi i vendimmarrjes luftarake dhe përdorimi i armëve autonome ngre sfida të rëndësishme etike. Ekziston nevoja për të siguruar që teknologjitë e IA të përdoren në mënyra që respektojnë normat ndërkombëtare dhe të drejtat njerëzore.

Nevoja për rregullim dhe bashkëpunim ndërkombëtar. Transformimi i luftës nga IA kërkon një qasje kolektive për të shmangur një garë të pakontrolluar armatimi. Marrëveshjet ndërkombëtare dhe dialogu midis shteteve janë thelbësore për të mbrojtur stabilitetin global.

Përmirësimi i sistemeve të mbrojtjes dhe rezistencës. IA mund të kontribuojë në forcimin e mbrojtjes kibernetike dhe mbrojtjes strategjike, duke rritur aftësinë e vendeve për të reaguar ndaj kërcënimeve të avancuara.

Rekomandime

Ndikimi i IA në luftë dhe strategji është një proces në zhvillim që sjell potencial të jashtëzakonshëm për inovacion dhe njëkohësisht krijon sfida serioze për sigurinë globale. Balancimi midis përfitimeve dhe rreziqeve do të përcaktojë se si do të formësohet mjedisi i ardhshëm i sigurisë ndërkombëtare.

Për sa më sipër, rekomandohet që strukturat arsimore të përmirësojnë kurrikulat duke bërë të mundur dhënien e këtij informacioni në të gjitha nivelet e arsimimit.

Literatura e shfrytëzuar:

1. Responsible AI in the Military Domain Summit 2023, Ministry of Foreign Affairs, Government of the Netherlands, January 24, 2024.
2. U.S. Department of Defense, DOD Adopts Ethical Principles for Artificial Intelligence, DOD Release, February 24, 2020.
3. DARPA, AI Next Campaign (Archived), Defense Advanced Research Projects Agency, March 25, 2024.
4. Frank Bajak, *Pentagon's AI initiatives accelerate hard decisions on lethal autonomous weapons*, The Associated Press, November 25, 2023.
5. Joseph Clark, *DOD Releases AI Adoption Strategy*, U.S. Department of Defense News, November 2, 2023.
6. U.S. Department of Defense, Data, Analytics, and Artificial Intelligence Adoption Strategy, DOD, June 27, 2023.
7. IRIA, AUKUS conducts trials for advanced AI-controlled robotic vehicles, IRIA News, February 7, 2024.
8. U.S. Department of State, Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, DOS Bureau of Arms Control, Deterrence, and Stability, November 9, 2023.
9. Rabi Sankar Bosu, *China's presence glorifies the AI Safety Summit 2023*, CGTN News, November 2, 2023.
10. Xinmei Shen, *China leads world in number of generative AI start-ups to receive funding in first half of 2023*, report finds, South China Morning Post, July 10, 2023.
11. Global Times, *Companies rush to launch LLMs amid global AI frenzy*, GT, November 7, 2023.
12. Benjamin P. Donham, *It's Not Just About the Algorithm: Development of a Joint Medical Artificial Intelligence Capability*, Joint Force Quarterly 111, National Defense University Press, October 2023.
13. Patrick Ferraris, *Aided Detection on the Future Battlefield, Army Artificial Intelligence Task Force*, DVIDS, January 24, 2020.

Modernizimi i teknologjisë dhe i burimeve njerëzore, si një proces përditësimi dhe vazhdimësie

Kolonel (R) Dr. Ahmet LEKA
Zëvendësdekan i FMS, AFA

Trajtesë e shkurtuar.

Ky punim sjell në vëmendje të lexuesve domosdoshmërinë e modernizimit të forcave të armatosura në epokën e inteligjencës artificiale dhe luftërave në zhvillim, në mënyrë specifike, procesin e modernizimit të forcave të armatosura amerikane për periudhën 2024-2034, në fushat kryesore të strategjisë së modernizimit si në aspektin teknologjik, ashtu edhe atë njerëzor.

Punimi nuk i bashkohet mendimeve të shumë ekspertëve ushtarakë, që mbështesin supermacinë absolute të UAS dhe armëve të tjera të reja të fushëbetejave të shekullit të 21-të, duke mohuar rolin e faktorit "njeri" në drejtimin e këtyre armëve. Në vitin 2024, modernizimi i ushtrive të NATO-s, sipas raporteve të shumta, pati një financim, përgjegjshmëri dhe rritje të fuqishme të prodhimeve ushtarake. Avancimi drejt sistemeve pa pilot, artileria me rreze të gjatë dhe armët me precizion të lartë, në raport me burimet njerëzore, pritet të rrisin dukshëm aftësinë e ushtrisë për mbajtur objektivat e arritura në fushat e betejës së shekullit të 21-të. Ushtritë kryesisht amerikane, angleze, gjermane dhe të shteteve baltike, si rezultat i rritjes së PPB mbi 2%, i rijetësuan disa nga programet e tyre kryesore në shumë linja të prodhimit të modernizuar.

Për të përballuar sfidat e së ardhmes, NATO dhe aleanca, pjesë e së cilës është

dhe Shqipëria, duhet të investojnë vazhdimisht në zhvillimin e vazhdueshëm të dy shtyllave vendimtare: modernizimit të teknologjisë dhe të burimeve njerëzore, si një proces përditësimi dhe vazhdimësie, për të siguruar dhe forcuar unitetin dhe bashkëpunimin mes shteteve anëtare, duke i mundësuar atyre të qëndrojnë të fortë dhe të koordinuar në një botë gjithnjë e më të pasigurt.

Fjalët kyçe: modernizim i teknologjisë, burimet njerëzore, forcë e armatosur, NATO, konflikt i armatosur, inteligjenca artificiale, sulm kibernetik etj.

Modernizimi në lidhje me konfliktet në zhvillim

Modernizimi i teknologjisë dhe i burimeve njerëzore është një proces i vazhdueshëm dhe i domosdoshëm për çdo organizatë, përfshirë NATO-n. Në një botë që po ndryshon me shpejtësi, këto dy komponentë janë thelbësorë për ruajtjen e efikasitetit dhe gatishmërisë për të përballuar kërcënimet e reja dhe për të mbajtur avantazhin konkurrues.

Teknologjia ka një rol kyç në përmirësimin e aftësive mbrojtëse dhe operacionale, si për shembull, përparimet në inteligjencën artificiale, sisteme të avancuara të mbrojtjes dhe mbikëqyrjes së hapësirës ajrore dhe detare, të cilat kanë ndihmuar NATO-n të reagojë më shpejt dhe më efektivisht ndaj kërcënimeve. Modernizimi i infrastrukturës teknologjike është i nevojshëm për të mundësuar komunikimin e sigurt dhe operacione të koordinuara mes shteteve anëtare, si dhe për të përballuar kërcënimet e reja si sulmet kibernetike dhe manipulimet informative.

Modernizimi i teknologjisë dhe zhvillimi i aftësive teknologjike në raport me konfliktet në zhvillim duhet të jetë një proces dinamik dhe i fokusuar në adaptimin ndaj natyrës gjithnjë e më komplekse të kërcënimeve. Modernizimi dhe zhvillimet teknologjike padyshim në shume raste, përbëjnë mundësi të adaptimit dhe vjedhjes nga shtete armike të patentës teknologjike dhe përdorimit të tyre si kundërvënie në të ardhmen.

Duke iu referuar konflikteve aktuale të zhvilluara në Irak dhe Ukrainë, është konstatuar se kundërshtarët e SHBA-së kanë marrë në zotërim tankun M1 Abrams të ushtrisë dhe automjetin luftarak të blinduar Bradley (BFV). Gjatë konfliktit kundër Shtetit Islamik (IS) në Irak, ushtria irakiane humbi më shumë se 10 tanke M1 Abrams, të cilët ranë në dorë të grupeve të milicisë shiite të lidhura me Iranin, të njohura si Forcat e Mobilizimit Popullor (PMF). Një raport i Inspektorit të Përgjithshëm të vitit 2017 drejtuar Kongresit deklaroi se PMF i mori këto tanke nga ISIS, i bleu këto tanke për në Iran për shfrytëzim dhe spiunazh teknologjik. Spekulime të mëtejshme sugjerojnë se inteligjenca iraniane mund t'i ketë ndarë të paktën një pjesë, të asaj inteligjence teknologjike me shtete që kërcënojnë SHBA si Rusia, Kina dhe Koreja e Veriut.

Në mënyrë të ngjashme, në shkurt 2024, Rusia kapi të paktën një BFV[1] në Ukrainë. Vendndodhja aktuale e kësaj BFV është e panjohur, por duhet supozuar se specialistët e inteligjencës dhe inxhinierisë ruse e kanë shfrytëzuar atë për të mbledhur informacione të dobishme në lidhje me aftësitë, kufizimet dhe mangësitë teknologjike të platformës luftarake. Kur bëhet fjalë për armaturën dhe sistemin kryesor të kontrollit të zjarrit me armë, BFV nuk posedon të njëjtat inovacione teknologjike si tanku M1 Abrams, por gjithsesi kjo rrjedhje e sekreteve teknologjike është shqetësuese për Shtetet e Bashkuara dhe aleatët që i përdorin ende këto sisteme.

Konfliktet e sotme janë shpesh të ndërlikuara, multidimensionale dhe të shpejta, duke përfshirë sulme kibernetike, manipulime informacioni, luftën hibride dhe përdorimin e armëve të reja si inteligjenca artificiale dhe robotika. Për të përballuar këto sfida, zhvillimi i modernizimit dhe përdorimi i teknologjisë duhet të jetë i shpejtë dhe i vazhdueshëm. Ushtria pothuaj në çdo shtet të NATO-s është në procesin e tranzicionit nga një forcë qendrore e luftës tokësore, e përbërë nga brigada dhe divizione, në një forcë të destinuar për të mbrojtur dhe mbështetur forcën e përbashkët dhe partnerët e koalicionit me theks në artileri dhe dron. Në SHBA, shkurtimet e programeve të ushtrisë si FARA[2] dhe ERCA[3] së bashku me eliminimin e forcave tokësore, po e zvogëlojnë aftësinë e Ushtrisë Amerikane për të kapërcyer kërcënimet e luftës tokësore të shekullit të 21-të. Kërkohen forca tokësore më të mëdha në numër dhe më të forta për të përballuar sfidat e paraqitura nga Rusia dhe Kina.

Strategjia e Modernizimit të Ushtrisë Amerikane 2021, AMS[4] e shpallur në shtator 2024, nga Sekretarja e shtetit Christine Wormuth deklaroi se Ushtria po trajton strategjinë e saj të modernizimit në tre afate kohore: (1) këtu dhe tani; (2) për dhjetë vjet 2024-2034; dhe (3) për periudhën përtej 2040. Koncepti i shumëpritur i Luftës për vitin 2040[5] i cili ka qenë në funksion për më shumë se tre vjet, është mënyra kryesore që Ushtria synon të komunikojë se si parashikon organizimin, pajisjen dhe funksionimin në përputhje me AWC për vitin 2040.

Teknologjia duhet të lejojë NATO-n dhe shtetet anëtare të kenë mundësinë të reagojnë në mënyrë të shpejtë dhe të koordinuar ndaj kërcënimeve që mund të shfaqen papritur. Kjo mund të përfshijë sisteme të avancuara për mbikëqyrjen e informacionit dhe inteligjencës, që mund të ofrojnë një pamje të gjerë dhe të detajuar të situatave të mundshme dhe të mundësojnë reagime të mençura

[1] https://battlefield.fandom.com/wiki/Category:Vehicles_of_Battlefield_V
[2] Future Attack Reconnaissance Aircraft
[3] Artileria e topave me rreze të zgjatur
[4] AMS - Army Modernization Strategy
[5] AWC 2040 - Army War Concept.

dhe të saktë. Për shembull, përdorimi i analizës së të dhënave të mëdha (*big data*) dhe algoritmeve të inteligjencës artificiale për parashikimin e sjelljes së kundërshtarëve dhe kërcënimeve të mundshme.

Mbështetje për ***luftën kibernetike*** dhe sigurinë e informacionit në një periudhë kur kërcënimet kibernetike janë bërë një shqetësim i madh për sigurinë ndërkombëtare, modernizimi i teknologjisë duhet të përfshijë ndërtimin e sistemeve të sigurisë kibernetike dhe të mbrojtjes ndaj sulmeve kibernetike. NATO dhe shtetet anëtare duhet të investojnë në mbrojtjen e infrastrukturës kritike, në përforcimin e kapaciteteve për luftë kibernetike dhe në zhvillimin e metodologjive për mbrojtjen e informacionit të ndjeshëm nga manipulimet dhe sulmet e jashtme. Në konfliktet moderne, NATO përballet gjithnjë e më shumë me luftëra hibride, ku aktorë të ndryshëm mund të përdorin një gamë të gjerë taktikash – nga lufta tradicionale ushtarake deri tek operacionet e informacionit, sulmet kibernetike dhe përdorimi i grupeve të armatosura të huaja. Modernizimi i teknologjisë duhet të përfshijë zhvillimin e sistemeve të përshtatshme për këtë lloj luftë, ku përfshihen kapacitetet e reja për menaxhimin e informacionit, ndihmën me manovra të shpejta dhe operacione të koordinuara, si dhe mbështetje për ushtritë për të ndihmuar në parandalimin e eskalimit të tensioneve dhe përdorimin e forcës së tepruar.

Në këtë pikëpamje, **integrimi i teknologjive të reja si robotika dhe inteligjenca artificiale, n**ë konfliktet e zhvilluara, përdorimi i teknologjive të reja si dronët, robotët luftarakë dhe inteligjenca artificiale do të bëhet gjithnjë e më i zakonshëm. NATO duhet të zhvillojë dhe modernizojë këto teknologji për të siguruar avantazhin në fushën e betejës dhe për të zvogëluar rrezikun për trupat ushtarake. Përdorimi i dronëve për mbikëqyrje, grumbullimin e inteligjencës dhe madje edhe për sulme kirurgjikale do të jetë një aspekt kyç i operacioneve ushtarake të ardhshme.

Teknologjitë e zhvilluara për mbrojtje dhe siguri duhet të jenë të integruara me sistemet e partnerëve të NATO-s dhe organizatave të tjera ndërkombëtare për të siguruar një reagim të koordinuar dhe të shpejtë ndaj kërcënimeve. Ky bashkëpunim mund të përfshijë ndarjen e informacionit, zhvillimin e standardeve të përbashkëta për teknologjitë dhe trajnimin e forcave të sigurisë për të operuar në një mjedis shumëkombësh.

Në aspektin e modernizimit, trajnimi dhe zhvillimi i burimeve njerëzore luajnë një rol të rëndësishëm për të mbështetur përdorimin e teknologjive të reja. Për këtë, NATO dhe forcat e armatosura të vendeve anëtare duhet të investojnë në trajnimin dhe edukimin e personelit të tyre për të kuptuar dhe për të operuar teknologjitë e fundit. Kjo përfshin jo vetëm aftësitë teknike, por edhe aftësinë për të menaxhuar dhe përdorur informacionin në një mënyrë etike dhe të sigurt.

Përdorimi i teknologjisë së avancuar, sidomos kur përdoret në konflikte të zhvilluara, duhet të jetë në përputhje me normat ndërkombëtare dhe të drejtat e njeriut. NATO duhet të sigurojë që përdorimi i teknologjive të reja të mos shkelë ligjet ndërkombëtare, siç janë konventat e Gjenevës dhe të drejtat e individëve, duke i dhënë përparësi mbrojtjes së civilëve dhe parandalimit të abuzimeve.

Modernizimi i komponentit tokësor, bazuar në dron dhe artileri

Në konfliktet moderne, NATO përballet gjithnjë e më shumë me luftëra hibride, ku aktorë të ndryshëm mund të përdorin një gamë të gjerë taktikash – nga lufta tradicionale ushtarake deri tek operacionet e informacionit, sulmet kibernetike dhe përdorimi i grupeve të armatosura të huaja. Modernizimi i teknologjisë duhet të përfshijë zhvillimin e sistemeve të përshtatshme për këtë lloj luftë, ku përfshihen kapacitetet e reja për menaxhimin e informacionit, ndihmën me manovra të shpejta dhe operacione të koordinuara, si dhe mbështetje për ushtritë për të ndihmuar në parandalimin e eskalimit të tensioneve dhe përdorimin e forcës së tepruar.

Modernizimi i forcave tokësore duke u bazuar në përdorimin e dronëve dhe artilerisë përbën një hap të rëndësishëm në adaptimin ndaj kërkesave të konflikteve moderne dhe ndihmon në përmirësimin e efikasitetit të operacioneve ushtarake. Këto teknologji të reja ofrojnë avantazhe të shumta për forcat tokësore, duke i mundësuar atyre të veprojnë me shpejtësi, precizitet dhe fleksibilitet më të madh. Duke marrë ndoshta mësimet e gabuara nga lufta në vazhdim Ruso-Ukrainase, koncepti i përdorimit në mënyrë të kombinuar, i zjarreve me rreze të gjatë, dronëve dhe një vëzhgim që lidh mbikëqyrjen e fushëbetejës, përcaktimin e objektivave dhe shpërndarjen e municioneve janë shkopi magjik që sjell fitoren në fushën e betejës. Tanket, këmbësoria dhe forcat e tjera luftarake të afërta që luftojnë përgjatë vijave të frontit janë një relike e së kaluarës. Sot, ato mund të zëvendësohen nga UAS me katërkopter me granata duke mbështetur zjarre me rreze të gjatë dhe pa dëmtuar efektivin. Ky ndryshim në strukturën e forcës nuk ka ardhur brenda natës. Në konfliktet e zhvilluara, përdorimi i teknologjive të reja si dronët, robotët luftarakë dhe inteligjenca artificiale do të bëhet gjithnjë e më i zakonshëm. NATO duhet të zhvillojë dhe modernizojë këto teknologji për të siguruar avantazhin në fushën e betejës dhe për të zvogëluar rrezikun për trupat ushtarake. Përdorimi i dronëve për mbikëqyrje, grumbullimin e inteligjencës dhe madje edhe për sulme kirurgjikale do të jetë një aspekt kyç i operacioneve ushtarake të ardhshme.

Që prej vitit 2021, ushtria amerikane ka pasur disa zhvillime strukturore në nivelin e divizioneve për të ardhur drejt konceptit të ri të zhvillimit të forcës 2030, i cili parashikon ndryshimet kryesore strukturore thelbësore. Në të

ardhmen gjithmonë dhe me shumë teknologjitë e zhvilluara për mbrojtje dhe siguri duhet të jenë të integruara me sistemet e partnerëve të NATO-s dhe organizatave të tjera ndërkombëtare për të siguruar një reagim të koordinuar dhe të shpejtë ndaj kërcënimeve. Ky bashkëpunim mund të përfshijë ndarjen e informacionit, zhvillimin e standardeve të përbashkëta për teknologjitë dhe trajnimin e forcave të sigurisë për të operuar në një mjedis shumëkombësh. Në shkurt 2024, ushtria amerikane publikoi një letër të bardhë mbi ndryshimet e ardhshme të strukturës së forcave. Siç vë në dukje letra e bardhë, ushtria do të çaktivizojë të gjitha divizionet e blinduara me përjashtim të një prej BCT[6]-ve të saj Stryker (SBCT)[7] dhe të gjitha skuadroneve të saj. Deri në korrik 2024, ushtria kishte çaktivizuar tashmë shumicën e këtyre formacioneve.

Në fund të korrikut 2024, Mary Shinn nga "*The Gazeta Kolorado Springs"* raportoi se Ushtria përdori heqjen e inxhinierëve të nivelit të brigadës dhe konsolidimin e aftësive inxhinierike në nivelin e divizionit, duke i lejuar ushtrisë të krijojë personel të lirë duke reduktuar numrin e saj të inxhinierëve. Kjo çoi jo vetëm në shkatërrimin e strukturës së forcës së nevojshme për të realizuar misionin e depërtimit, por u siguroi gjithashtu brigadave të blinduara dhe të motorizuara mjetet e përgjithshme të lëvizshmërisë, kundër-lëvizshmërisë dhe mbijetesës që u nevojiten për të ekzistuar në operacionet luftarake në shkallë të gjerë kundër konkurrentëve të tjerë. Këto teknologji të reja ofrojnë avantazhe të shumta për forcat tokësore, duke i mundësuar atyre të veprojnë me shpejtësi, saktësi dhe fleksibilitet më të madh. Task forca me shumë domene, ose MDTF[8], është vendi ku do të jetë pjesa më e madhe e rritjes së ardhshme të ushtrisë. Projektuar për të rritur thellësinë dhe shkallën në të cilën forcat e ushtrisë mund të *mbrojnë* forcat e përbashkëta dhe të koalicionit, të kryejnë mbledhjen dhe sinkronizimin e inteligjencës, të japin hapësirë jo-kinetike dhe efekte kibernetike për të formësuar operacionet dhe të hapin zjarre me rreze të gjatë në *mbështetje* të manovrës së përbashkët të forcave.

Zhvillimi i konceptit *multi domain* ka lehtësuar lëvizjen e Ushtrisë për të zëvendësuar formacionet e zbulimit të armëve të kombinuara, të tilla si artileria me UAS dhe lloje të tjera me sensorë. Një ide e ngjashme u tentua në mesin e viteve 2000. Ushtria eliminoi Regjimentet e Blinduara të cilat në atë kohë ishin shumë të rënda, shumë të shtrenjta dhe vdekjeprurëse për periudhën e shkurtër në të cilën u gjend ushtria. Në vend të tyre, ushtria amerikane rikonfiguroi tre brigada të inteligjencës ushtarake në brigada të mbikëqyrjes së fushëbetejës, me një kosto më të ulët.

[6] https://www.peogcs.army.mil/Project-Offices/PM-Stryker-Brigade-Combat-Team-SBCT/
[7] https://www.moore.army.mil/MCoE/MCDID/ACM-SBCT/
[8] Multi Domain Task Force

Jen Judson[9] raporton se plani që ushtria është duke u riorganizuar dhe riafirmuar në disa nga njësitë përbërëse të MDTF, është në rrugën e duhur. Lidhur me këtë, gjatë vitit 2025, mund të pritet të shihet një MDTF e aktivizuar në Gjermani, me disa nga njësitë e tij vartëse të vendosura në Fort Drum, Nju Jork. Raportimi i Judson mbështet ndryshimet e strukturës së forcës të shpallura nga ushtria amerikane më 27 shkurt 2024 në një letër të bardhë të botuar dhe titulluar "*Transformimi i Strukturës së Forcave të Ushtrisë"*.

Përdorimi i dronëve në Forcat Tokësore kanë një ndikim të madh në forcimin e aftësive të forcave tokësore, pasi mund të ofrojnë mbikëqyrje në kohë reale dhe të mundësojnë reagime të shpejta ndaj kërcënimeve. Dronët mund të sigurojnë mbikëqyrje dhe inteligjencë të vazhdueshme në monitorimin e terrenit, duke identifikuar kërcënime të mundshme, si lëvizjet e armikut, pozicionet e tij, dhe veprime të tjera që mund të rrezikojnë operacionet tokësore. Kjo mund të ndihmojë në marrjen e vendimeve të shpejta dhe të informuara. Ato mund të përdoren për sulme të precizuara ndaj objektivave të vogla ose të shpërndara, si dhe për shkatërrimin e objektivave të rëndësishme strategjike. Për shembull, dronët mund të sulmojnë me municione të vogla, duke eliminuar nevojën për ndërhyrje të fuqishme dhe duke minimizuar dëmet e mundshme ndaj forcave të tjera. Gjithashtu përdorimi i dronëve mund te gjeje vend për transportin e furnizimeve të vogla, si municione, mjekësi ose pajisje të tjera, duke mundësuar mbështetje më të shpejtë dhe më të sigurt në zona të vështira për t'u arritur.

Artileria e avancuar përbën një aspekt tjetër të modernizimit në zhvillimin e **konflikteve.** Modernizimi i artilerisë ka të bëjë me rritjen e saktësisë, shpejtësisë dhe mundësisë për të vepruar në mënyrë më fleksibël në terrenet e ndryshme. Artileria Vetëlëvizëse dhe Sistemet e Gjurmimit të Taktikave të Reja si auto-barrikadat me raketa dhe topa të shpejtë, mund të përdoren për të ofruar mbështetje të shpejtë dhe të fuqishme për forcat tokësore. Ato mund të kalibrohen për të goditur me saktësi objektiva të caktuara dhe për të shpërndarë armët me shpejtësi të lartë në zona të largëta. Sistemet e Artilerisë të Drejtuara me GPS ose sisteme të tjera të mundësuara nga teknologjia moderne siguron që predhat të godasin me saktësi të lartë, duke minimizuar humbjet kolaterale dhe duke maksimizuar ndikimin ndaj armikut.

Integrimi i Dronëve me Sistemet e Artilerisë bëhet duke përdorur informacionin e marrë nga dronët për të udhëzuar goditjet e artilerisë në kohë reale. Kjo bashkëpunim mund të ofrojë një nivel të ri efikasiteti në sulmet e shpejta dhe precize. Çfarë përfitimesh kemi nga **kombinimi i dronëve dhe artilerisë?** Kombinimi i tyre arrin të krijojë një kapacitet të fuqishëm operativ, duke i

[9] https://www.defensenews.com/author/jen-judson/

mundësuar forcave tokësore të përfitojnë avantazhet e të dyja teknologjive, disa prej të cilave janë: ***së pari,*** sulme të koordinuara dhe të shpejta, ku dronët mund të ofrojnë informacion dhe mbikëqyrje të drejtpërdrejtë, duke mundësuar që artileria të bëjë goditje të precizuara me saktësi, duke i mundësuar forcave tokësore të veprojnë më shpejt dhe të jenë më efektive në përballje me kërcënimet; ***së dyti,*** zvogëlimi të rrezikut për trupat tokësore, nëpërmjet përdorimit të dronëve për mbikëqyrje dhe sulme të drejtuara dhe artilerisë për goditje të largëta ndihmon në zvogëlimin e rrezikut për trupat e forcave tokësore. Kjo është veçanërisht e rëndësishme në mjedise të pasigurta ose të vështira, ku përfshirja direkte e trupave mund të jetë shumë e rrezikshme; ***së treti,*** fleksibilitet dhe adaptim, nëpërmjet kombinimit të këtyre teknologjive ato mundësojë që forcat tokësore të adaptohen më shpejt ndaj ndryshimeve të situatës. Dronët mund të sigurojnë informacion të përditësuar në kohë reale, ndërsa artileria mund të reagojë menjëherë për të ndihmuar forcën tokësore të realizojë objektivat e saj.

Megjithëse këto teknologji ofrojnë mundësi të mëdha, ka disa sfida që kërkojnë përpjekje të mëtejshme për t'u zhvilluar dhe për t'u integruar në mënyrë efektive, të cilat lidhen me:

Sigurinë dhe Mbrojtjen Kibernetike: Si dronët, ashtu edhe sistemet e artilerisë moderne janë të ndjeshme ndaj sulmeve kibernetike, kështu që siguria e teknologjive është thelbësore për të parandaluar manipulime dhe përdorim të paligjshëm.

Koordinimin dhe Integrimin e Sistemeve: Integrimi i dronëve dhe artilerisë kërkon sisteme të avancuara të komandës dhe kontrollit që mund të menaxhojnë dhe koordinojnë operacionet midis këtyre dy komponentëve, si dhe me forcat e tjera.

Koston dhe Mbështetjen Logjistike: Përdorimi i dronëve dhe artilerisë moderne kërkon investime të konsiderueshme në zhvillimin, mbajtjen dhe operimin e sistemeve të avancuara, duke përfshirë trajnimin e personelit dhe mbështetje logjistike për t'u siguruar që këto teknologji të funksionojnë në mënyrë të qëndrueshme dhe efikase.

Modernizimi duhet të guxojë të dalë përtej programeve dhe strategjive ekzistuese

Strategjia e modernizimit të forcave të armatosura AMS 2021 përdor modelin standard të strategjisë *ends-ways-mess*[10] për të përshkruar planin e tij për modernizimin. Qëllimi i saj është të gjenerojë një ushtri të modernizuar që

[10]https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3762221_code880750.pdf?abstractid=3762221&mirid=1

është e aftë të drejtojë MDO si pjesë e forcës së përbashkët brenda një teatri të vetëm deri në vitin 2028. Për më tepër, AMS kërkon të gjenerojë një ushtri që është e aftë të drejtojë MDO nëpër teatro të shumtë nga 2035. Mjetet ose burimet që posedon ushtria për të përmbushur këtë qëllim janë: (1) një ndërmarrje e riorganizuar e modernizimit të ushtrisë, (2) burimet me prioritet dhe (3) reagimet operacionale. Mënyrat me të cilat ushtria kërkon të përdorë mjetet e saj për të arritur këto qëllime janë gjithashtu të trefishta: fokusimi në (1) "Si luftojmë", (2) "Me çfarë luftojmë" dhe (3) "Kush jemi ne". *"Si luftojmë",* përbëhet nga konceptet, doktrina, organizatat dhe trajnimet që i nevojiten ushtrisë për të përmbushur gjendjen përfundimtare të synuar të AMS. Për më tepër, *"Me çfarë luftojmë"* janë zgjidhjet materiale që i nevojiten ushtrisë për të përmbushur gjendjen përfundimtare të AMS-së. Këto janë gjashtë prioritetet e modernizimit që kemi diskutuar më parë. Së fundi, *"Kush jemi ne"*, përshkruan zhvillimin e liderit dhe fushat e menaxhimit të talenteve që ushtria duhet të llogarisë për të ndihmuar dy mënyrat e tjera për të përmbushur gjendjen përfundimtare të AMS.

Duke marrë parasysh rëndësinë e MDO-së në ndjenjat e AMS dhe *Army Multi-Domain Transformation,* ia vlen të shqyrtohet koncepti. Manuali në terren, 3-0, *Operacionet,* përcakton MDO si "*Përdorimi i kombinuar i armëve të aftësive të përbashkëta dhe të ushtrisë për të krijuar dhe shfrytëzuar avantazhe relative që arrijnë objektivat, mposhtin forcat armike dhe konsolidojnë fitimet në emër të komandantëve të forcave të përbashkëta*". Koncepti MDO i përshkruar në *Operacionet* kërcen rreth kërkesave aktuale të Ushtrisë në luftimet tokësore me iluzione magjepsëse për sinkronizimin e aftësive të përbashkëta, hapësinore dhe kibernetike, krijimin e avantazheve, marrjen e iniciativës dhe marrjen e avantazheve relative. Pavarësisht gjuhës verbuese, MDO flet pak për logjikën e luftërave tokësore, aq më pak kërkesat e forcave tokësore që janë të ngarkuara për të bërë luftë tokësore. Në fakt, MDO është mënyra se si ushtria mbështet forcën e përbashkët dhe modernizimi kërkon t'i mundësojë ushtrisë të angazhohet në MDO për të force të përbashkët.

Për më tepër, "Si luftojmë" e AMS-së duhet të ofrojë një pasqyrë të logjikës së luftës tokësore dhe, brenda luftërave tokësore, gjërat që forcat tokësore do të thirren të bëjnë. Megjithatë, "Si luftojmë" në vend të kësaj tregon konceptet dhe doktrinën e ushtrisë, të cilat të dyja janë dokumente aspirative. Problemi me karakterin aspirativ të koncepteve dhe doktrinës së ushtrisë është se ato përshkruajnë lirshëm se si ushtria *dëshiron* të luftojë, jo se si do të *duhet* të luftojë në mënyrë të pashmangshme.

Pavarësisht nëse ushtrisë i kërkohet të luftojë në Evropën Lindore kundër Rusisë, ose nëse dërgohet përtej Oqeanit Paqësor për të ndihmuar në garantimin e sovranitetit kombëtar dhe territorial të Tajvanit, ajo duhet të

luftojë për kontroll dhe të luftojë për të mbajtur kontrollin e territorit. Kjo, në thelb, është logjika e luftës tokësore: ushtritë ekzistojnë për të luftuar forcat e tjera ushtarake (shtetërore dhe joshtetërore) për kontrollin e territorit. Kontrolli kërkon forca tokësore që nuk arrijnë kulmin në procesin e dhënies së fitoreve taktike dhe operacionale. Këto forca duhet të jenë mjaft të fuqishme dhe duhet të kenë thellësinë e tepricës për të përballuar ashpërsinë e luftimit sipas kontrollit - dhe megjithatë të ruajnë kapacitetin për të ndjekur dhe mposhtur një armik ose për të mbrojtur kundër një kundërsulmi.

Megjithatë, logjika e luftës tokësore qëndron në veprimet për të kontrolluar territorin, qoftë për qëllimet e tyre apo në mbështetje të objektivave të forcave të përbashkëta, për të ndihmuar në drejtimin e modernizimit. Strategjia e modernizimit duhet të llogarisë gjithashtu aktivitetet që çdo ushtri duhet të bëjë në mënyrë të përsëritur në çdo luftë tokësore - qoftë në Evropën Lindore, në Paqësor apo edhe në Lindjen e Mesme. Ushtritë, duke përfshirë ushtrinë amerikane, duhet të jenë (1) të afta të marrin dhe rimarrin territorin, jo vetëm në mbështetje të kërkesave të forcave të përbashkëta, por si qëllim në vetvete, (2) të afta të pastrojnë (d.m.th., të heqin ose eliminojnë sistematikisht) forcat armike nga territori i kontestuar, (3) të afta për të mbajtur territorin kundër përpjekjeve të armikut për të rimarrë atë tokë, (4) të afta për të mbrojtur popullatat, (5) të afta për të rrethuar forcat armiqësore për të lehtësuar shkatërrimin e tyre ose për t'i vënë ato në një pozicion për të negociuar një dorëzim dhe (6) të afta për të mbyllur kufijtë kundër forcave armiqësore. Ushtrisë do t'i shërbente mirë të bënte një hap prapa dhe të vlerësonte strategjinë e saj të modernizimit kundrejt këtyre kërkesave; UAS dhe pika qendrore e modernizimit të zjarreve me rreze të gjatë nuk pasqyrojnë fitoret dhe humbjet e konfliktit të armatosur të shekullit të 21-të në të gjithë globin. Për më tepër, UAS dhe qasja e zjarrit me rreze të gjatë nuk mposht një kundërshtar në lidhje me logjikën e luftës tokësore, dhe as nuk është një strategji që e vendos ushtrinë në një bazë më të afërt me fitoren pasi lidhet me logjikën e luftës tokësore.

Lufta për kontrollin e territorit nuk është një këndvështrim i përqendruar te ushtria; përkundrazi, është një pozicion që konsideron njësoj forcën e përbashkët dhe nevojat e saj. Forca e përbashkët nuk mund (aq lehtë) të përdorë fushat ajrore, të ndërtojë fuqi luftarake në fushat e betejës ekspeditare, të mbrojë portet ose të përmbushë shumë kërkesa të tjera pa një ushtri që mund të mposht forcat e tjera tokësore dhe të kontrollojë territorin. Përpjekjet për modernizimin e ushtrisë duhet, rrjedhimisht, të lidhen me logjikën e luftës tokësore. Proceset e modernizimit dhe zhvillimi i teknologjisë në ushtrinë amerikane janë një udhërrëfyes dhe shembull konkret edhe për ushtritë e tjera të NATO-s, ku Shqipëria, si anëtare e saj, duhet të adaptojë dhe zhvillojë koncepte në fushën e modernizimit, e zhvillimit teknologjik dhe strukturor dhe në aspektin e përdorimit operacional të forcës.

Disa përfundime

Për të arritur sukses dhe rritje të qëndrueshme, modernizimi i proceseve dhe përdorimi i teknologjive të reja është thelbësor. Teknologjia ndihmon në përmirësimin e efikasitetit, shpejtësisë dhe cilësisë së punës, duke mundësuar që organizatat të konkurrojnë në një treg global në zhvillim.

Modernizimi, teknologjia dhe burimet njerëzore janë të ndërvarura dhe të nevojshme për një zhvillim të qëndrueshëm dhe progres. Pa këto elemente, organizatat dhe shoqëritë do të hasin vështirësi në përshtatjen dhe konkurrimin në një mjedis gjithnjë e më dinamik dhe të globalizuar.

Modernizimi i teknologjisë dhe zhvillimi i burimeve njerëzore duhet të jenë të sinkronizuar dhe të fokusuar në përballimin e kompleksitetit të konflikteve moderne. Kjo do të mundësojë që NATO dhe shtetet anëtare të mbajnë një avantazh strategjik dhe të jenë të gatshme për t'u përballur me kërcënime të ndryshme dhe të papritura.

Modernizimi i forcave tokësore përmes përdorimit të dronëve dhe artilerisë përfaqëson një hap të rëndësishëm për të rritur efikasitetin dhe fleksibilitetin në operacionet ushtarake. Dronët ofrojnë mundësi të jashtëzakonshme për mbikëqyrje dhe goditje precize, ndërsa artileria moderne ofron mbështetje të fuqishme dhe të shpejtë. Përdorimi i këtyre teknologjive të avancuara mund të transformojë mënyrën se si forcat tokësore operojnë dhe të sigurojë avantazhe strategjike në konfliktet e së ardhmes.

Teknologjia dhe modernizimi nuk janë të suksesshëm pa investime të rëndësishme në burimet njerëzore. Trajnimi dhe zhvillimi i aftësive të punonjësve janë thelbësore për përdorimin efektiv të teknologjisë dhe për të siguruar që individët të jenë të gatshëm të adoptojnë risitë dhe ndryshimet që sjell modernizimi.

Ndërsa teknologjia përparon, trajnimi dhe përgatitja e personelit ushtarak për t'u njohur dhe për t'u përshtatur me teknologjitë e reja është një sfidë e vazhdueshme. Teknologjitë e avancuara kërkojnë një nivel të lartë të aftësive teknike dhe adaptimi të shpejtë.

Akademia e Forcave të Armatosura, si një institucion i Arsimit të Lartë, duhet të luajë rolin kryesor në paraprirjen e procesit të modernizimit, zhvillimit teknologjik dhe inovacionit. Ajo duhet të përshtatë në vijimësi programe të mësimit dhe të trajnimit që integrojnë teknologjitë e reja, si dhe të përgatitë burime njerëzore për të mbështetur këtë zhvillim.

Literatura e shfrytëzuar

1. *Strategjia e Modernizimit të Ushtrisë: Investimi në të Ardhmen* (Shtypshkronja e Qeverisë së SHBA, 2021).
2. "Modernizimi i ushtrisë: E nderuara Christine Wormuth", Konferenca e 8-të Vjetore e Lajmeve të Mbrojtjes, 4 shtator 2024, https://www.defensenews.com/video/2024/09/04/army-modernization-the-hon-christine-krimbi/
3. "Ushtria merr një pamje të zgjeruar deri në vitin 2040", Shoqata Ndërkombëtare e Forcave të Armatosura të Komunikimit dhe Elektronikës, 10 tetor 2022, https://www.afcea.org/signal-media/army-takes-extended-view-2040/
4. "Ushtria e bën Rrjetin e Bashkuar një Prioritet Kryesor", Mbrojtja Kombëtare, 20 tetor 2023, https://www.nationaldefensemagazine.org/articles/2023/10/20/army-makes-unified-network-a-top- prioritet/
5. Matthew Olay, *Sinjalet e eksperimentit premtues për integrimin e ardhshëm të teknologjisë së avancuar në njësitë e ushtrisë*, DOD News, 22 mars 2024, https://www.defense.gov/News/News-Stories/Article/Article/3716688/promising-experiment-signals-future-integration-of-advanced-tech-into-army-units/
6. John Deni & Lisa Aronsson, *Roli i Aleatëve Evropianë të Amerikës në Luftën Ruso-Ukrainase*, 2022–2024 (Kolegji i Luftës së Ushtrisë Amerikane, 2024), 97–98; "Eric Edelman dhe Thomas Mahnken mbi krizën e strategjisë së mbrojtjes së Amerikës", School of War (podcast), 24 shtator 2024, https://podcasts.apple.com/us/podcast/ep-146-eric-edelman-and-thomas-mahnken-on-americas/id1589160645?i=1000670516245.
7. Strategjia e Zhvillimit të Akademisë së Forcave të Armatosura 2023-2032.
8. Strategjia Kombëtare për Kërkimin Shkencor, Teknologjinë dhe Inovacionin 2023-2030.
9. Andrew Feickert, *Forca e Synimit të Ushtrisë dhe Iniciativat e Strukturës së Forcave të Ushtrisë 2030*, Shërbimi i Kërkimeve të Kongresit, IF11542 (janar 2022): 2.
10. Jennifer Bocanegra, *Divizioni i 1-rë i kalorësisë riaktivizon skuadrën e kalorësisë së divizionit*, Shërbimi i Lajmeve të Armatës, 8 mars 2023.
11. "Transformimi i Strukturës së Forcave të Ushtrisë", Letër e Bardhë, Departamenti i Ushtrisë, 27 shkurt 2024. https://api.army.mil/e2/c/downloads/2024/02/27/091989c9/army-white-letër-ushtri-forcë-

strukturë-transformim.pdf.

12. Mary Shinn, *Fort Carson duke u thënë lamtumirë 2 skuadroneve të kalorësisë, duke përfshirë njësinë që luftoi në ditën historike në Afganistan*, Gazeta, 29 korrik 2024.

13. Jen Judson, *Ushtria amerikane synon të kompletojë strukturën e Task Forcës me shumë fusha deri në FY28,* Defense News, 18 prill 2024, https:// www.defensenews.com/land/2024/04/18/us-army-aims -to-complete-multidomain-task-force-structure-by-fy28/

14. *Për ngritjen vertikale të ardhshme, shtylla kurrizore digjitale e FLRAA do të mbështesë gjithashtu FARA,*" Breaking Defense, 4 janar 2024, https:// breakingdefense.com/2024/01/for-future-vertical-lift-flraas-digital-backbone -do-gjithashtu-nën-fara/

15. Amos Fox, *Aviacioni i ushtrisë dhe vendosmëria në bregdetin ajror-tokësor*, Shoqata e Ushtrisë së Shteteve të Bashkuara, Dokumenti i Luftës Tokësore 163, gusht 2024, 2.

16. Ashely Roque, *Ushtria zgjedh 2 UAS " të atribuar " për rikonstruksionin, mbikëqyrjen dhe blerjen e objektivave në nivel kompanie*, Breaking Defense, 11 shtator 2024, https://breakingdefense.com/2024/09/army-selects-tëo-attritable-uass-for-company-level-recon-surveillance-and-target-acquisition/

17. Jon Harper, *Shef i Shtabit të Ushtrisë: Ne nuk kemi nevojë për një degë drone*, Scoop i Mbrojtjes, 21 maj 2024, https://defensescoop.com/2024/05/21/ army-chief-randy-george -nuk-duhet-dega-drone/; Daniel Gettinger dhe Andrew Freikert, "Propozimi për të krijuar një korpus drone të ushtrisë amerikane», Shërbimi i Kërkimit të Kongresit, IN12382, 18 qershor 2024, https://crsreports.congress.gov/product/pdf/IN/IN12382.

18. "Tryeza e Rrumbullakët e Mediave mbi Aviacionin Stand-Up", Shërbimi i Lajmeve të Armatës, 10 prill 2024.

19. Army Times, 10 prill 2024, https://www.armytimes.com/news/your-army/2024/04/10/army-pushes -më shumë-stërvitje-siguri-si-helikopter-përplaset-spike/

20. https://www.army.mil/article/267241/1st_armored_division_adapts_to_ new_challenges.

21. Scott Gourley, *Ushtria nuk heq dorë nga qëllimi i topave me rreze të zgjeruar*, Mbrojtja Kombëtare, 9 shtator 2024, https://www. nationaldefensemagazine.org/articles/2024/9/9/army-not-giving-up -on-extended-range-cannon-goal.

22. Cheryl Marino, *Atëherë dhe tani ATACMS në PRSM: Jashtë me të vjetrën, me të renë*, Army News Service, 26 korrik 2024.

23. "Ushtria amerikane kryen raketën e parë balistike kundër anijes SINKEX duke përdorur PrSM," Naval News, 23 qershor 2024, https://www.navalnews.com/naval-news/2024/06/us-army-conducts-first-kundër-anije-raketë-balistike-sinkex-përdor-prsm/

24. Joe Barnes, *Më shumë se 100 ushtarë rusë të vrarë në sulmin e ATACMS*, Telegraph, 2 maj 2024, https://www.telegraph.co.uk/world-news/2024/05/02/more-than-100-ushtarë-rusë-të-vranë-në-grevë-atacms/

25. David Axe, *Qindra trupa ruse u mblodhën në të hapur. Ata nuk e dinin që ukrainasi kishte drejtuar kundër tyre katër raketa ATACMS*, Forbes, 2 maj 2024.

26. Amos Fox, *Parimet për të Ardhmen e Luftës dhe Luftën e Qëndrimit*, Shoqata e Ushtrisë së Shteteve të Bashkuara, Eseja e Landpower nr. 24-4, prill 2024, 12.

E ARDHMJA E LOGJISTIKËS USHTARAKE DREJT PËRDORIMIT TË INTELIGJENCËS ARTIFICIALE

Kolonel (R) Msc. Arben DHULI
Shef Grupi në IKSHU

Trajtesë e shkurtuar.

Tema e "E ardhmja e logjistikës ushtarake drejt përdorimit të inteligjencës artificiale" shqyrton ndikimin e përparimeve të teknologjisë dhe aplikimin e inteligjencës artificiale (IA) në përmirësimin e operacioneve logjistike ushtarake. Logjistika ushtarake, e cila përfshin menaxhimin e furnizimeve, transportit dhe mbështetjes për njësi ushtarake, ka kaluar në një fazë të re zhvillimi përmes përdorimit të algoritmeve inteligjente dhe sistemeve autonome që mund të optimizojnë çdo aspekt të procesit.

Ky punim fokusohet në mënyrën se si IA mund të transformojë menaxhimin e zinxhirëve të furnizimit, parashikimin e kërkesave, monitorimin e automjeteve dhe pajisjeve, si dhe koordinimin në terren. Nëpërmjet analitikës parashikuese në logjistikën e ushtrisë, IA mund të ofrojë mundësi për përmirësimin e reagimeve të shpejta, uljen e gabimeve dhe ndihmën në menaxhimin e burimeve me më pak kosto dhe më shumë efikasitet, si dhe mund të përcaktojë kur pjesët e automjeteve të ndryshme do të kërkojnë zëvendësim, duke mundësuar mirëmbajtjen proaktive përpara se të ndodhi një avari. Për më tepër, përdorimi i dronëve dhe robotëve autonomë për dërgimin e furnizimeve dhe mbështetje tjetër mund të rrisë sigurinë dhe shpejtësinë e operacioneve. Artikulli ka për qëllim të shqyrtojë sfidat dhe mundësitë që ofron IA për logjistikën ushtarake dhe të parashikojë zhvillimet e ardhshme në këtë fushë, duke ofruar një pasqyrë të rëndësishme për politikat dhe strategjitë e ardhshme të mbrojtjes.

Fjalë kyçe: logjistika ushtarake, inteligjenca artificiale, analitika parashikuese, strategji, dronë, robotë autonomë, menaxhim i zinxhirit të furnizimit etj.

1. Inteligjenca artificiale dhe rëndësia e saj në logjistikën ushtarake

Gjenerali Dwight D. Eisenhower është shprehur: "Nuk do ta keni të vështirë të provoni se betejat, fushatat dhe madje edhe luftërat, janë fituar ose humbur kryesisht për shkak të logjistikës", ndërsa Gjeneral Omar N. Bradley ka thënë: "Amatorët flasin për strategji, ndërsa profesionistët vetëm për logjistikë". Kaq mjafton nga historiku i luftës, për të analizuar të ardhmen e logjistikës në një konflikt të armatosur. Në luftën moderne, kjo do të thotë sasi të mëdha të dhënash për të analizuar marrjen vendimeve në lidhje me furnizimin, transportin, komunikimin, e kështu me radhë. Në zhvillimet e sotme inteligjenca artificiale mund të adresojë shumë sfida të logjistikës dhe zinxhirit të furnizimit ku ajo mund të përdorë sisteme ushtarake si "sistemi i Mbështetjes së Vendimeve Globale" dhe "shërbimet e Zonës Funksionale të Logjistikës".

Kjo analizë gjithëpërfshirëse e të dhënave të vendimmarrjes më të informuar mund të krijojë një pamje gjithëpërfshirëse të mjedisit operacional, duke i lejuar komandantët të marrin vendime në kohë reale. Logjistika në ushtri përfshin më shumë funksione se sa mendohet, duke përfshirë këtu edhe sistemin e përshkrimit të rrugëve të lëvizjes të automjeteve. Ajo po krijon mundësi të reja të pashembullta për menaxhimin e zinxhirit të furnizimit. Megjithatë, shumë organizata mbeten të pasigurta për mënyrën më të mirë për ta zbatuar atë. Përdorimi i inteligjencës artificiale (IA) dhe mësimit të pajisjeve (Logjistika e FA) në një ose më shumë fusha të saj, mund të ndihmojë në përshpejtimin e këtij procesi të IA dhe ta bëjë atë më të zhdërvjellët. IA dhe logjistika ushtarake mund të kenë përfitime të mëdha, pavarësisht se ushtria është fokusuar në aplikimet e IA dhe LU edhe në fusha të tjera. Forcat e Armatosura kanë qenë të ngadaltë në përvetësim IA dhe shpesh pranon një status më të thjeshtë për logjistikën e saj në zonat aktive të luftës. Sidoqoftë, integrimi i IA në logjistikën ushtarake shoqërohet edhe me shqetësimet e veta, si për mbikëqyrje, ose ndonjë element tjetër. Çështjet e IA për logjistikën kanë të bëjnë me paparashikueshmërinë e natyrshme dhe cenueshmërinë ndaj shfrytëzimit. Fakti që kundërshtarët më të mëdhenj të SHBA-s po ndjekin në mënyrë agresive përdorimin e IA dhe në sistemet e tyre të mbrojtjes, dhe se të njëjtat sisteme përballen me të njëjtat rreziqe dhe dobësi, mund të paraqesë mundësi unike për Departamentin e Mbrojtjes (DoD) për të niveluar fushën e lojës. Por nga ana e DoD në SHBA çështja e përdorimit të IA për logjistikë në ushtrinë amerikane, po trajtohet nga Qendra e Përbashkët e Inteligjencës Artificiale e sapoformuar e quajtur (JAIC) e cila po udhëheq këtë proces. Autorët e «Përmbledhjes së Strategjisë së Inteligjencës Artificiale të Departamentit të Mbrojtjes 2018» theksojnë se "kombet e tjera, veçanërisht Kina dhe Rusia, po bëjnë investime të rëndësishme në IA për qëllime

ushtarake". Disa kritikë argumentojnë se "mbështetja në IA mund të çojë në mbi theksimin e teknologjisë në kurriz të problemeve njerëzore dhe intuitës (imagjinatës), të cilat janë në situata komplekse të paparashikueshme". Ekziston rreziku që IA mund të krijojë një ndjenjë të rreme sigurie, duke çuar në besim të tepruar dhe si rezultat një vendimmarrje të gabuar strategjike. Duke u përafruar me parimet udhëzuese në Doktrinën e Përbashkët DP 4-0, (Joint Logistics - Manuali në terren 4-0), Operacionet e Qëndrueshme, forcat e armatosura mund të zhvillojnë operacione logjistike adaptive, të përgjegjshme në një botë më komplekse dhe me zhvillim të shpejtë. Gjithë integrimi i IA në logjistikën e FA konsiston në disa sfida, të tilla si:

- Gjetja e ekuilibrit optimal të automatizimit dhe ekspertizës ndërmjet fuqisë njerëzore.
- Adresimi i çështjeve etike dhe përshtatja e fuqisë punëtore me peizazhin teknologjik gjithnjë në ndryshim.

Fuqia transformuese e IA në përmirësimin e disa mënyrave të menaxhimit të zinxhirit të informacionit brenda ushtrisë është e padiskutueshme. Siç ka nënvizuar ish-komandanti i Komandës së Materialeve të Ushtrisë (USA), Gjeneral Ed Daly, inteligjenca artificiale është vendimtare në ndikimin e shpejtësisë së rëndësisë së parë për logjistikën e praktikës (zbatuese). Vizioni i tij plotëson IA dhe mësimin e kompjuterëve duke u integruar pa probleme në çdo aspekt të procesit të logjistikës së ushtrisë, duke rezultuar në efikasitetin e pashembullt dhe kohë pas kohe për ushtarët në fushën e betejës. Një studim i botuar në International Journal of Production Economics zbuloi se integrimi i IA në menaxhimin e zinxhirit të rreziqeve mund të rrisë efikasitetin me 20% ose më shumë. Koleksioni i IA për të analizuar sasitë e mëdha të llogarive dhe për të krijuar tendencat e ndërmarrjeve dhe analizave të tyre është një tjetër avantazh i burimit të logjistikës së ushtrisë. Duke shfrytëzuar analitikën e drejtuar nga IA, rezulton se mund të parashikohet me saktësi më të madhe aftësia e përcaktimit nga ushtari, i cili nuk është në gjendje të gjejë destinacionin në kohë dhe në vendin e duhur. Për më tepër, analitika parashikuese, mund të optimizojë operacionet e ushtrisë duke përdorur zgjidhjen e personelit dhe teknikës. Analitika parashikuese në logjistikën e ushtrisë, mund të përcaktojë kur pjesët e automjeteve të ndryshme do të kërkojnë zëvendësim, duke mundësuar mirëmbajtjen proaktive përpara se të ndodhi një avari.

Kjo procedurë ndikon në kursimet e disa kostove të operacioneve, duke reduktuar gjasat e ndërprerjes së paplanifikuar për mirëmbajtjen dhe aksidentin. Për më tepër, analitika parashikuese mund të komunikojë me menaxhimin e zinxhirit të rrezikut, duke kontrolluar rrezikun për sigurinë dhe duke verifikuar se burimet e duhura janë të disponueshme në vendin dhe kohën e duhur. Kjo strategji rrit efikasitetin operacional, shkurton kohën e prodhimit dhe dukshmërinë e zinxhirit të qarkullimit.

2. Logjistika adaptive dhe vendimmarrja. Reagimi ndaj informacionit në kohë reale

Kapaciteti për t'iu përshtatur kushteve që kanë të bëjnë me shpejtësinë e veprimit në terren, si një komponent i operacioneve moderne ushtarake, është logjistika dhe vendimmarrja adaptive që kanë lidhje me efektivitetin dhe reagimin e ushtrisë në mjedisin kompleks. IA mund të revolucionarizojë potencialin e këtij aspekti të sigurisë ushtarake duke marrë informacion në kohë reale, analiza të sofistikuara dhe mjeteve të avancuara të veprimeve dhe të vendimeve. Një veprim i tillë është, IA në logjistikën adaptive, është aftësia për të gjetur dhe analizuar të njëjtat gjera nga burime të ndryshme, duke përfshirë këtu sensorët, satelitët dhe platformat e tjera të inteligjencës. Përveç kësaj, IA mund të aksesojë sistemet e të dhënave të regjistrimit nga sistemet e burimeve të ndryshme të ushtrisë, si sistemi i komandim-kontrollit, programi i modernizimit të logjistikës, mjeti i automatizimit të portit dhe informacioni i automatizuar i koordinatorëve të transportit.

Për Sistemin e Lëvizjeve II, inteligjenca artificiale mund të përdorë gjithashtu sisteme joushtarake si sistemi i mbështetjes së vendimeve globale dhe shërbimet e zonës funksionale të logjistikës. Ky informacion mund të krijojë një pamje gjithëpërfshirëse të mjedisit operacional, duke i lejuar komandantët të marrin vendime të informuara nga inteligjenca në kohë reale. Duke pasur akses të saktë dhe në kohë, ushtria mund të përgjigjet në mënyrë më efektive në zhvillim, duke minimizuar shpresat dhe mundësitë e mundshme.

Përveç dhënies së informacionit në kohë reale, IA mund të marrë vendimmarrjen duke u quajtur modele dhe tendenca që mund të mos jenë të mbrojtura nga informacioni për analistët njerëzorë. Nëpërmjet algoritmeve të mësimit të makinerive dhe analizave të avancuara të të dhënave, sistemet e IA mund të zbulojnë korrelacionet e fshehura dhe të gjenerojnë njohuri të zbatueshme për të informuar vendimet strategjike dhe taktike. Për më tepër, IA mund të jetë në një lëvizje të tillë, në lëvizjet e armikut, të parashikojë pengesat e logjistikës ose të bllokimit të ndërprerjeve të mundshme të rreziqeve të tilla të parashikuara. Bazuar në këto informacione, komandantët mund të marrin vendime më të informuara, të shpërndajnë burime në mënyrë më efikase dhe të një avantazhi konkurrues në fushën e betejës.

IA gjithashtu mund të ketë aftësi për t'iu përgjigjur ngjarjeve dhe kontigjencave të papritura duke automatizuar aspekte të veçanta të planifikimit të logjistikës dhe vendimmarrjes. Për shembull, sistemet e drejtuara nga IA mund të ridrejtojnë automatikisht ndryshimet dhe personelin, në ndryshimin e kushteve të mjedisit ose ndërprerjes së papritur në zinxhirin e furnizimit. Duke i automatizuar këto procese, ushtria mund të minimizojë burimet kritike duke u afruar një siguri më të madhe.

Një aplikim tjetër i IA në logjistikën adaptive është teknika e simulimit dhe optimizimit për të zgjidhur marrjen e informacionit në kushte komplekse dhe dinamike. Modelet e simulimit të fuqizuara nga IA i japin mundësinë komandantëve të eksplorojnë skenarë të ndryshëm, të vlerësojnë kurset e mundshme të veprimit dhe të bëjnë strategjitë më të efektshme për ndikimin e objektivave të tyre. Kjo mund të çojë në planin e dëshiruar logjistik, si dhe në përmirësimin e suksesit të përgjithshëm. Janë katër ide novatore që shfaqen te logjistika adaptive, të cilat do të trajtohen më poshtë:

• ***Shkurtimi i linjave të furnizimit me printim 3D në fushën e betejës.***

Në Samitin e Web-it në Lisbonë në nëntor 2023, një përfaqësues shtetëror i Ukrainës vuri në dukje se konflikti aktual në vendin e tij është më i avancuari teknologjikisht që bota ka parë ndonjëherë. Për të vërtetuar mendimin e tij, ai shtoi se kur një gjeneral pyeti se çfarë i nevojitej më shumë në vijën e parë të frontit, përgjigja e tij ishte "një printer 3D". Përdorimi i printerit 3D, si pajisje thelbësore për forcat ukrainase, filloi në ditët e para të konfliktit. Kjo nënkuptonte se printerët kompaktë 3D mund të transportoheshin dhe të vendoseshin lehtësisht. Ata u përdorën për të prodhuar sende relativisht të vogla si: pajisje mbrojtëse, tunika, periskopë, madje edhe pjesë për dronët e zbulimit.

Po kështu një ushtarak i lartë përgjegjës për qendrën e Ekspertizës së Prodhimit me vlerë të lartë në ministrinë e mbrojtjes britanike në vitin 2017, fillimisht prezantoi printimin 3D dhe është një avokat entuziast i përfitimeve të tij. Ndër të tjera ai komenton se: "Nëse mendoni se mbrojtja e Mbretërisë së Bashkuar ka një problem me zinxhirin e saj të furnizimit, përderisa ne punojmë në një mjedis ku mund ta ndërpresim shumë lehtë atë zinxhir furnizimi, atëherë duhet të kemi mjete të tjera për të qenë në gjendje të krijojmë artikuj të inventarit". "Nëse ne mund ta bëjmë këtë me printimin 3D, atëherë pse të mos e bëjmë?" Printimi 3D mund të ndihmojë gjithashtu në prodhimin e pjesëve që rrallë prishen dhe për këtë arsye nuk ruhen shpesh në depot lokale. "Ne duhet të kemi mjete të tjera për të qenë në gjendje të krijojmë artikuj të inventarit. Por nga ana tjetër kritikët argumentojnë se efikasitetet e pretenduara të printimit 3D nuk janë domosdoshmërisht ato që duken. "Dhjetë metra kub pjesë rezervë, është një numër i kufizuar i pjesëve rezervë specifike, ndërsa dhjetë metër kub fije, është çdo pjesë rezervë që dëshironi". Kuptimi i kësaj fjalie është që nëse në një depo ruhen dhjetë metra kub pjesë (aktive), por që është i limituar për llojshmërinë dhe artikullin po të mbahen dhjetë metra kub fije, (të cilat kthehen nëpërmjet teknologjisë printim 3D kthehet në një sasi të konsiderueshme dhe shumë herë me shumë pjesë ose artikuj aktive.

Duke kryer një vlerësim në terren, një printer i vogël e i lehtë, që mund të përdoret në një vendndodhje të vijës së përparuar, do të lejonte një përdorues të pa trajnuar ta përdorte atë. Tjetri ishte një kontejner transporti i madh

dhe shumë më pak i manovrueshëm, që strehonte printer metalikë 3D dhe një dyqan makinerish, e ardhmja qëndron në një njësi të pavarur, paksa si një makinë shitëse, e kombinuar me një portal në internet të skedarëve të printimit 3D. Ai gjithashtu sheh robotikën dhe automatizimin që luajnë një rol në rritje në printimin 3D në terren, që do të thotë se kërkohet më pak trajnim për operatorët.

Marinsat amerikanë kanë përdorur teknika ndërtimi me printim 3D për të ndërtuar një kazermë betoni prototip në vetëm 40 orë, krahasuar me pesë ditët që do t'u duheshin dhjetë marinsave për të ndërtuar një të ngjashme prej druri. Po kështu, Laboratori i Shkencës dhe Teknologjisë së Mbrojtjes në Mbretërinë e Bashkuar (Dstl), i sponsorizuar nga Ministria e Mbrojtjes, ka zhvilluar eksplozivë me porosi, të printuar në 3D, të cilët përfundimisht mund të krijohen sipas kërkesës në vijën e parë. "Ne mund të kursejmë miliona paund duke e ricikluar dhe duke e përdorur si lëndë ushqyese për printerët. Dhe mendoni për të gjitha shishet plastike dhe mbeturinat e tjera që gjeni në fushën e betejës. Ju mund ta zvogëloni atë dhe ta ripërdorni atë."

- ***Optimizimi i mirëmbajtjes së automjeteve me të dhëna.***

Zinxhirët e furnizimit po kalojnë një transformim. Përparimet me internetin, zgjerimi dhe lidhjet e gjërave me të dhe i kombinuar me fuqinë e inteligjencës artificiale, për të dalluar modelet në grupe të mëdha të dhënash dhe për të bërë parashikime, po i ndihmojnë organizatat të parashikojnë kërkesën dhe të minimizojnë ndërprerjet. Marrja e automjeteve në vendin e duhur është një gjë e rëndësishme, ndërsa mbajtja e tyre në gjendje të mirë pune për rrugë dhe për fluturim, është tjetër detyrë. Duke e njohur këtë, në fillim të vitit 2022, Defense Equipment & Support, krahu i prokurimit të Ministrisë së Mbrojtjes së Mbretërisë së Bashkuar, njoftoi një projekt të ri të quajtur "Shërbimi Operativ i Integruar i Tokës" (LIOS). Qëllimi i tij është të gjejë mënyra për të përmirësuar menaxhimin e flotës tokësore të ushtrisë, duke parë në mënyrë specifike fusha të tilla si mbështetja teknike, përmirësimet dhe mirëmbajtja. Është një detyrë komplekse. Flota përfshin më shumë se 30 lloje të ndryshme automjetesh, duke filluar nga tanket "Challenger 2 dhe Bulldog" të blinduar. Të gjitha këto automjete përmbajnë një gamë të gjerë komponentësh të lidhura me sistemet e të dhënave dhe rrjedhat e tyre. Kjo përfshin të dhëna nga sensorët në bord si në një makinë moderne, si dhe të dhënat e mirëmbajtjes, informacionin e zinxhirit të furnizimit dhe vizatimet inxhinierike. Nëse këto gjëra mund të bashkohen dhe shndërrohen në informacione vepruese, flota mund të menaxhohet në një mënyrë më të zgjuar. Por ka një problem. Për momentin, të gjitha llojet e ndryshme të të dhënave për të gjitha këto automjete të ndryshme ruhen në një sërë vendndodhjesh. "Mund të ketë disa SME që ofrojnë një pjesë të caktuar kritike të një automjeti, por të dhënat për

të janë të vendosura në një server në një park industrial diku dhe Ministria e Mbrojtjes nuk mund t'i qaset sepse ata as nuk e dinë se është atje." thotë Paine. Të dhënat e flotës ekzistojnë gjithashtu në forma të ndryshme, duke filluar nga letra e printuar te skedarët PDF, deri te fletët e llogaritura në Excel. Edhe nëse është digjital, ai mund të jetë "siled", që do të thotë se Ministria e Mbrojtjes është e kufizuar në nxjerrjen e njohurive prej tij falë mungesës së ndërveprimit. "Të gjitha të dhënat duhet të jenë kohezive, të indeksuara, të aksesueshme dhe në një vend të menaxhueshëm," shton Paine. Në vitin 2021, Microsoft eksploroi se si ta trajtonte atë problem përmes një projekti me flotën botërore të helikopterëve "Wildcat" të Marinës Mbretërore. Qëllimi i projektit ishte të shikonte tendencat afatgjata rreth mirëmbajtjes së helikopterëve, në mënyrë që të kishte një qasje më të zgjuar ndaj mirëmbajtjes së planifikuar. "Ata kishin një orar që u tregonte se sa shpesh duhet të bënin disa aktivitete të mirëmbajtjes, por ajo që ata nuk kishin, ishte njohuria rreth asaj, se sa efektive ishin ato aktivitete të mirëmbajtjes," thotë Luke Parker, menaxher i lartë i programit të biznesit të inxhinierisë qeveritare në Microsoft. "Ata donin të optimizonin orarin e tyre duke hequr aktivitetet që nuk sollën ndonjë përfitim për sa i përket disponueshmërisë ose vlefshmërisë ajrore."

Parker e përshkruan këtë si përdorim "të nivelit të parë" të të dhënave: bashkimi i tyre nga burime të ndryshme dhe grumbullimi i tyre në një mënyrë që lejon njeriun të marrë vendime të mira bazuar në to. Projekti LIOS synon ta çojë këtë në fazën e "nivelit të dytë": Sjellja e mirëmbajtjes së automjeteve të ushtrisë, plus të gjithë zinxhirin e furnizimit që u shërben atyre, në botën e Industrisë 4-0. Kjo nënkupton përdorimin e mësimit të makinerive dhe inteligjencës artificiale për të zgjidhur pyetje komplekse analitike rreth parashikimit të kërkesës dhe optimizimit të inventarit. Më pas proceset mund të automatizohen prej andej. Rasti i përdorimit është parashikimi kur do të nevojiten komponentë specifikë, bazuar në modele të hollësishme të kërkesës, dhe porositja e tyre paraprakisht. Imagjinoni që një tank kthehet në bazë dhe ka nevojë për një modifikim harduer. Inxhinieri thjesht hap një portal online, ku mund të gjejë të gjithë informacionin që i nevojitet për të bërë ndryshimin dhe mund të porosisë menjëherë komponentët e duhur nga magazina, sepse mësimi i makinerive do të ketë parashikuar kërkesat e tyre dhe do të sigurohet se janë në magazinë. Nuk ka më gjueti përreth. "Ai individ do të kuptojë gjithashtu, në mënyrë analitike, se si po funksionon ai automjet si një njësi, në lidhje me automjetet e tjera të ngjashme në terren," thotë Dan Haines, specialist i analitikes së të dhënave të sigurisë kombëtare në Microsoft. "Dhe ekziston një nivel i automatizimit të aplikacioneve, që do të thotë se të gjitha njoftimet e sinjalizimit për të marrë ato pjesë u dërgohen palëve përkatëse, dhe njoftimi gjithashtu i dërgohet përsëri personit që është duke projektuar automjetin, për të vazhduar ciklin e reagimit për ta bërë atë më të mirë.

• ***Vendosja e AR (realiteti i shtuar) në të gjithë zinxhirin e furnizimit.***

Gjetja e gjërave (aktiveve) në një depo nuk është e lehtë. Rreth gjysma e të gjithë kohës së shpenzuar në një magazinë tipike komerciale shpenzohet për "zgjedhjen e porosive" për gjetjen e artikujve në raftet dhe marrjen e tyre. Megjithatë, disa kompani kryesore logjistike tani po përdorin teknologjinë "zgjedh nga vizioni" bazuar në (realitetin e shtuar AR). Syzet inteligjente të dizajnuara posaçërisht mund t'i çojnë punonjësit të magazinës, me anë të shigjetave virtuale, në raftin e duhur dhe më pas të shfaqin informacione të mëtejshme rreth numrit të artikujve që do të zgjidhen dhe ku duhet t'i vendosni ato në karrocë. Një rishikim i vitit 2022 i Institutit të Inxhinierëve Elektrikë dhe Elektronikë i 23 studimeve të rasteve dhe artikujve kërkimorë mbi përdorimin e realitetit të shtuar, në sistemet e menaxhimit të magazinës zbuloi se: në 87 % të rasteve, u rrit produktiviteti dhe efikasiteti operacional. "Realiteti i përzier ofron mundësi masive, por shumë prej tyre nuk po realizohen për momentin." Në të vërtetë, AR tashmë po përdoret në kontekste të tjera të mbrojtjes: ushtria amerikane, p.sh., ka vlerësuar përdorimin e kufjeve të modifikuara të Microsoft HoloLens për realitetin e shtuar të ushtarëve në terren që nga viti 2017, me qëllim përmirësimin e navigimit, ndërgjegjësimit për situatën dhe vendimmarrjes. Një fushë që tashmë ka filluar të përfitojë është mirëmbajtja. Një studim i pavarur i kryer në emër të kompanisë së softuerit realitetin e shtuar "Taqtile" shqyrtoi mirëmbajtjen e motorit reaktiv në Forcën Ajrore të SHBA-së, ku mirëmbajtja rutinë kërkohet shpesh, pavarësisht se teknikët e kualifikuar nuk janë të disponueshëm, veçanërisht në vende të largëta. Në studim, teknikët që përdornin metoda tradicionale nuk ishin në gjendje të kryenin gati një të tretën e detyrave dhe kishin një shkallë gabimi prej 60 % në ato që përfunduan. Ata që përdorin kufjet i përfunduan të gjitha detyrat pa gabime. Edhe shembulli i fundit në Ukrainë: "Ju po u siguroni atyre sasi të konsiderueshme pajisjesh, por si t'i trajnoni më pas njerëzit që janë në vijën e parë për t'i përdorur ose mirëmbajtur pa i sjellë ata tek ju? AR mund të jetë e dobishme për këtë."

• ***Shpëtimi i jetëve me anë të robotëve.***

Në konfliktet e fundit në Irak dhe Afganistan, kolonat e gjata dhe të ngadalta të kamionëve të furnizimit që udhëtonin nëpër rrugë të parashikueshme u bënë një objektiv i lehtë për pajisjet shpërthyese të improvizuara të kundërshtarëve (IED). Një studim i fundit nga Shërbimi Kërkimor i Kongresit zbuloi se, ndërmjet viteve 2006 dhe 2021, pak më pak se gjysma e të gjitha vdekjeve të anëtarëve të shërbimit amerikan në Afganistan rezultuan nga IED. Nisur nga kjo, nga Instituti Mbretëror i Shërbimeve të Bashkuara është marrë në konsideratë dhe po studiohen dhe mendohen mënyra të ndryshme për furnizimin që minimizon rrezikun e humbjes së jetëve. Gjithashtu duke

marrë në konsideratë edhe aspektin e fuqisë punëtore, forcat e armatosura të Mbretërisë së Bashkuar po zvogëlohen dhe nëse ka më pak njerëz që duhet të jenë më të aftë në më shumë fusha, ata thjesht duhet të qëndrojnë gjallë.

Një mënyrë e re e të menduarit qëndron në sistemet robotike dhe autonome. Një provë e përbashkët nga (Dstl) dhe Qendra e Sistemeve të Automjeteve Tokësore të ushtrisë amerikane shqyrtoi përdorimin e kamionëve të rëndë gjysmë autonome në një kolonë, me ekuipazh vetëm automjetin kryesor. Këto automjete mund të lëvizin mallra me shumicë nga një pikë marrëse në një dyqan qendror furnizimi pranë fushës së operimit. Automjetet më të vogla robotike tokësore do të ofrojnë më pas dërgimin e "miljes së fundit" për trupat. Operacioni ishte pjesë e projektit të Koalicionit të Siguruar të Rifurnizimit Autonom (CAAR), i cili përfshinte gjithashtu sisteme ajrore pa ekuipazh që mund të ngrinin dhe lëshonin ngarkesa duke përfshirë municione, ushqime dhe furnizime mjekësore në zonat e vijës së parë ku trupat kanë nevojë për furnizime të shpejta. Ajo u rrit nga dëshira për të përfshirë teknologjitë autonome nga sektori tregtar në logjistikën e mbrojtjes. Përveç rrezikimit të më pak jetëve, përdorimi i automjeteve autonome në logjistikë mund të ketë avantazhe të tjera. Ndryshe nga njerëzit, ato nuk kanë nevojë të bëjnë pushime, që do të thotë se më shumë furnizime mund të dorëzohen duke përdorur të njëjtin numër automjetesh. Për shembull nëse operacionet kanë të ngjarë të bëhen më të shpërndara në konfliktin aktual në Ukrainë, vija e frontit shtrihet në qindra milje, atëherë autokolona të vogla të mjeteve tokësore plotësisht autonome, të mbështetura nga dronë ajror, një ditë mund të rezultojnë të jenë një metodë efektive e furnizimit. Por edhe kjo ka sfidat e veta siç është kostoja e zhvillimit dhe një tjetër është fakti që teknologjia e automjeteve autonome aktualisht me vështirësi mund të përballojë udhëtimet konvencionale në autostrada, ndërsa në një mjedis të kontestuar dhe rrugë pa rrugë është akoma më e vështirë. Për kompaninë e teknologjisë së mbrojtjes "QinetiQ", hapi i parë mund të jetë futja në automjetet ushtarake disa nga mjetet e avancuara të ndihmës së shoferit që janë aktualisht të disponueshme në makinat moderne. Kjo është teknologjia që do të ndihmojë për të mundësuar drejtimin autonom në të ardhmen, të tilla si ndjeshmëria e objekteve dhe zbulimi i skajeve të rrugës. Është diçka që është relativisht e lirë për t'u zbatuar, por mund të jetë shumë efektive.

"Të ngasësh në një kolonë ushtarake gjatë natës, me shumë mundësi duke lëvizur taktikisht pa dritë ose dritë të ulët, është një gjë e vështirë për t'u bërë dhe kjo kërkon nivele shumë të larta të vetëdijes për situatën nga drejtuesi i mjetit. Ka pasur raste të shumta në Afganistan të automjeteve të mëdha logjistike që hynin në kanale dhe si pasojë e kësaj ka pasur humbje jetësh. Automjetet autonome dhe dronët do të ishin në mënyrë ideale një manifestim

fizik i një zbatimi shumë më të gjerë të autonomisë në të gjithë zinxhirin e furnizimit, gjë që bazohet në analitiken e të dhënave dhe IA. Si përfundim organizimi i të dhënave dhe automatizimi i sistemet, e bën të gjithë procesin më efikas dhe kjo përfundimisht do japë një avantazh strategjik.

3. Mirëmbajtja parandaluese me ndihmën e IA

Një nismë e rëndësishme logjistike e inteligjencës artificiale nën JAIC (Qendra e Përbashkët e Inteligjencës Artificiale) është mirëmbajtja parandaluese, veçanërisht për avionët luftarakë. Një version i hershëm i mirëmbajtjes parandaluese të automatizuar për ushtrinë ishte testi i avionit luftarak F-35 i kryer nga Lockheed Martin në vitin 2015.

Ndihma e menjëhershme mjekësore nuk është gjithmonë e disponueshme në fushën e betejës. Mund të jetë mungesa e mjekëve aktualë në zonë, lëndime përtej aftësive të një mjeku, ose çështje tirazhi, ku personeli mjekësor i jep përparësi të lënduarve më keq. IA mund të japë disa përgjigje në këtë fushë të logjistikës. Inteligjenca artificiale në mjekësi është një fushë e mirëpërcaktuar në sektorin tregtar, por jo aq shumë në ushtri. Përpjekjet janë duke u zhvilluar për të korrigjuar këtë çekuilibër, me Qendrën e Kërkimit të Telemjekësisë dhe Teknologjisë së Avancuar të Ushtrisë (TATRC) që drejton akuzën. I quajtur sistemi i Automated Ruggedized Combat Casualty Care (ARC3), ai nuk do të jetë një IA mjekësore plotësisht e automatizuar, por më tepër softuer që mund të ndihmojë mjekët në diagnostikimin e lëndimeve, monitorimin e pacientëve dhe ofrimin e trajtimit kur evakuimi i menjëhershëm i pacientit nuk është i mundur. Sistemi është aktualisht në zhvillim e sipër. Charles River, gjithashtu lidhi një kontratë për të zhvilluar aplikacionin celular Ansamble Prediction for Combat Casualty Care (EPIC3). Ideja është t'i sigurohet mjekut një mbështetje vendimtare kur bëhet fjalë për trajtimin e lëndimeve traumatike. EPIC3 supozohet se paraqet hapat për të trajtuar ato lëndime përmes një ndërfaqe të thjeshtë dhe të lehtë për t'u përdorur, që përshtatet me nevojat dhe nivelin e aftësive të përdoruesit. Ky softuer është gjithashtu në zhvillim e sipër. AthenaGTX pretendoi se është në fazat e fundit të zhvillimit të bazuar për Sistemin e tij të kujdesit kritik të automatizuar (ACCS). Kompania e përshkroi atë si një "sistem" që "integrojnë monitorimin fiziologjik të pacientit me ndërhyrjet e kontrolluara nga algoritmet e softuerit për të ofruar kujdes mjekësor automatik për luftëtarët e plagosur rëndë". Kompania gjithashtu ka një pajisje të veshur që pretendon se mund të ndihmojë në kontrollimin e fushëbetejës.

I quajtur Wireless Vital Signs Monitor (WVSM), ai regjistron gjërat vitale të një pacienti dhe e transmeton atë në pajisje të përputhshme. Një *database* qendror informacioni mund të duket si një ide e keqe për ushtrinë, por në botën e logjistikës, është e nevojshme. Do të thotë kursime në kohë, përpjekje

dhe para nëse logjisticienët kanë të gjithë informacionin që u nevojitet për të marrë vendime të informuara kur lëvizin furnizimet dhe pajisjet për të mbështetur trupat. Në përputhje me këtë, IBM ofron shërbime cloud, si dhe akses në Watson për të ruajtur dhe përpunuar të dhëna logjistike që vijnë nga burime të ndryshme. Aktiviteti i mbështetjes së logjistikës, ose LOGSA, (tani Qendra e Analizës së të Dhënave Logjistike ose (LDCA)) si dhe aftësitë si Watson e bëjnë të jetë një mënyrë për t'i krijuar lehtësira për analistët nga disa punë më teknike, me qëllim për ta lënë makinën (pajisjen), të bëjë një pjesë të kësaj dhe për të shfrytëzuar ekspertizën profesionale të analistëve për të më tej se ku po shkon ushtria. Ideja është që të përdoret cloud për të ngarkuar të dhënat e sensorëve nga automjetet dhe pajisjet dhe për të kryer "mirëmbajtjen e bazuar të kondicionuar (CBM)", e cila është një qasje e riparimit kur nevojitet, e mundësuar me analizën e të dhënave të drejtuar nga IA. Në vitin 2019, ajo iniciativë ka lulëzuar në një kontratë shumë miliardësh me një ofrues të vetëm për ruajtje të sigurt cloud dhe softuer nën infrastrukturën e mbrojtjes së ndërmarrjeve të përbashkëta (JEDI) me disa kompani tregtare që konkurrojnë për të. Për agjencinë e logjistikës së mbrojtjes (DLA), ky është një problem i madh, pasi siguron atë që i nevojitet ushtrisë, si armë, pjesë riparimi dhe karburant, si dhe asgjëson pajisjet e tepërta. Duke qenë se DLA merr mesatarisht një milion oferta në ditë, mund të jetë praktikisht e lehtë për t'u realizuar disa transaksione të dyshimta. Për të adresuar këtë çështje, DLA iu drejtua softuerit IA dhe ML për të renditur malin e të dhënave private dhe publike, për të identifikuar dhe shënuar furnizuesit e dyshimtë ose anormalë.

Ajo ka identifikuar më shumë se 350 kode CAGE me rrezik të lartë ose subjekte furnizuese. Është ndoshta një nga shqetësimet tona kryesore tani nga këndvështrimi i procesit është rritja e numrit të kompanive mashtruese ose aktorëve të këqij që po përpiqen të hyjnë në biznesin tonë. Ky mjet i ri ka qenë shumë i dobishëm në identifikimin e kësaj që nga fillimi dhe duke na lejuar të vendosim kontrolle në sistemet tona për të mos lejuar që ata të marrin biznes nga DLA. Është e paqartë nëse DLA e ka zhvilluar veglën BDA brenda apo e ka kontraktuar atë me një nga disa kompani infoteknike dhe IA që kanë dhënë kontrata sipas programit J6 Enterprise Technology Services (JETS). Kapaciteti për t'iu përshtatur kushteve që kanë të bëjnë me shpejtësinë e veprimit në terren si një komponent i operacioneve moderne ushtarake është logjistika dhe vendimmarrja adaptive që kanë lidhje me efektivitetin dhe reagimin e ushtrisë në mjedisin kompleks. IA mund të revolucionarizojë potencialin e këtij aspekti të sigurisë ushtarake duke marrë informacion në kohë reale, analiza të sofistikuara dhe mjeteve të avancuara të veprimeve dhe të vendimeve.

Një veprim i tillë është IA në logjistikën adaptive, që është aftësia për të gjetur dhe analizuar të njëjtat gjera nga burime të ndryshme, duke përfshirë këtu

sensorët, satelitët dhe platformat e tjera të inteligjencës. Përveç kësaj, IA mund të aksesojë sistemet e të dhënave të regjistrimit nga sistemet e burimeve të ndryshme të ushtrisë, si sistemi i komandim-kontrollit, programi i modernizimit të logjistikës, mjeti i automatizimit të portit dhe informacioni i automatizuar i koordinatorëve të transportit. Mjetet pa shofer – dronët - po bëjnë shumë zhurmë në hapësirën e IA, por kryesisht për mbikëqyrje. Ajo që shumica e njerëzve ndoshta nuk e kuptojnë është se ushtria po shikon seriozisht automjetet vetë-drejtuese për të rifurnizuar postat dhe bazat nën programin e Rifurnizimit Autonom të Tokës. Kjo do t'i kursente (shoferët njerëzorë) nga vështirësitë dhe rreziqet e një kolone furnizimi. Ushtria tashmë i dha një kontratë Robotic Research LLC për të zhvilluar komplete autonome. Sidoqoftë, "ndonjëherë është më mirë të shkosh ndërsa korbi fluturon" dhe laboratori i kërkimeve të ushtrisë po shqyrton gjithashtu përdorimin e dronëve ajrorë në vend të mjeteve tokësore nën automjetin e përbashkët taktik të rifurnizimit ajror (JTARV). Natyrisht, ngarkesat do të duhej të ishin shumë më pak (fuqia transportuese e mallrave) , por mund të arrinte në destinacion më shpejt se sa një automjet tokësor. Për këtë qëllim, ushtria po punon me Malloy Aeronautics për të përdorur katërkopterin e saj ("hoverbike") si JTARV-in e parë. JTARV ideal do të jetë në gjendje të mbajë deri në 800 paund ngarkesë, dhe të ketë një shpejtësi deri në 60 mph dhe autonomi fluturimi deri në 125 milje.

Nëpërmjet algoritmeve të mësimit të makinerive dhe analizave të avancuara të të dhënave, sistemet e IA mund të zbulojnë korrelacionet e fshehura dhe të gjenerojnë njohuri të zbatueshme për të informuar vendimet strategjike dhe taktike. Për më tepër, IA mund të jetë në një lëvizje të tillë, ku mund të parashikojë pengesat e logjistikës ose të bllokimit të ndërprerjeve të mundshme të rreziqeve përpara se të ndodhin. Bazuar në këto informacione, komandantët mund të marrin vendime më të sakta, të shpërndajnë burime në mënyrë më efikase dhe të një avantazhi konkurrues në fushën e betejës. IA gjithashtu mund të ketë aftësi ushtarake për t'iu përgjigjur ngjarjeve dhe kontigjencave të papritura duke u automatizuar aspekte të veçanta të planifikimit të logjistikës dhe vendimmarrjes. Për shembull, sistemet e drejtuara nga IA mund të ridrejtojnë automatikisht ndryshimet dhe personeli në ndryshimin e kushteve të mjedisit ose ndërprerjes së papritur në zinxhirin e furnizimit. Duke i automatizuar këto procese, Ushtria mund të minimizojë atë që burimet kritike janë duke u kthyer në më shumë, edhe në mes të pasigurisë. Një aplikim tjetër i IA në logjistikën adaptive është teknika e simulimit dhe optimizimit për të zgjidhur marrjen në kushte komplekse dhe dinamike. Modelet e simulimit të fuqizuara nga IA i jep mundësinë komandantëve të eksplorojnë skenarë të ndryshëm të vlerësojnë mendimet e mundshme të veprimit dhe të bëjnë strategjitë më të efektshme për ndikimin e objektivave të tyre. Kjo mund

të çojë në planin e dëshiruar logjistik, si dhe në përmirësimin e suksesit të përgjithshëm të misionit. Kufizimet buxhetore dhe prioritetet konkurruese mund të bëjnë sfiduese ndarjen e burimeve të përmirësimit për integrimin e IA duke ndikuar potencialisht efektivitetin e saj. Një tjetër është cenueshmëria e IA ndaj sistemit të manipulimit të sulmeve. Ndërsa sistemet logjistike të ndërmarra nga IA sulm më kritik për operacionet e ushtrisë, ato të tjera objektive me vlerën më të lartë për ato që duan të prishin ose kompromet ojnë aftësitë e rëndësishme. Zhvillimi i masave të sigurisë është një problem, por nuk ka asnjë garanci që kjo mbrojtje të bëhet gjithmonë efektive kundër sfidave që evoluojnë me shpejtësi.

Përderisa Inteligjenca Artificiale në logjistikën e ushtrisë duhet të jetë e mundur, rezultojnë disa integrime të rëndësishme dhe dizavantazhe të tjera për t›u marrë parasysh. Disa kritikë argumentojnë se mbështetja në IA mund të çojë në mbi theksimin e teknologjisë në kurriz të problemeve njerëzore dhe imagjinatës, të cilat janë në situata komplekse të paparashikueshme. Ekziston rreziku që IA mund të krijojë një ndjenjë të rreme sigurie, duke çuar në besim të tepruar dhe si rezultat një vendimmarrje të gabuar strategjike. Një tjetër është cenueshmëria e IA ndaj sistemit të manipulimit të sulmeve (hakerimi). Ndërsa sistemet logjistike të ndërmarra nga IA sulm më kritik për operacionet e ushtrisë, ato të tjera objektive me vlerën më të lartë për ato që duan të prishin ose kompromet ojnë aftësitë e rëndësishme. Zhvillimi i masave të sigurisë është problem, por nuk ka asnjë garanci që kjo mbrojtje të bëhet gjithmonë efektive kundër sfidave që evoluojnë me shpejtësi.

Për më tepër, duke marrë parasysh çështjet etike që lidhen me IA në logjistikën ushtarake. Përdorimi i IA mund të çojë në vendimmarrjen e një personi, transparencën ose të padëshiruara. Përgjegjësia për veprimet e sistemeve të IA-së duhet të qartësojë për sigurinë e llogarisë në rast gabimesh ose dështimesh.

Përfundime

1. Integrimi i IA në logjistikën e forcave të armatosura mund të ketë risqe të padëshiruara për teknikën e logjistikës profesionale. Ndërsa automatizimi i detyrave të veçanta të mund të çojë në efiçencen, ai gjithashtu mund të rezultojë në ndryshimin e punës dhe nevojën për rikualifikim të konsiderueshëm të fuqisë së punës. Është e vështirë të sigurohet që ushtria të përshtatet me këto ndryshime të një fuqie të veçantë, por të bëjë specialistë dhe investime të tjera.
2. Integrimi i IA në logjistikën e FA ofron mundësi për të revolucionarizuar menaxhimin e zinxhirit të furnizimit, për të optimizuar zgjidhjen e burimeve dhe për të marrë proceset e vendimeve. Megjithatë, është e rëndësishme të njihen dhe të trajtohen sfidat dhe gjërat që lidhen me veprimet e IA-së, të

tilla si arritja e ekuilibrit të duhur ndërmjet automatizimit dhe ekspertizës njerëzore, sigurimi i mjekësisë kibernetike, adresimi i çështjeve etike dhe përshtatja e fuqisë punëtore me peizazhin e teknologjisë. në ndryshim.

3. Ushtria duhet të përfshijë një shoqëri gjithëpërfshirëse që investon në aktivitetin e saj, nxitjen dhe bashkëpunimin ndërmjet sektorëve të edukimit dhe trajnimit të krijimit të mundshëm të kushteve për personelin dhe potencialin publik të masave të ndryshme të qasjes kibernetike. Për më tepër, nuk është e tepërt që të mbahet një dialog i hapur rreth implikimeve etike të IA në logjistikën ushtarake dhe të bëhen udhëzime të qarqeve dhe strukturave të llogaridhënies për të vendosur vendosjen e përgjegjshme të IA.

4. Duke adoptuar një qasje të plotë, edhe FARSH-të, gjatë vitit 2025, lipset të kapërcejnë sfidat që lidhen me integrimin e IA, të zhbllokojnë potencialin transformues të IA, si dhe t'i përfshijnë këto qasje në doktrinën e re të Logjistikës, e cila aktualisht është në proces ripunimi.

Literatura e shfrytëzuar:

1. Bill Kobren, *Taking Life Cycle Logistics from History,* April 06, 2023.
2. Qendra e Përbashkët e Inteligjencës Artificiale e sapoformuar (JAIC). Përmbledhje e Strategjisë së Inteligjencës Artificiale të Departamentit të Mbrojtjes 2018.
3. Colonel Everett Bud Lacroix, *Future of Army Logistics - Exploiting AI, Overcoming Challenges, and Charting the Course Ahead*, August 1, 2023.
4. https://www.lockheedmartin.com/en-us/products/autonomic-logistics-information- system-alis.html.
5. https://dod.defense.gov/News/Article/Article/1747491/clear-skies-for-dod-cloud-initiative/.
6. https://www.dla.mil/.
7. https://orise.orau.gov/tatrc/ Qendra e Kërkimit të Telemjekësisë dhe Teknologjisë së Avancuar të Ushtrisë (TATRC).
8. https://www.armytimes.com/news/your-army/2018/06/27/heres-how-artificial-intelligence-could-predict-when-your-army-vehicle-will-break-down/.
9. https://www.washingtonpost.com/business/capitalbusiness/army-to-use-artificial-intelligence-to-predict-which-vehicles-will-.
10. Doktrina e Përbashkët DP 4-0, (Joint Logistics; Manuali në terren 4-0), Operacionet e qëndrueshme; dhe publikimi i Doktrinës së Ushtrisë 4-0.
11. Samiti i Web-it në Lisbonë, nëntor 2023.

Mbi aplikimin e ligjit ndërkombëtar në operacionet kibernetike

Dr. Ulsi META

Trajtesa e shkurtuar.

Zbatimi i ligjit ndërkombëtar në hapësirën kibernetike është një temë shumë e diskutueshme midis shteteve në lidhje me pranimin e një kornize për qëndrimin e përgjegjshëm të unifikuar të tyre në hapësirën kibernetike. Në përgjithësi, shtetet kanë mosdakordësi me njëri-tjetrin për një sërë çështjesh të së drejtës ndërkombëtare, si cenimi i sovranitetit të një shteti nga sulmet kibernetike, detyrimet e shteteve për moslejimin e veprimeve të paligjshme në hapësirën kibernetike, zbatimin e kundërmasave, përdorimin e forcës etj.

Në vitin 2009, Qendra e Ekselencës së Mbrojtjes Kibernetike të Bashkuar të NATO-s (NATO CCDCOE) në Talin, Estoni, ftoi një grup ekspertësh të pavarur nga Grupi Ndërkombëtar i Ekspertëve (GNE) të ligjit të konfliktit të armatosur për të hartuar një manual mbi luftën kibernetike. Kjo nismë e rëndësishme kërkimore, u kurorëzua me hartimin dhe botimin në vitin 2013 nga Universiteti i Kembrixhit i Manualit të Talinit 1.0 "Mbi aplikimin e ligjit ndërkombëtar në luftën kibernetike". Ky manual trajtonte operacionet më të rëndësishme kibernetike, që shkelin ndalimin e përdorimit të forcës dhe që u lejonte shteteve të ushtronin të drejtën e tyre të vetëmbrojtjes, ose që ndodhin gjatë konfliktit të armatosur.

Bazuar në Manualin e Talinit 1.0 dhe duke marrë parasysh rregullat e së drejtës ndërkombëtare që rregullojnë incidentet kibernetike që shtetet hasin çdo ditë, por që bien nën kufijtë e përdorimit të forcës ose konfliktit të armatosur, CCDCOE dhe Grupi Ndërkombëtar i Ekspertëvë e rishikuan

atë dhe në vitin 2017 u botua Manuali i Talinit 2.0 "Mbi aplikimin e ligjit ndërkombëtar në operacionet kibenetike".

Manuali i Talinit 2.0 është një dokument jo detyrues, që nuk ka fuqinë e ligjit, i cili interpreton normat dhe ligjin ndërkombëtar për të gjetur gjuhën e përbashkët në çështjet komplekse ligjore që përfshijnë luftën kibernetike dhe operacionet kibernetike dhe rideklarim objektiv i së drejtës ndërkombëtare të zbatuar në kontekstin kibernetik.

Nisur nga praktika e deritanishme, zhvillimet teknologjike, qëndrimet publike të industrisë, të forumeve akademike, të organizatave ndërkombëtare dhe shoqërisë civile mbi të drejtën ndërkombëtare kibernetike të shteteve, CCDCOE ka vlerësuar nevojën e përditësimit të Manualit të botuar në vitin 2017 dhe në vitin 2021 ka nisur Projektin e Manualit të Talinit 3.0, që do të përfshijë rishikimin e kapitujve ekzistues dhe eksplorimin e temave dhe çështjeve të reja me rëndësi për operacionet kibernetike.

Fjalët kyçe: Manuali i Talinit, operacionet kibernetike, rregulli, ligji ndërkombëtar.

1. Manuali i Talinit 2.0 dhe përmbajtja e tij

Aktivitetet kibernetike janë bërë pjesë integrale e marrëdhënieve ndërkombëtare. Lidhja e madhe e rrjeteve, teknologjive dhe proceseve kibernetike përtej kufijve i ka afruar shoqëritë dhe individët nga shtete dhe kontinente të ndryshme dhe ka krijuar mundësi të reja për bashkëpunim ndërmjet aktorëve shtetërorë dhe joshtetërorë. Në të njëjtën kohë, shtetet dhe shoqëritë janë shumë të varura nga funksionimi i infrastrukturës së teknologjisë së informacionit dhe komunikimit, gjë që ka krijuar dobësi të reja. Në hapësirën kibernetike, shpesh nevojiten vetëm disa burime të kufizuara për të shkaktuar dëme të konsiderueshme, duke shtuar kërcënimin ndaj sigurisë së shteteve dhe shoqërive. "Në shekullin e 21-të, bitet dhe bajtët mund të jenë po aq kërcënues sa plumbat dhe bombat"[1]. Teknologjitë kibernetike, me shumëllojshmërinë e tyre dhe rreziqet shoqëruese, po paraqesin gjithnjë e shumë vështirësi në lidhje me identifikimin dhe zbatimin e ligjit ndërkombëtar për përdorimin e tyre.

Manuali i Talinit 2.0 "Mbi aplikimin e ligjit ndërkombëtar në operacionet kibenetike" shqyrton statusin aktual të së drejtës ndërkombëtare dhe mënyrën se si mund të zbatohet në skenarë të ndryshëm. Në 154 rregulla trajtohen një sërë çështjesh ligjore që mund të dalin dhe gjejnë zgjidhje në operacionet

[1] Lynn, William. J. (2011): Remarks on the Department of Defense Cyber Strategy. Nga http:// www.defense.gov/ speeches/speech.aspx?speechid=1593

e ndryshme kibernetike. Çdo rregull është shoqëruar me disa komente, që kanë si qëllim identifikimin e bazës së tyre ligjore, shpjegimin e përmbajtjes së tyre normative, adresimin e implikimeve praktike në kontekstin kibernetik dhe parashtrimin e pozicioneve të ndryshme për sa i përket fushëveprimit ose interpretimit.

Manuali përbëhet nga katër pjesë. Në pjesën I trajtohet "E drejta e përgjithshme ndërkombëtare dhe hapësira kibernetike"; pjesa II përfshin "Regjimet e veçanta të së drejtës ndërkombëtare dhe hapësira kibernetike"; pjesa III trajton "Paqja dhe siguria ndërkombëtare dhe aktivitetet kibernetike" dhe pjesa IV "Ligji i konfliktit të armatosur kibernetik". Në këtë material janë trajtuar pjesa I dhe pjesa II.

2. E drejta e përgjithshme ndërkombëtare dhe hapësira kibernetike

Pjesa I "E drejta e përgjithshme ndërkombëtare dhe hapësira kibernetike", në Manualin e Talinit 2.0, është trajtuar nëpërmjet 33 rregullave në disa drejtime, si: sovraniteti, kujdesi i duhur, juridiksioni, ligji i përgjegjësisë ndërkombëtare dhe operacionet kibernetike që nuk rregullohen në vetvete nga e drejta ndërkombëtare.

2.1. Sovraniteti

Paragrafi mbi sovranitetin përfshin pesë rregulla: sovraniteti (parimi i përgjithshëm); sovraniteti i brendshëm; sovraniteti i jashtëm; shkelja e sovranitetit dhe imuniteti dhe paprekshmëria sovrane. Në rregullin e parë të Manualit, theksohet se "Parimi i sovranitetit zbatohet për hapësirën kibernetike"[2]. Në dy rregullat vijues bëhet dallimi midis sovranitetit të brendshëm dhe të jashtëm[3] dhe rregulli 3 parashikon se "Një shtet është i lirë të kryejë aktivitete kibernetike në marrëdhëniet e tij ndërkombëtare që i përkasin çdo rregulli të kundërt të së drejtës ndërkombëtare detyrues për atë"[4]. Nisur nga rregulli 2 dhe 3, në rregullin 4 është përcaktuar se "një shtet nuk duhet të kryejë operacione kibernetike që cenojnë sovranitetin e një shteti tjetër"[5]. Rregulli 5 "Imuniteti dhe paprekshmëria sovrane" i referohet infrastrukturës kibernetike të vendosur në bordin e platformave në det të hapur, në hapësirën ajrore ndërkombëtare ose në hapësirën e jashtme dhe përcakton se "Çdo ndërhyrje nga një shtet në infrastrukturën kibernetike në bordin e një platforme

[2] Manuali i Talinit 2.0, faqe 12, rregulli 1.

[3] Manuali i Talinit 2.0, faqe 13; rregulli 2: "Një shtet gëzon autoritet sovran në lidhje me infrastrukturën kibernetike, personat dhe aktivitetet kibernetike të vendosura brenda territorit të tij, në varësi detyrimeve të tij ligjore ndërkombëtare".

[4] Manuali i Talinit, faqe 16, rregulli 3.

[5] Manuali i Talinit, faqe 17, rregulli 4.

kudo që ndodhet, që gëzon imunitet sovran, përbën shkelje të sovranitetit”[6].

2.2. Kujdesi i duhur

Paragrafi për kujdesin e duhur përfshin dy rregulla: kujdesi i duhur (parimi i përgjithshëm) dhe pajtueshmëria me parimin e kujdesit të duhur. Në lidhje me parimin e përgjithshëm të kujdesit të duhur në hapësirën kibernetike caktohet që “Një shtet duhet të ushtrojë kujdesin e duhur për të mos lejuar që territori i tyre, ose territori ose infrastruktura kibernetike nën kontrollin e tyre qeveritar, të përdoren për operacione kibernetike që prekin të drejtat dhe shkaktojnë pasoja serioze negative për shtetet e tjera”[7].

Që një shtet të jetë përgjegjës për zbatimin e kujdesit të duhur për të parandaluar dëmtimin ndërkufitar, shteti duhet të ketë ose objektivisht duhet të kishte informacion për dëmin. Në momentin kur një shtet ka të dhëna për dëmin ndërkufitar, kërkohet të marrë “të gjitha masat që janë të mundshme në kushtet për t’i dhënë fund operacioneve kibernetike”[8]. Me fjalë të tjera, shteti duhet të marrë masa që janë “në mënyrë të arsyeshme të disponueshme dhe praktike”[9], ndonëse mjetet me anë të të cilave kjo arrihet janë në zgjedhjen e shtetit nga i cili vjen dëmi[10].

2.3. Juridiksioni

Paragrafi i Manualit mbi juridiksionin përfshin gjashtë rregulla: juridiksioni (parimi i përgjithshëm); juridiksioni territorial; juridiksioni urdhërues jashtëterritorial; juridiksioni detyrues jashtëterritorial; imuniteti i shteteve nga ushtrimi i juridiksioni dhe bashkëpunimi ndërkombëtar në zbatimin e ligjit. Juridiksioni (parimi i përgjithshëm) përkufizohet si “kompetenca e shteteve për të rregulluar individët, objektet dhe sjelljen sipas ligjit të tyre kombëtar, brenda kufijve të vendosur nga e drejta ndërkombëtare”[11]. Në rregullin e parë mbi juridiksionin pohohet se “si subjekt i kufizimeve të përcaktuara në të drejtën ndërkombëtare, një shtet mund të ushtrojë juridiksion territorial dhe jashtëterritorial mbi aktivitetet kibernetike”[12]. Kjo do të thotë se “në parim, aktivitetet kibernetike dhe individët që angazhohen në to i nënshtrohen të njëjtave të drejtave dhe kufizimeve juridiksionale si çdo formë tjetër aktiviteti”[13].

---

[6] Manuali i Talinit, faqe 27, rregulli 5.
[7] Manuali i Talinit 2.0, faqe 30, rregulli 6.
[8] Manuali i Talinit 2.0, faqe 43, rregulli 7.
[9] Manuali i Talinit 2.0, faqe 43, rregulli 7.
[10] Manuali i Talinit 2.0, faqe 44.
[11] Manuali i Talinit 2.0, faqe 51.
[12] Manuali i Talinit 2.0, rregulli 8, faqe 51.
[13] Manuali i Talinit 2.0, rregulli 8, faqe 51.

Manuali trajton tre llojet tradicionale të juridiksionit: urdhëruese, detyruese dhe gjykuese dhe diskuton aspektet kryesore të secilit. Në lidhje me juridiksionin urdhërues, Manuali shpjegon se në thelb shtetet janë të papenguar në lidhje me juridiksionin urdhërues brenda territorit të tyre sovran dhe mund të ushtrojnë juridiksionin urdhërues në mënyrë jashtëterritoriale (bazuar në vendndodhjen e aktivitetit kibernetik ose efektet e tij) nëse mbështetet në një nga bazat për juridiksionin jashtëterritorial[14].

Rregulli 9, përcakton juridiksionin territorial dhe konfirmon se juridiksioni territorial subjektiv dhe objektiv zbatohen për aktivitetet kibernetike. "Një shtet mund të ushtrojë juridiksion territorial mbi:

(a) infrastrukturën kibernetike dhe personat e përfshirë në aktivitete kibernetike në territorin e tij;

(b) aktivitetet kibernetike me origjinë ose të përfunduara në territorin e tij; ose

(c) aktivitetet kibernetike që kanë një efekt thelbësor në territorin e tij"[15].

Rregulli 10, pranon se shtetet mund të kërkojnë gjithashtu juridiksion jashtëterritorial (ekstraterritorial). "Një shtet mund të ushtrojë juridiksion urdhërues ekstraterritorial në lidhje me aktivitetet kibernetike:

(a) kryer nga shtetasit e tij;

(b) kryer në bordin e anijeve dhe avionëve që zotërojnë shtetësinë e tij;

(c) të kryera nga shtetas të huaj dhe të projektuara për të minuar seriozisht interesat thelbësore të shtetit;

(d) të kryera nga shtetas të huaj kundër shtetasve të tij, me disa kufizime; ose

(e) që përbëjnë krime sipas të drejtës ndërkombëtare që i nënshtrohen parimit të universalitetit"[16].

Rregulli 11, ka të bëjë me juridiksionin detyrues. Ashtu si me juridiksionin urdhërues, shtetet mund të ushtrojnë juridiksion detyrues në territorin e tyre, por kanë mundësi më të kufizuara për të ushtruar juridiksionin detyrues jashtëterritorial. "Një shtet mund të ushtrojë juridiksion detyrues jashtëterritorial vetëm në lidhje me persona, objekte dhe aktivitete kibernetike në bazë të:

(a) një caktimi specifik të autoritetit sipas ligjit ndërkombëtar; ose

(b) pëlqimit të vlefshëm nga një qeveri e huaj për të ushtruar juridiksion në territorin e saj"[17].

[14] Manuali i Talinit 2.0, faqe 51-52.
[15] Manuali i Talinit 2.0, rregulli 9, faqe 55.
[16] Manuali i Talinit 2.0, rregulli 10, faqe 60.
[17] Manuali i Talinit 2.0, rregulli 11, faqe 66.

Këndvështrimi i Manualit të Talinit 2.0 është se e drejta ndërkombëtare, duke përfshirë traktate të veçanta si ligji i detit, i hapësirës së jashtme dhe traktatet në lidhje me aktivitetet e aviacionit, mund të mbështesin ushtrimin e juridiksionit detyrues jashtë vendit. Në fakt, disa traktate, siç është Konventa e Këshillit të Evropës për krimin kibernetik, mund të kërkojnë në mënyrë specifike disa të drejta të zbatimit jashtëterritorial[18].

Në lidhje me imunitetin e shteteve nga ushtrimi i juridiksionit, në Manual është përcaktuar që "Një shtet nuk mund të ushtrojë juridiksion detyrues ose gjyqësor në lidhje me personat e angazhuar në aktivitete kibernetike ose infrastrukturën kibernetike që gëzojnë imunitet sipas ligjit ndërkombëtar"[19]; ndërsa për bashkëpunimin ndërkombëtar në zbatimin e ligjit është parashikuar se "megjithëse si çështje e përgjithshme, shtetet nuk janë të detyruar të bashkëpunojnë në hetimin dhe ndjekjen penale të krimit kibernetik, një bashkëpunim i tillë mund kërkohet nga kushtet e një traktati të zbatueshëm ose detyrimi tjetër të së drejtës ndërkombëtare"[20].

2.4. Ligji i përgjegjësisë ndërkombëtare.

Për shkak të natyrës së aktiviteteve aktuale kibernetike, paragrafi i Ligjit të përgjegjësisë ndërkombëtare është jashtëzakonisht i rëndësishëm në Manual. Ai zbaton doktrinën e përgjegjësisë shtetërore, të kodifikuar kryesisht në nenet e Komisionit të së Drejtës Ndërkombëtare mbi përgjegjësinë e shtetit[21], për aktorët kibernetikë dhe aktivitetet kibernetike. Kështu, e drejta e ndërkombëtare e përgjegjësisë shtetërore zbatohet për aktivitetet kibernetike[22]. Si rrjedhim, në rregullin 14 thuhet se "një shtet mban përgjegjësi ndërkombëtare për një akt të lidhur kibernetik që i atribuohet shtetit dhe që përbën shkelje të një detyrimi ligjor ndërkombëtar"[23]. Që një akt kibernetik të jetë një akt ndërkombëtarisht i padrejtë, nuk nevojitet as dëmi fizik dhe as lëndimi, si dhe gjeografia nuk është përcaktuese në caktimin e përgjegjësisë së shtetit[24].

Nën ligjin e përgjegjësisë ndërkombëtare, zë vend edhe koncepti i atributit për aktet kibernetike[25]. Rregullat 15 deri në 17 e trajtojnë këtë çështje në lidhje me operacionet kibernetike. Rregulli 15 vë në dukje se veprimet kibernetike të

[18] Council of Europe: Convention on Cybercrime, ETS 185, 23.XI.2001; Article 22 – Jurisdiction.
[19] Manuali i Talinit 2.0, rregulli 12, faqe 71.
[20] Po aty, rregulli 13, faqe 75.
[21] http://assets.cambridge.org/sample/9780521813532ws.pdf: Responsibility of states for Internationaly wrongful acts; 2002.
[22] Manuali i Talinit 2.0, faqe 80.
[23] Manuali i Talinit 2.0, rregulli 14. faqe 84.
[24] Po aty, faqe 86-87.
[25] Atributi kibernetik është procesi i gjurmimit dhe identifikimit të autorit të një sulmi kibernetik ose të një operacioni tjetër kibernetik.

organeve shtetërore, të tilla si ato ushtarake e të zbulimit, i atribuohen shtetit edhe nëse janë jashtë autoritetit të miratuar ose ligjor të një organizate. Për këtë qëllim, në organet e shtetit gjithashtu do të përfshihen aktorë që nuk janë organe me ligj, por që kanë "varësi të plotë" nga shteti dhe personat ose subjektet që janë të autorizuar të ushtrojnë elemente të autoritetit qeveritar. Në rastin kur një organ i shtetit vihet në dispozicion të një shteti tjetër, nëse ai organ funksionon ekskluzivisht nën kontrollin e shtetit pritës dhe ndërmerr veprime për qëllime dhe në emër të atij shteti, veprimet e organit i atribuohen shtetit pritës[26].

Çështja më e vështirë ligjore në fushën e atributit kibernetik vjen nga aktorët joshtetërorë që mund të punojnë si përfaqësues të një shteti ose që në një farë mënyre veprojnë në emër të një shteti pa autoritet të qartë ligjor për ta bërë këtë. Bazuar në nenin 8 të Përgjegjësisë së shteteve për aktet e padrejta ndërkombëtare"[27], në manual pohohet se "Operacionet kibernetike të kryera nga një aktor joshtetëror i atribuohen një shteti kur: (a) është i angazhuar në përputhje me udhëzimet e tij ose nën drejtimin ose kontrollin e tij; ose (b) shteti pranon dhe miraton operacionet si të tijat"[28].

Rregulli 18 mbulon parimet e mbështetjes, ndihmës dhe përgjegjësinë për veprimet e shteteve të tjera[29]. Në lidhje me mbështetjen dhe ndihmën, është e rëndësishme që shteti të dijë se ai në të vërtetë po ofron mbështetje dhe ndihmë për aktin e padrejtë ndërkombëtarisht dhe se shteti synon ta bëjë këtë. Gjithashtu, është e rëndësishme të theksohet se shteti mbështetës është përgjegjës vetëm për mbështetjen dhe ndihmën dhe jo për aktin e gabuar aktual[30].

Në Manual argumentohet se për aktivitetet kibernetike zbatohen të gjitha rrethanat normale që përjashtojnë gabimin. "Padrejtësia e një akti që përfshin operacionet kibernetike përjashtohet në rastin e: (a) pëlqimit; (b) vetëmbrojtjes; (c) kundërmasave; (d) nevojës; (e) forcave madhore; ose (f) shqetësimit"[31].

---

[26] Manuali i Talinit 2.0, faqe 93.

[27] UN: Draft articles on Responsibility of States for Internationally Wrongful Acts; 2001: "Veprimi i një personi ose grupi personash do të konsiderohet akt i një shteti sipas të drejtës ndërkombëtare nëse personi ose grupi i personave në fakt vepron sipas udhëzimeve ose nën drejtimin e tij, ose kontrollin e atij shteti në kryerjen e veprimit".

[28] Manuali i Talinit 20, rregulli 17, faqe 94.

[29] Manuali i Talinit 2.0, rregulli 18, faqe 100: "Në lidhje me operacionet kibernetike, një shtet është përgjegjës për: (a) mbështetjen ose ndihmën e tij për një shtet tjetër në kryerjen e një akti të gabuar ndërkombëtarisht kur shteti ofron mbëhtetjen ose ndihmën duke ditur për rrethanat e aktit të padrejtë ndërkombëtarisht dhe se akti do të ishte ndërkombëtarisht i gabuar nëse kryhet prej tij; (b) aktin e padrejtë ndërkombëtarisht të një shteti tjetër që ai drejton dhe kontrollon nëse shteti e bën këtë duke ditur rrethanat e aktit të padrejtë ndërkombëtarisht dhe se akti do të ishte i padrejtë ndërkombëtarisht nëse kryhet prej tij; ose
(c) një akt ndërkombëtarisht i padrejtë që detyron një shtet tjetër ta kryejë".

[30] Manuali i Talinit 2.0, faqe 101-102.

[31] Manuali i Talinit 2.0, rregulli 19, faqe 104.

Në Manual trajtohen veçanërisht kundërmasat, të cilat nuk duhet të ngrihen në nivelin e përdorimit të forcës, aktivitetet kibernetike duhet të përshtaten me modelin më të mirëpranuar nga e drejta ndërkombëtare[32]. Është e rëndësishme të theksohet se kundërmasat janë të disponueshme vetëm kundër shteteve dhe nuk do të përjashtojnë paligjshmërinë e një akti nëse drejtohet kundër aktorëve joshtetërorë, veprimet e të cilëve i atribuohen një shteti. Megjithatë, kundërmasa kibernetike nuk duhet të synojë organin specifik të shtetit që po shkel të drejtën ndërkombëtare kur vetë shteti është objektivi[33]. Për më tepër, kundërmasat kibernetike nuk kufizohen në përgjigjen e njëjtë "në natyrë". Pra, një shtet mund t'i përgjigjet një shkeljeje jokibernetike me një kundërmasë kibernetike dhe një shkeljeje kibernetike me një kundërmasë jokibernetike.

Në Manual përcaktohet se kundërmasat kibernetike nuk mund të shkelin një normë urdhëruese. "Kundërmasat, qofshin ato në natyrë kibernetike ose jo, nuk mund të përfshijnë veprime që prekin të drejtat themelore të njeriut, të cilat përfshijnë raprezaljet luftarake të ndaluara, ose shkelin një normë urdhëruese. Një shtet që merr kundërmasa duhet të përmbushë detyrimet e tij në lidhje me paprekshmërinë diplomatike dhe konsullore"[34]. Gjithashu, kundërmasat duhet të jenë proporcionale. "Kundërmasat, qofshin ato në natyrë kibernetike ose jo, duhet të jetë në proporcion me dëmtimin për të cilin ata reagojnë"[35].

Në vijim, Manuali përmban rregulla dhe komente si: mbi efektin e *kundërmasave ndaj palëve të treta,* ku tregohet që "Një kundërmasë, qoftë në natyrë kibernetike ose jo, që shkel një detyrim ligjor që i detyrohet një shteti të tretë ose palës tjetër është i ndaluar"[36]; mbi *justifikimin e domosdoshmërisë*, ku parashikohet se "Një shtet mund të veprojë në përputhje me justifikimin e domosdoshmërisë në përgjigje të akteve që paraqesin një rrezik të rëndë dhe të afërt, qoftë në natyrë kibernetike ose jo, për një interes thelbësor, zbatimi i të cilave është mjeti i vetëm për ta mbrojtur atë"[37]; *mbi detyrimet e shteteve për aktet e paligjshme ndërkombëtare* [(rregulli 27: Ndërprerja, siguritë, garancitë), (rregulli 28*:* Dëmshpërblimi-parimi i përgjithshëm), (rregulli 29: Format e dëmshpërblimit), (rregulli 30: Shkelja e angazhimeve që i detyrohen komunitetit ndërkombëtar në tërësi)][38] dhe një rregull *mbi përgjegjësinë e organizatave ndërkombëtare* (rregulli 31: Parime të përgjithshme)[39].

[32] Michael N. Schmitt: "The Countermeasures Response Option and International Law"; paragrafi I, II, III; Virginia Journal of International Law, 54 (3); 2014.
[33] Manuali i Talinit 2.0, faqe 112-113.
[34] Manuali i Talinit 2.0, rregulli 22, faqe 122.
[35] Manuali i Talinit 2.0, rregulli 23, faqe 127.
[36] Manuali i Talinit 2.0, rregulli 23, faqe 133.
[37] Manuali i Talinit 2.0, rregulli 23, faqe 135.
[38] Manuali i Talinit 2.0, faqe 142-152.
[39] Manuali i Talinit 2.0, faqe 153-157.

2.5. Operacionet kibernetike që nuk rregullohen në vetvete.

Në këtë seksion të Manualit pranohet se disa veprime nga shtetet nuk janë të rregulluara në mënyrë specifike nga e drejta ndërkombëtare, por evidentohet një grup i ngushtë veprimesh që bien në këtë kategori. Rregulli 32 zbatohet për spiunazhin kibernetik në kohë paqeje dhe merr një ton pothuajse mbrojtës. Pa deklaruar faktikisht se spiunazhi kibernetik lejohet nga e drejta ndërkombëtare, rregulli thotë se "edhe pse spiunazhi kibernetik në kohë paqeje nga shtetet nuk cenon në vetvete të drejtën ndërkombëtare, metoda me të cilën kryhet ai mund ta bëjë këtë"[40]. Për qëllime të rregullit, spiunazhi kibernetik përkufizohet si "çdo akt i ndërmarrë në mënyrë klandestine ose nën pretendime të rreme që përdor aftësitë kibernetike për të mbledhur ose tentuar të mbledhë informacion"[41]. Pavarësisht pikëpamjes se nuk ka ndalim në vetvete, pranohet se "spiunazhi mund të kryhet në një mënyrë që shkel të drejtën ndërkombëtare për shkak të faktit se disa metoda të përdorura për të kryer spiunazh kibernetik janë të paligjshme"[42]. Nga trajtimi në manual dhe shtimi i spiunazhit kibernetik, evidentohet se nuk ka një kuptim aktual të qartë lidhur me zbatimin e sovranitetit në fushën e hapësirës kibernetike, gjë që dikton nevojën e saktësimit në kontekstin e të drejtës ndërkombëtare.

Rregulli tjetër në seksionin e operacioneve kibernetike të parregulluara thotë se "e drejta ndërkombëtare rregullon operacionet kibernetike nga aktorët joshtetërorë vetëm në raste të kufizuara"[43]. Me përjashtim të regjimeve të së drejtës ndërkombëtare të zbatueshme në mënyrë specifike për individët, si ligji për të drejtat e njeriut dhe ligji i konfliktit të armatosur, pohohet se e drejta ndërkombëtare nuk rregullon aktorët joshtetërorë[44]. Kjo lihet të rregullohet nga shtetet nëpërmjet ligjit të brendshëm.

3. Regjimet e veçanta të së drejtës ndërkombëtare dhe hapësira kibernetike

Pjesa II përfshin operacionet kibernetike që nuk rregullohen në vetvete nga e drejta ndërkombëtare dhe nëpërmjet 31 rregullave trajtohet zbatimi i regjimeve të veçanta të së drejtës ndërkombëtare (si: ligji ndërkombëtar i të drejtave të njeriut; e drejta diplomatike dhe konsullore; ligji i detit; ligji i ajrit; ligji i hapësirës dhe ligji ndërkombëtar i telekomunikacionit) për aktivitetet kibernetike.

---

[40] Manuali i Talinit 2.0, rregulli 32, faqe 168.
[41] Po aty, faqe 168.
[42] Po aty, faqe 168.
[43] Po aty, rregulli 33, faqe 174.
[44] Po aty, faqe 175.

3.1. Ligji ndërkombëtar i të drejtave të njeriut

Regjimi i parë i veçantë i përfshirë në Manual është ligji ndërkombëtar për të drejtat e njeriut. Rregulli 34, përcakton parimin e përgjithshëm të zbatueshmërisë, ku thuhet se "ligji ndërkombëtar për të drejtat e njeriut është i zbatueshëm për aktivitetet e lidhura me kibernetikën"[45]. Në përcaktimin e zbatueshmërisë, pranohet se "si një parim i përgjithshëm, ligji ndërkombëtar zakonor për të drejtat e njeriut zbatohet në kontekstin kibernetik përtej territorit të një shteti në situatat në të cilat ai shtet ushtron "pushtet ose kontroll efektiv, ashtu siç ai bën në kushtet e tjera normale"[46]. Rregulli 35, nënvizon se "Individët gëzojnë të njëjtat të drejta njerëzore ndërkombëtare si në aspekte të tjera edhe për sa i përket aktiviteteve të lidhura me kibernetikën"[47]. Këtu përfshihen mbrojtja e lirisë së shprehjes, të drejtës për dhënien e një opinioni, të drejtës së privatësisë, konfidencialitetit të komunikimeve, të dhënave mbi jetën private të individit, etj [48].

Në rregullin 36, thuhet se "në lidhje me aktivitetet kibernetike, një shtet duhet:

(a) të respektojë të drejtat ndërkombëtare njerëzore të individëve; dhe

(b) të mbrojë të drejtat njerëzore të individëve nga abuzimi nga palët e treta"[49].

Detyrimi për të mbrojtur ose garantuar respektimin e të drejtave të njeriut zbatohet përgjithësisht për të drejtat e theksuara në rregullin e mësipërm jashtë territorit si të drejta të pranuara dhe është një detyrim afirmativ për shtetet. Rregulli 37, thekson "Detyrimet për të respektuar dhe mbrojtur të drejtat ndërkombëtare të njeriut, me përjashtim të të drejtave absolute, mbeten subjekt i disa kufizimeve që janë të nevojshme për të arritur një qëllim legjitim, jodiskriminues dhe të autorizuar me ligj"[50] Ky rregull pranon se shtetet duhet të vendosin një ekuilibër midis aktiviteteve kibernetike, të drejtave individuale dhe përgjegjësive të tjera të rëndësishme, si rendi publik dhe siguria kombëtare dhe sqaron se "në përgjithësi konsiderohet e nevojshme të kufizohet liria e shprehjes në internet ose e drejta për privatësi me qëllim eliminimin e pornografisë së fëmijëve, shfrytëzimin e fëmijëve, mbrojtjen e të drejtave të pronësisë intelektuale dhe ndalimin e nxitjes së gjenocidit"[51]. Përveç kufizimeve, shtetet mund të bëjnë përjashtime ose lehtësime nga disa detyrime për të drejtat e njeriut. "Një shtet mund të shmangë traktatin për detyrimet e tij për të drejtat e njeriut në lidhje me aktivitetet kibernetike kur

[45] Manuali i Talinit 2.0, rregulli 34, faqe 182.
[46] Po aty, faqe 184.
[47] Po aty, rregulli 35, faqe 187-188.
[48] Po aty, faqe 188-192.
[49] Po aty, rregulli 36, faqe 196.
[50] Po aty, rregulli 37, faqe 201-202
[51] Po aty, faqe 202-203.

lejohet dhe sipas kushteve të përcaktuara nga traktati në fjalë"[52].

3.2. E drejta diplomatike dhe konsullore

Paragrafi mbi të drejtën diplomatike dhe konsullore është bazuar në Konventën e Vjenës e vitit 1961 mbi Marrëdhëniet Diplomatike dhe Konventën e Vjenës e vitit 1963 mbi Marrëdhëniet Konsullore. Rregulli i parë në këtë paragraf pasqyron një nga parimet themelore të së drejtës diplomatike dhe konsullore, paprekshmërinë e ambienteve në të cilat ndodhet infrastruktura kibernetike[53]. Rregulli 40 pohon që "një shtet pritës duhet të marrë të gjitha hapat e duhura për të mbrojtur infrastrukturën kibernetike në mjediset e misionit diplomatik ose postit konsullor të një shteti dërgues kundër ndërhyrjeve ose dëmtimeve"[54]. Zbatimi i këtij rregulli varet nga "madhësia e kërcënimi ndaj objekteve, shkalla në të cilën shteti pritës është në dijeni për një kërcënim specifik dhe kapaciteti i shtetit pritës për të ndërmarrë veprime në këto rrethana".

Rregulli 41 përcakton mbrojtjen e njëjtë të arkivave diplomatike dhe konsullore, dokumenteve dhe korrespondencës zyrtare dhe të versioneve elektronike të tyre. "Arkivat, dokumentet dhe korrespondenca zyrtare të një misioni diplomatik ose konsullor që janë në formë elektronike janë të paprekshme"[55]. Rregulli 42 ka të bëjë me të drejtën e lirisë së komunikimit dhe pohon se "një shtet pritës duhet të lejojë dhe mbrojë komunikimin e lirë kibernetik të një misioni diplomatik ose posti konsullor për të gjitha qëllimet zyrtare"[56]. Në vijim, theksohet që shtetet pritëse "nuk mund të ndërhyjnë me hyrje në faqen e internetit të misionit diplomatik ose postit konsullor që përdoret për të përcjellë informacione thelbësore për qytetarët e tij në vend, për të ndërprerë ose ngadalësuar lidhjen në internet të një misioni diplomatik ose posti konsullor, ose bllokuar se ndërhyrë në telefonat celularë ose pajisje tjera të tyre të telekomunikacionit[57]. Në rregullin 43, trajtohen ambientet dhe personeli diplomatik i shteteve dhe thuhet:

a) lokalet e një misioni diplomatik ose posti konsullor nuk mund të përdoren për t'u përfshirë në aktivitete kibernetike që janë të papajtueshme me funksionet diplomatike ose konsullore, dhe

(b) agjentët diplomatikë dhe zyrtarët konsullorë nuk mund të angazhohen në aktivitete kibernetike që ndërhyjnë në punët e brendshme të shtetit pritës ose janë të papajtueshme me ligjet[58].

[52] Manuali i Talinit 2.0, rregulli 38, faqe 207.
[53] Manuali i Talinit 2.0, rregulli 39, faqe 212, thotë "Infrastruktura kibernetike në ambientet e një misioni diplomatik ose posti konsullor mbrohet nga paprekshmëria e atij misioni ose posti".
[54] Manuali i Talinit 2.0, rregulli 40, faqe 217.
[55] Po aty, rregulli 41, faqe 219.
[56] Po aty, rregulli 42, faqe 225.
[57] Po aty, faqe 225.
[58] Po aty, faqe 227-228.

Në interperetimet për këtë rregull renditen disa aktivitete kibernetike që do të ishin të lejueshme sipas këtij rregulli në një kontekst kibernetik. Por, aty është theksuar se kryerja e spiunazhit kibernetik nuk lejohet. Rregulli 44 ka lidhje me privilegjet dhe imunitetet e personelit diplomatik dhe konsullor[59] dhe arrin në përfundimin se të njëjtat privilegje dhe imunitete zbatohen edhe për aktivitetet e lidhura me kibernetikën.

3.3. Ligji i detit

Bazuar në Konventën e Kombeve të Bashkuara për të Drejtën e Detit, në Manual janë paraqitur 10 rregulla që lidhen me operacionet kibernetike. Rregulli 45 thekson parimin e përgjithshëm të zbatueshmërisë dhe konfirmon se"... operacionet kibernetike në det të hapur mund të kryhen vetëm për qëllime paqësore, përveç rasteve kur parashikohet ndryshe nga ligji ndërkombëtar"[60]. Rregulli 46 thotë "Një anije luftarake ose një anije tjetër e autorizuar sipas rregullave mund të ushtrojë të drejtën e vizitës në bordin e një anijeje, pa pëlqimin e shtetit flamurin e të cilit ajo mban, në det të hapur ose brenda një zone ekonomike ekskluzive nëse ka arsye të pranueshme për të dyshuar se anija po përdor mjete kibernetike për t'u përfshirë në piraterinë, tregtimin e skllevërve ose transmetimin e paautorizuar; ose në bordin e një anijeje që duket se është pa shtetësi ose është e shtetit të anijes vizituese"[61]. Më tej, në Manual konfirmohet zbatimi i standardit të respektimit të duhur ndaj veprimeve kibernetike të ndërmarra në zonën ekonomike ekskluzive [62]. Për sa i përket detit territorial dhe të drejtës së kalimit të pafajshëm, në rregullin 48, thuhet se "në mënyrë që një anije të kërkojë të drejtën e kalimit të pafajshëm përmes detit territorial të një shteti bregdetar, çdo operacion kibernetik i kryer nga anija duhet të jetë në përputhje me kushtet e vendosura për këtë të drejtë[63]. Në lidhje me konfliktin e armatosur ndërkombëtar, në rregullin 49 përcaktohet se "gjatë një konflikti të armatosur ndërkombëtar, një shtet bregdetar neutral nuk mund të bëjë diskriminim ndërmjet palëve ndërluftuese në lidhje me operacionet kibernetike në detin territorial të atij shteti[64]. Rregulli 50 i kthehet rregullave më të përgjithshme dhe ka të bëjë me juridiksionin detyrues në

[59]Manuali i Talinit 2.0, rregulli 44: "Në masën që agjentët diplomatikë dhe zyrtarët konsullorë gëzojnë imunitete nga juridiksioni penal, civil dhe administrativ, ata gëzojnë edhe imunitetet në lidhje me aktivitetet e tyre kibernetike", faqe 230.

[60] Manuali i Talinit 2.0, rregulli 45, faqe 233.

[61] Po aty, rregulli 46, faqe 235.

[62] Manuali i Talinit 2.0, faqe 239: rregulli 47: "Në ushtrimin e të drejtave dhe detyrave të tij, një shtet që kryen operacione kibernetike në zonën ekskluzive ekonomike të një shteti tjetër duhet të ketë detyrim në lidhje me të drejtat dhe detyrat e atij shteti në zonë dhe operacionet kibernetike duhet të kryhen për qëllime paqësore, përveç rasteve kur parashikohet ndryshe nga ligji ndërkombëtar".

[63] Manuali i Talinit 2.0, rregulli 48, faqe 241.

[64] Po aty, rregulli 49, faqe 245.

detin territorial[65]. Të drejtat e detit zbatohen për operacionet kibernetike *në zonën e afërt*, ku përcaktohet se: "Në lidhje me anijet e vendosura në një zonë të afërt të shtetit bregdetar, ky shtet mund të përdorë mjete kibernetike për të parandaluar ose adresuar shkeljet, brenda territorit të tij ose në detin territorial, e ligjeve të tij fiskale, imigruese, sanitare ose doganore, përfshirë shkeljet të kryera me mjete kibernetike"[66]; *në ngushticat e përdorura për lundrim ndërkombëtar*, ku përcaktohet se "Operacionet kibernetike në një ngushticë të përdorur për lundrim ndërkombëtar duhet të jenë në përputhje me të drejtën e kalimit transit"[67]; *në ujërat arkipelagë*, ku përcaktohet se "Operacionet kibernetike në ujërat arkipelagë duhet të jenë në përputhje me regjimin ligjor të zbatueshëm në të"[68] dhe *kabllot nëndetar*, ku përcaktohet se "Rregullat dhe parimet e së drejtës ndërkombëtare të aplikueshëm për kabllot nënujor zbatohen për kabllot e komunikimit nënujor detar"[69].

3.4. Ligji i ajrit

Rregullat për aktivitetin kibernetik në hapësirën ajrore të fluturimit të aviacionit civil ndërkombëtar burojnë nga dispozitat e Konventës së vitit 1944 mbi Aviacionin Civil Ndërkombëtar (ICAO), ose siç njihet "Konventa e Çikagos". Rregulli 55 pasqyron rregullin e zbatueshmërisë së përgjithshme të ligjit të hapësirës ajrore për operacionet kibernetike në avionë në hapësirën ajrore kombëtare[70].

Në ndryshim nga hapësira ajrore kombëtare, operacionet kibernetike në hapësirën ajrore ndërkombëtare përgjithësisht lejohen. Në rregullin 56 thuhet se "Nën kufizimet e përfshira në të drejtën ndërkombëtare, një shtet mund të kryejë operacione kibernetike në hapësirën ajrore ndërkombëtare"[71]. Shtetet nuk mund të pretendojnë sovranitet mbi hapësirën ajrore ndërkombëtare. Për më tepër, kur kryejnë operacione kibernetike në hapësirën ajrore ndërkombëtare, shtetet kanë detyrimin të zbatojnë vetëm kufizimet e përcaktuara në të drejtën ndërkombëtare. Nisur nga rëndësia që ka siguria në aviacion, shtetet janë të

[65] Manuali i Talinit 2.0, rregulli 50: "Një shtet bregdetar mund të ushtrojë juridiksionin detyrues të shoqërimit të anijes në detin territorial në lidhje me aktivitetet kriminale që përfshijnë operacionet kibernetike nëse: pasojat e krimit shtrihen në shtetin bregdetar; krimi është i një lloji që prish rendin dhe sigurinë publike të shtetit bregdetar ose rendin normal të detit territorial; kapiteni i anijes ose shteti, flamurin e të cilit mban anija, ka kërkuar ndihmën e autoriteteve të shtetit bregdetart; ose sipas nevojës për të luftuar trafikun e drogës"; faqe 246.

[66] Manuali i Talinit 2.0, rregulli 51, faqe 248.

[67] Po aty, rregulli 52, faqe 249.

[68] Po aty, rregulli 53, faqe 251.

[69] Po aty, rregulli 54, faqe 252.

[70] Manuali i Talinit 2.0, faqe 261, rregulli 55: "Një shtet mund të rregullojë veprimtarinë e avionëve, përfshirë ato që kryejnë operacione kibernetike, në hapësirën e tij ajrore kombëtare"

[71] Manuali i Talinit 2.0, rregulli 56, faqe 265.

përjashtuar nga kryerja e çdo operacioni kibernetik që mund të rrezikojë sigurinë e aviacionit ndërkombëtar[72].

3.5. Ligji i hapësirës

Pavarësisht mopërcaktimit të saktë të ligjit që rregullon hapësirën ajrore dhe hapësirën (e jashtme), ndryshimet midis këtyre hapësirave janë mjaft të dallueshme, veçanërisht në lidhje me ushtrimin e autoritetit sovran. Rregulli 58 vë në dukje ndryshimin në ndalimet ligjore për përdorimin e kibernetikës në hënë dhe trupa të tjerë qiellorë dhe në hapësirë në përgjithësi. Rregulli thekson: "(a) Operacionet kibernetike në hënë dhe trupa të tjerë qiellorë mund të kryhen vetëm për qëllime paqësore. (b) Operacionet kibernetike në hapësirën e jashtme i nënshtrohen kufizimeve të së drejtës ndërkombëtare për përdorimin e forcës"[73]. Si rezultat i këtij rregulli, aftësitë sulmuese kibernetike nuk mund të vendosen në Hënë, ndërsa në përgjithësi nuk ekziston një ndalim i ngjashëm për hapësirën e jashtme[74].

Rregulli 59 thotë "(a) një shtet duhet të respektojë të drejtën e shteteve të regjistrit për të ushtruar juridiksion dhe kontroll mbi objektet hapësinore që shfaqen në regjistrat e tyre; (b) një shtet duhet të kryejë operacionet e tij kibernetike që përfshijnë hapësirën e jashtme duke pasur parasysh nevojën për të shmangur ndërhyrjen në aktivitetet paqësore hapësinore të shteteve të tjera"[75]. Në përputhje me këtë rregull, shtetet kanë juridiksion mbi satelitët e tyre dhe objektet e tjera hapësinore dhe personat në to, por ky juridiksion mund të mos jetë ekskluziv. Duke respektuar përgjegjësitë e shteteve për aktivitetet kibernetike në hapësirën e jashtme[76], rregulli 60 thotë:

"(a) një shtet duhet të autorizojë dhe mbikëqyrë aktivitetet kibernetike në hapësirën e jashtme të entiteteve të tij joqeveritare dhe

(b) operacionet kibernetike që përfshijnë objekte hapësinore i nënshtrohen regjimit të përgjegjësisë dhe detyrimit të ligjit të hapësirës"[77].

3.6. Ligji ndërkombëtar i telekomunikacionit

Përcaktimi i rregullave të këtij paragrafi është mbështetur në Rregullat e Telekomunikacionit Ndërkombëtar të Bashkimit Ndërkombëtar të Telekomunnikacioneve (ITU), të cilat "vendosin parime të përgjithshme që

[72]Manuali i Talinit 2.0, rregulli 57, faqe 268: "Një shtet nuk mund të kryejë operacione kibernetike që rrezikojnë sigurinë e aviacionit civil ndërkombëtar".

[73] Manuali i Talinit 2.0, rregulli 58, faqe 273.

[74] Manuali i Talinit 2.0, faqe 273-275.

[75] Manuali i Talinit 2.0, faqe 277

[76]UN General Assembly: "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies".

[77] Manuali i Talinit 2.0, rregulli 60, faqe 279-280.

kanë të bëjnë me ofrimin dhe funksionimin e shërbimeve ndërkombëtare të telekomunikacionit të ofruara për publikun, ... mjetet themelore të transmetimit ndërkombëtar të telekomunikacionit që përdoren për të ofruar shërbime të tilla", si dhe "vendosin rregullat e zbatueshme për administratat"[78].

Rregulli 61 thekson se "një shtet duhet të marrë masa për të siguruar krijimin e infrastrukturës ndërkombëtare të telekomunikacionit që kërkohet për telekomunikime ndërkombëtare të shpejta dhe të pandërprera. Nëse, në përputhje me këtë kërkesë, shteti krijon infrastrukturë kibernetike për telekomunikacionet ndërkombëtare, ai duhet ta ruajë dhe mbrojë atë infrastrukturë"[79]. Shtetet në përgjithësi mund të ushtrojnë autoritetin e tyre sovran për të pezulluar ose ndaluar komunikimet. Për këtë, në rregullin 62 thuhet:

"(a) Një shtet mund të pezullojë, pjesërisht ose plotësisht, shërbimet e komunikimit kibernetik ndërkombëtar brenda territorit të tij. Shteteve të tjera duhet t'u jepet njoftim i menjëhershëm për një pezullim të tillë.

(b) Një shtet mund të ndalojë transmetimin e një komunikimi privat kibernetik që duket në kundërshtim me ligjet e tij kombëtare, rendin publik, moralin, ose që është i rrezikshëm për sigurinë kombëtare"[80].

Në rregullin 63 është përcaktuar se "përdorimi i radiostacioneve nga një shtet nuk mund të ndërhyjë në mënyrë të dëmshme në përdorimin e radiofrekuencave të mbrojtura nga shtetet e tjera për komunikime apo shërbime kibernetike me valë"[81]. Ky rregull përfshin ndërhyrjet e shkaktuara nga një shtet në frekuencat e përdorura nga një tjetër, që mundësojnë komunikime ose shërbime kibernetike, kudo që ato komunikime ose shërbime realizohen, duke përfshirë edhe hapësirën e jashtme.

Duke marrë në konsideratë radiostacionet ushtarake, në rregullin 64 thuhet se "një shtet ruan të gjithë lirinë e tij sipas ligjit ndërkombëtar të telekomunikacionit në lidhje me instalimet e radiove ushtarake"[82]. Edhe pse rregulli kufizohet në instalimet e radios, ai gjithashtu përfshin "pajisjet që mundësojnë transmetimin me valë të të dhënave përmes radiovalëve" dhe "zbatohet vetëm për instalimet vërtet "ushtarake" dhe jo radioinstalimet e tjera të vëna në përdorim nga ushtria me një kapacitet të dyfishtë ushtarak dhe civil"[83].

[78] "International Telecommunication Regulations", article 1.
[79] Manuali i Talinit 2.0, rregulli 61, faqe 288.
[80] Manuali i Talinit 2.0, rregulli 62 (a,b), faqe 291.
[81] Manuali i Talinit 2.0, rregulli 63, faqe 294.
[82] Manuali i Talinit 2.0, rregulli 64, faqe 298.
[83] Manuali i Talinit 2.0, faqe 299.

Përfundime

Manuali i Talinit 2.0 paraqet një mori çështjesh ligjore që lindin zakonisht në operacionet kibernetike dhe tregon se si ato bazohen dhe zbatohen në të drejtën ndërkombëtare. Dukuritë e operacioneve kibernetike nuk janë në një vakum ligjor, por i nënshtrohen ligjeve, rregullave dhe parimeve të mirëpërcaktuara. Ky manual pasqyron ligjin ndërkombëtar ekzistues në kontekstin ndaj sfidave të hapësirës kibernetike.

Manuali i Talinit 2.0 ofron orientime, sqaron konceptet ligjore dhe prezanton një kuptim të përbashkët se si ligji ndërkombëtar lidhet me aktivitetet kibernetike, duke shërbyer si një burim dhe kornizë thelbësore për të ndihmuar në administrimin e fushës kibernetike. Ai ofron shpjegime dhe aplikime të sakta të koncepteve aktuale të së drejtës ndërkombëtare në mjedisin e hapësirës kibernetike. Kjo qartësi mundëson që strukturat shtetërore dhe specialistët e ndryshëm të kuptojnë më mirë detyrat dhe të drejtat e tyre në fushën digjitale. Ai, gjithashtu nënvizon rëndësinë e llogaridhënies dhe përgjegjësisë së shtetit për veprimet kibernetike, duke dekurajuar aktivitetet keqdashëse dhe duke promovuar stabilitetin.

Manuali është një mjet me ndikim për këshilltarët ligjorë, ekspertët e politikave që merren me çështjet kibernetike dhe ndihmon strukturat shtetërore dhe vendimmarrësit për një kuptim të përgjithshëm të konsensusit global në lidhje me hapësirën kibernetike dhe për hartimin e politikave dhe akteve të nevojshme ligjore dhe nënligjore. Gjithashtu, u shërben specialistëve të fushës së sigurisë dhe mbrojtjes kibernetike për të përcaktuar masat e nevojshme të lejuara në operacionet kibernetike dhe procedurat e zbatimit të tyre.

Manuali është thelbësor në orientimin e shteteve dhe aktorëve të tjerë drejt një mjedisi kibernetik më të rregulluar dhe më të sigurt në një botë ku kërcënimet kibernetike i tejkalojnë kufijtë gjeografikë. Megjithëse nuk prek të gjitha sfidat në zhvillimin aktual të teknologjisë kibernetike, të tilla si armët kibernetike plotësisht autonome të fuqizuara nga inteligjenca artificiale, ekzistenca e tij nxit diskutime dhe konsiderata për evolucionin e ardhshëm të administrimit të hapësirës kibernetike.

Në kuadër të zbatimit të masave të sigurisë dhe mbrojtjes kibernetike, është e rëndësishme që strukturat dhe specialistët përkatës të njohin, kuptojnë dhe zbatojnë me rigorozitet bazën e duhur ligjore kombëtare dhe ndërkombëtare, konventat, marrëveshjet dhe rregullat e ndryshme në nivel rajonal e botëror mbi operacionet kibernetike.

Literatura e shfrytëzuar:

1. Lynn, William J. (2011, 14 July): Remarks on the Department of Defense Cyber Strategy. Nga: https://www.defense.gov/ speeches/speech. aspx?speechid=1593
2. Manuali i Talinit 2.0; 2017; faqe 11-300.
3. Council of Europe: Convention on Cybercrime, ETS 185, 23.XI.2001; Article 22- Jurisdiction.
4. "Marrëveshja për Statusin e Organizatës së Traktatit të Atlantikut të Veriut, të përfaqësuesve kombëtarë dhe personelit ndërkombëtar", Otava, 19.09.1951;
5. "Marrëveshja ndërmjet palëve të Traktatit të Atlantikut të Veriut për statusin e forcave të tyre", Londër, 19.06.1951.
6. https://www.assets.cambridge.org/sample/9780521813532ws.pdf: Responsibility of states for Internationaly wrongful acts; 2002.
7. UN: Draft articles on Responsibility of States for Internationally Wrongful Acts; 2001.
8. Michael N. Schmitt: "The Countermeasures Response Option and International Law"; paragrafi I, II, III; Virginia Journal of International Law, 54 (3); 2014.
9. UN General Assembly: "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies".
10. International Telecommunication Regulations", article 1.
11. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf: United Nations Convention on the Law of the Sea.
12. Ligji nr.9055, datë 24.4.2003 "Për aderimin e Republikës së Shqipërisë në "Konventën mbi të Drejtën e Detit" të OKB-së.
13. https://www.icao.int/publications/Documents/chicago.pdf: Convention on International Civil Aviation.
14. https://www.itu.int/en/council/Documents/basic-texts/Convention-E.pdf: Convention of the International Telecommunication Union.
15. https://www.assets.cambridge.org/9781107177222_frontmatter.pdf: "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations"; faqe 4-10.

Inteligjenca me burime të hapura (OSINT) për sulmet kibernetike në sektorin e energjisë

Msc. Laureta BETA
Juriste në Drejtorinë e Trajnimit dhe Licencimit në Albcontrol

Trajtesë e shkurtuar.

Në mars 2018, Departamenti i Sigurisë Kombëtare (Department of Homeland Security - DHS) i SHBA-së dhe Byroja Federale e Hetimit (Federal Bureau of Investigation-FBI) lëshuan një alarm të përbashkët kritik (TA18-074A) për një fushatë të vazhdueshme nga aktorë kërcënues rusë që synonte entitetet e qeverisë amerikane dhe sektorët të infrastrukturës kritike. Fushata synonte organizatat e infrastrukturës kritike kryesisht në sektorin e energjisë dhe përdorte, midis teknikave të tjera, Inteligjencën me Burim të Hapur (OSINT) për të nxjerrë informacione. Në një përpjekje për të kuptuar masën dhe cilësinë e informacionit që mund të mblidhet me OSINT, këtu nuk trajtohen aktorët e kërcënimit por trajtohen dhe eksplorohen burimet e disponueshme nga publiku, të cilat mund të ofrojnë e gjenerojnë inteligjencë në lidhje me sistemet e energjisë në çdo vend. Është marrë një rast studimi i një sistemi të vërtetë energjie në shkallë të gjerë, ku shfrytëzohen burimet OSINT për të ndërtuar modelin e sistemit të energjisë, për ta vërtetuar atë dhe në fund, për të identifikuar vendndodhjen kritike të tij. Qëllimi është demonstrimi i fizibilitetit në kryerjen e studimeve të thelluara e të hollësishme, duke shfrytëzuar burimet publike dhe në të njëjtën kohë informimi i palëve të interesuara të sistemit energjetik në vlerësimin e rreziqeve, që vijnë nga ekspozimi i informacionit kritik te publiku.

Fjalë kyçe: OSINT, analizë kontingjenti, sulm kibernetik, modelim sistemi energjetik, vektor sulmi, shodan, zinxhir furnizimi, strategji parandalimi.

Hyrje

Sistemet e energjisë elektrike kanë evoluar ndjeshëm në vite dhe janë bërë thelbësore në jetën tonë të përditshme. Pritshmëria jonë për furnizim të pandërprerë me energji elektrike në përditshmëri ilustrohet më tej nga ndikimi i gjerë që shkaktohet nga ndërprerjet e kësaj energjie. (Shih tab. 1)

Viti	Vendi	Të prekur	Shkaku
2012	India	620 milion	Keqfunksionim
2015	Pakistan	140 milion	Shkatërrim keqdashës
2014	Bangladesh	100 milion	Dështimi i pajisjeve
2009	Brazil & Paraguai	87 milion	Kushtet e këqija të motit
2015	Turqia	70 milion	Mirëmbajtje dhe mbingarkesë
2003	SHBA & Kanada	55 milion	Qark i shkurtër për shkak të pemëve

Tabela 1. Disa nga ndërprerjet më të mëdha/dukshme të energjisë elektrike të fillim-shekullit XXI

Shembujt tregojnë larminë e shkaqeve të mundshme dhe renditen sipas ndikimit të matur të tyre në miliona njerëz të prekur. Shumica e ndërprerjeve të vërejtura deri më sot janë rezultat i defekteve të pajisjeve, fenomeneve natyrore, kafshëve apo dhe të gabimeve njerëzore. Megjithatë, ekziston një shqetësim në rritje në komunitetin ndërkombëtar në lidhje me sulmet kibernetike që synojnë rrjetet e energjisë[1]. Kur diskutohet për sulmet kibernetike ndaj sistemeve kibernetike dhe infrastrukturës kritike, kutia e Pandorës u hap në vitin 2010 me Stuxnet, një pajisje që synon krimbin në një central bërthamor në Iran[2]. Vlerësohet se sulmi i parë kibernetik që synonte sistemet e energjisë është një incident në Ukrainë, raportuar në dhjetor 2015. Sulmi kishte qëllim sistemet kompjuterike të tre ndërmarrjeve të shpërndarjes së energjisë dhe gjykohet të jetë vepër e një aktori shtet-komb[3]. Ndërprerja e energjisë elektrike preku kryesisht rajonin Ivano-Frankivsk, duke lënë pa energji për orë të tëra, rreth 230,000 konsumatorë fundorë[4]. Një sulm i dytë kibernetik në shkallë më të vogël kundër rrjetit të energjisë po në Ukrainë goditi Kievin një vit më vonë, por këtë herë duke synuar rrjetin e transmetimit[5]. Një fushatë e vijuar e Kërcënimit të Avancuar të Vazhdueshëm (Advanced Persistent Threat-APT) në shkallë të gjerë nga aktorët rusë që synojnë sektorët kritikë të infrastrukturës së SHBA

[1] https://doi.org/10.1115/1.2017-Mar-6

[2] Konstantinou C, Maniatakos M (2015) *Impact of firmware modification attacks on power systems field devices*. In: International Conference on Smart Grid Communications. IEEE.

[3] How an entire nation became Russia's test lab for cyberwar?. http://wired.com

[4] https://doi.org/10.1109/SmartGridComm.2015.7436314

[5] Ukraine's power outage was a cyber-attack: Ukrenergo. http://reuters.com

u raportua në mars 2018 nga Departamenti i Sigurisë Kombëtare të SHBA (DHS) dhe Byroja Federale e Hetimit (FBI) në US-CERT Technical Alert 18-074A[6]. Sipas Symantec, i cili ka monitoruar nga afër grupin pas kësaj fushate, sektori i energjisë është objektivi kryesor i fushatës dhe fokusi i sulmit nuk është i kufizuar në SHBA[7]. Për mbledhjen e informacionit gjatë fazës së zbulimit, aktorët e kërcënimit besohet se përdorën disa teknika, duke përfshirë zbulimin me burime të hapura, të njohur gjithashtu si OSINT.

OSINT i referohet të dhënave dhe informacionit të mbledhur dhe analizuar në mënyrë pasive nga burime të disponueshme publikisht dhe mund të përshkruhet si një depo në internet që përfshin një numër të madh mjetesh (aplikacione, shërbime) për të kryer kërkime në burime të hapura informacioni. Funksionon si një skedar që ruan dhe klasifikon mjetet në fjalë që do të përdoren në hetimet OSINT. Këto mjete mund të zbulojnë e mbledhin të dhëna si: emrat e përdoruesve, adresat e postës elektronike, adresat IP, burimet multimedia, profilet në rrjetet sociale, vendndodhja, etj.

Disa nga burimet publike nga ku studiuesit e OSINT mbledhin të dhëna janë: ***motorët e kërkimit në internet*** *si Google, DuckDuckGo, Yahoo, Bing dhe Yandex;* ***mediat e shtypura*** *dhe* ***lajmet online****, përfshi gazetat, revistat, faqet e lajmeve;* ***llogaritë e rrjeteve sociale*** *në platforma të tilla si Facebook, Instagram dhe LinkedIn;* ***forumet online****, blog-et dhe Internet Relay Chats (IRC);* ***web i errët****, një zonë e koduar e internetit që nuk indeksohet nga motorët e kërkimit;* ***drejtoritë online*** *të numrave të telefonit, adresave të e-mailit dhe atyre fizike;* ***të dhënat publike,*** *përfshi lindjet, vdekjet, dokumentet gjyqësore dhe ato të biznesit;* ***të dhënat qeveritare*** *si transkriptet e mbledhjeve, buxhetet, fjalimet, njoftimet për shtyp të bëra nga qeveritë lokale, shtetërore dhe federale/kombëtare;* ***kërkime akademike*** *përfshi gazetat, tezat, revistat;* ***të dhëna teknike*** *si adresat IP, API-të, portat e hapura dhe metadondonet e faqeve të internetit.*

Ndër mjetet më të njohura OSINT përmendim: ***Osintframework.com***-një direktori e gjerë mjetesh dhe burimesh OSINT falas online; ***Maltego***-një zgjidhje në kohë reale për të dhënat në platformat Windows, Mac dhe Linux që ofron përfaqësime grafike të modeleve dhe lidhjeve të të dhënave; ***Spiderfoot***-mjet integrimi i burimit të të dhënave për informacione të tilla si adresa e-email-it, numra telefoni, adresa IP, nëndomen etj.; ***Shodan***-një motor kërkimi për pajisjet e lidhur me internetin që mund të japë informacion mbi metadondonet dhe portat e hapura. Ky mjet mund të identifikojë dobësitë e sigurisë për miliona pajisje, dhe si i tillë ai mund të jetë i dobishëm si për

[6] Symantec: Dragonfly: Western energy sector targeted by sophisticated attack group. http://symantec.com

[7] Siemens: High voltage substation references. http://energy.siemens.com

profesionistët e sigurisë kibernetike, ashtu edhe për cyberkriminals; ***Babel X***-një mjet kërkimi shumëgjuhësh, i mundësuar nga inteligjenca artificiale i aftë për të kërkuar në internet dhe web të errët në më shumë se 200 gjuhë; **Metasploit**-një mjet testimi penetrimi që mund të identifikojë dobësitë e sigurisë në rrjetet, sistemet dhe aplikacionet.

Shkrimi ndërmerr një studim të burimeve publikisht të disponueshme që kanë të bëjnë me sistemet e energjisë, në një përpjekje për të kuptuar masën dhe cilësinë e inteligjencës që mund të gjenerohet me OSINT, si dhe fizibilitetin e ndërtimit të vektorëve të shfrytëzimit bazuar në këto burime. Po kështu në material tregohet zbatueshmëria praktike e studimeve të bazuara në OSINT duke modeluar një rrjet të vërtetë kombëtar të energjisë me përdorimin e burimeve OSINT, si dhe verifikohet modeli duke përdorur burime dytësore dhe duke identifikuar pikat kritike operacionale të modelit përmes studimeve të sigurisë së energjisë. Gjithashtu ofron disa burime publikisht të disponueshme që kanë të bëjnë me sistemet e energjisë. Këto mund të përdoren nëpërmjet teknikave OSINT për të nxjerrë inteligjencë, për identifikimin e pikave kritike operacionale dhe për ndërtimin e vektorëve të sulmit kundër sistemeve të synuara. Po kështu, shkrimi nxjerr në pah rëndësinë e inteligjencës së bazuar në OSINT duke marrë si rast studimi të një sistemi të vërtetë energjie, duke ndërtuar dhe vërtetuar modelin e këtij sistemi dhe duke e analizuar atë për të identifikuar pikat kritike të funksionimit të tij. Duke vlerësuar se një nga arsyet kryesore aktualisht është pasiguria që vërehet midis aktorëve të ndryshëm të industrisë së energjisë, duke përfshirë qeveritë, shitësit dhe ndërmarrjet e energjisë elektrike, në lidhje me kërcënimin real të sulmeve kibernetike ndaj sistemeve të energjisë, shkrimi mund të ndihmojë palët e interesuara të marrin vendime bazuar në informacion, duke rritur ndërgjegjësimin në lidhje me rreziqet e zbulimit të informacionit më shumë se të kërkuar për publikun dhe duke shfaqur implikimet e mundshme të shpërndarjes publike të informacionit të ndjeshëm.

1. Analizat e synimeve dhe metodologjia

Modeli i kërcënimit i supozuar merr në konsideratë kundërshtarët me ekspertizë të lartë të sistemeve të energjisë, objektivi i të cilëve është të shkaktojnë ndërprerje të energjisë në shkallë të gjerë. Supozohet se kundërshtarët nuk kanë domosdoshmërisht baza brenda organizatave të synuara, si dhe nuk kanë as akses fizik në qendrën e kontrollit dhe mbledhjes së të dhënave (SCADA) ose nënstacionet e energjisë. Duke qenë se fokusi është te burimet e disponueshme publikisht për gjenerimin e inteligjencës dhe formulimin e vektorëve të sulmit, grupet kundërshtare të përfaqësuara në këtë model kërcënimi nuk janë të kufizuara brenda një shteti apo nga organizata private/qeveritare dhe janë të financuara shumë mirë.

1.1. Analiza e objektivave strategjikë

Një nga hapat e parë të një fushate është studimi i sistemit të synuar në një nivel të lartë abstraksioni për të kuptuar dhe identifikuar asetet strategjike të interesit[8]. Për fushatat kundër sektorit të energjisë, ky hap ka të bëjë *me identifikimin e shqetësimeve se cilat faza të sistemeve të energjisë apo kombinimi i këtyre fazave* janë më të përshtatshme për arritjen e objektivave të kërkuara.

Në përgjithësi, sistemet energjetike përbëhen nga katër faza: gjenerimi, transmetimi, shpërndarja dhe konsumi. Faza e parë është ***prodhimi***, ku prodhohet energjia elektrike. Ajo më pas transferohet pranë qendrave të konsumit në fazën e ***transmetimit*** dhe shpërndahet te konsumatorët fundorë në fazën e ***shpërndarjes***. Së fundi, energjia elektrike përdoret në fazën e ***konsumit*** nga konsumatorët industrialë, komercialë ose rezidencialë. Për të shkaktuar një ndërprerjeje në shkallë të gjerë të energjisë, faza e konsumit nuk është shumë "tërheqëse"/"e goditur", sepse do të duhej të rrezikohej një numër shumë i madh i konsumatorëve për të arritur rezultatin e kërkuar. Duke përdorur një arsyetim të ngjashëm, kamerat kundërshtare ka të ngjarë të mos synojnë rrjetin e shpërndarjes, sepse sulmi do të kërkonte kompromisin e një numri të madh nënstacionesh të shpërndarjes, ndoshta të kontrolluara nga disa kompani të shërbimeve të energjisë. Faza e prodhimit, në të cilën gjenerohet energjia elektrike mund të jetë një objektiv premtues. Megjithatë, termocentralet janë të drejtuara 24/7 dhe zakonisht përdorin një sërë mekanizmash mbrojtës, duke përfshirë sigurinë fizike, duke i bërë sulmet kundër tyre në mënyrë të dukshme më të vështira. Përveç kësaj, rivendosja e kapacitetit të humbur nga humbjet e gjeneratorëve mund të jetë shumë i shpejtë, siç tregohet nga shpërthimi i Qipros i vitit 2011, i cili shkatërroi 60% të kapacitetit të instaluar të shtetit-ishull[9]. Edhe pse rrjeti i ishullit nuk ishte i ndërlidhur me rrjetet e tjera kombëtare, kërkesa për energji u plotësua në një kohë të shkurtër. Duke marrë parasysh vështirësinë e sulmit dhe shkëmbimet e ndikimit të sulmit, objektivi më tërheqës është rrjeti i transmetimit. Ai plotëson kërkesën e ndikimit në shkallë të gjerë, duke zvogëluar gjithashtu, në të njëjtën kohë, vështirësinë e nisjes së një sulmi. Disa nënstacione të transmetimit janë pa pilot dhe të vendosura në zona të largëta ose në zona të pa populluara.

*1.2. Analiza e objektivave taktik*ë

Pas analizës së objektivit strategjik, analiza e objektivave taktikë mund të identifikojë objektiva *specifik*ë në një sistem energjetik (p.sh., linjat e transmetimit apo nënstacionet) që mund të përmbushin kërkesën për të shkaktuar një ndërprerje

[8] https://doi.org/10.1109/MWSCAS.2016.787000 6

[9] Technavio: *Global smart grid transmission and distribution equipment market 2016–2020*. http://technavio.com

të energjisë në shkallë të gjerë, dhe si të sulmohen këto objektiva. Për një përzgjedhje të suksesshme të objektivit identifikohen dy parakushte. ***Së pari***, kundërshtarët duhet të krijojnë një *model* të sistemit të synuar që mundëson studimin e energjisë dhe të mund të gjenerojë inteligjencë në lidhje me të gjithë sistemin energjetik. ***Së dyti***, modeli i ndërtuar duhet të përpunohet dhe analizohet drejt identifikimit të pikave specifike të interesit, kompromisi i të cilave mund të çojë në një ndërprerje në shkallë të gjerë të energjisë.

Pasi të identifikohen pikat specifike kritike të interesit, duhet të ndërtohen ***vektorët e sulmit*** për shfrytëzimin e këtyre pikave. Për më tepër, kontrolli nëpërmjet sinjaleve rele i CB, lejon kontrollin e qarkun të urdhërojë CB-të e ndryshme të hapen dhe të ndërpresin ose ridrejtojnë rrjedhën e energjisë elektrike. Referuar kritikitetit të tyre, 70% e shqetësimeve të mëdha në SHBA janë të lidhura me funksionimin e gabuar të sinjaleve të CB-ve[10]. Për ndërtimin e vektorëve të sulmit, teknikat OSINT mund të përdoren për të detyruar CB-të të hapin/mbyllnin lidhjet në një sistem objektiv.

1.3. Metodologjia

Në përmbushjen e hapave kundër objektivave në fazën e transmetimit siç identifikohen në analizën e objektivit taktik, kundërshtarët duhet të krijojnë një model përfaqësues të sistemit energjetik, të kryejnë studime të fuqisë mbi modelin për të nxjerrë pikat e tij kritike operacionale dhe në fund të ndërtojnë vektorët e sulmit kundër këtyre pikave specifike. Në këtë çështje, fokusi adresohet në inteligjencën e bazuar në OSINT e cila mund të përdoret drejt arritjes së këtyre hapave, si dhe nënvizohet fakti se aktorët e kërcënimit duhet të shfrytëzojnë çdo mundësi përdorimi të burimeve publikisht të disponueshme për të arritur këtë objektiv. Fillimisht kryhen kërkime të gjera mbi burimet e informacionit mbi sistemet e energjisë të cilat janë të disponueshme për publikun. Burime të tilla mund të ofrojnë informacion të fragmentuar/*të copëzuar* që më pas mund të kombinohet drejt krijimit të modelit/eve të sistemit/ve të energjisë. Më pas, eksplorohen llojet e studimeve të sistemit elektroenergjetik, të cilat janë të nevojshme për identifikimin e pikave kritike operacionale të një sistemi të synuar. Analizat e emergjencës janë të rëndësishme veçanërisht për arritjen e objektivave të tillë si ndërprerjet e energjisë në shkallë të gjerë. Më pas, shqyrtohen burimet OSINT që mundësojnë ose mund të ndihmojnë ndërtimin e vektorëve të sulmit kundër sistemeve të energjisë.

Së fundi, në hetimin e fizibilitetit të shfrytëzimit të inteligjencës OSINT dhe vlerësimin e cilësisë së analizave të mundësuara prej tij, ndërmerret një studim

[10] Lee RM, Assante MJ, Conway T., (2016) Analysis of the cyber-attack on the Ukrainian power grid. Technical report, SANS Industrial Control Systems

i thellë i një rasti të një rrjeti të vërtetë energjie në shkallë të gjerë. Materiali fokusohet duke u mbështetur vetëm në inteligjencën OSINT dhe në bashkimin e informacionit nga një shumëllojshmëri burimesh për të ndërtuar fillimisht të gjithë modelin dhe më pas për ta vërtetuar atë (me burime dytësore OSINT). Duke përdorur mjetet e analizës së emergjencës mbi modelin e ndërtuar, identifikohen gjithashtu pikat kritike të modelit.

2. Burimet OSINT për modelimin e një sistemi energjetik

Këtu ofrohen burime përfaqësuese, jo shteruese, publikisht të disponueshme, të cilat mund të gjenerojnë inteligjencë dhe të ofrojnë informacion të ndjeshëm për sistemet energjetike dhe komponentët e tyre. Duke përdorur OSINT, është e mundur të merret informacioni i kërkuar për të modeluar një sistem energjetik, duke mundësuar analiza taktike të objektivave përmes studimeve të fuqisë në modelin e ndërtuar.

a. Bazat e të dhënave të sistemeve energjetike. Disa baza të të dhënave të sistemeve energjetike janë të disponueshme publikisht, duke ofruar akses në të dhënat që lidhen me sistemet reale në të gjithë globin. P.sh., platforma e të Dhënave të Hapura të Sistemit të Energjisë (Open Power System Data) ofron të dhëna në lidhje me termocentralet, kapacitetet gjeneruese dhe ngarkesat për disa sisteme energjetike evropiane[11]. Një burim tjetër i të dhënave është Rrjeti Evropian i Operatorëve të Sistemit të Transmetimit të Energjisë Elektrike *(European Network of Transmission System Operators for Electricity -ENTSO-E)*, i krijuar si një përpjekje për të siguruar funksionimin optimal të tregut të brendshëm të energjisë të BE-së. Të dhënat përfshijnë hartat e rrjeteve të transmetimit, detajet e ndërlidhjes së rrjetit, flukset ndërkufitare në kohë reale, ngarkesat historike dhe të parashikuara dhe statistikat e gjenerimit, si dhe planet e zhvillimit[12]. Në SHBA, Open Energy Information (OpenEI) është një faqe interneti bashkëpunuese e qeverisë që ofron akses publik në të dhënat e energjisë[13]. Në shkallë botërore, baza e të dhënave semantike *Enipedia* përmban shumë të dhëna për ngarkesën, gjenerimin, topologjinë dhe karakteristikat e linjës për sistemet e energjisë në të gjithë globin[14].

b. Sistemet e informacionit gjeografik. Topologjia e një sistemi elektroenergjetik mund të ndërtohet ose vërtetohet duke vëzhguar komponentët fizikë të sistemit dhe ndërlidhjet e tyre. Në vend të gjurmimit në terren të strukturave fizike, është e mundur të gjenerohet topologjia e rrjetit të një sistemi duke përdorur

[11] Open power system data platform. http://open-power-system-data.org
[12] European network of TSOs for electricity. http://entsoe.eu
[13] Open energy information. http://openei.org
[14] Davis CM, Overbye TJ. (2011) *Multiple element contingency screening*. Trans Power Syst 26(3):1294–1301

imazhe satelitore nga Sistemet e Informacionit Gjeografik (*Geographic Information System-GIS)*. Kjo mundëson kryerjen e një analize të një sistemi, gjë e cila mund të kryhet nga distanca. Shembuj të komponentëve të sistemit të energjisë siç paraqiten në një GIS jepen në figurë. Informacioni i vendndodhjes së strukturave fizike të fuqisë nuk mund të fshihet nga satelitët në orbita ose nga avionët e fotografimit ajror, përveç rasteve të kabllove nëntokësore.

Megjithatë, pjesa më e madhe e linjave të transmetimit nuk janë nën tokë por janë mbi tokë[15]. Gjetja e topologjisë së një sistemi energjetik me GIS mund të automatizohet përmes teknikave të mësimit të makinerive dhe përpunimit të imazhit. Rrjetet e energjisë të nënprojektit OpenStreetMap ndjekin këtë qasje[16].

c. Raportet publike. Shpeshherë ndërmarrjet energjetike, Operatorët e Sistemit të Transmetimit (OST) ose agjencitë qeveritare botojnë raporte për publikun që *përmbajnë detaje operacionale dhe informacion* në lidhje me sistemin/et e tyre energjetik/e. Këto dokumente mund të jenë në formën e raporteve të cilat i kërkon ligji, raporteve financiare vjetore për aksionarët dhe deklaratave që përshkruajnë kërkesat e ardhshme dhe mënyrën se si ato do të përmbushen.[17] [18]

Në mënyrë ironike, raportet e ndërprerjeve të energjisë mund të përmbajnë gjithashtu informacione të ndjeshme në lidhje me një sistem energjie. Këto raporte ndërprerje i bëhen me dije publikut, kryesisht për arsye transparence dhe zakonisht përmbajnë detaje teknike në një përpjekje për të identifikuar dhe shpjeguar burimin e ndërprerjes. Për më tepër, raportet nga iniciativat që synojnë të rrisin elasticitetin e rrjetit të energjisë dhe të përshpejtojnë modernizimin e rrjetit mund të përmbajnë informacione që lidhen me sistemet specifike të energjisë. P.sh., faqja e internetit e Iniciativës së SynchroPhasor të Amerikës së Veriut (North American SynchroPhasor Initiative-NASPI) përfshin një raport që liston vendndodhjen gjeografike të njësisë matëse të fazorit *(Phasor Measurement Unit-PMU)* në SHBA[19]. PMU ose sinkrofasor, është një mjet kyç i përdorur në sistemet elektrike për të përmirësuar dukshmërinë e operatorëve ndaj asaj që po ndodh në të gjithë rrjetin. Një PMU është një pajisje që mat një sasi të quajtur fazor. Një fazor tregon madhësinë dhe këndin e fazës për tensionin ose rrymën në një vend të caktuar në një linjë elektrike. Ky informacion mund të përdoret gjithashtu për të përcaktuar frekuencën dhe është i dobishëm për identifikimin dhe analizimin e kushteve të sistemit.

---

[15]Alonso F, Greenwell C (2016) *Underground vs. Overhead: power line installation-cost comparison and mitigation*. Electr. Light Power 22

[16] OpenStreetMap: Power networks. http://openstreetmap.org

[17] U.K. Electricity Ten Years Statement 2016. http://nationalgrid.com

[18] Eles: *Slovenia's transmission network: annual report 2015*. http://eles.si

[19] Map of PMUs with synchrophasor data flows in North America. http://naspi.org

d. Deklarata për shtyp. Kundërshtarët mund të nxjerrin informacion në lidhje me një sistem energjetik dhe nga informacioni i publikuar në shtyp. Një informacion i tillë mund të jetë në formën e buletineve, njoftimeve për shtyp nga operatorët e sistemit energjetik, histori suksesi nga shitësit të cilët kanë instaluar komponentët e sistemit, prezantime të korporatave, etj. Disa shembuj përfshijnë qendrat mediatike të shitësve që përfshijnë referenca për të shpërblyer, përfunduar dhe projekte në vazhdim[20], raporte nga ofruesit e zgjidhjeve "me çelës në dorë" ku renditen informacionet mbi nivelet e tensionit dhe linjat e transmetimit[21] dhe historitë e suksesit të shitësve që zbulojnë protokollet e komunikimit dhe topologjinë e sistemit[22]. Burimet e mësipërme, si dhe informacioni shtesë që mund të mblidhet përmes kanaleve të tjera OSINT apo përmes teknikave të tjera si dhe burimeve jopublike, mund të shkrihen për të krijuar një model të një sistemi energjetik. Informacioni mund të përdoret për të nxjerrë topologjinë e sistemit dhe për të vlerësuar karakteristikat operacionale për kryerjen e studimeve të fuqisë. Për më tepër, informacioni nga burime të ndryshme mund të krahasohet dhe për të vlerësuar saktësinë e modelit të ndërtuar.

3. Studimet e sistemit energjetik: Analiza e kontingjenteve

Modelimi i një sistemi energjetik mundëson kryerjen e studimeve të fuqisë në sistem. Studime të ndryshme të fuqisë mund të jenë të nevojshme për objektiva të ndryshëm të fushatës. Për fushatat që synojnë të prishin sistemin dhe të shkaktojnë ndërprerje, studimet e që lidhen me sigurinë e sistemit energjetik mund të ofrojnë informacion të vlefshëm për kundërshtarët se cilët objektiva specifikë janë të nevojshëm dhe të mjaftueshëm për të destabilizuar të gjithë sistemin. Siguria e sistemit energjetik përkufizohet si probabiliteti i pikës së funksionimit të sistemit për të qëndruar brenda intervaleve të pranueshme duke pasur parasysh kufizimet e sistemit, probabilitetet e ndryshimeve (kontigjencat) dhe mjedisin e tij[23]. Analiza e kontigjencës është një operacion i mirënjohur në Sistemet Moderne të Menaxhimit të Energjisë (EMS), i cili i siguron operatorit të sistemit informacionin e nevojshëm për sigurinë statike të sistemit. Në kontrast me vlerësimin e gjendjes, i cili konsiderohet një aplikim në internet, analiza e kufizuar e rasteve është një aplikacion *offline* për planifikimin dhe funksionimin e sistemit të energjisë[24]. Në mënyrë abstrakte, analiza e emergjencës mund të shihet si një simulator i skenarit "po sikur" që

[20] Siemens: High voltage substation references. http://energy.siemens.com
[21] SCADA Innovations: Success stories. http://scadainnovations.com
[22] ProSoft Technology: Power success stories. http://prosoft-technology.com
[23] Morison K, Wang L, Kundur P (2004) *Power system security assessment.* Power Energy Mag 2(5):30–39
[24] Pajic S (2007) *Power system state estimation and contingency constrained optimal power flow: a numerically robust implementation.* Worcester Polytechnic Institute

vlerëson, prodhon dhe rendit ndikimin e ngjarjeve të paplanifikuara në një sistem energjetik. P.sh., një emergjencë mund të jetë dështimi ose humbja e një elementi të sistemit (p.sh., gjeneratori, transformatori, linja e transmetimit), ose hapja e paplanifikuar e një ndërprerësi qarku (*Circuit Breakers-CB*). Këto ngjarje formojnë listën e emergjencës, e cila më pas përdoret nga algoritmet e analizës së emergjencës për të vlerësuar efektet në sistemin e përgjithshëm. Objektivi i analizës së rrjedhës së fuqisë është të përftojë një sërë madhësish dhe këndesh të tensionit për çdo element në sistemin energjetik që korrespondon me një ngarkesë të caktuar dhe gjendjen e gjenerimit. Më pas, flukset e fuqisë aktive dhe reaktive në secilën degë dhe gjenerator përcaktohen në mënyrë analitike. Humbja ose dështimi i çdo ngjarje emergjente simulohet në modelin e rrjetit duke hequr atë pjesë nga sistemi i simuluar i energjisë. Modeli i rrjetit që rezulton zgjidhet për të llogaritur rrjedhat e fuqisë, rrymat dhe tensionet përkatëse për elementët e mbetur. Veçanërisht që një model sistemi energjie të jetë i mjaftueshëm për analiza të paparashikuara, kërkohen këto të dhëna[25]: topologjia e sistemit (skajet: linjat e transmetimit / transformatorët, nyjet: elementet fundore); parametrat e linjës së transmetimit; vendndodhjet dhe vlerësimet e linjës; parametrat e transformatorit dhe të ndërrimit të fazave; vendndodhja, vlerësimet dhe kufijtë e gjeneratorëve; vendndodhja e ngarkesës dhe kompensimi i ngarkesës.

Në përgjithësi, sistemet e energjisë duhet të jenë në gjendje të mbajnë një kusht të vetëm emergjence (N-1) për të mundësuar operacionet e mirëmbajtjes, ku N është numri i komponentëve (zakonisht N-degët e një rrjeti). Korporata e Besueshmërisë Elektrike e Amerikës së Veriut (North America Electric Reliability Corporation-NERC) dhe agjencitë e tjera rregullatore zbatojnë standarde strikte të sigurisë së energjisë që kërkojnë që operatorët e sistemit të energjisë të plotësojnë kufizimin e sigurisë N-1. Standardet NERC kërkojnë gjithashtu që operatorët të sigurojnë performancë të mjaftueshme të sistemit në raste të disa situatave të paparashikuara. Megjithatë, problemi i identifikimit të rastësive mbetet sfidues për shkak të numrit total të ngjarjeve të mundshme iniciuese: ai rritet në mënyrë eksponenciale si rezultat i numrit të elementeve që shkaktojnë ndërprerjen.

4. Ndërtimi i vektorëve të sulmit me OSINT

Duke pasur njohuri për pikat kritike të një sistemi energjetik nga hapat e modelimit dhe analizës, kundërshtarët duhet të gjejnë pikat hyrëse të sulmit dhe të ndërtojnë vektorë sulmi kundër sistemit.

[25]Grainger J, Grainger W, Stevenson W., (1994) *Power system analysis*. McGraw-Hill Education, New York

Më konkretisht, ata duhet të krijojnë mjete drejt shkyçjes së linjave kritike të transmetimit të afta për një skenar të paqëndrueshëm emergjence, pasi ato identifikohen duke përdorur teknikat e përshkruara më poshtë. Këtu ofrohen burime përfaqësuese, por jo shteruese të informacionit publik që mund të shfrytëzohen drejt këtij objektivi nëpërmjet analizës OSINT.

Rrjeti: Një pikë e mundshme hyrëse është ajo mbi rrjet. Mund të disponohen kanale të drejtpërdrejta të rrjetit në pajisjet industriale në vendet e synuara të identifikuara përmes internetit publik. Për këtë qëllim, mund të përdoret *Shodan*[26]. Shodan përdor "zvarritës" *(metadata* që serveri i dërgon përsëri klientit) që indeksojnë periodikisht web-in, duke kërkuar për porta të hapura dhe një shumëllojshmëri të gjerë protokollesh me përfshirje të disa prej tyre.

Protokoll	Porta	Pajisjet e indeksuara
DNP3	20000	341
Modbus	502	13575
IEC 104	2404	445
IEC 61850	102	161

Tabela 2: Pajisjet e rrjetit elektrik të lidhur në internet të indeksuara nga Shodan

Shodan është një motor kërkimi që lejon përdoruesit të kërkojnë lloje të ndryshme serverësh (webcam, router, server etj.), të lidhur me internetin duke përdorur një sërë filtrash; është një bazë të dhënash me miliarda adresa IP të disponueshme publikisht dhe përdoret, për të analizuar sigurinë e rrjetit, nga ekspertët e sigurisë. Ky mund të jetë informacion rreth softuerit të serverit, ose rreth opsioneve që mbështet shërbimi, ose një mesazh mirëseardhjeje apo çdo gjë tjetër që klienti mund të zbulojë përpara se të ndërveprojë me serverin. Përdoruesit mund të kryejnë një kërkim, me Shodan, bazuar në një adresë IP, emrin e pajisjes, qytetin dhe/ose një sërë kategorish teknike.

Tabela 2 është një fotografi e pajisjeve të indeksuara nga *Shodan* për katër protokollet kryesore më të përdorura në industrinë e energjisë (marrë në 30.03.2018). Për të siguruar rezultate efikase, është e mundur që sulmuesit të lëshojnë "*zvarritësit*" e tyre. Lëshimi i mjeteve efikase të skanimit me burim të hapur si ZMap, i cili mund të skanojë të gjithë gamën e IPv4 në pak minuta, mundëson skanime në shkallë të gjerë të internetit me burime të kufizuara. Studimet e teleskopit të rrjetit të fokusuara në protokollet industriale kanë treguar se disa fushata skanimi synojnë në mënyrë specifike protokollet industriale që përdorin këto mjete. Situata përkeqësohet më shumë duke marrë në konsideratë sigurinë e dobët që përdorin shumica e protokolleve

[26] Shodan search engine. http://shodan.io

industriale, duke lejuar akses të paautorizuar[27]. Për të nxjerrë IP-të me interes nga grupi i rezultateve, sulmuesit mund të identifikojnë organizatën që kontrollon vendndodhjet e synuara (p.sh., njësia e energjisë elektrike ose organizata qeveritare) dhe të gjejnë adresat IP që lidhen me organizatën përmes kërkimeve të kundërta WHOIS. Të gjitha adresat IP që i përkasin organizatës janë pika të mundshme hyrjeje; dhe kompromet imi i tyre mund të mundësojë hyrjen brenda rrjetit të organizatës. Rezultatet më premtuese qëndrojnë në kryqëzimin midis IP-ve në pronësi të kompanisë dhe pajisjeve industriale të indeksuara nga fushatat e skanimit. Me adresën IP publike të një pajisjeje të njohur, sulmuesit mund të përdorin teknika të ndryshme për të identifikuar specifikat e pajisjes industriale[28].

Shitësi	**Listimet**
ASEA Brown Boveri (ABB)	216
General Electric (GE)	458
Schneider elektrike	373
Siemens	271

Tabela 3. Statistikat e listimit të eBay në lidhje me pajisjet e rrjetit të energjisë, nga katër shitësit kryesorë, të aktivizuar nga mikroprocesorët, me pjesën më të madhe të tregut, (30 mars 2018).

Zinxhiri i furnizimit. Kur dihet informacioni specifik i markës dhe modelit për pajisjet e synuara, sulmuesit mund të kryejnë studime specifike për pajisjen. Për këtë qëllim, një opsion i mundshëm për një sulmues është të marrë një kopje fizike të pajisjes së synuar për eksperimente të mëtejshme praktike. Me akses në kopjet fizike të pajisjeve të sistemit të energjisë, sulmuesi mund të vërtetojnë dobësitë e njohura dhe të testojë strategjitë e sulmit të zhvilluara për të rritur probabilitetin e suksesit gjatë sulmit përfundimtar. Përveç shitësve zyrtarë, tregjet online si *eBay*, *Amazon*, *Alibaba* dhe kompani të tjera të palëve të treta ofrojnë pajisje industriale të përdorura ose të reja për shitje. Shumica e tyre kanë të bëjnë me pajisje të tepërta ose të çmontuara, të shitura zakonisht me një çmim më të ulët se çmimi origjinal.

Raportet e cenueshmërisë. Bazat e të dhënave të dobësive të disponueshme publikisht, të tilla si: këshillimet dhe sinjalizimet e Ekipit të Reagimit të Emergjencave Kibernetike të Sistemeve të Kontrollit Industrial *(Industrial Control Systems Cyber Emergency Response Team-ICS-CERT)*, dhe Baza Kombëtare e të Dhënave të Cenueshmërisë *(National Vulnerability Database-*

[27]Igure VM, Laughter SA, Williams RD. (2006) *Security issues in SCADA networks*. Compute Secure 25(7):498–506

[28]Keliris A, Maniatakos M. (2016) *Remote field device fingerprinting using device-specific Modbus information*. In: 2016 IEEE 59th international Midwest symposium on circuits and systems (MWSCAS), pp 1-4. https://doi.org/10.1109/MWSCAS.2016.7870006

NVD) mund të ofrojnë një burim publik për dobësitë për pajisjet e synuara[29]. Baza e të dhënave të tilla përditësohen vazhdimisht me dobësi të zbuluara në pajisjet industriale, duke përfshirë këtu dhe pajisjet e sistemit të energjisë.

Zhvillimi i cenueshmërisë Në rast se nuk ekzistojnë dobësi të njohura, ose objektivat e një sulmi nuk mund të përmbushen me dobësitë e njohura, kundërshtarët mund të zhvillojnë dobësitë e tyre të ditës zero. Kjo qasje kërkon më shumë burime, por nga njëra anë ka një probabilitet më të lartë suksesi dhe nga ana tjetër ka një probabilitet më të ulët zbulimi. Për ta arritur këtë, sulmuesit mund të ndjekin disa strategji. Me akses në një pajisje fizike, ata mund të nxjerrin firmuerin e pajisjes dhe ta analizojnë atë për dobësi, të monitorojnë trafikun e rrjetit të shkëmbyer në kërkim të dobësive në grupin e rrjetit dhe të ekzaminojnë softuerin e konfigurimit për pikat hyrëse të sulmit.

(Firmueri është një klasë specifike e softuerit kompjuterik që siguron kontrollin e nivelit të ulët për harduerin specifik të një pajisjeje. Firmueri, si BIOS-i i një kompjuteri personal, mund të përmbajë funksionet bazë të një pajisjeje dhe mund të ofrojë shërbime të abstraksionit të harduerit për softuerët e nivelit më të lartë si sistemet operative. Për pajisjet më pak komplekse, firmueri mund të veprojë si sistemi i plotë operativ i pajisjes, duke kryer të gjitha funksionet e kontrollit, monitorimit dhe manipulimit të të dhënave)[30]. Disa artikuj të disponueshëm publikisht, që përshkruajnë qasjet dhe teknikat hap pas hapi për hakerimin e sistemeve të integruara dhe pajisjeve të Internetit të Gjërave (IoT) përmbajnë njohuri që transferohen drejtpërdrejt në pajisjet e sistemit të energjisë, p.sh., kopjet e imazheve të firmuerit mund të merren nga faqet e internetit të shitësve. Nëse kjo nuk është e mundur, ose nëse firmueri është i koduar, ai mund të hidhet drejtpërdrejt nga pajisja fizike nëpërmjet portave të korrigjimit, ose të nxirret nga memoria flesh e pajisjes duke përdorur teknikat e mjekësisë ligjore me çip-off[31].

Projektet me burime të hapura *(Open source projects).* Nga një vëzhgim i nxjerrë nga analiza e mësipërme rezulton se ekziston një bollëk i softuerit me burim të hapur që mund të luajë një rol mundësues gjatë dizajnimit të një sulmi. Pjesa më e madhe e këtij softueri është krijuar për përdorime të mira (p.sh., grumbullimi i statistikave, edukimi, testimi), por ai mund të keqpërdoret nga kundërshtarët me agjenda keqdashëse. Ky është rasti për fushatën e vazhdueshme kundër infrastrukturës kritike të SHBA-së, ku përdoren mjete me kod të hapur[32]. Përveç rolit të drejtpërdrejtë mundësues të projekteve me

[29]Industrial Control Systems Cyber Emergency Response Team. http://ics-cert.us-cert.gov
[30] https://sq.wikipedia.org/wiki/Firmueri
[31] https://doi.org/10.1109/SmartGridComm.2015.7436314
[32] U.S. DHS and FBI: US-CERT: advanced persistent threat activity targeting energy and other critical infrastructure sectors. http://us-cert.gov/ncas/alerts/TA18-074A

burime të hapura, mjetet dhe bibliotekat me burime të hapura mund të bëhen pika hyrëse të sulmit. Kundërshtarët mund të kontribuojnë në projektet me burim të hapur që ata e dinë se përdoren nga organizata e synuar (p.sh., një projekt i tillë i përdorur gjerësisht në industrinë e energjisë është openSCADA. *(OpenSCADA është një zbatim i hapur i sistemeve SCADA (Kontrolli i Mbikëqyrës dhe Blerja e të Dhënave-Supervisory Control and Data Acquisition) dhe ndërfaqes njeri-makinë-(Human-Machine Interface-HMI)*[33]. Të fshehura brenda përditësimeve, ato mund të injektojnë kode me qëllim të keq apo e thënë ndryshe "dyer të pasme".

5. Vlerësimi eksperimental i teknikave OSINT

Për të vlerësuar në mënyrë eksperimentale ndikimin dhe cilësinë e informacionit të gjeneruar me teknikat OSINT, zakonisht përdoret një qasje OSINT, për të ndërtuar një model të një sistemi të madh, real dhe për ta analizuar atë me teknikat e analizës së emergjencës, në mënyrë që të identifikohen pikat e tij kritike të funksionimit. Kompromet imi apo kontrolli nga kundërshtari i këtyre pikave është i mjaftueshëm për të krijuar një ndërprerje të gjerë të sistemit.

5.1. Modelimi i një sistemi real energjie

Në këtë punim paraqiten informacione anonime dhe jo identifikuese, për shkak të ndjeshmërisë së trajtesës. Sistemi në këtë material do të referohet si Toka e Ndërprerë (*Outage Land*). Teknikat OSINT përdoren për të gjeneruar modelin e Tokës së Ndërprerë, duke identifikuar disa burime informacioni për sistemin energjetik, përfshi prezantimet e korporatave të disponueshme publikisht, raportet e planifikimit të zgjerimit dhe historitë e suksesit të shitjeve. Nga këto burime publike fillimisht nxirren të gjithë pikat/gjurmët e tensionit të lartë dhe lidhjet ndërmjet tyre, si dhe vendndodhjen e nënstacioneve të transmetimit dhe gjenerimit.

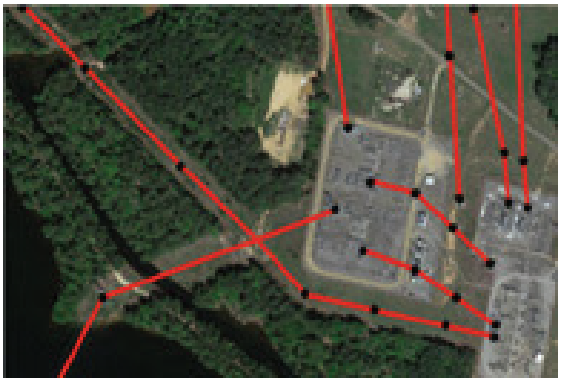

Figura. 1. Gjurmimi i linjave të transmetimit në shërbimet GIS

[33] Reimann J, Rose J (2015) *Eclipse SCADA: the definite guide*

Nëpërmjet kësaj analize krijohet një hartë topologjike të sistemit. Pas saj verifikohen topologjia e ndërtuar përmes shërbimeve GIS, duke gjurmuar manualisht linjat e tensionit të lartë dhe shtyllat e transmetimit në të gjithë Tokën e Ndërprerë. Figura 2 tregon një shembull të një impianti gjenerimi, një nënstacioni transmetues dhe linjat hyrëse/dalëse të transmetimit. Kullat e transmetimit përshkruhen si pika të zeza dhe linjat e transmetimit si vija të kuqe. Përmes shërbimeve GIS, ndërmerret procesi i mundimshëm manual i gjenerimit të topologjisë së të gjithë rrjetit të transmetimit të Tokës së Ndërprerë dhe ky krahasohet me topologjinë e nxjerrë përmes burimeve të tjera publike.

Hartëzimi nëpërmjet Sistemit të Informacionit Gjeografik (*GIS*), për të gjithë sistemin, kërkon rreth dy ditë punë. Edhe pse ky proces mund të jetë i automatizuar, ne nuk e bëjmë këtë për shkak të Termave dhe Kushteve kufizuese të softuerit komercial GIS që nuk lejojnë nxjerrjen automatike të imazheve satelitore. Për të mundësuar studimet e paparashikuara të Tokës së Ndërprerë nevojitet përsëri mbështetja në teknikat OSINT për nxjerrjen e karakteristikave operacionale të sistemit energjetik. Pas kësaj bashkohet informacioni nga burime të ndryshme, për të identifikuar nivelet e tensionit, detajet e instaluara të gjenerimit, karakteristikat e linjës së transmetimit dhe vlerësimet e ngarkesës.

6. Diskutim

Ky material konsideron se kërcënimi kibernetik kundër sistemeve të energjisë është i nënvlerësuar, pasi shërben si një provë e konceptit që sulmet mundësohen nga burimet e shumta publike të informacionit. Por duhet pasur parasysh elasticiteti dhe qëndrueshmëria e rrjeteve të energjisë, si dhe gatishmëria dhe përvoja e inxhinierëve të energjisë në trajtimin e ndërprerjeve të energjisë. Vetëm në SHBA, në vitin 2016, u raportuan 3879 ndërprerje, duke zgjatur mesatarisht vetëm 48 minuta dhe duke prekur pothuajse 18 milionë njerëz në të gjithë vendin, duke shkaktuar një humbje vjetore monetare prej 150 miliardë dollarë[34]. Në gjithë botën, ndërprerjet e energjisë janë një dukuri e zakonshme e shkaktuar zakonisht nga fenomene të motit, aksidente, kafshë, dështime të pajisjeve etj. Si pasojë, operatorët e sistemit energjetik kanë përvojë në trajtimin e skenarëve të ndërprerjeve të energjisë. Për më tepër, industria energjetike dhe palët e interesuara të qeverisë kanë stimuj të drejtpërdrejtë financiarë, përveç detyrimeve shoqërore për të drejtuar përpjekjet dhe financimin në mekanizmat e parashikimit dhe parandalimit të ndërprerjeve të energjisë, dhe sigurimin e periudhave më të shkurtra të rikuperimit.

Objekti i shkrimit është trajtimi i modelit të kërcënimit, për shkaktimin e një ndërprerjeje të gjerë të energjisë elektrike, e cila nuk është e njëjtë me një

[34] Eaton: *Blackout tracker* (2017) United States annual report 2016

ndërprerje të zgjatur të energjisë. P.sh., ndërprerjet e gjata mund të kërkojnë shkatërrimin ose paaftësimin e pajisjeve kritike që nuk janë në gjendje (p.sh., transformatorët dhe gjeneratorët), diçka që zakonisht kërkon ndërhyrje fizike. Në përgjithësi, shpërndarja në publik e informacionit dhe transparenca janë të dobishme për progresin. Qëllimi i shkrimit nuk është kufizimi i nxjerrjes e informacionit, duke i konsideruar të gjitha informacionet e rrjetit të energjisë elektrike si të klasifikuara, por përkundrazi, synohet të nxirret në pah ndjeshmëria e pjesëve të caktuara të informacionit që mund t'iu bëjë të mundur kundërshtarëve keqdashës të nisin sulme kibernetike kundër një sistemi energjetik si dhe të ndihmohet të kuptohet më mirë informacioni publik në lidhje me ndjeshmërinë e këtyre sistemeve.

6.1. Pse informacioni i ndjeshëm është i disponueshëm publikisht?

Në rastin e identifikimit të vendndodhjes së aseteve të sistemit elektroenergjetik përmes GIS, ka rrjedhje të paqëllimshme të informacionit për shkak të natyrës së teknikave të hartës satelitore. Vlerësimet e gabuara të rrezikut nga operatorët e sistemit energjetik mund të rezultojnë gjithashtu në nxjerrjen e informacionit të ndjeshëm. Informacioni mund të rrjedhë nga palë të treta, të tilla si shitësit e pajisjeve të sistemit të energjisë, kur ata publikojnë histori suksesi që përfshijnë detaje operacionale të sistemeve reale. Përndryshe, informacioni mund të publikohet qëllimisht. Duke pasur parasysh varësinë e fortë të vendeve nga furnizimi me energji elektrike, industria e energjisë shpesh konsiderohet pjesë e infrastrukturës së shërbimeve publike. Edhe në rastet kur ndërmarrjet energjetike janë korporata private, ato rregullohen nga komisionet e shërbimeve publike. P.sh., në SHBA, Komisioni Federal i Rregullatorit të Energjisë *(FERC)* rregullon të gjitha kompanitë e shërbimeve të energjisë. Si ndërmarrje publike, disa nga detajet në lidhje me funksionimin e sistemeve energjetike, duhet të jenë transparente për qytetarët, në disa raste të mandatuara me ligj. P.sh., në disa juridiksione duhet të jepen detaje operacionale dhe procedurale për të justifikuar tarifat e çmimit të energjisë[35]. Qeveria po kështu mund të kërkojnë publikimin e të dhënave për të siguruar transparencë dhe konkurrencë të ndershme mes kompanive private të cilat mund të publikohen drejt promovimit të një rrjeti energjie më të besueshëm dhe efikas.

6.2. Strategji parandalimi dhe zbutje

Në trajtimin e kërcënimit kibernetik ndaj sistemeve të energjisë, përpjekjet duhet të drejtohen drejt strategjive efikase të parandalimit dhe zbutjes. Këto mund të fillojnë duke ndjekur praktikat e duhura të sigurisë kibernetike. Disa udhëzues praktikash më të mira, të tilla si Udhëzuesi për Sigurinë e

[35] International energy statistics (2017). http://eia.gov

Sistemeve të Kontrollit Industrial nga NIST[36] dhe standarde, si ANSI/ISA-62443[37], ofrojnë praktika që mund të pengojnë sulmet kundër sistemeve të energjisë. Shitësit e pajisjeve të sistemit të energjisë duhet të forcojnë sigurinë e produkteve të tyre duke rishikuar modelet e tyre të kërcënimit, të cilat mund të mos e konsiderojnë ndërhyrjen me qëllim të keq si një kërcënim serioz. Duke pasur parasysh ndikimin e drejtpërdrejtë të elasticitetit të sistemit elektroenergjetik për publikun e gjerë, politikëbërësit mund të përshpejtojnë veprimet me politika rregullatore që nxisin operatorët e sistemit energjetik dhe shitësit të adoptojnë praktika të mira sigurie. Nga pikëpamja teknike, pajisjet në terren mund të ngurtësohen në shtresa të ndryshme të sistemit, përkatësisht në harduerin, firmuerin, softuerin, rrjetin dhe shtresat e funksionimit[38].

Mbështetja e harduerit për operacionet kriptografike mund të mundësojë përdorimin e primitivëve të sigurt kriptografik në sistemet e energjisë. Për firmware, imazhet statike duhet të kodohen dhe përditësimet e firmuerit duhet të nënshkruhen nga shitësit përkatës. Në shtresën e softuerit, mekanizmat e duhur të sigurisë dhe vlerësimet e rrezikut janë të nevojshëm, së bashku me aftësinë e përditësimeve të sigurta dhe verifikuese që nuk kërkojnë ndërprerje. Për sa i përket shtresës së rrjetit, pajisjet industriale të vendosura në sistemet e energjisë nuk duhet të lidhen asnjëherë drejtpërdrejtë me internetin dhe rrjetet në terren dhe rrjetet e biznesit duhet të segmentohen për të penguar sulmet që mbështeten në lëvizjen anësore. Protokollet industriale pa mekanizma sigurie duhet të ridizajnohen ose zëvendësohen me homologë të sigurt.

Në shtresën e funksionimit duhet të përdoren mekanizma efektivë të sigurisë fizike dhe funksionimi i përgjithshëm i sistemit mund të informojë skemat e zbulimit të anomalive që synojnë të veprojnë si tregues të hershëm të sulmeve duke grumbulluar të dhëna në të gjithë sistemin. Lidhur me informacionin që mund të ekspozojë karakteristikat kritike operacionale dhe/ose të mundësojë vektorët e sulmit kundër një sistemi energjetik, duhet të kihet më shumë kujdes kur vendoset për klasifikimin e tij dhe audiencën e synuar. Aksionarët e sistemit elektroenergjetik mund të kryejnë rishikime periodike të informacionit që ka të bëjnë me sistemet e tyre dhe që është i disponueshëm për publikun. Përveç kësaj, mund të përcaktohen kërkesat dhe metodat për trajtimin dhe kontrollin e duhur të informacionit potencialisht kritik. P.sh., teknikat që anonimizojnë ose randomizojnë informacionin përpara publikimit të tij mund të ofrojnë njëkohësisht transparencë duke mbrojtur të dhënat kritike dhe të ndjeshme.

---

[36] Stouffer K, Falco J, Scarfone K (2011) *Guide to industrial control systems security*. NIST Spec Publ 800(82):16

[37] International Society of Automation (2018) ISA 62443 security for industrial automation and control systems.

[38] Konstantinou C, Maniatakos M., (2017), *Security analysis of smart grid. Common Control Secure Challenges Smart Grid* 2:451

Përfundime

Të motivuar nga vëzhgimi se kundërshtarët përdorin në mënyrë aktive teknikat OSINT për fushatat kundër sektorit të energjisë, është ndërmarrë një studim i sasisë dhe cilësisë së inteligjencës që mund të nxirret duke përdorur burime të disponueshme publikisht. Është paraqitur një studim i gjerë mbi burimet e inteligjencës që mund të përdoren për të modeluar një sistem të madh energjie, për të analizuar modelin dhe në fund studiohet se si ta shfrytëzojmë atë. Vlerësohet eksperimentalisht realizueshmëria e një fushate me burim të hapur duke ndërtuar dhe vërtetuar modelin e një sistemi real duke përdorur vetëm informacionin e disponueshëm publikisht dhe duke analizuar sistemin për të identifikuar pikat e tij kritike duke përdorur analizën e kontigjencës.

Me këtë shkrim synohet të ofrohet një pasqyrë e kërcënimit të sulmeve kibernetike bazuar në burimet e disponueshme publikisht për sistemet e energjisë. Kjo mund të ndihmojë palët e interesuara dhe rregullatorët e sektorit të energjisë të marrin vendime të informuara dhe të trajtojnë më me kujdes shpërndarjen e informacionit që lidhet me karakteristikat e ndjeshme të sistemeve të tyre të energjisë.

Literatura e shfrytëzuar:

1. Binwalk firmware analysis tool. https://github.com/ReFirmLabs
2. Blackout watch: Brazilian blackout 2009. http://pacw.org
3. European network of TSOs for electricity. http://entsoe.eu
4. India Northern Regional Load Despatch Centre. http://nrldc.in
5. Industrial Control Systems Cyber Emergency Response Team. http://ics-cert.us-cert.gov
6. National Vulnerability Database. http://nvd.nist.gov
7. Network data of real transmission networks (2013). http://maths.ed.ac.uk
8. Open energy information. http://openei.org
9. Open power system data platform. http://open-power-system-data.org
10. Ukraine's power outage was a cyber attack: Ukrenergo. http://reuters.com
11. Abraham S, Efford JR (2004) Final report on the August 14, 2003 blackout in the U.S. and Canada. Technical report, Power System Outage Task Force
12. Alonso F, Greenwell C (2016) Underground vs. Overhead: power line installation-cost comparison and mitigation. Electr. Light Power 22
13. Bakshi S (2012) Report of the enquiry committee on grid disturbance in Northern region on 30th July 2012 and in Northern, Eastern & North-Eastern

region on 31st July 2012. Technical report, Indian Ministry of Power

14. Bernstein A, Bienstock D, Hay D, Uzunoglu M, Zussman G (2014) Power grid vulnerability to geographically correlated failures – analysis and control implications. In: IEEE INFOCOM 2014 – IEEE conference on computer communications, pp 2634–2642. https://doi.org/10.1109/
15. Campbell RJ (2012) Weather-related power outages and electric system resiliency. Technical report, Congressional Research Service
16. Davis CM, Overbye TJ (2011) Multiple element contingency screening. Trans Power Syst 26(3):1294–1301
17. Davis C, Chmieliauskas A, Nikolic I (2015) Enipedia. Energy & Industry group, Faculty of Technology, Policy and Management, TU Delft
18. Durumeric Z, Wustrow E, Alex Halderman J (2013) ZMap: fast internet-wide scanning and its security applications. In: Presented as part of the 22nd USENIX security symposium (USENIX Security 13), Washington, DC. USENIX, pp 605–620. https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/durumeric,ISBN:978-1-931971-03-4
19. Eaton: Blackout tracker (2017) United States annual report 2016
20. Eles: Slovenia's transmission network: annual report 2015. http://eles.si
21. Fachkha C, Bou-Harb E, Keliris A, Memon N, Ahamad M (2017) Internet-scale probing of CPS: inference, characterization and orchestration analysis. In: Proceedings of the 24th network and distributed system security symposium (NDSS'17), San Diego, Feb 2017
22. Grainger J, Grainger W, Stevenson W (1994) Power system analysis. McGraw-Hill Education, New York
23. Igure VM, Laughter SA, Williams RD (2006) Security issues in SCADA networks. Comput Secur 25(7):498–506
24. International Society of Automation (2018) ANSI/ISA 62443 security for industrial automation and control systems. ISA
25. Kaplunovich P, Turitsyn K (2016) Fast and reliable screening of N-2 contingencies. Trans Power Syst 31(6):4243–4252
26. Keliris A, Maniatakos M (2017) Demystifying advanced persistent threats for industrial control systems. ASME Mech Eng 139(03): S13–S17. https://doi.org/10.1115/1.2017-Mar-6
27. Knake R (2017) A cyberattack on the U.S. power grid. Contingency planning memorandum, vol 31. Council on Foreign Relations. https://www.cfr.org/report/cyberattack-us-power-grid. 3Apr2017

28. Konstantinou C, Maniatakos M (2015) Impact of firmware modification attacks on power systems field devices. In: International Conference on Smart Grid Communications. IEEE, pp 283–288. https://doi.org/10.1109/SmartGridComm.2015.7436314
29. Lee RM, Assante MJ, Conway T (2016) Analysis of the cyber attack on the Ukrainian power grid. Technical report, SANS Industrial Control Systems
30. Momoh J, Mili L (2009) Economic market design and planning for electric power systems, vol 52. Wiley, Hoboken
31. Morison K, Wang L, Kundur P (2004) Power system security assessment. Power Energy Mag 2(5):30–39 45. NERC: Disturbance Reports 1992–2009
32. Orebaugh A, Ramirez G, Beale J (2006) Wireshark & Ethereal network protocol analyzer toolkit. Syngress, Rockland Open Source Intelligence for Energy Sector Cyberattacks 281
33. Project Group Turkey (2015) Report on blackout in Turkey on 31st March 2015. Technical report, European Network of Transmission System Operators for Electricity
34. Reimann J, Rose J (2015) Eclipse SCADA: the definite guide
35. Roland Berger (2014) Study regarding grid infrastructure development: European strategy for raising public acceptance. Technical report, European Commission Tender No. ENER/B1/2013/371
36. Stott B, Alsac O, Alvarado F (1985) Analytical and computational improvements in performance-index ranking algorithms for networks. Int J Electr Power Energy Syst 7(3): 154–160
37. Stouffer K, Falco J, Scarfone K (2011) Guide to industrial control systems security. NIST Spec Publ 800(82):16
38. Symantec: Dragonfly: Western energy sector targeted by sophisticated attack group. http://symantec.com
39. Turitsyn KS, Kaplunovich PA (2013) Fast algorithm for N-2 contingency problem. In: 46th Hawaii international conference on system sciences (HICSS). IEEE, pp 2161–2166. https://doi.org/10.1109/HICSS.2013.233
40. Zachariadis T, Poullikkas A (2012) The costs of power outages: a case study from Cyprus. Energy Policy 51(Supplement C):630–641
41. Zimmerman RD, Murillo-Sánchez CE, Thomas RJ (2011) MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education. Trans Power Syst 26(1):12–19

RUBRIKA E TRETË

STUDIME HISTORIKE

Arti ushtarak në rrjedhat e Luftës Antifashiste Nacionalçlirimtare dhe veçori të përdorimit të tij

Prof. Asoc. Dr. Bernard ZOTAJ
Msc. Arben ZAVALANI
Specialist në IKSHU

Trajtesë e shkurtuar.

Gjatë Luftës së Dytë Botërore, Lufta Antifashiste Nacionalçlirimtare e popullit shqiptar lindi si nevojë dhe domosdoshmëri për të çliruar vendin nga pushtuesit fashistë dhe njëkohësisht për rikthimin e pavarësisë dhe të sovranitetit. Në mungesë të një ushtrie të qëndresës së organizuar kundër pushtuesve, forcat politike kryesore shqiptare, që u krijuan në luftë, formuan dhe zhvilluan forcat luftarake, të cilat kishin veçori të përbashkëta dhe dalluese midis tyre.

Në rrjedhën e luftës, u zbatua dhe u përsos më tej arti ushtarak i luftës me ndryshimet dhe veçoritë dalluese në zbatimin e luftimit, betejës dhe operacionit. Në skenën politike shqiptare të viteve të luftës, ku Shqipëria u bë viktima e parë, dolën forca kryesore luftarake, të cilat u ngritën, u organizuan dhe u udhëhoqën nga grupime politike që u krijuan në luftë. Forcat luftarake ishin: Ushtria Partizane Vullnetare Nacionalçlirimtare, që u krijua dhe udhëhiqej nga PKSH, forca të Ballit Kombëtar dhe të Legalitetit, si dhe forca nacionaliste të veçuara në zonat e Veriut.

Forcat luftarake kishin mision, strategji dhe slogane të ndryshme nga njëratjetra. Këto forca luftarake kishin të përbashkëta, por edhe dukuri që dallonin midis tyre në artin luftarak që përdornin. Ngjashmëritë dhe dallimet vihen re dukshëm në organizim, luftim, disiplinë, armatim, veshje, etj., por në drejtim dhe aftësi luftarake, në taktikë dhe përgjithësisht, në artin dhe mënyrat e

të bërit të luftës kishte ndryshime thelbësore. Këto u shfaqën dukshëm në rrjedhën e luftimeve dhe të operacioneve të kryera në vitet e luftës.

Fjalë kyçe: Arti ushtarak, Lufta Antifashiste Nacionalçlirimtare, Ushtria Partizane Vullnetare Nacionalçlirimtare, PKSH, Balli Kombëtar, Legaliteti, çetë partizane, batalion, brigade, etj.

Lufta Antifashiste Nacionalçlirimtare e popullit shqiptar, që u zhvillua në rrjedhën e Luftës së Dytë Botërore, lindi si nevojë për të çliruar vendin nga pushtuesit fashistë dhe rikthimin e pavarësisë e të sovranitetit të tij. Në mungesë të një ushtrie dhe të qëndresës së organizuar kundër pushtuesve, si dhe për të realizuar dhe konkretizuar luftën, forcat politike kryesore shqiptare që lindën në skenën politike shqiptare, formuan forcat e tyre luftarake, të cilat kishin veçoritë dalluese dhe, natyrisht edhe të përbashkëtat midis tyre. Njëherësh, në rrjedhën e kësaj lufte, u zbatua dhe u zhvillua edhe *vetë arti luftarak* apo ndryshe arti i të bërit të luftës. Por natyrisht, nga njëra forcë te tjetra, arti ushtarak pati ndryshimet dhe veçoritë dalluese në zbatimin e elementit të tij, nga njëri luftim apo operacion te tjetri. Për ta bërë më të qartë tablonë, na duhet të përshkruajmë shkurtimisht cilat ishin forcat kryesore luftarake, të cilat u ngritën dhe u udhëhoqën nga grupimet politike që ishin krijuar dhe zotëronin skenën politike shqiptare të viteve të Luftës Antifashiste Nacionalçlirimtare, gjatë Luftës së Dytë Botërore, viktimë e parë e së cilës ishte edhe Shqipëria.

Këto forca ishin *Ushtria Partizane Vullnetare Nacionalçlirimtare*, që u krijua dhe udhëhiqej *nga PKSH,* forcat luftarake *të Ballit Kombëtar* si dhe ato *të Legalitetit,* të cilat gjithashtu drejtoheshin nga forcat e tyre politike. Përveç tyre, gjatë luftës, në trevat e Veriut vepruan edhe disa forca nacionaliste të veçuara nga tri forcat e tjera të grupuara. Natyrisht, siç kishin misionin, strategjitë, madje edhe sloganet e tyre krejt të ndryshme nga njëra-tjetra, këto forca luftarake kishin të përbashkëta dhe veçoritë që i dallonin ato midis tyre në arti luftarak që përdornin. Për rrjedhojë përngjashmëritë dhe dallimet vihen re dukshëm që në performancat organizative, në disiplinën, armatimet, veshjen dhe, sigurisht në drejtimin dhe sidomos në aftësitë luftarake, në taktikën dhe, përgjithësisht, në artin apo mënyrat e të bërit të luftës. Kjo e dyta shfaqet qartë në rrjedhën e luftimeve dhe operacioneve që u kryen gjatë viteve të Luftës Antifashiste në Shqipëri.

Në pikëpamje organizative, forcat luftarake fillimisht ishin të thjeshta, madje në fillimet e Lëvizjes Antifashiste formacionet e para luftarake ishin vetëm pak çeta, të cilat nuk kishin përkatësi partiake. Ato, në thelb, ishin vërtet çeta nacionaliste, të organizuara për të kundërshtuar pushtimin fashist të vendit. Çeta e parë antifashiste u formua pikërisht nga nacionalistët.

Çetat e para, me përkatësi partiake u "pagëzuan" në Konferencën e Pezës, të 16 shtatorit 1942, kohë kur lindën dhe u njohën "çetat partizane", të cilat në simbolet e tyre, përmbi shqiponjën e zezë, vendosën dhe yllin e kuq. Në drejtimet e tyre, krahas Komandantit u shtua edhe posti i Komisarit Politik, i cili përfaqësonte linjën e Partisë Komuniste. Çeta e parë partizane ishte pikërisht ajo e Myslym Pezës, me komisar politik komunistin Vasil Shanto që, në vijim të luftës, u pasua nga afro 70 të tjera në gjithë trevat e vendit.

Më pas, me krijimin e Ballit Kombëtar, tek çetat e tij, luftëtarët mbanin për simbol vetëm shqiponjën e zezë me dy krena. Por kjo situatë i përkiste fillimeve të LANÇ, që përkon pikërisht me Konferencën pluraliste të Pezës, të shtatorit të viti 1942. Përkrah Lëvizjes Antifashiste Nacionalçlirimtare, që frymëzohej dhe udhëhiqej nga PKSH, krahas çetave, lindi dhe u fuqizua dukshëm edhe një formacion i vogël, i cili u quajt njësiti gueril, që përbëhej kryesisht nga anëtarë që vinin nga klasa punëtore. Këto organizime që shkonin deri në 15 vetë[1] vepronin, si rregull, nëpër qytete por shpejt u përhapën edhe në fshatrat pranë qyteteve dhe drejtoheshin nga komitetet qarkore të PKSH-së, më saktë nga përgjegjësi ushtarak, i cili ishte një prej anëtarëve të Komitetit të Qarkorit të PKSH-së, në qarkun përkatës. Ndryshe nga njësitet guerile, luftëtarët e çetave partizane ishin efektive, që do të thotë se bënin jetë të përhershme të grupuar, si në një ushtri të rregullt, përveç faktit thelbësor se ata ishin vullnetarë dhe nuk paguheshin![2]

Çetat vullnetare partizane ishin formacione të vogla të përmasave taktike që, së bashku me njësitet guerile, mbizotëronin fazën e parë të LANÇ-it. Ato ishin të armatosura me armë të lehta brezi dhe krahu, përbëheshin nga efektivë që varionin nga 15-25 deri në 80-100 luftëtarë por, në raste të rralla kishte çeta të veçanta që arritën numrin nga 250 deri në 300 luftëtarë. Të tilla ishin çeta "Çamëria" dhe ajo e Kurveleshit, e para shpejt u shndërrua në batalion, kurse e dyta u nda në dy çeta. Çetat zakonisht si rregull, ndaheshin në skuadra dhe komandoheshin prej Komandantit dhe Komisarit Politik. Çetat partizane u shoqëruan me krijimin e "çetave territoriale", të cilat nuk ishin përherë në veprim, por vetëm në situata të caktuara kërcënuese. Ato ngriheshin dhe vepronin në përgjithësi në bazë krahine apo dhe fshati. Këto çeta dallonin edhe nga simbolet që mbanin prej atyre partizane të rregullta. Këtë dallim e shpjegon shumë qartë në librin e tij, misionari anglez në Shqipëri, Reginald Hibert, i cili pati shkruar: "Partizanët mbajnë yll të kuq me pesë cepa përveç flamurit shqiptar. Në gazetat klandestine ata përmenden si të veçantë nga çetat vullnetare, të cilat mbajnë për simbol vetëm flamurin shqiptar. Megjithatë, partizanët dhe vullnetarët luftojnë në të njëjtën çetë dhe, kur një çetë partizane

[1] Proletar Hasani, *Histori e Pashkruar*, shtëpia botuese "FLLAD", Tiranë, 1999, f. 17.
[2] Po aty, f. 26.

është e zënë ngushtë, një çetë vullnetare nxiton që ta shpëtojë dhe anasjelltas".[3] Megjithëse çetat partizane dhe ato territoriale, së bashku me njësitet guerile, dominuan fazën e parë të LANÇ, në Shqipëri, ende pa u përmbyllur kjo fazë, në maj të viti 1943, në skenën shqiptare të luftës, u shfaq imazhi i një formacioni të ri, më të madh luftarak. Ky ishte batalioni partizan, i cili do të mbizotëronte veprimet luftarake të formacioneve antifashiste shqiptare edhe në pjesën më të madhe të fazës së dytë të LANÇ, së bashku me një formacion tjetër që u krijua rishtazi.

Formacioni i emërtuar Grupi Partizan, u ngrit në disa qarqe të vendit dhe përmblidhte të gjitha formacionet e krijuara më herët në secilin qark, që nga çetat dhe batalionet partizane. Për të drejtuar dhe bashkërenduar veprimtarinë e Grupit u ngrit Shtabi i Qarkut. Ky organizim ushtarak, jo vetëm që solli shumim dhe larmi të forcave që luftonin pushtuesit fashistë, por edhe mundësoi një drejtim të përqendruar, si dhe bashkërendim të veprimeve luftarake shqiptare. Por, deri këtu, në krijimin e këtyre formacioneve nuk ka asgjë të veçantë sepse, ndonëse pak më vonë, edhe te Balli Kombëtar u krijuan një numër çetash dhe batalionesh të cilat ndryshe nga ato të LANÇ, u emërtuan çeta dhe batalione balliste. Ajo që solli risi dhe bëri dallime tejet të dukshme në organizimin e forcave luftarake te Lëvizja Antifashiste, në përqasje me forcat luftarake të B. Kombëtar, gjë që ndodhi në fillimet e fazës së dytë të Luftës Antifashiste, më 10 korrik 1943, pa diskutim ishte krijimi i Shtabit të Përgjithshëm, në pikëpamje të drejtimit të përgjithshëm, sidomos në aspektin e strukturës organizative të asaj që mori emrin Ushtria Partizane Vullnetare NÇ.

Formacioni i ri, që lindi vetëm një muaj e gjysmë pas krijimit të vetë Shtabit të Përgjithshëm të Ushtrisë NÇ Shqiptare, ishte i panjohur dhe jo tradicional deri atëkohë në Shqipëri. Ky formacion, që përbënte risi në skenën shqiptare të Luftës Antifashiste, ishte pikërisht Brigada Sulmuese, e cila shfaqej për herë të parë në Shqipëri, në ndryshim nga forcat luftarake të Ballit Kombëtar dhe më pas edhe të Legalitetit. Në të vërtetë, në krijimin dhe përurimin e Brigadës së Parë Sulmuese, në gusht të viti 1943, në vend nisi era e krijimit të formacioneve të mëdha luftarake që, në fazën e tretë të Luftës, në maj 1944, do të pasohej me formimin e njësive më të mëdha operative-strategjike. Brigadat, që nisën të krijohen me shpejtësi, gjithsej 24 të tilla, u vlerësuan si formacioni bazë luftarak i Ushtrisë NÇ. Dhe kjo për disa arsye, që duhen kërkuar në fuqizimin e Lëvizjes dhe të Luftës Antifashiste NÇ, në shtimin e numrit të forcave luftarake, antifashiste dhe nacionaliste, në nevojën për zgjerimin e veprimeve në pikëpamje sipërfaqësore, në hapësirë dhe në kohë, por edhe si nevojë për bashkërendimin dhe drejtimin e veprimeve luftarake të reparteve dhe njësive të deriatëhershme luftarake të Ushtrisë NÇ Shqiptare.

[3] Reginald Hibbert, *Fitorja e hidhur*. TOENA, Tiranë, 1993, f. 10.

Në fazën e tretë dhe të fundit të LANÇ-it, kohë kur u krye njësimi i Komandës së Përgjithshme, kur u rivendos shndërrimi i UNÇ-së në ushtri të rregullt, me grada ushtarake dhe kalimi në mësymje për çlirimin e plotë të vendit, u kalua në krijimin e divizioneve sulmuese dhe të korparmatave. Në këtë rrjedhë, deri në prag të çlirimit të vendit ishin krijuar 8 divizione sulmuese dhe 3 korparmata, me forca më të shumta, me mundësi më të mëdha luftarake për çlirimin dhe mbrojtjen e zonave të çliruara, si dhe mbrojtjen e kufijve të vendit.

Kështu, zhvillimi i operacioneve luftarake provoi se një divizion sulmues i UNÇ-së mundi të kryente veprime luftarake në një zonë me sipërfaqe 90 km të gjerë dhe 30-40 km të thellë, ashtu si dhe në një hapësirë prej 2.000 deri në 3.000 km^2.[4] Më pas, korparmata e UNÇ, mundi të kryente operacione luftarake, duke përdorur njëherësh 4.000-6.000, por edhe 8.000 forca, në një sipërfaqe që shkonte deri në 3.500-4.000km^2 e më shumë.[5] Pra kuptohen mundësitë dhe arsyet e përdorimit luftarak të këtyre formacioneve të mëdha nga Ushtria NÇ Shqiptare.

Forcat e UNÇ, që ishin më të shumta në numër, paraqitën një sërë veçorish në pikëpamje të disiplinës, të zbatimit të artit të luftës dhe i shkuan kësaj lufte deri në fund, deri në kurorëzimin e saj me çlirimin e plotë të vendit. Në fundin e luftës, UNÇ u shndërrua në një ushtri e rregullt, gradualisht, duke u përshtatur si një ushtri e kohës së paqes. Që UNÇ ishte një ushtri më e madhe në numër, kjo u vërtetua fazë pas faze në rrjedhën e LANÇ-it. Kështu, në fundin e fazës së parë, që u përmbyll në fillim të korrikut 1943, formacionet që i përkisnin Lëvizjes NÇ, numëronin afro 20. 000 luftëtarë,[6] kurse në përfundim të fazës së dytë, që nis më 10 korrik 1943 dhe shtrihet deri më 24 maj 1944, UNÇ kishte arritur shifrën 35. 000 vetë.[7]

Deri në fundin e Luftës dhe çlirimin e vendit kjo ushtri, e cila që pas Kongresit Antifashist të Përmetit (24-28 maj 1944) kishte nisur të shndërrohej në ushtri të rregullt, me grada ushtarake, Komandë të Përgjithshme të njësuar, me rregullore dhe hierarki ushtarake, u rrit në 70. 000 oficerë, nënoficerë dhe partizanë-ushtarë.[8] Përveç burimeve të njohura të historiografisë shqiptare, numri i mësipërm shpesh dhe me teprime, konfirmohet edhe përmes disa burimeve dhe autorëve të huaj, njohës të kësaj periudhe. Një ndër ta, historiani italian Alfonso Bartolini ka shkruar se… UNÇ arriti deri në 70. 000, të ndarë në tri korparmata…, të paktën edhe 50. 000 shqiptarë të tjerë vepronin në

[4] Histori e Pashkruar, cituar më parë, f. 99. (Shih edhe Historia e Artit Ushtarak të LANÇ të popullit shqiptar. Tiranë, 1989, f. 239).
[5] Po aty, f. 107. (Shih edhe Historia e Artit Ushtarak të LANÇ …, e cituar, f. 239 etj.).
[6] Historia e Luftës Antifashiste e popullit shqiptar, vëll. 2, e cituar, f. 239.
7 Revista Ushtarake. nr. 4, viti 2004, f. 41.
[8] Po aty.

organizatat politike dhe të prapavijës për mbështetje.[9] Ndërsa një autor tjetër, gjermani Heinz Künrich (Hainz Kynrih), e çon shifrën deri në 75. 000 luftëtarë, anëtarë të UNÇ-së![10] Kjo epërsi, në pikëpamje numerike të forcave të UNÇ, bie në sy, në përqasje me dy forcat e tjera luftarake, të B. Kombëtar dhe Legalitetit. Sipas vetë njërit prej eksponentëve drejtues më të njohur të krahut aktiv të kësaj force, Abaz Ermenjit, në fundin e vitit 1943, B. Kombëtar numëronte afro 12. 000 luftëtarë.[11]

Ndërkohë Legaliteti ishte më inferior në pikëpamje të numrit të forcave luftarake që mund të grumbullonte. Sipas misionarit anglez Bill Macklean (Bill Maklin), Legaliteti mund të mblidhte 3000-5000 luftëtarë.[12] Ndërsa konsulli i përgjithshëm gjerman në Tiranë, në vitin 1944, shkruante se Abaz Kupi, Komandant i Përgjithshëm i forcave luftarake të Legalitetit ka,"… rreth 1000-1500 vetë".[13] Një tjetër anëtare gjithashtu angleze, Elizabeth Barker (Elizabet Barker) është pranë shifrës reale teksa shkruante se forcat luftarake të Legalitetit ithtarë të ish-Mbretit Zog, arrinin në "… 3000 zogistë".[14]

Këta autorë që sjellin të dhëna që vinë nga burime të huaja dhe që, më së shumti, përqasen me ato shqiptare, dëshmojnë përmes krahasimeve, epërsinë në pikëpamje të numrit të forcave të UNÇ. Nga ana tjetër këta tregues numerikë përforcojnë dhe vënë në pah më tepër epërsinë e këtyre formacioneve të UNÇ ndaj të tjerave, por dhe në përballjet, shpesh të suksesshme, me forcat pushtuese fashiste. Këtë epërsi në forca dhe në luftime, UNÇ-së ia mundësonte struktura organizative efektive dhe racionale, e cila, sidomos pas fazës së parë të Luftës, ishte larg atyre tradicionale. Ishte koha kur UNÇ, me krijimin e Shtabit të Përgjithshëm kaloi në strukturën me brigada sulmuese, një Zonë Operative, divizione sulmuese e deri në Korparmatë. Ky efektivitet u përfaq dukshëm në fazën e tretë të Luftës, kur UNÇ e drejtuar nga një Komandë e Përgjithshme, me shndërrimin në ushtri të rregullt, me grada dhe hierarki ushtarake, me një drejtim të përqendruar dhe më efektiv.

Organizimi ushtarak i përzgjedhur dhe i zbatuar nga drejtuesit dhe hallkat drejtuese të kësaj force, ishin më bashkëkohore, pa mohuar trashëgiminë tradicionale dhe luftarake në formacionet e para, çetat nacionaliste pro PKSH, të organizuar sidomos në vitin 1942. Tashmë ishte fakt dhe një e vërtetë

[9] Antonio Bartolini, *Storia della rezistenca all estero*, Padova, 1965, f. 239.
[10] Heinz Künrich, *Die Partizanen-Krieg Europa, 1939-1945*. Marrë nga revista "Mbrojtja", nr. 4, viti 1998, f. 76.
[11] Gazeta "Liria", datë 2 nëntor 1945. Intervistë për LANÇ në Shqipëri, 1939-1945.
[12] Raporti i B. Macklean, PRO, FO. 371/43549 dhe FO. 204.9461, dhjetor 1943.
[13] AQSH. Fondi i ushtrive pushtuese. Telegram i shifruar, nr. 148, datë 9 nëntor 1943.
[14] Elizabeth Barker, *Politika britanike në Evropën Juglindore gjatë Luftës së Dytë Botërore*, Bristol. 1976, f. 22.

e pranuar edhe nga vetë misionarët e huaj ushtarakë, që vepruan pranë tri forcave të armatosura shqiptare në vitet e LANÇ, organizimi ushtarak i zbatuar nga UNÇ kishte përparësi në disa aspekte. E tillë ishte ajo në përshtatjen me taktikën e luftës së mundshme në territorin tipik shqiptar; në rritjen e qëndrueshmërisë në mbrojtje dhe të shpirtit luftarak në mësymje (sulm); në disiplinën e luftëtarëve; në motivimin dhe ruajtjen e moralit të tyre etj.

Ky model organizimi, i gërshetuar dhe i zbatuar me rigorozitet, shpesh edhe me fanatizëm, provoi se kishte përparësi në përqasje me sistemet e organizimit të dy forcave të tjera luftarake, të cilat vepruan gjatë viteve 1942-1944 në Shqipëri. Përparësitë dhe sidomos dizavantazhet e tyre, i kanë vënë në pah edhe disa nga misionarët e huaj ushtarakë që vepruan në Shqipëri në këto vite. Midis tyre ishte majori anglez B. Maklean përcaktoi dy formacionet luftarake si"…të paorganizuar fare", kurse më poshtë ai vijon se "… në përgjithësi të gjithë ballistët nuk dinë përdorimin e topave, mortajave …, duke qenë injorantë në njohjen e luftës moderne".[15] Madje ai shkon deri aty sa të shkruaj se, për shkak të formave tradicionale, të vjetruara të organizimit dhe të disiplinës së tyre të keqe, ata kishin "…një vlerë të vogël luftarake".[16] Sipas vlerësimeve angleze, këto forca nuk arritën të kishin as "organizim të mirëfilltë" ushtarak.

Ndërkohë, mjaft drastik shfaqet në vlerësimet e tij edhe ish-eksponenti i Ballit Kombëtar, Abaz Ermenji, madje kësaj radhe me vetë drejtuesit e formacioneve të kësaj force. Ai ka shkruar se "kuadrot e çetave" nuk e kaluan cakun e një niveli provincial, duke mbetur kështu, fshatarë gjer në fund, të cilët nuk kishin as bindjen, as disiplinën e kuadrove fanatikë dhe djalosharë komunistë …".[17] Po ky ish-drejtues ballist, duke përcaktuar vlerat organizative dhe luftarake të forcave legaliste, në një libër më të njohur të tij, ka përcaktuar se, "… ky grup, si forcë luftonjëse u pa qysh në fillim se ishte i një shkalle më të ulët …".[18] Nga ana tjetër, anglezi Hibert jep për to vlerësimin e një force që nuk përbënte as imazhin e një "… faktori ushtarak".[19]

Në të kundërt të kësaj tabloje vjen përcaktimi për UNÇ nga ish-misionarët ushtarakë aleatë, që vepruan në Shqipëri në vitet e LANÇ. Një prej tyre, pikërisht Macklean i "portretizonte" kështu forcat e UNÇ: "Repartet e rregullta të LNÇ janë të vetmet trupa me të vërtetë të organizuara në vend. Ata janë të ndarë në çeta, batalione partizane bile edhe në brigada sulmuese të pajisura me pushkë, mitraloza, topa antitank, mortaja dhe topa malorë".[20]

---

[15] Dokumente të PRO për Shqipërinë, FO, 371/443549, Tiranë 1974, f. 47.
[16] Po aty, f. 48.
[17] A. Ermenji, *Vendi që zë Skënderbeu në historinë e Shqipërisë*, Paris, 1968, f. 47.
[18] Dokumente të PRO për Shqipërinë, FO, 371/443549, Tiranë 1974, f. 47.
[19] Abaz Ermenji, libër i cituar, f. 469.
[20] B. Macklean. Raporti i dhjetorit 1943, PRO, FO, 371/43549 dhe EO 204.94461, i cituar

Këta tregues, si dhe disiplina, morali, përzgjedhja e drejtuesve ushtarako-politikë edhe nga radhët e ushtarakëve të karrierës etj., sigurisht që do të pasqyroheshin dhe do të jepnin përfundime të suksesshme edhe në fushën e veprimeve luftarake kundër pushtuesve të huaj. Ky ishte edhe treguesi më shprehës, pasi siç dihen përfundimet, gjatë veprimeve luftarake, tek e fundit vendosen pikërisht në fushën e luftimit midis palëve ndërluftuese. Dhe forcat luftarake të armatosura ishin formuar pikërisht për kryerjen e veprimeve kundër pushtuesit të huaj.

Forcat e kësaj ushtrie përballuan një operacion të madh e të fuqishëm nazist dhe të bashkëpunëtorëve të tij vendas pikërisht kundër forcave të UNÇ, i organizuar dhe i kryer në Dimrin e vitit 1943-1944, i cili përbëhej nga disa operacione që shtriheshin pothuajse në zonat më kryesore të vendit dhe ka hyrë në historinë e LANÇ me emërtimin "Operacioni nazist (armik) i Dimrit 1943-1944". Formacionet luftarake të UNÇ ndonëse pësuan humbje dhe dëme të ndjeshme, falë organizimit ushtarak, cilësisë së luftëtarëve dhe komandantëve e të shtabeve drejtuese, taktikës së përdorur shpesh me mjeshtëri si dhe të shfrytëzimit të karakteristikave të terrenit e të mbështetjes së popullsisë me mjaft zona të operacionit, i a dolën që të mbijetonin. Madje, ato nisën që të rigjallëroheshin dhe të ripërtëriheshin shumë shpejt. Kësisoj, në pranverën e vitit 1944 morën nismën luftarake dhe nisën të shtoheshin me forca dhe formacione të reja të mëdha, si brigadat, divizionet sulmuese dhe korparmatat.

Në qershor 1944 pushtuesit nazistë ndërmorën një mësymje të dytë të përgjithshme, në një brez të gjerë më se 7.000 km^2, midis lumenjve Shkumbin dhe Vjosa, kundër forcave të UNÇ, që gjendeshin në të. Edhe në këtë operacion, që u emërtua së pari "Einhorn" dhe më pas "Geimsbock", megjithëse nazistët arritën ta shkelnin një pjesë të zonës, nuk ia dolën që të realizonin qëllimin kryesor, asgjësimin e forcave kryesore të UNÇ, që ndodheshin në të. Madje forcat e UNÇ këtu dhe ato jashtë zonës, kaluan në kundërmësymje të përgjithshme në Veri të lumit Shkumbin, më 29 qershor 1944, për të vijuar më pas më lart, drejt Verilindjes dhe Veriut të Shqipërisë, për çlirimin e plotë të vendit.

Një ndër operacionet më të mëdhenj të UNÇ ka qenë pa dyshim ai për çlirimin e kryeqytetit të vendit, Tiranës, që u përmbyll me sukses më 17 nëntor 1944 dhe ku morën pjesë afro 12 brigada sulmuese të Korparmatës I të UNÇ. UNÇ, në të vërtetë dhe në thelb ishte ushtri vullnetare, tërësisht tokësore, këmbësore dhe sulmuese. Kjo ushtri ishte e tillë për shkak të artit ushtarak që përdorte në fushën e luftës. Prandaj ajo ishte mjaft efektive dhe racionale, me gjithë kufizimet e shumta, shpesh të dukshme në armatime dhe taktikën e luftës. Prandaj ajo kishte epërsi ndaj dy forcave të tjera luftarake shqiptare bashkëkohëse.

Në një intervistë me mediat, studiuesi i njohur i Historisë së Shqiptare dhe të Luftës së Dytë Botërore, Bernd J. Fischer është shprehur se: "Partizanët ishin

dominuar nga komunistët,…”.[21] Kjo është krejt e kuptueshme pasi UNÇ u krijua nga PKSH dhe udhëhiqej prej saj. Por, jo vetëm UNÇ. Kështu ndodhi edhe me dy forcat e tjera luftarake. Nuk dihet nëse ai e ka fjalën për numrin e komunistëve në UNÇ apo për partizanët që udhëhiqeshin nga komunistët e PKSH, të cilët gjendeshin në komandat ose shtabet e formacioneve partizane të çdo niveli, nga çetat deri në korparmata dhe Shtabi i Përgjithshëm e Komanda e Përgjithshme e UNÇSH.

Nga historia e Luftës Antifashiste dhe nga studimet e posaçme, që kanë për objekt pikërisht forcat e Ushtrisë NÇ Shqiptare, dihet që, pas Konferencës së Pezës, pranë çdo çete, më pas edhe çdo batalioni, grupi partizan apo brigade, divizioni sulmues ose Korparmate të kësaj ushtrie ashtu si dhe në krye të Shtabit të Përgjithshëm, krahas komandantit gjendej edhe Komisari Politik. Ky post ishte politik e partiak sepse Komisari ishte i dërguari i PKSH dhe përçonte në çdo kohë vijën dhe direktivat e saj për Luftën Antifashiste NÇ. Përveç këtij fakti krejt të dukshëm dhe të njohur për gjithkënd që e njeh historinë e Luftës dhe sidomos atë të UNÇSH, në çdo nënrepart, repart ose njësi të kësaj ushtrie ngriheshin dhe funksiononin forumet e PKSH, si celulat, organizatat deri tek byrotë dhe komitetet e PKSH që drejtoheshin nga sekretarët e tyre.

Roli i tyre në formacionet e UNÇ ishte jo vetëm udhëheqja me shembullin dhe frymëzimin e anëtarëve të partisë të efektivave partizane paparti, që përbënin shumicën dërrmuese. Prej kësaj organet e partisë, madje, merreshin edhe me miratimin e planeve të aksioneve, luftimeve apo operacioneve luftarake të formacionit të tyre që e realizonin drejtpërdrejt më anën e komisarit politik. Por, nëse B. Fisher e ka fjalën për numrin e anëtarëve të PKSH-së në UNÇSH, atëherë këtu duhet të ndalemi sepse gjërat qëndrojnë disi më ndryshe. Sipas të dhënave dokumentare të kohës së LANÇ, në Fazën e Parë të saj, që u përmbyll në fillim të muajit korrik 1943, që përkon me atë të krijimit të njësiteve guerile, çetave dhe batalioneve partizane, kohë kur forcat partizane arritën në afro 10.000 luftëtarë,[22] PKSH numëronte vetëm 700 anëtarë[23] të saj në radhët e tyre. Kjo shifër përbënte më pak se 1 për qind të krejt efektivit partizan.

Ndërsa tre vite më vonë, në nëntor 1944, kur UNÇSH, prej disa muajve kishte nisur procesin e shndërrimit në Ushtri të rregullt, me një Komandë të Përgjithshme, të unifikuar dhe me grada e rregullore ushtarake, si në ushtritë e rregullta klasike, kur ajo numëronte 70.000 luftëtarë, numri i anëtarëve të Partisë Komuniste nuk i kalonte 4-5 për qind, apo 2800 deri 3.500 vetë.[24]

---

[21] Gazeta DITA, Tiranë, 24 tetor 2014, f. 2.

[22] Historia e LANÇ të Popullit Shqiptar, 1939-1944, Vëll. 2. Shtypshkronja “8 Nëntori”, Tiranë 1986, f. 308.

[23] Po aty, f. 128.

[24] Histori e Pashkruar, e cituar, f. 171.

Nga ana tjetër, nuk duhet harruar se, dukuria e përfshirjes së faktorit partiak-politik në drejtimin ushtarak të formacioneve luftarake, që nuk kishte traditë në Shqipëri, mund të thuhet se nuk u përfaq vetëm tek UNÇSH. Ka argumente të mjaftueshme për të besuar se, kjo dukuri ishte e prekshme dhe e dallueshme edhe tek dy forcat e tjera, ndonëse jo në këto përmasa, sisteme dhe skema si te forcat e UNÇ Shqiptare. Kjo është një e vërtetë historike e pakundërshtueshme sepse është fakt që faktori politik-partiak ka qenë i pranishëm në të tre fazat kryesore luftarake shqiptare që vepruan më dukshëm në skenën e luftës në Shqipëri.[25]

Ndër veçoritë e tjera të forcave luftarake të UNÇ ishin mënyrat se si ishte zgjidhur dhe arritur disiplina ushtarake në të gjitha aspektet e saj. Në disa raste madje ajo ishte shumë e fortë dhe e ashpër në dënimet për shkeljet e saj. Por, ashpërsia justifikohej me faktin e të qenit një ushtri jo e rregullt, por vullnetare, prandaj shpesh përdorte dënime të ashpra për të ndëshkuar shkeljet dhe fajet disiplinore. Lidhur me këto shfaqje, misionari anglez R. Hibbert do të shkruante se në sistemin disiplinor të UNÇ bënte pjesë edhe gjyqi, gjë që kishte krijuar,"…pothuajse nga hiçi një ushtri të rreckosur, por të bashkuar, në pranverën e viti 1944".[26]

Kjo nënkuptonte se një ushtri vullnetare, sidomos në dy fazat e para të LANÇ-it, siç ishte UNÇSH, i kishte të justifikuara masat e shtrënguara disiplinore ushtarake, por natyrisht pa përdorimin e tepruar apo ekstremin në disa raste!

Sot, teksa përkujtojmë jo për shkak të zakonit, por sepse e meritojnë gjithë ato forca antifashiste që organizuan dhe bënë Luftën Antifashiste NÇ dhe që çuan në çlirimin e vendit. Ata e bënë këtë duke u rreshtuar përkrah Aleatëve të Mëdhenj të Koalicionit Antifashist botëror, duke ndihmuar me mundësitë dhe përmasat e tyre në mposhtjen e fashizmit, në kuadrin e Luftës së Dytë Botërore. Përvoja e forcave luftarake që morën pjesë aktive në LANÇ të popullit shqiptar është shumëpalëshe, përfshi edhe ato në fushën e organizimit dhe artit ushtarak, përvojë që jo vetëm duhet përkujtuar me respekt. Ajo duhet analizuar dhe rivlerësuar duke e zhveshur nga teprimet, kultet dhe mitet por me realizëm dhe argument të shkruhet historia e tyre, mbi bazën e një optike sa më reale, të besueshme dhe sidomos, mbi bazën e një dokumentacioni të plotë dhe shumëpalësh. Kështu, kjo pjesë e historisë ushtarake dhe kjo përvojë krejt natyrshëm dhe pranueshëm do t'u shërbejë brezave dhe pasurimit të historisë së popullit shqiptar.

[25] Revista Ushtarake, nr. 4, viti 2005, f. 39.
[26] *Fitorja e Hidhur*, libër i cituar, f. 223.

Mbrojtja e Shkodrës gjatë Luftërave Ballkanike 1912–1913

Nënkolonel Msc. Gentian HALILAJ
Pedagog në FMS, AFA

Trajtesë e shkurtuar.

Studimi mbi luftën e Shkodrës është përpjekur të japë një përshkrim qartësues të panoramës së kohës sidomos nga ana ushtarake. Aty paraqitet konteksti historik i gadishullit ballkanik, veprimtaria diplomatike e fuqive të mëdha, mënyra si erdhën shtetet fqinje deri në këto vite dhe më kryesorja gjendja e rajonit të Shkodrës para fillimit të luftës.

Më pas shkrimi vijon me një analizë më të detajuar të fushës ushtarake për palët ndërluftuese. Si e kishin organizuar ushtrinë, shërbimin, cilat ishin doktrinat e tyre. Do të shohim me kujdes karakteristikat e terrenit ku zhvillohej teatri i luftimeve, konceptet e planet operacionale, drejtimet e afrimit të sulmeve dhe organizimin për detyrë të njësive ushtarake osmane, malazeze e serbe. Gjithashtu në përshtatje me doktrinën tonë ushtarake, do të shohim se si e organizoi divizioni i Shkodrës mbrojtjen dhe masat që u morën për realizimin me sukses të detyrës. Përveç këtyre do të zbresim më në detaje, për të parë se si u zhvilluan veprimet luftarake mësymëse dhe mbrojtëse, kundërsulmet, bashkërendimi i njësive, aplikimi i metodave tradicionale dhe moderne të luftimit në atë kohë. Literatura e shfrytëzuar për realizimin e temës është mbështetur në gërshetimin e rrëfimeve të dëshmitarëve të ngjarjes (ditarët dhe raportimet vetjake), të analizës politike dhe sociale nga historianë të fushës dhe të studimeve ushtarake për analizën e betejave. Lufta për Shkodrën si pjesë e luftërave ballkanike ka tërhequr vëmendjen e studiuesve, por edhe të opinionit të gjerë vendas dhe të huaj. Kjo për shkak të shumë ngjarjeve vendimtare, të cilat rrodhën brenda një periudhe 7-mujore dhe që do të ndikonin në të ardhmen e krahinës.

Fjalë kyçe: Ballkani, Shkodra, Hasan Riza pasha, fuqitë e mëdha, perandoria osmane, shqiptarët, luftërat ballkanike.

Hyrje

Rrethimi i Shkodrës në vitet 1912-1913 është një ngjarje historike e luftërave ballkanike, që ka lënë gjurmë të pashlyeshme në kujtesën e kombit tonë. Para dhe gjatë rrethimit jemi dëshmitarë të zhvillimeve të vrullshme politike dhe ushtarake në rrafshin rajonal dhe ndërkombëtar. Lufta për Shkodrën si pjesë e luftërave ballkanike ka tërhequr vëmendjen e studiuesve, por edhe të opinionit të gjerë vendas dhe të huaj.

Kërkimet dhe burimet e mëparshme janë përpjekur të hedhin dritë mbi arsyen se përse ngjarjet shkuan në atë mënyrë, por ndoshta të ndikuara edhe nga faktorë të jashtëm, janë përfshirë në vorbullën e interpretimit duke errësuar disi faktet. Përmbajtja e temës ka si qëllim të sjellë vetëm faktet, ashtu siç janë marrë nga burime autoritare, duke ia lënë në dorë lexuesve analizën e tyre, në bazë të asaj që lexojnë, pa e ndikuar gjykimin e tyre.

Punimi dëshmon se garnizoni i Shkodrës përbën një rast të veçantë të reparteve të ushtrisë osmane të vendosura në Ballkan. Ai synon të përcjellë një mesazh për ushtarakët, se "për të pasur sukses dhe për të përmbushur detyrën me njësitë e tyre, duhet të mbështeten vetëm në bindjen e uniformës dhe flamurit që mbajnë mbi vete".

1. Situata gjeopolitike e Ballkanit dhe interesat e fuqive të mëdha në fund të shekullit XIX dhe në fillim të shekullit XX

Gadishulli i Ballkanit për pothuajse pesë shekuj ka qenë "oborri para shtëpisë" i perandorisë osmane. Ajo kishte zotërimin absolut dhe nuk kishte lejuar asnjë fuqi "të interesuar" për të ndërhyrë në punët e saj brenda këtij territori. Por me kalimin e kohërave gjendja do të ndryshojë dhe një kombinim i faktorëve politiko-ushtarakë, të brendshëm dhe të jashtëm, do të sillte dobësimin e autoritetit të Portës së Lartë në gadishull.

Pjesa evropiane e Perandorisë Osmane përfshinte "një sipërfaqe prej 165,400 km^2, me një popullsi prej 5,500,000 banorësh dhe ndahej në 6 vilajete"[1] Nga të gjithë popujt e gadishullit, vetëm shqiptarët, maqedonasit dhe vllehët nuk kishin arritur të siguronin njohje si kombe dhe si shtet-formim. Grekët ishin të parët që përfituan nga mbështetja e fuqive të mëdha duke arritur pavarësinë më 1829-ën. Serbia dhe Mali i Zi me ndihmën e pakushtëzuar ruse fituan pavarësinë më 1878-ën dhe Bullgaria më 1908.[2] Rusia, kishte qëllimin e saj kryesor të shkatërronte Perandorinë Osmane dhe gjithashtu kishte si synim që të mbante larg fuqitë e tjera evropiane nga zona e saj e interesit.

[1] Joseph Swire, *Shqipëria ngritja e një mbretërie*, Tiranë: Dituria 2005, fq. 73.
[2] Xhafer Sadiku, *Shqipëria 1878-1928*, Tiranë: Pika pa sipërfaqe 2021, fq. 84.

Mendimi i saj parësor për zotërimin e rajonit ishte "të bashkonte të gjithë sllavët nën drejtimin rus"[3] për të shfrytëzuar me sukses ideologjinë pansllaviste. Kjo gjë do t'i shërbente si bazë për të dalë në Mesdhe nga Egjeu pasi të shtinte në dorë ngushticën e Dardaneleve bashkë me Kostandinopojën. Austro-Hungaria, kohët e fundit, e kishte shndërruar Ballkanin për politikën e saj të jashtme në interes strategjik dhe politiko-ekonomik. Pas daljes në skenë si fuqi perandorake e Gjermanisë në Evropë, Ballkani për Habsburgët u bë jetik, pasi Gjermania i rrëmbeu skenën kryesore evropiane duke i lënë vetëm një derë të hapur nga jugu i kufijve të saj.

Italia interesin kryesor e kishte që, në bregun përballë saj në Adriatik, të mos shfaqej asnjë shtet i fuqishëm, i cili do të pengonte qëllimet e saj në këtë drejtim. Franca kishte arritur që të kontrollonte ekonominë Osmane dhe rrymat politike që i dhanë hov zhvillimeve të vrullshme, gjithashtu kërkonte të shtinte në dorë territore të osmanëve në Siri dhe Liban. Anglia i qëndronte besnike parimeve të diplomacisë dhe interesave të saj. Ajo pasi kishte siguruar rrugët tregtare aq të rëndësishme për ekonominë dhe industrinë e saj, i kishte vënë syrin fushave naftëmbajtëse të Arabisë dhe Irakut[4]. Interes tjetër madhor kishte edhe ndalimin e Rusisë për të marrë ngushticën e Dardaneleve. Interesat e Gjermanisë në Stamboll ishin të gjithanshëm "me orientim të theksuar financiar"[5]. Prandaj ajo shqetësohej të ruante sa më shumë *status quo*-në e Perandorisë Osmane.

Gjendja e trojeve shqiptare në fillim të shekullit XX paraqitej e vështirë në të gjitha drejtimet. Në çdo fushë shqiptarët i karakterizonte një prapambetje e thellë. Megjithatë elita e kombit po bënte përpjekje që të dilnin nga kjo gjendje. Shqipëria sipas Sami Frashërit në botimin e tij të vitit 1889, "kishte një sipërfaqe prej 80 mijë km^2, me popullsi prej dy milionë e gjysmë banorë. Ajo ishte e ndarë në katër vilajete, Vilajeti i Shkodrës, Vilajeti i Shkupit, Vilajeti i Manastirit dhe Vilajeti i Janinës. Shkodra ishte e ndarë në dy sanxhakë, Shkodra dhe Durrësi, dhe dhjetë kaza, me pesëqind e pesëdhjetë mijë banorë"[6], pothuajse dyfishin e popullsisë së Malit të Zi. Pas shtypjes së Lidhjes Shqiptare të Prizrenit dhe vendimeve të Kongresit të Berlinit, Shkodra kishte humbur disa pjesë historike të saj kufitare me Malin e Zi si, Kuçi, Koja, Triepshi, Podgorica, Nikshiqi, Zhabjaku bashkë me Ulqinin dhe Tivarin.

Malësorët i druheshin ndarjes së tokave të tyre nga demarkacioni i kufirit osmano-malazez. Ky fakt do të shpinte në një konflikt të hapur shqiptaro-osman, që sipas historianit Romeo Gurakuqi do të shtrihej në tre dimensione; "arsim-

[3] Hamdi Ertuna *Mbrojtja e Shkodrës dhe Hasan Riza Pasha*, Tiranë: Jehona Study Center, 2006, fq.18
[4] Po aty, fq. 21.
[5] Romeo Gurakuqi, *Shqipëria 1911-1914*, Tiranë: UET PRESS 2012, fq. 283.
[6] Përparim Rexhepi, *Mbrojtja e Shkodrës 1912-1913,* Tiranë: Globus 2001, fq. 97.

kulturë, dhe ekonomik e ushtarak"[7]. Ky konflikt do të ishte i ashpër, intensiv dhe i pandërprerë deri në pavarësinë e Shqipërisë. Elementi shqiptar do të kishte shumë problematika gjatë kohës, për shkak të ndikimit të pjesës pavetëdije kombëtare që i shërbente pushtetit Osman dhe në momente të caktuara "do të frenonte dëshirat për shkëputje nga Porta"[8]. Por do të ishte kjo periudhë kur nacionalizmi shqiptar shfaqet më energjik dhe i organizuar, për arritjen e qëllimit historik. Ky fakt shqetësoi shtetet fqinjë që pretendonin zgjerimin mbi tokat shqiptare. Shqiptarët ndodheshin në këtë kohë në trysni të dyanshme nga reformat centralizuese të Xhonturqve dhe rrezikut të gllabërimit nga fqinjët.

Rrjedha e ngjarjeve ndiqej me kujdes nga mbreti i Malit të Zi, pasi zhvilloheshin paralelisht me një moment shumë të rëndësishëm në historinë moderne të malazezëve. "Ata siguruan lejen nga fuqitë e kohës për t'u shndërruar nga principatë në mbretëri"[9]. Çdo veprim që do të kryhej nga malësorët në Shkodrën fqinje, do të studiohej mirë nga malazezët, do të peshohej me kujdes dhe do të bëheshin të gjitha përpjekjet që të kanalizoheshin këto veprime drejt përfitimeve territoriale të mundshme në të ardhmen e afërt. Prandaj loja politike duhej të krijonte idenë se malazezët mbështesnin shqiptarët kundër osmanëve, duke i nxitur ata për luftë. Me zgjatjen sa më shumë të konfliktit të armatosur, krajl Nikolla arrinte dy qëllime: konsumimin e energjive të malësorëve dhe dobësimin ushtarak të osmanëve. Në këtë mënyrë "i lehtësonte punë vetes për aneksimin e Shkodrës"[10]. Ndërkaq, Mali i Zi kishte nisur edhe manovrimet diplomatike duke dërguar "mesazhe sekrete në Beograd për të ditur se si do të reagonte Serbia nëse ai do të ndërhynte për zgjidhjen e problemit shqiptar"[11].

Më 24 mars 1911 "filloi kryengritja e malësorëve"[12] të udhëhequr nga Dedë Gjo Luli, i cili sulmoi dhe pushtoi pikat kufitare të ruajtura nga osmanët. Më 30 mars u mor qyteti i Tuzit, ndërsa garnizoni osman u mbyll në kështjellën e Shipshanikut. Po më 30 mars kryengritësit i drejtuan një memorandum fuqive të mëdha, ku kërkesat shtriheshin në rrafshin kombëtar. Malësorët kishin marrë "pishtarin e flakës së revoltës kombëtare"[13]. Më 6 prill 1911 në Bratilë të Deçiqit u ngrit për herë të parë pas 500 vjetëve flamuri kombëtar me

[7] Romeo Gurakuqi, Shqipëria 1911-1914, Tiranë: UET PRESS 2012, fq. 51.
[8] Po aty, fq. 51.
[9] Po aty, fq. 99.
[10] Joseph Swire, *Shqipëria ngritja e një mbretërie*, Tiranë: Dituria 2005, fq. 103.
[11] Romeo Gurakuqi, *Shqipëria 1911-1914*, Tiranë: UET PRESS 2012, fq. 109.
[12] Po aty, fq. 125.
[13] Në të kërkohej paprekshmëria e tokave shqiptare, gjuha shqipe si gjuhë zyrtare në të katër vilajetet, në zyra e gjyqe dhe si gjuhë mësimi ndër shkolla, të gjithë nëpunësit në Shqipëri të ishin shqiptarë me kombësi dhe kjo kombësi të njihej zyrtarisht, te ardhurat buxhetore të shpenzoheshin për dobi të vendit, ushtarë shqiptarë të mos kalonin kufijtë me përjashtim të rasteve të luftës.

shqiponjën dykrenore fakt që tregon karakterin atdhetar dhe kombëtar të kësaj kryengritjeje. Për mbrojtjen e tij ranë heroikisht shtatë dëshmorë shqiptarë. Në gjysmën e dytë të prillit mbërriti në Shqipëri ekspedita ndëshkuese osmane, me komandant Turgut Pashën. Beteja të ashpra janë zhvilluar për rimarrjen e postave kufitare dhe rivendosjen e gjendjes në këto zona. Kjo periudhë luftimesh ndiqej me kujdes nga malazezët të cilët shikonin afrimin e ëndrrës së tyre për zgjerim në jug, pasi shqiptarët dhe osmanët kacafyteshin mes tyre. Më 23 qershor 1911 kryengritësit paraqitën kërkesat e tyre në atë që quhet "Memorandumi i Greçës"[14]. Aty përfshihej edhe kërkesa për autonomi kombëtare. Gjatë kësaj periudhe, qeveria Osmane ishte përpjekur për të ulur tensionet duke dërguar imzot Jak Serreqin, Arqipeshkv i Shkodrës, për të bindur malësorët të ktheheshin.

Pas shumë diskutimesh për kushtet e ofruara nga qeveria, kryengritësit pranuan të ktheheshin. Më 4 gusht 1911 kryengritja u shua. Kjo kryengritje pati 4 faza kulmore gjatë zhvillimit të saj:

1. Ngritja e flamurit të Skënderbeut në tokën shqiptare, pas 500 vjetësh të pushtimit osman, gjë që tregoi se nga e merrnin frymëzimin luftëtarët malësorë.
2. Hartimi i memorandumit të Greçës që tregoi se synimet e shqiptarëve nuk kishin më karakter lokal por kombëtar.
3. Për herë të parë çështja shqiptare diskutohej nga kancelaritë diplomatike evropiane, jo më si "shprehje gjeografike", por si komb me autonomi të Shqipërisë, megjithëse e paqartë nga ana e kufijve.
4. Për herë të parë gjatë 500 viteve pushtim, osmanët uleshin në bisedime me shqiptarët duke nënshkruar marrëveshje dypalëshe që do të shërbente si bazë juridike për kërkesat e ardhshme për autonomi të Shqipërisë.

Në përfundim kjo kryengritje ishte faza kalimtare drejt ballafaqimit përfundimtar shqiptaro-osman më 1912-ën dhe po ashtu edhe me fqinjët. Marrëveshja e 1911-ës nuk po zbatohej, ajo po zvarritej nga osmanët. Shqiptarët po organizoheshin përsëri për revolta të cilat kësaj radhe do të organizoheshin në çdo krahinë. Shkëndija u dha në Kosovë dhe u përhap gjithandej duke çliruar qytetet shqiptare njëri pas tjetrit. Nga Mitrovica në Manastir, nga Shkodra në Janinë, trupat osmane u çorganizuan dhe rendi e

[14]Memorandumi përfaqësonte programin politik të lëvizjes kombëtare shqiptare. Ky program përfshinte kërkesën për njohjen e autonomisë së Shqipërisë në bazën e decentralizimit administrativ. Garanci kundër trajtimeve jokushtetues, emërimin e një inspektori të përgjithshëm për vilajetet shqiptare, njohjen e nacionalitetit shqiptar, kryerjen e shërbimit ushtarak brenda krahinës, kthimin e armëve të konfiskuara, përdorimin e gjuhës shqipe, të drejtën e shkollës shqipe, caktimin e zyrtarëve shqiptarë etj.

ligji ishte në dorë të shqiptarëve. Ata iu drejtuan sulltanit me kërkesa që u bashkëngjiteshin "Manifestit të Ismail Qemalit, ku kërkohej autonomia e Shqipërisë"[15]. Por ekzistonte një ndarje e "grupimeve që udhëhiqnin lëvizjen me objektiva të ndryshëm"[16], qeveria osmane pranoi kushtet e kryengritësve me përjashtim të mbajtjes së armëve, duke kënaqur një pjesë të udhëheqësve të saj. Me këtë lëvizje, qeveria fitoi kohë duke ruajtur pozitat e saj në trojet shqiptare. Kjo gjendje solli amulli dhe çorganizim politik, administrativ dhe ushtarak duke u treguar fqinjëve haptazi dobësitë. Në këtë gjendje e gjen vilajetin e Shkodrës, pragu i luftës së parë ballkanike. Dukej se projekti dhe ëndrra e Nikollës së Malit të Zi po realizohej.

2. Strukturat ushtarake, organizimi për detyrë dhe planet operacionale të palëve ndërluftuese të luftës së Shkodrës

Struktura ushtarake e osmanëve përmbante një ushtri të rregullt profesioniste. Personeli përbëhej nga nizamët (ushtarë aktivë), redifët (rezervistët), mustafëz (forca territoriale), Ajo kishte pajisje dhe armatim modern për kohën dhe përvojë luftimi. Osmanët kishin marrë modelet perëndimore të organizimit ushtarak duke përshtatur doktrinat franceze, britanike dhe gjermane, me këtë të fundit mbizotëruese. Në kohë paqeje malazezët kishin një organizatë paraushtarake, por jo një ushtri të mirëfilltë. Ajo përbëhej nga 2 divizione mësimore këmbësorie dhe deri më 1910-ën "stërvitja zhvillohej në bazë fshati"[17]. Ushtria nuk kishte as shtab madhor e as komandë të lartë, komandant i përgjithshëm ishte mbreti. Serbët kishin ndërtuar një sistem të stërvitjes ushtarake sipas modelit dhe doktrinave ruse dhe franceze. Stërvitja ndahej në verore dhe dimërore duke ndërthurur disiplinat dhe armët për kompaktësimin dhe bashkërendimin e njësive në shkallë të gjerë. Njësia bazë e ushtrisë ishte divizioni i këmbësorisë me 4 regjimente. Njësitë e mëdha grupoheshin në nivel armate dhe ishin tre të tilla.

Për mbrojtjen e Shkodrës ishte caktuar "divizioni 24 i komanduar nga koloneli Hasan Riza pasha"[18] Në rast lufte kalonte në korpus me emërtimin "Korpusi i Shkodrës" duke u përforcuar me divizionet e rezervistëve, "gjithsej 49

[15] Romeo Gurakuqi, *Shqipëria 1911-1914*, Tiranë: UET PRESS 2012, fq. 378.

[16] Po aty, fq. 399. "Grupet shqiptare të Kosovës përshkruhen në këtë mënyrë nga diplomati britanik, për sa i përket orientimeve politike. Ai dallon tri grupime politike brenda lëvizjes shqiptare në vilajetin e Shkupit: 1. Grupi i parë është ai Ententist, i kryesuar nga Hasan Prishtina (në opozitë me xhonturqit). 2. Grupimi politik autonomist i përfaqësuar nga Riza beu. 3. Partia reaksionare e përfaqësuar nga Isa Boletini (përfaqësonte fiset malore dhe qëllimi i tyre ishte ruajtja e shoqërisë tradicionale)

[17] Përparim Rexhepi, *Mbrojtja e Shkodrës 1912-1913,* Tiranë: Globus 2001, fq. 20.

[18] Divizioni 24 i Shkodrës ishte autonom dhe kishte në organikë R70K, R71K, R72K me 9 batalione, R24AT, batalionin 24 të qitësve (nishanxhi) dhe kompanitë kufitare, kompani xheniere, ndërlidhjeje dhe banda muzikore.

batalione këmbësorie, 15 nga 49 batalione ishin forca shqiptare"[19] të shpërndarë në gjithë vilajetin e Shkodrës. Duhet theksuar se kompletimi me personel në fillim të sulmit ishte i dobët. Ushtria osmane e kishte filluar mobilizimin më 1 tetor, "pas një vendimi absurd të qershorit 1912 për çmobilizim"[20]. Në prag të luftës ushtria osmane "karakterizohej nga një amulli dhe mungesë disipline në radhët e saj"[21]. Malazezët për herë të parë e krijuan strukturën ushtarake më 4 divizione, divizioni I i Cetinës, komandant gjenerali Ivo Goroviç, divizioni II i Podgoricës me komandant gjeneralin Boshkoviç, divizioni III i Nikshiqit me komandant gjeneralin Nikoliç dhe divizioni VI i Kolashinit me komandant gjeneralin Jankoviç.

Ushtria malazeze synonte që ta sulmonte Shkodrën "nga tre drejtime, veri, jug dhe qendër"[22]. Për zhvillimin e operacioneve sipas idesë së mbretit, "ushtria u nda në tre grupime operacionale: a) grupimi i Zetës, b) i Lindjes dhe c) i Jugut".[23] Goditja kryesore parashikohej të jepej në dy drejtime, i pari më kryesori ishte Podgoricë-Tuz-Koplik-Shkodër dhe i dyti ndihmues ishte Virpazar-Tarabosh dhe Ulqin-Tarabosh. Divizioni 24 i Shkodrës, do t'i kundërpërgjigjej malazezëve në dy drejtime kryesore, Tuz-Podgoricë dhe Beranë-Andrijevicë-Podgoricë, me qëllim për t'i futur mes dy zjarresh.

Komanda e divizionit 24 kishte planëzuar se forcat kryesore do t'i fuste në luftim në dy objekte të fortifikuara, Tuz dhe Shkodër[24]. Serbia, pas hyrjes në luftë, caktoi armatën e tretë të krijonte "Grupimin e Shqipërisë" "për të lëvizur në drejtim të Shëngjinit"[25] duke kapur Lezhën nga dy drejtime, Zhur-Lumë-Orosh dhe Qafë-Mali-Pukë-Mjedë. Osmanët ishin të detyruar që të planifikonin masat e tyre për t'u mbrojtur dhe një delegacion i lartë ushtarak i kryesuar nga mareshali Fevzi Çamak caktoi katër fronte të rëndësishme: Rajoni i Veriut; i Lindjes, i Perëndimit (Taraboshi) dhe i Jugut".[26] Vetë komanda e korpusit "nxori detyrat e saj, duke caktuar pesë rajone kryesore të mbrojtjes së qytetit"[27]: a) Taraboshi, b) Shtoji, c) Bardhaj, ç) Kodra e Tepes dhe d) Bërdica. Secili rajon formën e mbrojtjes e kishte me skemë rrethore. U morën masa për fortifikimin dhe "objektet fortifikuese u ndërtuan me transhe,

[19] Përparim Rexhepi, *Mbrojtja e Shkodrës 1912-1913,* Tiranë: Globus 2001, fq. 73.
[20] Po aty, fq. 15.
[21] Hamdi Ertuna, *Mbrojtja e Shkodrës dhe Hasan Riza Pasha*, Tiranë: Jehona Study Center, 2006, fq. 23, 35, 36. "Në veçanti marrja e ushtarakëve me politikë, prishte disiplinën e ushtrisë dhe e bënte atë të merrte fund".
[22] Po aty, fq. 42
[23] Përparim Rexhepi, *Mbrojtja e Shkodrës 1912-1913,* Tiranë: Globus 2001, fq. 22-23.
[24] Po aty, fq. 31.
[25] Po aty, fq. 68.
[26] Hamdi Ertuna, *Mbrojtja e Shkodrës dhe Hasan Riza Pasha*, Tiranë: Jehona Study Center, 2006, fq. 41-42.
[27] Po aty, fq. 41

radhë telash me gjemba dhe në formën e patkoit"[28].

Shkodrën e ndihmonte edhe terreni, i cili ofronte mbrojtje natyrore duke favorizuar veprimet mbrojtëse dhe duke vështirësuar ato sulmuese. Pengesat ujore, sistemi i kodrave dhe maleve, moçalishtet mes Vaut të Dejës, Zadrimës dhe Gjadrit ishin të pakalueshme dhe pengonin hapjen e trupave në rendim luftimi, sidomos në dimër. Për t'u harmonizuar me terrenin, mbrojtja e qytetit u organizua në dy vija: a) Vija e jashtme që fillonte në veriperëndim nga shpati perëndimor i Taraboshit, vijonte në lindje dhe juglindje përgjatë Bërdicës, Vukatanës dhe Rencit, zgjatej në veri dhe verilindje në liqen, Shtoj dhe Drisht dhe përfundonte në Lodërtunë, Bardhaj, Renc. b) Vija e dytë fillonte po nga Taraboshi, kodrat e Tepes, Bardhaj i Vogël, Kir, Golem e Dobraç. Artileria ishte vendosur në majën e Bajrakut 395 m dhe Tarabosh 591 dhe 521 m, në Bërdicë, Tepe, Bardhaj, Myselim dhe Shtoj. "Qendër rëndese për terrenin vlerësohej Taraboshi"[29] Fortifikimit të Taraboshit iu kushtua rëndësi e veçantë dhe aty u caktua pjesa më e madhe e trupave dhe fuqisë së zjarrit.

Ishin planifikuar edhe trupa që do të mbronin krahët nga Velipoja, por edhe për ruajtjen e lidhjes me limanin e Shëngjinit nga mund të vinin furnizimet dhe përforcimet. Në punimet fortifikuese të sistemit mbrojtës të Shkodrës, ishin ndërthurur me mjeshtëri nga Hasan Riza pasha, të gjitha teknikat e nevojshme tradicionale dhe të reja për kohën. Sistemi ishte ndërtuar duke pasur parasysh mbulimin e hapësirave nga forcat e pakta të vendosura në pika mbizotëruese. Kishte gropa thithëse, llogore të mbushura me ujë dhe ndriçim me prozhektorë. Të gjitha rajonet komunikonin në mënyrë të pandërprerë më qendrën dhe njëri-tjetrin. "Gjatësia e vijës mbrojtëse arrinte 37 km"[30]. Në vazhdën e përgatitjeve u morën masa për furnizimin me armatim-municion, ushqime, mbledhjen dhe racionimin e rezervave ushqimore, lëndë djegëse etj.

3. Veprimet luftarake të ushtrive ndërluftuese

Më 8 tetor 1912, Mali i Zi i shpalli luftë shtetit osman, njoftimi komandës së Shkodrës iu dha një ditë më vonë. Ndërkohë Grupimi i Lindjes i komanduar nga gjenerali Vukotiç kaloi kufirin nga jugu i liqenit të Shkodrës dhe iu drejtua Beranës, Gjakovës dhe "zuri Pejën më 4 nëntor, duke u takuar me divizionin serb Drini I"[31]. Kështu krahu verilindor i ushtrisë osmane u thye duke mos i rezistuar dot sulmit. Grupimi i Zetës iu drejtua Tuzit që ishte pengesa e parë drejt Shkodrës. Për marrjen e Tuzit, "në krah të forcave malazeze u radhitën

[28] Përparim Rexhepi, *Mbrojtja e Shkodrës 1912-1913,* Tiranë: Globus 2001, fq. 39.

[29] Po aty, fq. 41. "Kush kishte Taraboshin, kishte Shkodrën". Aty u ndërtuan 9 nga 21 pikëmbështetjet për këmbësorinë dhe 5 nga 8 për artilerinë, me 3 vija mbrojtëse të përforcuara me 4-8 radhë pengesash me tela me gjemba.

[30] Po aty, fq. 108.

[31] Po aty, fq. 29

edhe një numër i madh malësorësh shqiptarë"[32], të cilët luajtën një rol kryesor për marrjen e Deçiqit, Vuksanlekajt, Traboinit etj. Më 13 tetor Tuzi u pushtua duke i dhënë mundësi grupimit të Zetës të bashkohej me grupin e Jugut i cili që nga 8 tetori sulmonte Taraboshin. Nga sulmi i parë malazezët arritën të marrin malin e Krajës duke përparuar në malet e Sukës, Golishtit, Goricës dhe Selitës. Osmanët duke përfituar nga një pasivitet i malazezëve, arritën të përforcojnë Taraboshin me 3 batalione dhe kundërsulmuan për të rimarrë territorin e humbur.

Më 20 tetor, u pushtua Kopliku nga grupimi i Zetës dhe më 26 tetor të dy grupimet kaluan njëkohësisht në mësymje, duke marrë lartësitë 277 m dhe 262 m në Lodërtunë. Osmanët kundërsulmuan një ditë më pas dhe vetëm më 30 tetor arritën të rimarrin lartësitë e humbura. Malazezët humbën 1500 ushtarë, besimin për sukses dhe gjenerali i divizionit III u shkarkua nga detyra. Ky mosrealizim objektivi bëri që ata të pezullonin përkohësisht veprimet dhe të rimendonin manovrën. Shkodra s'do sulmohej me trupa, por me artileri. Gjatë kësaj kohe trupat serbe pasi kishin marrë Kosovën, krijuan dy grupime nga armata e 3, "me detyrë që të kapnin bregdetin shqiptar nga Shëngjini deri në Durrës"[33]. Këto grupime do të niseshin nga Gjakova në drejtimin Qafë-Mali-Pukë-Mjedë për të pushtuar Lezhën dhe Shëngjinin dhe Prizreni në drejtimin Zhur-Lumë-Orosh të dilte në Lezhë dhe në të pastajmen do të pushtonte Krujën, Tiranën dhe Durrësin. Serbët morën Lezhën më 18 nëntor e në të njëjtën ditë pushtuan edhe Shëngjinin dhe më 28-29 nëntor morën Krujën dhe Tiranën duke vendosur Shkodrën nën rrethim, si nga toka ashtu edhe nga deti. Në mes të nëntorit mbërriti në Shkodër edhe Esad pashë Toptani me rezervistët e tij duke sjellë një ngërç në zinxhirin e komandimit, pasi si detyrë (komandant korpusi dhe vali i Shkodrës) i takonte Hasan Riza pashës (kolonel), ndërsa si gradë dhe për numrin e forcave i takonte Esadit (gjeneral brigade). Kjo u zgjidh duke graduar gjeneral, Hasan Rizain.

Gjatë kohës kishin ndodhur ndryshime në sferën politike dhe diplomatike. Shqipëria shpalli pavarësinë dhe asnjanësinë e saj më 28 Nëntor 1912, më 17 dhjetor në Londër u mblodh konferenca e ambasadorëve të fuqive të mëdha, për të gjetur një zgjidhje për luftën ballkanike. Në lidhje më këto ngjarje Mali i Zi shtoi përpjekjet për marrjen e Shkodrës, për ta bërë fakt të kryer marrjen e qytetit dhe të legjitimonte kërkesat e tij në sytë e ambasadorëve. Mbreti Nikolla duke parë se marrja e Shkodrës po zgjatej tej parashikimeve fillestare, vendosi të dërgonte njësi shtesë në terren. Tani malazezët nuk bombardonin vetëm njësitë ushtarake, por edhe popullsinë civile në lagjet e qytetit, me qëllim demoralizimin e saj, duke shkelur kështu konventat ndërkombëtare të kohës.

[32] Edith Durham, *Brenga e Ballkanit dhe vepra të tjera për Shqipërinë*, Tiranë: 8 Nëntori 1991, fq.267
[33] Përparim Rexhepi, *Mbrojtja e Shkodrës 1912-1913,* Tiranë: Globus 2001, f. 67

"Shënjestër ishin lagjet myslimane, më pas edhe ato katolike si dhe selitë diplomatike të fuqive të mëdha"[34] Më 16 dhe më 22-24 nëntor, malazezët sulmuan fuqishëm pas një bombardimi të gjatë, Bardhajn, Shtojin, Taraboshin e Rencin, por pa sukses. Hasan Riza Pasha ndaloi edhe korrespondencën diplomatike, "në qytet as hynte e as dilte asnjë lajm"[35]. Më 3 dhjetor u arrit një armëpushim mes shteteve ndërluftuese, por Hasan Riza pasha e refuzoi atë, "duke mos zbatuar urdhrin e ardhur nga Stambolli"[36]. Pas këtij akti egërsia e sulmeve malazeze u rrit dhe më 5 dhjetor grupimi i Zetës sulmoi gjithë vijën e mbrojtjes së Bardhajt, ku luftimet zgjatën 8 orë pa ndërprerje. Hasan Riza pasha dha urdhër për të mos bërë asnjë hap pas, duke treguar një vendosmëri të admirueshme, madje tregohej edhe i guximshëm duke zhvilluar një mbrojtje aktive me kryerjen e kundërsulmeve për rimarrjen e territoreve të humbura. Kështu ai sulmoi malazezët në Oblikë më 11 nëntor dhe 24 dhjetor në Bardhaj dhe serbët më 16 dhjetor në Mjedë duke u rimarrë Paçramin, Pistullin dhe Hajmelin. Deri më 20 janar 1913 gjendja ishte e qetë dhe u shfrytëzua nga palët për të rigrupuar forcat, për të përmirësuar planet luftarake dhe për të riparuar fortifikimet. Një ngjarje e papritur ndryshoi rrjedhën e ngjarjeve. Hasan Riza pasha u vra në një atentat pasditen e 31 janarit 1913 dhe komandën e garnizonit osman e mori Esad pashë Toptani. Ka shumë hipoteza mbi vrasjen e tij, disa akuzojnë pashain tiranas, disa oficerët xhonturq e disa mendojnë se shkaku ishte moszbatimi i urdhrit të armëpushimit të 3 dhjetorit 1912.

Në fillim të shkurtit mbreti Nikolla kishte planifikuar të ndërmerrte një sulm, për këtë ai kërkoi ndihmën e ushtrisë serbe për bashkërendim sulmi për marrjen e qytetit dhe më 5 shkurt 1913 mbreti Nikolla dha urdhrin për sulm të përgjithshëm për marrjen e Shkodrës, me goditje kryesore kundër Bardhajt e Taraboshit. Sulmin do ta kryente grupimi i Zetës kundër Bardhajt të Madh dhe Bardhajt të Vogël, grupimi i Jugut do të sulmonte Taraboshin, ndërsa serbët me divizionet e tyre do të sulmonin vijën Bërdicë-Beltojë. Pas 3 orësh zjarri me artileri, në orën 11:00 të datës 7 shkurt 1913 serbo-malazezët sulmuan. Intensiteti dhe ashpërsia e sulmit i kaloi kufijtë e imagjinatës. Luftimet më brutale ishin në Myselim, Lodërtunë, Bardhaj e Renç. Sulmi rifilloi të nesërmen deri në përleshje trup me trup. Malazezët arritën të merrnin dy transhetë e para në Shtoj dhe Shirokën në Tarabosh. Megjithatë garnizoni i Shkodrës urdhëroi një kundërsulm gjatë natës dhe deri në mëngjes i rimorën transhetë e humbura të Shtojit. Në Bardhaj të Madh malazezët bombarduan rajonin e mbrojtjes për 11 orë rresht dhe pas

[34] Xhino Berri, *Rrethimi i Shkodrës,* Tiranë, SHBU 1998, fq. 80, 165, 166, 175, 176

[35] Hortense von Zambaur, *Rrethimi i Shkodrës,* Tiranë: Argeta 2019, fq. 31.

[36] Përparim Rexhepi, Mbrojtja e Shkodrës 1912-1913, Tiranë: Globus 2001, fq. 91. "Tashmë Shkodra është qytet shqiptar dhe nuk mund të marrë urdhra nga një komandë turke dhe se qytetit dëshiron të mbrojë pavarësinë e vet kundër malazezëve".

sulmit me këmbësori arritën ta merrnin atë, por nga lodhja dhe duke mos qenë të vetëdijshëm për shthurjen dhe panikun e mbrojtësve nuk e zhvilluan ndjekjen për pushtimin e Bardhajt të Vogël. Gjenerali Vukotiç dha urdhër për të ndaluar dhe për të mbajtur Bardhajn e Madh, Lodërtunën dhe Myselimin. Me gjithë rraskapitjen nga luftimet e përgjakshme, komanda e Shkodrës kundërsulmoi në mbrëmje, por nuk arriti t'i rimerrte.

Me qëllim që të mbanin të angazhuara forcat osmane, malazezët iu lutën serbëve të sulmonin nga Bërdica. Serbët sulmuan natën me dy kolona në një terren moçalor. Krahu i majtë nuk e çau dot moçalin dhe nga errësira humbi kontaktet me komandën eprore dhe për pasojë komandanti i kolonës vendosi të mos përparojë. Kështu që krahu i djathtë sulmoi i vetëm, por mbrojtja i asgjësoi nën dritën e prozhektorëve, të futur në kurth nga gardhet me tela dhe gropat e thella të tokës moçalore. Sipas burimeve serbo-malazezët patën rreth 3100 të vrarë, grupimi i Zetës humbi rreth 40% të njerëzve, ndërsa mbrojtësit 700 të vrarë e 1700 të plagosur. Ky operacion zgjati 3 ditë e net pothuajse pa ndërprerje. Llogaritet se u harxhuan 6 milionë fishekë dhe ushtarët nuk patën kohë as për t'u ushqyer. Në përfundim të këtij operacioni forcat armike ishin konsumuar aq shumë sa që deri më 31 mars nuk kryen asnjë veprim, ndërsa serbët kaluan në pozita mbrojtëse dhe kërkuan përforcime nga Beogradi.

Këto përforcime erdhën në Shëngjin nga porti i Selanikut me anijet e flotës greke, të ndarë në tre konvoje. U transportuan 15 mijë trupa dhe 4 aeroplanë luftarakë me një kosto 1 milion dinarë. Gjatë kësaj kohe gjenerali Bozhidar Jankoviç, për të vazhduar luftën, i vuri kushte mbretit Nikolla. Ai kërkoi tërheqjen e malazezëve nga Kosova, komanda serbe të ishte e lirë në planet e saj dhe të merrte drejtimin e luftës duke përfshirë edhe drejtimin e trupave malazeze. Në vazhdim Nikolla ndjente peshën e kohës. Sa më shumë rezistonte Shkodra aq më shumë zvogëloheshin mundësitë që ambasadorët në Londër të vendosnin në favor të Malit të Zi. Më në fund pas tre muajsh debatesh, diskutimesh dhe propozimesh, në Londër u vendos që Shkodra t'i mbetej Shqipërisë së pavarur. Shqiptarët me rezistencën e tyre "kishin arritur një fitore diplomatike për rastin e Shkodrës"[37] Deri më tani rrethimi kishte hyrë në muajin e gjashtë, rezervat ushqimore të qytetit ishin pakësuar, njerëz nga popullsia civile vdisnin nga uria, lëndët e para pothuajse ishin mbaruar, racionimi dhe zvogëlimi i racioneve ushqimore për ushtrinë kishte filluar të aplikohej dhe shumica e ndërtesave të qytetit ishin djegur ose rrënuar nga bombardimet. Më 10 prill serbët morën urdhër që të tërhiqeshin nga Shqipëria dhe më 15 prill filluan lëvizjen nga Shëngjini e Durrësi. Arsenalin ushtarak ua lanë malazezëve. Por më 23 prill 1913 ngjarjet do të rrokulliseshin, pasi qyteti pas negociatave dhe marrëveshjes iu dorëzua malazezëve.

[37] Përparim Rexhepi, *Mbrojtja e Shkodrës 1912-1913,* Tiranë: Globus 2001, fq. 150.

Pas 434 vitesh në Shkodër përfundoi sundimi osman, por liria nuk erdhi. Pas firmosjes së marrëveshjes së dorëzimit me kushtet e caktuara nga të dy palët, princi Danillo hyri "triumfues" në kështjellën e Shkodrës dhe me ceremoni u ul flamuri osman dhe u ngrit ai malazez. Pushtimi i malazezëve do të zgjaste deri më 14 maj 1913, kur të detyruar nga fuqitë e mëdha, braktisën Shkodrën dhe qyteti kaloi nën administrimin ndërkombëtar.

Përfundime

Mbrojtja e Shkodrës pa frikë mund të konsiderohet si një epope e lavdishme e shtetit të sapoformuar shqiptar dhe akt heroik i korpusit 24 autonom të Shkodrës, ndryshe nga pjesa më e madhe e ushtrive osmane në Ballkan. Komanda e korpusit luajti një rol të pazëvendësueshëm në organizimin dhe drejtimin e veprimeve luftarake. Ajo ndryshe nga komandat simotra në Ballkan, nuk u demoralizua dhe nuk u përkul për t'u dorëzuar përballë armikut. Përkundrazi, ajo edhe pas disfatës në Tuz, ku humbi gjysmën e efektivit për atë moment, nuk mendoi të braktiste Shkodrën, por shfaqi vendosmëri dhe mori të gjitha masat për të luftuar nën rrethim. Komandantët e korpusit 24 autonom, shtabi, komandantët e njësive të rajoneve të mbrojtjes, zbatuan të gjitha njohuritë e tyre profesionale, përvojën e fituar gjatë viteve të shërbimit, duke vlerësuar drejt dhe me objektivitet të gjithë faktorët kyç që të garantonin suksesin. Ata shfaqën karakter, disiplinë, profesionalizëm, guxim dhe trimëri në të gjitha situatat duke u bërë shembull për vartësit e tyre. Ruajtja e rregullit ushtarak, disiplinës dhe moralit për një trupë në rrethim, është një detyrë e vështirë, por ushtarakët e Shkodrës e realizuan atë më së miri. Garnizoni i Shkodrës është i vetmi repart ushtarak osman që u dorëzua me kushte, duke ruajtur flamurin, armatimin dhe pajisjet.

Ky garnizon u dorëzua një muaj pas Edërnesë dhe një muaj e gjysmë pas Janinës, edhe pse këto të dyja kishin forca më shumë se Shkodra. Për arritjen e qëllimit, komanda e Shkodrës i bazoi planet e saj operacionale mbi doktrinën ushtarake osmane të kohës, mbi shfrytëzimin me mjeshtëri të terrenit, mbi llogaritjen e saktë të vendosjes së forcave dhe fuqisë së zjarrit, mbi planifikimin e saktë logjistik dhe zbatimin e metodave tradicionale dhe moderne të artit ushtarak. Gjithashtu u arrit që të lexohej mirë edhe mangësia e kundërshtarit në organizim, personel dhe manovër.

Për 7 muaj në Shkodër luftuan rreth 80 mijë forca; "24 mijë, garnizoni osman dhe 55 mijë, serbo-malazezë"[38]. Humbjet e armikut llogariten në 18 mijë forca (13.000 malazezë dhe 5.000 serbë), ndërsa të palës osmane 6.000 forca. Për herë të parë u përdorën transhetë me disa vija si dhe aviacioni si armë, megjithëse vetëm për detyra zbuluese. Malazezët shpresonin ta merrnin shpejt

[38] Përparim Rexhepi, *Mbrojtja e Shkodrës 1912-1913,* Tiranë: Globus 2001, fq. 188.

Shkodrën, pasi ishin të vetëdijshëm për kapacitetet e tyre të kufizuara, por nuk i bënë llogaritë mirë për kundërshtarin. Megjithëse bënë parapërgatitje intensive dy vjeçare, duke pasur në krahun e tyre 3.000 malësorë shqiptarë dhe megjithëse u ndihmuan nga serbët, ata nuk e morën Shkodrën me luftë. Mungesa e një shtabi të përgjithshëm dhe udhëheqja e ushtrisë sipas orekseve të mbretit, bënë që drejtimi i operacioneve të çalonte shumë. Serbët treguan se hasnin vështirësi në luftim kundër qendrave të fortifikuara, ndryshe nga sukseset në Kosovë dhe Maqedoni, në Shkodër ata dështuan.

Roli i shqiptarëve në këtë luftë ishte i madh si në komandim, ashtu edhe në zbatim. Shifrat flasin për 10.000 shqiptarë pjesë e njësive të ushtrisë osmane. Gjeografia e tyre shtrihej nga Malësia deri në Lushnjë e Pogradec. Vendosmëria e shqiptarëve së bashku me mbështetjen e popullsisë civile të qytetit, bëri të mundur që fuqitë e mëdha të bindeshin se ata donin të ishin pjesë e shtetit shqiptar. Në luftën e Shkodrës dallojmë katër faza luftimi: *faza e parë* 8 deri më 17 tetor 1912 kur ushtria malazeze arriti fitoret e para në Tuz dhe Rrafshin e Dukagjinit; *faza e dytë*, 17 tetor deri më 19 nëntor 1912 kur ushtritë malazeze dhe serbe arritën të vendosnin garnizonin e Shkodrës nën rrethim të plotë; *faza e tretë* 19 nëntor 1912 deri më 9 shkurt 1913 kur ushtritë armike përgatitën dhe ndërmorën pa sukses mësymjen e madhe për të bindur konferencën e ambasadorëve në Londër; *faza e katërt* nga 9 shkurti deri më 23 prill 1913 kur aktiviteti luftarak u zvogëlua, por bombardimi me artileri vazhdonte intensivisht deri në dorëzimin e garnizonit të Shkodrës.

Literatura e shfrytëzuar:

1. Edith Durham, “Brenga e Ballkanit dhe vepra të tjera për Shqipërinë dhe shqiptarët” Tiranë më 8 nëntor, 1991.
2. Hamdi Ertuna, “Mbrojtja e Shkodrës dhe Hasan Riza Pasha”, Jehona Study Center, Tiranë 2006.
3. Hortense von Zambaur, “Rrethimi i Shkodrës” Argeta, Tiranë 2019.
4. Jozef Suajër, “Shqipëria, ngritja e një mbretërie” Dituria, Tiranë 2005.
5. Xhino Berri, “Rrethimi i Shkodrës” SHBU, Tiranë 1998.
6. Xhafer Sadiku, “Shqipëria 1878-1928 Roli i elitës politike” Pika pa sipërfaqe, Tiranë 2021.
7. Romeo Gurakuqi, “Shqipëria 1911-1914” UET Press, Tiranë 2012.
8. Përparim Rexhepi, “Mbrojtja e Shkodrës 1912-1913” Globus, Tiranë 2001.
9. Xhani Baj Makario, “Balcani” La Prora, Milano 1937.
10. Hasan Bello, “Lufta e Shkodrës 1912-1913 Ditar anonim” ASA, Tiranë 2001.